
**ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΑΛΑΜΑΤΑΣ (Παράρτημα Σπάρτης)**

**Τμήμα Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών**

# ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

**«Αλγόριθμοι Αυθεντικοποίησης και Ψηφιακών Υπογραφών»**

**Νικολάου – Κούφα Γεωργία**

**Επιβλέπων Καθηγητής : κ. Καραγιώργος Γρηγόριος**

**Σπάρτη 08/06/2011**

# ΑΛΓΟΡΙΘΜΟΙ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ ΚΑΙ ΨΗΦΙΑΚΩΝ ΥΠΟΓΡΑΦΩΝ

# Περίληψη

Η ανάπτυξη του διαδικτύου, το ηλεκτρονικό εμπόριο και οι συναλλαγές μέσω ανοιχτών δικτύων κάνουν επιτακτική την ανάγκη ασφάλειας στις συναλλαγές. Ο χρήστης που συναλλάσσεται ηλεκτρονικά επιθυμεί τα δεδομένα (π.χ. ένα μήνυμα ή ένα κείμενο) που στέλνει να μην μπορούν να αποκαλυφθούν ή να διατεθούν σε μη εξουσιοδοτημένα γι αυτό άτομα (*εμπιστευτικότητα*). Τα δεδομένα, δεν θα πρέπει να είναι δυνατόν να αλλοιωθούν κατά την μετάδοσή τους. Ο παραλήπτης θα πρέπει να τα λάβει όπως ακριβώς ο αποστολέας τα έστειλε και να είναι σίγουρος ότι τα δεδομένα που λαμβάνει είναι αυτά που ο αποστολέας έχει στείλει (*ακεραιότητα*). Επιπλέον, σε μία τέτοια συναλλαγή, είναι απαραίτητο ο παραλήπτης να είναι σίγουρος για την ταυτότητα του αποστολέα (αυθεντικότητα). Τέλος, συμμετέχοντας σε μία ηλεκτρονική συναλλαγή (π.χ. ηλεκτρονικό εμπόριο) θα πρέπει να μην είναι δυνατόν τα εμπλεκόμενα μέρη να αρνηθούν εκ των υστέρων την συμμετοχή τους στη συναλλαγή αυτή (*μη αποποίηση ευθύνης*).

Οι παραπάνω ιδιότητες, (εμπιστευτικότητα, ακεραιότητα, αυθεντικότητα, μη αποποίηση) στον ηλεκτρονικό κόσμο, αποτελούν αντικείμενο της επιστήμης που ασχολείται με την ασφάλεια των πληροφοριών. Διάφοροι μηχανισμοί, τεχνικές και τεχνολογίες έχουν αναπτυχθεί αποσκοπώντας να διασφαλίσουν τις ιδιότητες αυτές σε μία ηλεκτρονική συναλλαγή.

Στην εργασία αυτή, γίνεται προσπάθεια προσέγγισης αυτών των ιδιοτήτων και των τεχνικών και μηχανισμών που συντελούν για τη διασφάλιση τους.

Στο πρώτο κεφάλαιο, γίνεται μια γενική αναφορά στην Κρυπτογραφία και τους αναγκαίους λόγους λειτουργίας της. Στο δεύτερο γίνεται μελέτη και ανάλυση των τεχνικών των αλγορίθμων αυθεντικοποίησης, καθορίζοντας την πρόσβαση σε πόρους σχετικά με την ασφάλεια των πληροφοριών, των υπολογιστών και του έλεγχου πρόσβασης. Στο τρίτο και τελευταίο κεφάλαιο, γίνεται περιγραφή δύο γενικών μοντέλων για σχήματα ψηφιακών υπογραφών.

**Λέξεις κλειδιά:** Ασφάλεια, εμπιστευτικότητα, ακεραιότητα, αλγόριθμος, αυθεντικοποίηση, ταυτοποίηση, ψηφιακή υπογραφή, πρωτόκολλα.

# Ευχαριστίες

Η παρούσα πτυχιακή μελέτη εκπονήθηκε από την φοιτήτρια Νικολάου – Κούφα Γεωργία του Τμήματος Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών στο Α.Τ.Ε.Ι Καλαμάτας(Παράρτημα Σπάρτης), κατά το ακαδημαϊκό έτος 2010-2011, υπό την επίβλεψη του καθηγητή του τμήματος κ. Καραγιώργου Γρηγόριου.

Στον κύριο Καραγιώργο οφείλω τις θερμές μου ευχαριστίες για την καθοδήγηση και την υποστήριξη του καθ' όλη τη διάρκεια διεκπεραίωσης της παρούσας πτυχιακής.

Ένα μεγάλο ευχαριστήσω τους φίλους μου για την ανυπολόγιστη ηθική υποστήριξη και κατανόηση τους.

Τέλος, ένα ευχαριστώ από καρδιάς στην οικογένεια μου για τη συνεχή συμπαράσταση, την αγάπη και την κατανόηση όχι μόνο κατά τη διάρκεια της εκπόνησης της πτυχιακής εργασίας, αλλά καθ' όλη τη διάρκεια των σπουδών μου φροντίζοντας για την καλύτερη δυνατή μόρφωση μου.

# ΠΕΡΙΕΧΟΜΕΝΑ

Εισαγωγή.....σελ.9

## Κεφάλαιο 1ο

### Εισαγωγή στην Κρυπτογραφία

1.1 Κρυπτογραφία και Κρυπτανάλυση.....σελ.10

1.1.1 Κρυπτογραφικοί αλγόριθμοι.....σελ.10

1.2 Αναγκαιότητες της Κρυπτογραφίας.....σελ.11

1.2.1 Απειλές και επιπτώσεις παραβίασης της ασφάλειας.....σελ.11

1.2.2 Βασικοί στόχοι ασφάλειας.....σελ.12

1.2.3 Μέσα προστασίας.....σελ.13

1.3 Εξέλιξη της Κρυπτογραφίας.....σελ.14

1.3.1 Πρώτη Περίοδος Κρυπτογραφίας (1900 π.Χ. – 1900 μ.Χ.).....σελ.14

1.3.2 Δεύτερη Περίοδος Κρυπτογραφίας (1900 μ.Χ. – 1950 μ.Χ.) .....σελ.15

1.3.3 Τρίτη Περίοδος Κρυπτογραφίας (1950 μ.Χ. – Σήμερα) .....σελ.15

# Κεφάλαιο 2ο

## Προσδιορισμός και αυθεντικοποίηση οντοτήτων


2.1 Εισαγωγή.....σελ.17

2.1.1 Στόχοι αναγνώρισης και εφαρμογές.....σελ.18

2.1.2 Ιδιότητες των πρωτοκόλλων αναγνώρισης.....σελ.20

2.2 Οι κωδικοί πρόσβασης (ασθενής ταυτότητας) .....σελ.21

2.2.1 Σταθερά κωδικοποιημένα συστήματα: τεχνικές.....σελ.21

2.2.2 Σταθερά συστήματα κωδικών πρόσβασης: επιθέσεις.....σελ.24

2.2.3 κωδικοί πρόσβασης UNIX.....σελ.27

2.2.4 Οι κωδικοί αριθμοί PIN's και οι κωδικοί πρόσβασης.....σελ.28

2.2.5 One-time κωδικοί πρόσβασης (ισχυρής αυθεντικοποίησης) .....σελ.30

2.3 Πρόκληση-απάντηση αναγνώρισης (ισχυρή αυθεντικοποίηση) .....σελ.30

2.3.1 Time-variant παράμετροι.....σελ.31

2.3.2 Πρόκληση-απόκριση με τεχνικές συμμετρικού κλειδιού.....σελ.34

2.3.3 Πρόκληση-απάντηση με τεχνικές δημόσιου κλειδιού.....σελ.37

2.4 Πρωτόκολλα ταυτοποίησης προσαρμοσμένης και μηδενικής γνώσης.....σελ.39

2.4.1 Επισκόπηση της μηδενικής γνώσης εννοιών.....σελ.39

2.4.2 Πρωτόκολλο ταυτοποίησης Feige-Fiat-Shamir.....σελ.43

2.4.3 Πρωτόκολλο ταυτοποίησης GQ(Guillou-Quisquater).....σελ.45

2.4.4 Πρωτόκολλο ταυτοποίησης Schnorr.....σελ.46

2.4.5 Σύγκριση: Fiat-Shamir, GQ, και Schnorr.....σελ.48

2.5 Επιθέσεις σε πρωτόκολλα αναγνώρισης.....σελ.49

# Κεφάλαιο 3ο

## Ψηφιακές Υπογραφές


**3.1 Εισαγωγή.....σελ.53**

**3.2 Ένα πλαίσιο για μηχανισμούς ψηφιακών υπογραφών.....σελ.53**

**3.2.1 Βασικοί ορισμοί.....σελ.53**

**3.2.2 Σχήματα ψηφιακών υπογραφών με παράρτημα.....σελ.55**

**3.2.3 Σχήματα ψηφιακών υπογραφών με ανάκτηση μηνύματος.....σελ.56**

**3.2.4 Τύποι επιθέσεων σε σχήματα υπογραφών.....σελ.58**

**3.3 RSA και συναφή σχήματα υπογραφών.....σελ.60**

**3.3.1 Το σχήμα υπογραφών RSA.....σελ.60**

**3.3.2 Πιθανές επιθέσεις στις υπογραφές RSA.....σελ.61**

**3.3.3 Οι υπογραφές RSA στην πράξη.....σελ.62**

**3.3.4 Το σχήμα υπογραφών δημόσιου κλειδιού Rabin.....σελ.64**

**3.3.5 Τυποποίηση ISO/IEC 9796.....σελ.69**

**3.3.6 Μορφοποίηση PKCS #1.....σελ.72**

**3.4 Τα σχήματα υπογραφών Fiat-Shamir.....σελ.75**

**3.4.1 Το σχήμα ψηφιακών υπογραφών Feige-Fiat-Shamir.....σελ.75**

**3.4.2 Το σχήμα υπογραφών GQ.....σελ.77**

**3.5 Ο DSA και τα σχετικά σχήματα υπογραφών.....σελ.79**

**3.5.1 Ο Αλγόριθμος Ψηφιακών Υπογραφών (DSA -** Digital Signature Algorithm)**.....σελ.80**

**3.5.2 Το σχήμα υπογραφών ElGamal.....σελ.82**

**3.5.3 Το σχήμα υπογραφών Schnorr.....σελ.89**

**3.5.4 Το σχήμα υπογραφών ElGamal με ανάκτηση μηνύματος.....σελ.90**

**3.6 Ψηφιακές υπογραφές μιας χρήσης.....σελ.92**

**3.6.1 Το σχήμα υπογραφών μιας χρήσης Rabin.....σελ.90**

**3.6.2 Το σχήμα υπογραφών μιας χρήσης Merkle.....σελ.94**

**3.6.3 Δέντρα πιστοποίησης αυθεντικότητας και υπογραφές μιας χρήσης.....σελ.96**

**3.7 Άλλα σχήματα υπογραφών.....σελ.102**

**3.7.1 Επιτηδευόμενες ψηφιακές υπογραφές.....σελ.102**

**3.7.2 ESIGN(**Efficient digital SIGNature - αποδοτική ψηφιακή υπογραφή) **.....σελ.103**

**3.8 Υπογραφές με επιπρόσθετη λειτουργικότητα.....σελ.106**

**3.8.1 Σχήματα τυφλών υπογραφών.....σελ.106**

**3.8.2 Σχήματα αδιαμφισβήτητων υπογραφών.....σελ.107**

**3.8.3 Σχήματα υπογραφών αποτυχίας-τερματισμού (fail-stop) .....σελ.110**

**Συμπεράσματα.....σελ.115**

**Βιβλιογραφία.....σελ.117**

# ΕΙΣΑΓΩΓΗ

Η παρούσα εργασία ασχολείται με την «Ασφάλεια της Πληροφορίας». Σήμερα η χρήση υπολογιστή και η χρήση του email (ηλεκτρονικού ταχυδρομείου) είναι περισσότερο διαδεδομένη σαν μορφή επικοινωνίας από το παραδοσιακό ταχυδρομείο. Με την υπηρεσία αυτή εξασφαλίζεται η ταχύτητα και η ευκολία αποστολής και παράδοσης, όμως δεν υπάρχει η απαιτούμενη προστασία με τη χρήση φακέλου όπως γίνεται στο παραδοσιακό ταχυδρομείο με αποτέλεσμα κάποιο εμπιστευτικό μήνυμα, ή κάποια προσωπικά δεδομένα να είναι εκτεθειμένα. Επιτακτική κρίθηκε η ανάγκη για προστασία. Η συνηθέστερη λύση είναι το μήνυμα να κρυπτογραφηθεί, ώστε ακόμα και αν κάποιος ανεπιθύμητος παραλήπτης καταφέρει αν έχει πρόσβαση, να μη μπορεί να διαβάσει το περιεχόμενο του. Η χρήση κρυπτογραφίας για την προστασία των emails δεν είναι ακόμη ευρύτατα διαδεδομένη, αλλά η χρήση της γίνεται ολοένα και πιο δημοφιλής.

Πριν το 1970 η χρήση της κρυπτογραφίας γινόταν μόνο από λίγους επιλεγμένους ανθρώπους, οι οποίοι συνήθως κατείχαν κυβερνητικές και στρατιωτικές θέσεις. Σήμερα, πέρα του ότι αποτελεί βασικό κλάδο της μαθηματικής επιστήμης και διδάσκεται σε αρκετά εκπαιδευτικά ιδρύματα, η χρήση της κρυπτογραφίας είναι διαδεδομένη τόσο στις εταιρίες όσο και στους απλούς πολίτες. Υπάρχουν αρκετές εξηγήσεις για την εξάπλωση, με πιο σημαντικές εκείνες της αυξανόμενης χρήσης της πληροφορικής από τις εταιρίες καθώς και τη διαδεδομένη χρήση του διαδικτύου ως επικοινωνιακό κανάλι. Πολλές εταιρίες, πλέον, θέλουν να συναλλάσσονται, τόσο μεταξύ τους όσο και με τους πελάτες τους, μέσω του διαδικτύου, αλλά και οι κυβερνήσεις θέλουν να επικοινωνούν ηλεκτρονικά πλέον με τους πολίτες( π.χ ηλεκτρονική συμπλήρωση και αποστολή φορολογικής δήλωσης).

Στην καθημερινότητα μας, συχνά χρησιμοποιούμε την υπογραφή για την εξασφάλιση της αυθεντικότητας και της προσωποποίησης μας. Έτσι, δημιουργήθηκε η ανάγκη για ένα ισοδύναμο ηλεκτρονικό μηχανισμό. Στον ηλεκτρονικό κόσμο οι φυσικές υπογραφές (handwritten signatures) δεν μπορούν να χρησιμοποιηθούν. Η κρυπτογραφία παρέχει έναν κατάλληλο μηχανισμό, τις ψηφιακές υπογραφές, παρ' όλο που στα παραπάνω ζητήματα οι πληροφορίες δε χρειάζεται να είναι κρυπτογραφημένες ( encrypted).

Σύμφωνα με τον Διεθνή Οργανισμό Προτύπων ( International Standards Organization – ISO) ο όρος ψηφιακή υπογραφή θεωρείται σαν μια συγκεκριμένη τεχνική πιστοποίησης ταυτότητας που χρησιμοποιείται για να αποδεικνύει την προέλευση του μηνύματος ώστε να επιλύει τυχόν διαφορές σχετικά με το ποιο μήνυμα έχει σταλθεί (εάν έχει σταλθεί).

Μια ψηφιακή υπογραφή, λοιπόν, αποτελείται από ορισμένα δεδομένα τα οποία επιβεβαιώνουν την ακεραιότητα των περιεχομένων ενός μηνύματος και τα οποία ο παραλήπτης μπορεί να τα χρησιμοποιήσει σαν απόδειξη. Μια ψηφιακή υπογραφή πρέπει αν είναι εύκολο να υπολογιστεί και να επιβεβαιωθεί υπολογιστικά από οποιονδήποτε ενδιαφερόμενο και θα έχει χαμηλές απαιτήσεις. Τέλος, η ψηφιακή υπογραφή θα πρέπει να είναι αδύνατο να αντιγραφεί.

Καθώς στον «πραγματικό κόσμο» υπάρχουν πολλές περιπτώσεις και συναλλαγές που βασίζονται στο γνήσιο της υπογραφής μας. Καθώς οι ψηφιακές υπογραφές τείνουν να χρησιμοποιούνται στον ηλεκτρονικό κόσμο προς αντικατάσταση των πραγματικών υπογραφών πρέπει με κάποιο τρόπο να εξακριβώνεται η γνησιότητα τους.

Για να είναι αποτελεσματικό ένα σύστημα δημοσίου κλειδιού πρέπει να βεβαιωθούμε πως κάθε δημόσιο κλειδί είναι αυθεντικό, δηλαδή πως κάθε δημόσιο κλειδί αντιστοιχεί σε ένα ιδιωτικό κλειδί το οποίο είναι άρρηκτα συνδεδεμένο με τον κάτοχο του.

Χρειάζεται λοιπόν, μια κατάλληλη Αρχή Πιστοποίησης (Certification Authority ή CA) η οποία βεβαιώνει τη γνησιότητα της υπογραφής. Η CA μπορεί να είναι οποιαδήποτε οντότητα εμπνέει κάποια μορφή εμπιστοσύνης στους χρήστες ενός συστήματος δημόσιου κλειδιού και μπορεί να είναι μια εταιρία, ένας κυβερνητικός οργανισμός, μια τράπεζα, ένα εκπαιδευτικό ίδρυμα κ.ο.κ

Υπάρχουν πολλές τεχνικές αυθεντικοποίησης και ταυτοποίησης των χρηστών ενός πληροφοριακού συστήματος. Η βέλτιστη επιλογή μεταξύ των διαφορετικών τεχνικών αποτελεί βασικό στοιχείο της ασφάλειας των υπολογιστικών και επικοινωνιακών συστημάτων.

# Κεφάλαιο 1ο

## 1.1 Κρυπτογραφία και Κρυπτανάλυση

*Βασικοί όροι*

Κρυπτογραφία είναι ο επιστημονικός κλάδος που πραγματεύεται τη μελέτη και σχεδίαση κρυπτογραφικών τεχνικών, συστημάτων και πρωτοκόλλων. Μαζί με τον κλάδο της Κρυπτανάλυσης, που ασχολείται με τη μελέτη τρόπων παραβίασης αυτών, απαρτίζουν την Επιστήμη της Κρυπτολογίας. Έτσι, Κρυπτολογία είναι η επιστήμη της απόκρυψης, από τη μια πλευρά και, από την άλλη, της αποκάλυψης του περιεχομένου κωδικοποιημένων μηνυμάτων ή δεδομένων.

Η επιθυμία προστασίας του περιεχομένου μηνυμάτων οδήγησε στην επινόηση και χρήση κρυπτογραφικών τεχνικών και συστημάτων τα οποία επιτρέπουν το μετασχηματισμό μηνυμάτων ή δεδομένων κατά τέτοιον τρόπο ώστε να είναι αδύνατη η υποκλοπή του περιεχομένου τους κατά τη μετάδοσή ή αποθήκευσή τους και, βεβαίως, την αντιστροφή του μετασχηματισμού. Η διαδικασία μετασχηματισμού καλείται κρυπτογράφηση και η αντίστροφή της αποκρυπτογράφηση.

Η συνάρτηση ή το σύνολο των κανόνων, στοιχείων και βημάτων που καθορίζουν την κρυπτογράφηση και την αποκρυπτογράφηση ονομάζεται κρυπτογραφικός αλγόριθμος. Η υλοποίηση του κρυπτογραφικού αλγόριθμου καλείται κρυπτογραφικό σύστημα. Μερικές φορές, ο κρυπτογραφικός αλγόριθμος καλείται και κωδικοποιητής (cipher). Πρωτόκολλα που χρησιμοποιούν κρυπτογραφικούς αλγόριθμους καλούνται κρυπτογραφικά πρωτόκολλα. Επειδή η αποθήκευση μπορεί να θεωρηθεί ως μετάδοση στη διάσταση του χρόνου, εφεξής θα μιλάμε για μετάδοση εννοώντας μετάδοση ή αποθήκευση.

### 1.1.1 Κρυπτογραφικοί αλγόριθμοι

Οι κρυπτογραφικοί αλγόριθμοι χρησιμοποιούν, κατά κανόνα, (κρυπτογραφικά) κλειδιά (keys), η τιμή των οποίων επηρεάζει την κρυπτογράφηση και την αποκρυπτογράφηση. Το σύνολο των δυνατών τιμών των κλειδιών λέγεται πεδίο τιμών (keyspace). Υπάρχουν δύο κατηγορίες κρυπτογραφικών αλγόριθμων, και κατά συνέπεια συστημάτων: οι συμμετρικοί και οι ασύμμετροι αλγόριθμοι. Η ασύμμετρη κρυπτογραφία ( public-key cryptography) χρησιμοποιεί δύο διαφορετικά κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση. Κάθε χρήστης έχει στην κατοχή του ένα ζεύγος κλειδιών, το ένα καλείται δημόσια κλείδα και το άλλο καλείται μυστική κλείδα. Η ανάγκη ο αποστολέας και ο παραλήπτης να μοιράζονται το ίδιο κλειδί εξαφανίζεται και μαζί και πολλά προβλήματα που θα δούμε παρακάτω. Η μόνη απαίτηση της ασύμμετρης κρυπτογραφίας είναι η εμπιστεύσιμη και επιβεβαιωμένη συσχέτιση των δημόσιων κλείδων με τους κατόχους τους ώστε να μην είναι δυνατή η σκόπιμη ή μη πλαστοπροσωπία. Η ασύμμετρη κρυπτογράφηση μπορεί να χρησιμοποιηθεί όχι μόνο για κρυπτογράφηση, αλλά και για παραγωγή ψηφιακών υπογραφών.

Η ιδιωτική κλείδα είναι μαθηματικά συνδεδεμένη με την δημόσια κλείδα. Τυπικά, λοιπόν, είναι δυνατόν να νικηθεί ένα τέτοιο κρυπτοσύστημα ανακτώντας την ιδιωτική κλείδα από

την δημόσια. Η επίλυση αυτού του προβλήματος είναι πολύ δύσκολη και συνήθως απαιτεί την παραγοντοποίηση ενός μεγάλου αριθμού.

Η κρυπτογράφηση με χρήση της ασύμμετρης κρυπτογραφίας γίνεται ως εξής: όταν ο χρήστης Α θέλει να στείλει ένα μυστικό μήνυμα στον χρήστη Β, χρησιμοποιεί την δημόσια κλείδα του Β για να κρυπτογραφήσει το μήνυμα και έπειτα το στέλνει στον Β. Ο χρήστης Β, αφού παραλάβει το μήνυμα, κάνει χρήση της ιδιωτικής του κλείδας για να το αποκρυπτογραφήσει. Κανένας που "ακούει" την σύνδεση δεν μπορεί να αποκρυπτογραφήσει το μήνυμα. Οποιοσδήποτε έχει την δημόσια κλείδα του Β μπορεί να του στείλει μήνυμα και μόνο αυτός μπορεί να το διαβάσει γιατί είναι ο μόνο που γνωρίζει την ιδιωτική κλείδα.

Συνοψίζοντας, μπορούμε να πούμε ότι τα κρυπτογραφικά συστήματα βασίζονται στη χρήση ενός τουλάχιστον μυστικού κρυπτογραφικού κλειδιού για την κρυπτογράφηση ή/και αποκρυπτογράφηση μηνυμάτων ή δεδομένων. Από την άλλη πλευρά, οι τεχνικές της Κρυπτανάλυσης στοχεύουν στην αποκρυπτογράφηση κρυπτογραφημένων μηνυμάτων χωρίς τη γνώση του μυστικού κρυπτογραφικού κλειδιού. Είναι φανερό πως η Κρυπτογραφία και η Κρυπτανάλυση έχουν πολύ στενή σχέση μεταξύ τους. Έτσι, για τη σχεδίαση και τη βελτίωση ενός ισχυρού κρυπτογραφικού συστήματος είναι καθοριστικής σημασίας η γνώση των κρυπταναλυτικών δυνατοτήτων, που επίσης εξελίσσονται. Από την άλλη πλευρά, για την Κρυπτανάλυση, δηλαδή το «σπάσιμο» ενός κρυπτογραφικού συστήματος, απαιτείται η μελέτη των σχεδιαστικών κριτηρίων και του μαθηματικού υπόβαθρου αυτού.

## 1.2 Αναγκαιότητα της Κρυπτογραφίας

### 1.2.1 Απειλές και επιπτώσεις παραβίασης της ασφάλειας

Οι δυνατές απόπειρες παραβίασης της ασφάλειας (απειλές), ακούσιες ή εκ προθέσεως, και οι αντίστοιχες επιπτώσεις διακρίνονται στις εξής κατηγορίες: διακοπής ή άρνησης υπηρεσίας, υποκλοπής, παραποίησης, πειρατείας και αμφισβήτησης.
Η Διακοπή (interruption).
Τα αντικείμενα του συστήματος χάνονται, δεν είναι διαθέσιμα ή είναι μη χρησιμοποιήσιμα. Παραδείγματα είναι η ηθελημένη καταστροφή μιας συσκευής, το σβήσιμο ενός προγράμματος ή ενός αρχείου δεδομένων, ή η δυσλειτουργία του διαχειριστή αρχείων του λειτουργικού συστήματος, έτσι ώστε να μην μπορεί να βρεθεί ένα συγκεκριμένο αρχείο στο δίσκο.

*Η Παρεμπόδιση (interception).*
Σημαίνει πως μια μη εξουσιοδοτημένη ομάδα έχει κερδίσει το δικαίωμα πρόσβασης σε ένα αντικείμενο. Αυτή η εξωτερική ομάδα μπορεί να είναι είτε πρόσωπα, είτε προγράμματα ή ακόμα και παρέμβαση ενός άλλου πληροφοριακού συστήματος. Παραδείγματα αυτού του είδους της αποτυχίας είναι η παράνομη αντιγραφή των προγραμμάτων ή των αρχείων δεδομένων ή οι υποκλοπές των τηλεφωνημάτων για την απόκτηση δεδομένων από το δίκτυο. Παρόλο που μια απώλεια μπορεί να αποκαλυφθεί σχετικά γρήγορα, ο υποκλοπέας μπορεί να μην αφήσει καθόλου ίχνη για την ανίχνευση της ύπαρξης του εάν μια μη εξουσιοδοτημένη ομάδα όχι μόνο προσπελάσει τα δεδομένα, αλλά ανακατευτεί και με κάποια αντικείμενα, τότε μιλάμε για τροποποίηση (modification). Για παράδειγμα κάποιος μπορεί να αλλάξει τις τιμές σε μια βάση δεδομένων ή να μετατρέψει ένα πρόγραμμα έτσι

ώστε να εκτελεί επιπλέον υπολογισμούς ή να τροποποιεί τα δεδομένα που μεταφέρονται ηλεκτρονικά. Είναι ακόμα δυνατό να τροποποιηθεί και το υλικό μέρος του συστήματος. Τέλος μια μη εξουσιοδοτημένη ομάδα μπορεί να κατασκευάσει (fabricate) πλαστά αντικείμενα. Ο εισβολέας μπορεί να προσθέσει εγγραφές σε μια υπάρχουσα βάση δεδομένων. Μερικές φορές αυτές οι προσθέσεις ανιχνεύονται σαν πλαστές, αλλά εάν έχουν γίνει περίτεχνα τότε είναι αδιαχώριστες από τα πραγματικά αντικείμενα.

## 1.2.2 Βασικοί Στόχοι Ασφάλειας

Στο πλαίσιο της ασφάλειας υπολογιστικών και επικοινωνιακών συστημάτων τίθενται ως βασικοί στόχοι η διατήρηση (διασφάλιση) τριών ιδιοτήτων ή χαρακτηριστικών (δηλαδή η αντιμετώπιση των αντίστοιχων κινδύνων): της «εμπιστευτικότητας», της «ακεραιότητας» και της «διαθεσιμότητας». Στη συνέχεια θα δούμε συνοπτικά τις τρεις αυτές ιδιότητες.

*Εμπιστευτικότητα (Confidentiality)*: είναι η ιδιότητα των δεδομένων ή πληροφοριών να είναι προσπελάσιμα μόνο από τις εξουσιοδοτημένες προς αυτά λογικά ή φυσικά αντικείμενα (π. χ. προγράμματα, άνθρωποι κ.ά.). Η εμπιστευτικότητα αναφέρεται στο περιεχόμενο ηλεκτρονικών εγγράφων ή, γενικά, αρχείων και μηνυμάτων, στην ύπαρξή τους και στην ταυτότητα αυτών που εκτελούν ενέργειες και ανταλλάσσουν μηνύματα. Επίσης, αναφέρεται στο χρόνο και την ποσότητα μηνυμάτων που ανταλλάσσονται. Η εμπιστευτικότητα, μερικές φορές, καλείται και «ιδιωτικότητα» ή «μυστικότητα» ή «προστασία του απορρήτου».

*Ακεραιότητα (Integrity)*
Η ακεραιότητα είναι η ιδιότητα των δεδομένων και πληροφοριών και των υπολογιστικών και επικοινωνιακών πόρων να τροποποιούνται μόνο από εξουσιοδοτημένες οντότητες κατά εξουσιοδοτημένο τρόπο. Η ακεραιότητα έχει να κάνει με την ακρίβεια και τη συνέπεια στη λειτουργία συστημάτων και διεργασιών. Τα δεδομένα σε κάθε σύστημα πρέπει να παραμένουν πλήρη και ορθά. Η ακεραιότητα διατηρείται όταν διατηρούνται και οι ιδιότητες: η ακρίβεια, η μη τροποποίηση ή τροποποίηση από εξουσιοδοτημένους χρήστες ή διεργασίες, με συνέπεια, κατά αποδεκτό τρόπο. Έχουν αναγνωριστεί τρεις καθοριστικές συνιστώσες του όρου ακεραιότητα: οι «εξουσιοδοτημένες ενέργειες», ο «διαχωρισμός και η προστασία αγαθών» και, τέλος, «η ανίχνευση και διόρθωση σφαλμάτων».

*Διαθεσιμότητα (Availability)*
Η διαθεσιμότητα είναι η ιδιότητα των δεδομένων ή πληροφοριών και των υπολογιστικών και επικοινωνιακών πόρων να είναι διαθέσιμα στους εξουσιοδοτημένους προς τούτο χρήστες σύμφωνα με τα δικαιώματά τους. Η διαθεσιμότητα –όπως και η ακεραιότητα– είναι μια σύνθετη έννοια. Η διαθεσιμότητα αναφέρεται τόσο στα δεδομένα όσο και στις υπηρεσίες που πρέπει να παρέχονται. Οι προσδοκίες του χαρακτηριστικού της *διαθεσιμότητας* περιλαμβάνουν:

- Παρουσία του αντικειμένου και της υπηρεσίας με χρησιμοποιήσιμο τρόπο.
- Ικανότητα χειρισμού των απαιτούμενων πόρων
- Συγκεκριμένος χρόνος αναμονής.
- Κατάλληλος χρόνος διάθεσης των πόρων

Σκοπός της Διαθεσιμότητας είναι:

• Δίκαιη κατανομή των πόρων

• Έγκαιρη ανταπόκριση στη διάθεση των δεδομένων

• Ελεγχόμενη συμφωνία, δηλαδή χειρισμός δοσοληψιών, αποκλειστική πρόσβαση, χειρισμός του φαινομένου deadlock.

• Χρησιμότητα, οι πόροι και τα δεδομένα μπορούν να χρησιμοποιηθούν όπως σχεδιάστηκαν.

Πέρα από τα παραπάνω χαρακτηριστικά, στην πράξη υπάρχουν και άλλα, όπως η αυθεντικότητα, η αξιοπιστία, η δυνατότητα ελέγχου κ.α. που πρέπει να λαμβάνονται υπόψιν.

## 1.2.3 Μέσα προστασίας

Η διατήρηση (διασφάλιση) τριών παραπάνω ιδιοτήτων ή χαρακτηριστικών επιτυγχάνεται με την εφαρμογή φυσικών, οργανωτικών – διοικητικών και λειτουργικών μέτρων. Στα λειτουργικά μέτρα περιλαμβάνονται μηχανισμοί γνησιότητας προέλευσης και περιεχομένου, εμπιστευτικότητας, ελέγχου πρόσβασης και μη αμφισβήτησης. Το βασικό συστατικό στοιχείο όλων αυτών των μηχανισμών είναι τα κρυπτογραφικά συστήματα.

*Φυσικά μέτρα*
Αναφέρονται στον έλεγχο φυσικής πρόσβασης στους υπολογιστικούς και επικοινωνιακούς πόρους, όπως επίσης και στην προστασία από φυσικά φαινόμενα ή ατυχήματα, όπως διαρροή νερού ή πλημμύρες, φωτιά, σεισμό κ.ά.

*Οργανωτικά* – διοικητικά μέτρα
Αναφέρονται στη διαχείριση ασφάλειας, στην εκπόνηση ανάλυσης επικινδυνότητας, στην κατάρτιση σχεδίου ασφάλειας, πολιτικής ασφάλειας και σχεδίου έκτακτης ανάγκης. Τα μέτρα αυτά εξετάζονται και αναθεωρούνται σε τακτά χρονικά διαστήματα.

*Λειτουργικά μέτρα*
Αναφέρονται σε όλους εκείνους τους μηχανισμούς που πρέπει να ενεργοποιούνται κατά τη λειτουργία συστημάτων υπολογιστών. Στα μέτρα αυτά συγκαταλέγονται οι ακόλουθες κατηγορίες: της γνησιότητας (authentication) προέλευσης δεδομένων ή ταυτότητας χρηστών (της ακεραιότητας ή γνησιότητας περιεχομένου (integrity) της εμπιστευτικότητας (confidentiality) του ελέγχου πρόσβασης(access control) της μη αμφισβήτησης (non-repudiation).

## 1.3 Εξέλιξη της Κρυπτογραφίας

### 1.3.1 Πρώτη Περίοδος Κρυπτογραφίας (1900 π.Χ. – 1900 μ.Χ.)

Κατά την διάρκεια αυτής της περιόδου αναπτύχθηκε μεγάλο πλήθος μεθόδων και αλγορίθμων κρυπτογράφησης, που βασίζονταν κυρίως σε απλές αντικαταστάσεις γραμμάτων. Οι μέθοδοι αυτές δεν απαιτούσαν εξειδικευμένες γνώσεις και πολύπλοκες συσκευές, αλλά στηρίζονταν στην ευφυΐα και την ευρηματικότητα των δημιουργών τους. Όλα αυτά τα συστήματα έχουν στις μέρες μας κρυπταναλυθεί και έχει αποδειχθεί ότι, εάν είναι γνωστό ένα μεγάλο κομμάτι του κρυπτογραφημένου μηνύματος, τότε το αρχικό κείμενο μπορεί σχετικά εύκολα να επανακτηθεί.

Όπως προκύπτει από μία μικρή σφηνοειδή επιγραφή, που ανακαλύφθηκε στις όχθες του ποταμού Τίγρη, οι πολιτισμοί που αναπτύχθηκαν στην Μεσοποταμία ασχολήθηκαν με την κρυπτογραφία ήδη από το 1500 π.Χ. Η επιγραφή αυτή περιγράφει μία μέθοδο κατασκευής σμάλτων για αγγειοπλαστική και θεωρείται ως το αρχαιότερο κρυπτογραφημένο κείμενο (με βάση τον Kahn ).

Επίσης, ως το αρχαιότερο βιβλίο κρυπτοκωδικών στον κόσμο, θεωρείται μία σφηνοειδής επιγραφή στα Σούσα της Περσίας, η οποία περιλαμβάνει τους αριθμούς από το ένα έως και το οκτώ και από το τριάντα δύο έως το τριάντα πέντε, τοποθετημένους τον ένα κάτω από τον άλλο, ενώ απέναντι τους βρίσκονται τα αντίστοιχα για τον καθένα σφηνοειδή σύμβολα.

Η πρώτη στρατιωτική χρήση της κρυπτογραφίας αποδίδεται στους Σπαρτιάτες. Γύρω στον πέμπτο π.Χ. αιώνα εφηύραν την «σκυτάλη», την πρώτη κρυπτογραφική συσκευή, στην οποία χρησιμοποίησαν για την κρυπτογράφηση την μέθοδο της αντικατάστασης. Όπως αναφέρει ο Πλούταρχος, η «Σπαρτιατική Σκυτάλη», ήταν μια ξύλινη ράβδος, ορισμένης διαμέτρου, γύρω από την οποία ήταν τυλιγμένη ελικοειδώς μια λωρίδα περγαμηνής. Το κείμενο ήταν γραμμένο σε στήλες, ένα γράμμα σε κάθε έλικα, όταν δε ξετύλιγαν τη λωρίδα, το κείμενο ήταν ακατάληπτο εξαιτίας της ανάμειξης των γραμμάτων. Το «κλειδί» ήταν η διάμετρος της εκάστοτε σκυτάλης.

Στην αρχαιότητα χρησιμοποιήθηκαν κυρίως συστήματα, τα οποία βασίζονταν στην στεγανογραφία και όχι τόσο στην κρυπτογραφία. Οι Έλληνες συγγραφείς δεν αναφέρουν αν και πότε χρησιμοποιήθηκαν συστήματα γραπτής αντικατάστασης γραμμάτων, αλλά τα βρίσκουμε στους Ρωμαίους, κυρίως την εποχή του Ιουλίου Καίσαρα.

Ο Ιούλιος Καίσαρας έγραφε στον Κικέρωνα και σε άλλα πρόσωπα, αντικαθιστώντας τα γράμματα του κειμένου, με γράμματα, που βρίσκονται τρεις θέσεις μετά, στο Λατινικό Αλφάβητο. Έτσι, σήμερα, το σύστημα κρυπτογράφησης που στηρίζεται στην αντικατάσταση των γραμμάτων του αλφαβήτου με άλλα που βρίσκονται σε καθορισμένο αριθμό θέσης πριν ή μετά, λέγεται κρυπτοσύστημα αντικατάστασης του Καίσαρα. Ο Καίσαρας χρησιμοποίησε και άλλα, πιο πολύπλοκα συστήματα κρυπτογράφησης, για τα οποία έγραψε ένα βιβλίο ο Valerius Probus, το οποίο δυστυχώς δεν διασώθηκε, αλλά αν και χαμένο, θεωρείται το πρώτο βιβλίο Κρυπτολογίας. Το σύστημα αντικατάστασης του Καίσαρα, χρησιμοποιήθηκε ευρύτατα και στους επόμενους αιώνες.

Στην διάρκεια του Μεσαίωνα, η κρυπτογραφία στην Ευρώπη ήταν κάτι το απαγορευμένο και αποτελούσε μια μορφή αποκρυφισμού και μαύρης μαγείας, κάτι που συντέλεσε στην καθυστέρηση της ανάπτυξης της. Η εξέλιξη, τόσο της κρυπτογραφίας, όσο και των μαθηματικών, συνεχίζεται στον Αραβικό κόσμο. Οι Άραβες είναι οι πρώτοι που επινόησαν αλλά και χρησιμοποίησαν μεθόδους Κρυπτανάλυσης.

## 1.3.2 Δεύτερη Περίοδος Κρυπτογραφίας (1900 μ.Χ. – 1950 μ.Χ.)

Η δεύτερη περίοδος της κρυπτογραφίας όπως προαναφέρθηκε τοποθετείται στις αρχές του εικοστού αιώνα και φτάνει περίπου μέχρι το 1950. Καλύπτει, επομένως, τους δύο παγκόσμιους πολέμους, εξαιτίας των οποίων (λόγω της εξαιρετικά μεγάλης ανάγκης που υπήρξε για ασφάλεια κατά την μετάδοση ζωτικών πληροφοριών μεταξύ των στρατευμάτων των εμπλεκομένων χωρών) αναπτύχθηκε η κρυπτογραφία τόσο όσο δεν είχε αναπτυχθεί τα προηγούμενα 3000 χρόνια. Τα κρυπτοσυστήματα αυτής της περιόδου αρχίζουν να γίνονται πολύπλοκα, και να αποτελούνται από μηχανικές και ηλεκτρομηχανικές κατασκευές, οι οποίες ονομάζονται «κρυπτομηχανές». Η Κρυπτανάλυση τους, απαιτεί μεγάλο αριθμό προσωπικού, το οποίο εργαζόταν επί μεγάλο χρονικό διάστημα ενώ ταυτόχρονα γίνεται εξαιρετικά αισθητή η ανάγκη για μεγάλη υπολογιστική ισχύ.

Παρά την πολυπλοκότητα που αποκτούν τα συστήματα κρυπτογράφησης κατά την διάρκεια αυτής της περιόδου η κρυπτανάλυση τους είναι συνήθως επιτυχημένη. Η πιο γνωστή κρυπτογραφική μηχανή εκείνης της περιόδου είναι το Enigma. Η φήμη της πηγάζει κυρίως από τον αποφασιστικό ρόλο που διαδραμάτισε η αποκρυπτογράφησή της στην τελική έκβαση του δευτέρου παγκοσμίου πολέμου. Το όνομα Enigma οι δημιουργοί της το δανείστηκαν από την ελληνική λέξη αίνιγμα και με αυτό ήθελαν να δώσουν έμφαση στην περίπλοκη δομή της, καθώς και στην απόλυτη ασφάλεια των μηνυμάτων που αυτή κρυπτογραφούσε. Το παραπάνω σύστημα χρησιμοποιήθηκε εκτεταμένα από τους Γερμανούς, σε διάφορες παραλλαγές του.

Παρόλα αυτά δεν κατάφερε να εξασφαλίσει το απόρρητο των επικοινωνιών των γερμανικών δυνάμεων και η αποκρυπτογράφηση της έδωσε ένα σημαντικό πλεονέκτημα στις συμμαχικές δυνάμεις έναντι αυτών του άξονα.

## 1.3.3 Τρίτη Περίοδος Κρυπτογραφίας (1950 μ.Χ. – Σήμερα)

Αυτή η περίοδος χαρακτηρίζεται από την έξαρση της ανάπτυξης στους επιστημονικούς κλάδους των μαθηματικών, της μικροηλεκτρονικής και των υπολογιστικών συστημάτων. Η εποχή της σύγχρονης κρυπτογραφίας αρχίζει ουσιαστικά με τον Claude Shannon, ο οποίος είναι αναμφισβήτητα ο πατέρας των μαθηματικών συστημάτων κρυπτογραφίας.

Το 1949δημοσίευσε το έγγραφο «Θεωρία επικοινωνίας των συστημάτων μυστικότητας» (Communication Theory of Secrecy Systems) στο τεχνικό περιοδικό Bell System και λίγο αργότερα στο βιβλίο του, «Μαθηματική Θεωρία της Επικοινωνίας» (Mathematical Theory of Communication),μαζί με τον Warren Weaver.

Αυτά, εκτός από τις άλλες εργασίες του επάνω στην θεωρία δεδομένων και επικοινωνίας καθιέρωσαν μια στερεά θεωρητική βάση για την κρυπτογραφία και την κρυπτανάλυση.

Εκείνη την εποχή η κρυπτογραφία εξαφανίζεται και φυλάσσεται από τις μυστικές υπηρεσίες κυβερνητικών επικοινωνιών όπως η NSA (National Security Agency) των Η.Π.Α..

Πολύ λίγες εξελίξεις δημοσιοποιήθηκαν ξανά μέχρι τα μέσα της δεκαετίας του 1970, όταν όλα άλλαξαν .Στα μέσα αυτής της δεκαετίας έγιναν δύο σημαντικές δημόσιες (δηλαδή μη-μυστικές) πρόοδοι. Πρώτα ήταν η δημοσίευση του σχεδίου προτύπου κρυπτογράφησης DES (Data Encryption Standard) στον ομοσπονδιακό κατάλογο της Αμερικής στις 17 Μαρτίου 1975. Το προτεινόμενο DES υποβλήθηκε από την IBM, στην πρόσκληση του Εθνικού Γραφείου των Προτύπων (τώρα γνωστό ως NIST), σε μια προσπάθεια να αναπτυχθούν ασφαλείς ηλεκτρονικές εγκαταστάσεις επικοινωνίας για επιχειρήσεις όπως τράπεζες και άλλες μεγάλες οικονομικές οργανώσεις. Μετά από τις συμβουλές και την τροποποίηση από την NSA, αυτό το πρότυπο υιοθετήθηκε και δημοσιεύθηκε ως ένα ομοσπονδιακό τυποποιημένο πρότυπο επεξεργασίας πληροφοριών το 1977 (αυτήν την περίοδο αναφέρεται σαν FIPS 46-3). Ο DES ήταν ο πρώτος δημόσια προσιτός αλγόριθμος κρυπτογράφησης που εγκρίνεται από μια εθνική αντιπροσωπεία όπως η NSA.

Η απελευθέρωση της προδιαγραφής της από την NBS υποκίνησε μια έκρηξη δημόσιου και ακαδημαϊκού ενδιαφέροντος για τα συστήματα κρυπτογραφίας DES αντικαταστάθηκε επίσημα από τον AES (Advanced Encryption Standard) το 2001 όταν ανήγγειλε το Εθνικό Γραφείο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology NIST) το FIPS (Federal Information Processing Standard) 197. Μετά από έναν ανοικτό διαγωνισμό, το NIST επέλεξε τον αλγόριθμο Rijndael, που υποβλήθηκε από δύο Φλαμανδούς κρυπτογράφους, για να \είναι το AES. Ο DES και οι ασφαλέστερες παραλλαγές του όπως ο 3-DES ή TripleDES χρησιμοποιούνται ακόμα σήμερα, ενσωματωμένοι σε πολλά εθνικά και οργανωτικά πρότυπα.

Εντούτοις, το βασικό μέγεθος των 56 bits έχει αποδειχθεί ότι είναι ανεπαρκές να αντισταθεί στις επιθέσεις ωμής βίας (μια τέτοια επίθεση πέτυχε να σπάσει τον DES σε 56 ώρες ενώ το άρθρο που αναφέρεται ως το σπάσιμο του DES δημοσιεύτηκε από τον O'Reilly and Associates). Κατά συνέπεια, η χρήση απλής κρυπτογράφησης με τον DES είναι τώρα χωρίς καμία πλέον αμφιβολία επισφαλής για χρήση στα νέα σχέδια των κρυπτογραφικών συστημάτων και μηνύματα που προστατεύονται από τα παλαιότερα κρυπτογραφικά συστήματα που χρησιμοποιούν DES, και όλα τα μηνύματα που έχουν αποσταλεί από το 1976 με την χρήση DES, διατρέχουν επίσης σοβαρό κίνδυνο αποκρυπτογράφησης. Ανεξάρτητα από την έμφυτη ποιότητά του, το βασικό μέγεθος του DES (56 bits) ήταν πιθανά πάρα πολύ μικρό ακόμη και το 1976, πράγμα που είχε επισημάνει oWhitfield Diffie.

Υπήρξε επίσης η υποψία ότι κυβερνητικές οργανώσεις είχαν ακόμα και τότε ικανοποιητική υπολογιστική δύναμη ώστε να σπάσουν μηνύματα που είχαν κρυπτογραφηθεί με τον DES.

# Κεφάλαιο 2ο

# Προσδιορισμός και Αυθεντικοποίηση οντοτήτων

## 2.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα εξετάσουμε τις τεχνικές που αφορούν στη λειτουργία της αυθεντικοποίησης.

Η αυθεντικοποίηση είναι η λειτουργία που καθορίζει τα δικαιώματα πρόσβασης σε πόρους, η οποία σχετίζεται με την ασφάλεια των πληροφοριών και της ασφάλειας των υπολογιστών γενικότερα, και ελέγχου της πρόσβασης συγκεκριμένα. Πιο συγκεκριμένα να καθορίσει την πολιτική πρόσβασης. Για παράδειγμα, το ανθρώπινο δυναμικό προσωπικό που είναι κανονικά εξουσιοδοτημένο με την πρόσβαση στις εγγραφές υπαλλήλων, και η πολιτική αυτή είναι γενικά τυποποιημένη με κανόνες για τον έλεγχο της πρόσβασης σε ένα σύστημα υπολογιστή.

Κατά τη λειτουργία, το σύστημα χρησιμοποιεί τους κανόνες ελέγχου πρόσβασης για να αποφασίσει αν οι σχετικές αιτήσεις πρόσβασης είναι επικυρωμένες , οι καταναλωτές πρέπει να εγκρίνονται( εγκρίνεται) ή έχουν απορριφθεί (απορρίπτεται). Οι πόροι περιλαμβάνουν μεμονωμένα αρχεία ή αντικείμενα δεδομένων, προγράμματα ηλεκτρονικών υπολογιστών, συσκευές ηλεκτρονικών υπολογιστών και τη λειτουργικότητα που παρέχεται από τις εφαρμογές του υπολογιστή .

Παραδείγματα καταναλωτών είναι οι χρήστες ηλεκτρονικών υπολογιστών, τα προγράμματα ηλεκτρονικών υπολογιστών και άλλων συσκευών στον υπολογιστή. Η πιο κοινή τεχνική είναι από τον ελεγκτή που ελέγχει την ακρίβεια ενός μηνύματος (ενδεχομένως σε απάντηση σε ένα προηγούμενο μήνυμα) που καταδεικνύει ότι ο ενάγων κατέχει ένα μυστικό που συνδέεται από το σχέδιο με το γνήσιο συμβαλλόμενο μέρος.

Τα ονόματα για τέτοιες τεχνικές περιλαμβάνουν τον προσδιορισμό, την επικύρωση οντοτήτων, και (λιγότερο συχνά) την επαλήθευση ταυτότητας. Μια σημαντική διαφορά μεταξύ της επικύρωσης οντοτήτων και της επικύρωσης μηνυμάτων (όπως προβλέπεται από τις ψηφιακές υπογραφές ή MAC's) είναι ότι η επικύρωση ίδιων μηνυμάτων δεν παρέχει καμία εγγύηση επικαιρότητας όσον αφορά όταν δημιουργήθηκε ένα μήνυμα, ενώ η επικύρωση οντοτήτων περιλαμβάνει επιβεβαίωση της ταυτότητας ενός ενάγοντος μέσω των πραγματικών επικοινωνιών με έναν σχετικό ελεγκτή κατά τη διάρκεια της εκτέλεσης του ίδιο πρωτοκόλλου (δηλ., στον πραγματικό χρόνο, ενώ η οντότητα επαλήθευσης αναμένει). Αντιθέτως, η επικύρωση οντοτήτων δεν περιλαμβάνει χαρακτηριστικά κανένα σημαντικό μήνυμα εκτός από την αξίωση της ύπαρξης μιας ιδιαίτερης οντότητα, όπως η επικύρωση μηνυμάτων.
Οι τεχνικές που παρέχουν την επικύρωση οντοτήτων και τη βασική καθιέρωση σε μερικές περιπτώσεις, είναι ουσιαστικά η επικύρωση μηνυμάτων, όπου το μήνυμα είναι το κλειδί.

## 2.1.1 Στόχοι αναγνώρισης και εφαρμογές

Η γενική ρύθμιση για ένα πρωτόκολλο προσδιορισμού περιλαμβάνει έναν ενάγοντα Α και έναν ελεγκτή Β. Ο ελεγκτής παρουσιάζεται ή θεωρείται εκ των προτέρων, η ταυτότητα του ενάγοντος. Στόχος είναι να επιβεβαιώσει ότι η ταυτότητα του ενάγοντος είναι πράγματι Α, ώστε να παρέχει την επικύρωση οντοτήτων.

*Ορισμός:* Η επικύρωση οντοτήτων είναι η διαδικασία με το οποίο ένα συμβαλλόμενο μέρος βεβαιώνεται (μέσω της απόκτησης των ενισχυτικών στοιχείων) για την ταυτότητα ενός δεύτερου συμβαλλόμενου μέρους που συμμετέχει σε ένα πρωτόκολλο, και ότι το δεύτερο έχει συμμετάσχει πραγματικά (δηλαδή είναι ενεργός, ή αμέσως πριν από αυτό το χρόνο τα στοιχεία αποκτήθηκαν).

*Παρατήρηση* . Ο ορισμός της ορολογίας του προσδιορισμού και της επικύρωσης οντοτήτων χρησιμοποιούνται ταυτόσημα. Η διάκριση γίνεται μεταξύ της αδύνατης, ισχυρής, και βασισμένης στην μηδέν-γνώση επικύρωσης. Σε άλλες βιβλιογραφίες, μερικές φορές ο προσδιορισμός υπονοεί μόνο μια απαιτημένη ή δηλωμένη ταυτότητα ενώ η επικύρωση οντοτήτων προτείνει μια επιβεβαιωμένη ταυτότητα.

(i)Στόχοι των πρωτοκόλλων αναγνώρισης
Από την άποψη του ελεγκτή, η έκβαση ενός πρωτοκόλλου επικύρωσης οντοτήτων είναι είτε αποδοχή της ταυτότητας του ενάγοντος ως αυθεντική (ολοκλήρωση με την αποδοχή), είτε λήξη χωρίς αποδοχή (απόρριψη). Πιο συγκεκριμένα, οι στόχοι ενός πρωτοκόλλου προσδιορισμού περιλαμβάνουν τα εξής:

1. Στην περίπτωση των τίμιων συμβαλλόμενων μερών Α και Β, το Α είναι σε θέση να επικυρωθεί επιτυχώς στο Β, δηλ., το Β θα ολοκληρώσει το πρωτόκολλο δεχόμενο ως ταυτότητα το Α.

2. Δυνατότητα μεταβίβασης. Το Β δεν μπορεί να επαναχρησιμοποιήσει μια ανταλλαγή προσδιορισμού με το Α ώστε να υποδύεται επιτυχώς το Α σε έναν τρίτο Γ.

3. Προσωποποίηση. Η πιθανότητα είναι αμελητέα ότι κάθε Γ μέρος διακρίνεται από το Α, που μεταφέρεται από το πρωτόκολλο και παίζει το ρόλο του Α, μπορεί να προκαλέσει το Β για να ολοκληρωθεί και να το δεχτεί ως ταυτότητα του. Εδώ αμελητέα συνήθως σημαίνει "είναι τόσο μικρή που δεν έχει πρακτική σημασία " και ο ακριβής ορισμός εξαρτάται από την εφαρμογή.

4. Τα προηγούμενα σημεία παραμένουν αληθινά ακόμα κι αν ένας μεγάλος αριθμός προηγούμενων επικυρώσεων μεταξύ του Α και του Β έχει παρατηρηθεί και το αντίπαλο Γ έχει συμμετάσχει στις προηγούμενες εκτελέσεις πρωτοκόλλου με καθεμία ή και Α και Β και οι πολλαπλάσιες περιπτώσεις του πρωτοκόλλου, που αρχίζουν ενδεχομένως από το Γ, μπορούν να οργανωθούν ταυτόχρονα.
Η ιδέα της μηδενικής γνώσης πρωτοκόλλων είναι ότι οι εκτελέσεις του πρωτοκόλλου δεν χρειάζεται καν αποκαλύπτουν τυχόν αποσπασματικές πληροφορίες που καθιστά το έργο της Γ ευκολότερο.

Μια ταυτότητα (ή οντότητα ταυτότητας) είναι μια "πραγματικού χρόνου" διαδικασία υπό την έννοια ότι παρέχει την εγγύηση ότι το κόμμα σε έλεγχο ταυτότητας λειτουργεί κατά το χρόνο της εκτέλεση του πρωτοκόλλου , αφού προέβη σε κάποια ενέργεια από την έναρξη της εκτέλεσης του πρωτοκόλλου. Αναγνώριση πρωτοκόλλων παρέχουν εγγυήσεις μόνο στην

συγκεκριμένη στιγμή στο χρόνο της επιτυχούς ολοκλήρωσης του πρωτοκόλλου. Σε περίπτωση που απαιτούνται διαβεβαιώσεις, επιπρόσθετα μέτρα μπορεί να είναι απαραίτητα.

(ii)Βάση της αναγνώρισης
Οι τεχνικές επικύρωσης οντοτήτων μπορούν να διαιρεθούν σε τρεις κύριες κατηγορίες, ανάλογα με την ασφάλεια:

1. *κάτι γνωστό*. Τα παραδείγματα περιλαμβάνουν τους τυποποιημένους κωδικούς πρόσβασης (που χρησιμοποιούνται μερικές φορές για να παραγάγουν ένα συμμετρικό κλειδί), τους προσωπικούς αριθμούς αναγνώρισης (PINs), και τα μυστικά ή ιδιωτικά κλειδιά η των οποίων γνώση καταδεικνύεται στα πρωτόκολλα πρόκλησης-απάντησης.

2. *κάτι που κατέχεται*. Αυτό είναι χαρακτηριστικά ένα φυσικό εξάρτημα, μοιάζοντας με ένα διαβατήριο στη λειτουργία. Τα παραδείγματα περιλαμβάνουν τις μαγνητικές κάρτες, τα chipcards (πλαστικές κάρτες το μέγεθος των πιστωτικών καρτών, που περιέχουν έναν ενσωματωμένο μικροεπεξεργαστή ή ένα ολοκληρωμένο κύκλωμα επίσης αποκαλούμενες έξυπνες κάρτες ή κάρτες ολοκληρωμένου κυκλώματος, και τους φορητούς προσαρμοσμένους υπολογιστές (γεννήτριες κωδικού πρόσβασης) που παρέχουν τους time-variant κωδικούς πρόσβασης.

3. *κάτι έμφυτο* (σε ένα ανθρώπινο άτομο). Αυτή η κατηγορία περιλαμβάνει τις μεθόδους που χρησιμοποιούν τα ανθρώπινα φυσικά χαρακτηριστικά και τις ακούσιες ενέργειες (βιομετρική), όπως οι χειρόγραφες υπογραφές, τα δακτυλικά αποτυπώματα, η φωνή, τα αμφιβληστροειδικά σχέδια, η γεωμετρία χεριών, και τα δυναμικά χαρακτηριστικά πληκτρολόγησης. Αυτές οι τεχνικές είναι χαρακτηριστικά μη-κρυπτογραφικές.

(iii) Οι αιτήσεις των πρωτοκόλλων αναγνώρισης

Ένας από τους αρχικούς σκοπούς του προσδιορισμού είναι να διευκολυνθεί ο έλεγχος πρόσβασης σε έναν πόρο, όταν συνδέεται ένα προνόμιο πρόσβασης με μια ιδιαίτερη ταυτότητα (π.χ., τοπική ή εξ' αποστάσεως πρόσβαση στους απολογισμούς αποσύρσεων υπολογιστών από τους αυτοματοποιημένους διανομείς μετρητών, τις άδειες επικοινωνιών μέσω ενός λιμένα επικοινωνιών, πρόσβαση στις εφαρμογές λογισμικού, φυσική είσοδος στις περιορισμένες περιοχές ή τις διασταυρώσεις συνόρων). Ένα σχέδιο κωδικού πρόσβασης που χρησιμοποιείται για να επιτρέψει την πρόσβαση στον απολογισμό υπολογιστών ενός χρήστη μπορεί να αντιμετωπισθεί ως απλούστερη περίπτωση μιας μήτρας ελέγχου πρόσβασης: κάθε πόρος έχει έναν κατάλογο ταυτοτήτων που συνδέονται (π.χ., ένας απολογισμός υπολογιστών που οι εξουσιοδοτημένες οντότητες μπορούν να έχουν πρόσβαση), και επιτυχής επιβεβαίωση μιας ταυτότητας που επιτρέπει την πρόσβαση στους εξουσιοδοτημένους πόρους όπως απαριθμούνται για εκείνη την οντότητα. Σε πολλές εφαρμογές (π.χ., κυψελοειδής τηλεφωνία) το κίνητρο για τον προσδιορισμό είναι να επιτραπεί η χρήση των πόρων για να ακολουθηθεί στις προσδιορισμένες οντότητες, για να διευκολύνει την κατάλληλη τιμολόγηση. Ο προσδιορισμός είναι επίσης χαρακτηριστικά μια έμφυτη απαίτηση στα επικυρωμένα βασικά πρωτόκολλα καθιερώσεων.

## 2.1.2 Ιδιότητες των πρωτοκόλλων αναγνώρισης

Τα πρωτόκολλα προσδιορισμού μπορούν να έχουν πολλές ιδιότητες. Οι ιδιότητες ενδιαφέρουσες στους χρήστες περιλαμβάνουν:

1. *αμοιβαιότητας αναγνώρισης*. Είτε ένα ή και τα δύο μέρη μπορούν να πιστοποιήσουν την ταυτότητά τους στο άλλο, παρέχοντας, αντίστοιχα, μονομερή ή αμοιβαία αναγνώριση. Ορισμένες τεχνικές, όπως η εργασία ορισμένου κωδικού συστημάτων, είναι δυνατό να δεχθούν μια οντότητα που θέτουν ως ελεγκτή μόνο και μόνο για να συλλάβει τον κωδικό πρόσβασης ενός ενάγοντος

2. *υπολογιστική αποδοτικότητα*. Ο αριθμός των ενεργειών που απαιτούνται για την εκτέλεση ενός πρωτοκόλλου

3. *Ανακοίνωση της αποτελεσματικότητας*. Αυτό περιλαμβάνει τον αριθμό των περασμάτων (ανταλλαγής μηνυμάτων)και του εύρους ζώνης που απαιτείται (συνολικός αριθμός των bits που διαβιβάζονται).

4. *σε πραγματικό χρόνο συμμετοχή ενός τρίτου* (ενδεχομένως). Τα παραδείγματα των τρίτων περιλαμβάνουν μια απευθείας σύνδεση εμπιστευμένου τρίτου για να διανείμουν τα κοινά συμμετρικά κλειδιά στην επικοινωνία των οντοτήτων για λόγους επικύρωσης και μια σε απευθείας σύνδεση (untrusted) υπηρεσία καταλόγου για τη διανομή των δημόσιων - βασικών πιστοποιητικών, που υποστηρίζονται από μια σε μη απευθείας σύνδεση αρχή πιστοποίησης

5. *φύση της εμπιστοσύνης που απαιτείται σε έναν τρίτο* (ενδεχομένως). Τα παραδείγματα περιλαμβάνουν την εμπιστοσύνη για έναν τρίτο για να επικυρώσουν σωστά και να δεσμεύσουν το όνομα μιας οντότητας σε ένα δημόσιο κλειδί και έναν εμπιστευμένο τρίτο με
τη γνώση του ιδιωτικού κλειδιού μιας οντότητας.
6. *εγγυήσεις ασφαλούς φύσης*. Τα παραδείγματα περιλαμβάνουν τις αποδείξιμες ιδιότητες ασφάλειας και μηδενικής γνώσης

7. *αποθήκευση των μυστικών*. Αυτό περιλαμβάνει τη θέση και τη μέθοδο χρησιμοποιουμένων (π.χ., λογισμικό μόνο, τοπικοί δίσκοι, σημεία υλικού, κ.λπ....) για να αποθηκευτεί το κρίσιμο υλικό διαμόρφωσης.

***Σχέση μεταξύ ταυτότητας και υπογραφής συστημάτων***

Τα σχέδια προσδιορισμού συσχετίζονται πολύ με, αλλά απλούστερα από, ψηφιακά σχέδια υπογραφών, τα οποία περιλαμβάνουν ένα μεταβλητό μήνυμα και παρέχουν χαρακτηριστικά ότι μια μη αρνητική άδεια χαρακτηριστικών γνωρισμάτων αμφισβητεί για να επιλυθεί από τους δικαστές μετά από το γεγονός. Για τα σχέδια προσδιορισμού, η σημασιολογία του μηνύματος καθορίζεται μια απαιτημένη ταυτότητα στην τρέχουσα στιγμή. Η αξίωση είτε επιβεβαιώνεται είτε απορρίπτεται αμέσως, με τα σχετικά προνόμια που χορηγούνται ή αμφισβητούνται στον πραγματικό χρόνο. Οι προσδιορισμοί δεν έχουν "τη διάρκεια ζωής" δεδομένου ότι οι υπογραφές- διαφωνίες δεν χρειάζονται να επιλυθούν με έναν προγενέστερο προσδιορισμό, και οι επιθέσεις που μπορούν να γίνουν εφικτές στο

μέλλον δεν έχουν επιπτώσεις στην ισχύ ενός προγενέστερου προσδιορισμού. Σε μερικές περιπτώσεις, τα σχέδια προσδιορισμού μπορούν επίσης να μετατραπούν στα σχέδια υπογραφών χρησιμοποιώντας μια τυποποιημένη τεχνική.

## 2.2 Οι κωδικοί πρόσβασης (ασθενής ταυτότητας)

Τα συμβατικά σχέδια κωδικού πρόσβασης περιλαμβάνουν τους χρονικά αμετάβλητους κωδικούς πρόσβασης, οι οποίοι παρέχουν την αποκαλούμενη αδύνατη επικύρωση. Η βασική ιδέα είναι η ακόλουθη. Ένας κωδικός πρόσβασης, που συνδέεται με κάθε χρήστη (οντότητα), είναι χαρακτηριστικά μια σειρά 6 έως 10 ή περισσότερων χαρακτήρων που ο χρήστης είναι σε θέση στη μνήμη. Αυτό χρησιμεύει ως ένα κοινό μυστικό μεταξύ του χρήστη και του συστήματος. (Τα συμβατικά σχέδια κωδικού πρόσβασης εμπίπτουν έτσι στην κατηγορία συμμετρικών-βασικών τεχνικών που παρέχουν τη μονομερή επικύρωση.) Για να αποκτήσει πρόσβαση σε έναν πόρο συστημάτων (π.χ., απολογισμός υπολογιστών, εκτυπωτής, ή εφαρμογή λογισμικού), ο χρήστης εισάγει ένα (ταυτότητα χρήστη, κωδικός πρόσβασης) ζευγάρι, και ρητά ή σιωπηρά διευκρινίζει έναν πόρο εδώ η ταυτότητα χρήστη είναι μια αξίωση της ταυτότητας, και ο κωδικός πρόσβασης είναι τα στοιχεία που υποστηρίζουν την αξίωση. Το σύστημα ελέγχει ότι ο κωδικός πρόσβασης ταιριάζει με τα αντίστοιχα στοιχεία που φυλάσσει για εκείνη την ταυτότητα χρήστη, και ότι η δηλωμένη ταυτότητα εξουσιοδοτείται για να έχει πρόσβαση στον πόρο. Η επίδειξη της γνώσης αυτού του μυστικού (με την αποκάλυψη ο ίδιος του κωδικού πρόσβασης) γίνεται αποδεκτή από το σύστημα ως επιβεβαίωση της ταυτότητας της οντότητας.

Τα διάφορα σχέδια κωδικού πρόσβασης διακρίνονται με τα μέσα με τα οποία οι πληροφορίες που επιτρέπουν την επαλήθευση κωδικού πρόσβασης αποθηκεύονται μέσα στο σύστημα, και τη μέθοδο επαλήθευσης. Η συλλογή των ιδεών που παρουσιάζονται στα εξής τμήματα παρακινεί τις αποφάσεις σχεδίου γίνονται στα χαρακτηριστικά σχέδια κωδικού πρόσβασης. Ένα επόμενο τμήμα συνοψίζει τις τυποποιημένες επιθέσεις που αυτά τα σχέδια αντιδρούν. Οι απειλές που πρέπει να φρουρηθούν περιλαμβάνουν: την κοινοποίηση κωδικού πρόσβασης (σύστημα εξωτερικού) και τη γραμμή που κρυφακούει (μέσα στο σύστημα).Και τα δύο επιτρέπουν την επόμενη επανάληψη και τον κωδικό πρόσβασης που υποθέτει, συμπεριλαμβάνει τις επιθέσεις λεξικών.

### 2.2.1 Σταθερά κωδικοποιημένα συστήματα: τεχνικές

*(i)Αποθηκευμένα αρχεία με κωδικό πρόσβασης*
Η πιο προφανής προσέγγιση είναι το σύστημα αποθήκευσης κωδικών πρόσβασης χρηστών cleartext σε ένα σύστημα αρχείου κωδικών πρόσβασης, για ανάγνωση και προστασία εγγραφής (π.χ., μέσω της εκμετάλλευσης της πρόσβασης στο σύστημα ελέγχου προνομίων). Κατά την εισαγωγή κωδικού πρόσβασης από ένα χρήστη, το σύστημα συγκρίνει τον κωδικό πρόσβασης που δόθηκαν από το αρχείο κωδικών πρόσβασης για τον αντίστοιχο χρήστη χωρίς τη χρήση μυστικών κλειδιών ή κρυπτογραφικά αρχέτυπα όπως η κρυπτογράφηση. Η περίπτωση αυτή χαρακτηρίζεται ως μη κρυπτογραφική τεχνική. Ένα μειονέκτημα αυτής της μεθόδου είναι ότι δεν παρέχει καμία προστασία έναντι προνομιακής μυημένων χρηστών (ειδικά userids τα οποία έχουν πλήρη δικαιώματα πρόσβασης σε αρχεία του συστήματος και πόρων). Η αποθήκευση των αρχείων κωδικών πρόσβασης μέσα σε αντίγραφα ασφαλείας είναι επίσης μια ανησυχία ασφάλειας, δεδομένου ότι το αρχείο περιέχει cleartext κωδικούς πρόσβασης.

*(ii) Αρχεία πρόσβασης με "κρυπτογραφημένο" κωδικό*
Παρά την αποθήκευση ενός cleartext κωδικού πρόσβασης χρηστών σε ένα (διαβασμένο και προστατευμένο) αρχείο κωδικού πρόσβασης, μια μονόδρομη λειτουργία κάθε κωδικού πρόσβασης χρηστών αποθηκεύεται αντί ο ίδιος του κωδικού πρόσβασης. Για να ελέγξει έναν χρήστη με εισαγμένο κωδικό πρόσβασης, το σύστημα υπολογίζει τη μονόδρομη λειτουργία του πληκτρολογημένου προσωπικού κωδικού, και συγκρίνει αυτό με την αποθηκευμένη είσοδο για τη δηλωμένη ταυτότητα χρήστη. Στις επιθέσεις preclude, το αρχείο κωδικού πρόσβασης χρειάζεται μόνο να γραφτεί ώστε να προστατευθεί.

**Παρατήρηση**:(μονόδρομη λειτουργία εναντίον της κρυπτογράφησης) με σκοπό την προστασία των αρχείων κωδικού πρόσβασης, η χρήση μιας μονόδρομης λειτουργίας είναι γενικά προτιμητέα στην αντιστρέψιμη κρυπτογράφηση. Οι λόγοι include αφορούσαν τους περιορισμούς εξαγωγής, και την ανάγκη για το υλικό. Εντούτοις, σε όλες τις περιπτώσεις, για ιστορικούς λόγους, οι προκύπτουσες τιμές αναφέρονται χαρακτηριστικά ως «κρυπτογραφημένοι» κωδικοί πρόσβασης. Η προστασία των κωδικών πρόσβασης είτε με τη μέθοδο πριν από τη μετάδοση πέρα από τις δημόσιες γραμμές communications εξετάζει την απειλή του συμβιβασμού ο ίδιος του κωδικού πρόσβασης, αλλά μόνο δεν αποκλείει την κοινοποίηση είτε την επανάληψη της μετάδοσης.

*(iii) Κανόνες κωδικών πρόσβασης*
Οι επιθέσεις λεξικών είναι πάντα επιτυχής ενάντια στους προβλέψιμους κωδικούς πρόσβασης, μερικά συστήματα επιβάλλουν τους «κανόνες κωδικού πρόσβασης» για να αποθαρρυνθούν ή να αποτραπούν οι χρήστες από τη χρησιμοποίηση των «αδύνατων κωδικών πρόσβασης». Οι χαρακτηριστικοί κανόνες κωδικού πρόσβασης περιλαμβάνουν έναν χαμηλότερο που δεσμεύεται στο μήκος κωδικού πρόσβασης (π.χ., 8 ή 12 χαρακτήρες) μια απαίτηση για κάθε κωδικό πρόσβασης να περιληφθεί τουλάχιστον ένας χαρακτήρας από κάθε ένα σύνολο κατηγοριών (π.χ., κεφαλαία, αριθμητικός, μη-αλφαριθμητικός) ή έλεγχοι ότι οι κωδικοί πρόσβασης δεν βρίσκονται σε απευθείας σύνδεση με διαθέσιμα λεξικά, και δεν αποτελούνται από τις σχετικές πληροφορίες όπως τα userids ή τα substrings του χρήστη. Γνωρίζοντας ποιοι κανόνες είναι σε ισχύ, ένας αντίπαλος μπορεί να χρησιμοποιήσει μια τροποποιημένη στρατηγική επίθεσης λεξικών που λαμβάνει υπόψη τους κανόνες, και που στοχεύει στην πιο αδύνατη μορφή κωδικών πρόσβασης που εν τούτοις ικανοποιούν τους κανόνες. Ο στόχος των κανόνων κωδικού πρόσβασης είναι να αυξηθεί η εντροπία (κι όχι το ακριβές μήκος) των κωδικών πρόσβασης χρηστών πέρα από την εύκολη πρόσβαση του λεξικού και των εξαντλητικών επιθέσεων αναζήτησης. Η εντροπία αναφέρεται εδώ στην αβεβαιότητα ενός κωδικού πρόσβασης εάν λάβουμε υπ' όψιν ότι όλοι οι κωδικοί πρόσβασης είναι εξίσου πιθανοί, η εντροπία είναι μέγιστη και ίση του log2 πιθανών κωδικών πρόσβασης.

Οι μέθοδοι που ένας αντίπαλος μπορεί να υιοθετήσει σε μία προσπάθεια να νικηθούν τα πρωτόκολλα προσδιορισμού είναι ένα υποσύνολο, και οι τύποι αντιπάλων μπορούν να ταξινομηθούν ομοίως (π.χ., ενεργητικός εναντίον ενεργού, μέλος εναντίον του ξένου) για μια συζήτηση των επιθέσεων σχετικά με τα απλά σχέδια κωδικού πρόσβασης. Όμως, δεδομένου ότι δεν υπάρχει κανένα ζήτημα ενός αντιπάλου που μαθαίνει ένα προηγούμενο κλειδί συνόδου, ή που αναγκάζει ένα παλαιό κλειδί για να επαναχρησιμοποιηθεί, οι ακόλουθοι ορισμοί γίνονται:

1. *προσωποποίηση*: μια εξαπάτηση με το οποίο μια οντότητα ισχυρίζεται ότι είναι άλλη.

2. *επίθεση επανάληψης*: μια προσωποποίηση ή άλλη εξαπάτηση που περιλαμβάνει τη χρήση των πληροφοριών από μια ενιαία προηγούμενη εκτέλεση πρωτοκόλλου, για έναν ίδιο ή διαφορετικό ελεγκτή. Για τα αποθηκευμένα αρχεία, το ανάλογο μιας επίθεσης επανάληψης αποκαθιστά την επίθεση, με το οποίο ένα αρχείο αντικαθίσταται από μια προηγούμενη έκδοση.

3. *επίθεση παρεμβολής λευκών σελίδων*: μια προσωποποίηση ή άλλη εξαπάτηση που περιλαμβάνει τον εκλεκτικό συνδυασμό πληροφοριών από μια ή περισσότερες προηγούμενες ή ταυτόχρονα τρέχουσες εκτελέσεις πρωτοκόλλου (παράλληλες σύνοδοι), συμπεριλαμβανομένης της πιθανής αρχικής σύνταξης μιας ή περισσότερων εκτελέσεων πρωτοκόλλου από ο ίδιος έναν αντίπαλο.

4. *επίθεση αντανάκλασης*: μια επίθεση παρεμβολής λευκών σελίδων που περιλαμβάνει αποστολή πληροφοριών από μια τρέχουσα εκτέλεση πρωτοκόλλου πίσω στο δημιουργό τέτοιων πληροφοριών.

5. *αναγκασμένη καθυστέρηση*: μια αναγκασμένη καθυστέρηση εμφανίζεται όταν παρεμποδίζει ένας αντίπαλος ένα μήνυμα (χαρακτηριστικά που περιέχουν έναν αριθμό ακολουθίας), και το αναμεταδίδει σε κάποιο πιο πρόσφατο χρονικό σημείο. Σημειώστε ότι το καθυστερημένο μήνυμα δεν είναι μια επανάληψη.

6. *επίθεση επιλεγμένων κειμένων*: μια επίθεση σε ένα πρωτόκολλο πρόκλησης-απάντησης όπου ένας αντίπαλος επιλέγει στρατηγικά τις προκλήσεις σε μία προσπάθεια να εξαχθούν οι πληροφορίες για το μακροπρόθεσμο κλειδί του ενάγοντος.

Οι επιθέσεις επιλεγμένων κειμένων αναφέρονται μερικές φορές ως χρησιμοποιήσεις του ενάγοντος ως χρησμό, δηλ., για να λάβουν τις πληροφορίες μη υπολογίσιμες από τη γνώση του δημόσιου κλειδιού ενός ενάγοντος μόνο.
Μια άλλη τεχνική με σκοπό τη βελτίωση της ασφάλειας κωδικού πρόσβασης είναι η διαδικασία παλαιότητας ενός κωδικού πρόσβασης. Ορίζεται μια χρονική περίοδος περιορίζοντας τη διάρκεια ζωής του εκάστοτε κωδικού πρόσβασης (π.χ., 30 ή90 ημέρες). Αυτό προϋποθέτει ότι οι κωδικοί πρόσβασης πρέπει να αλλάζονται περιοδικά.

*(iv) Επιβράδυνση της χαρτογράφησης κωδικού πρόσβασης*
Για να επιβραδύνει τις επιθέσεις που συνεπάγονται δοκιμές σε μεγάλο αριθμό κωδικών πρόσβασης γίνεται έλεγχος του κωδικό πρόσβασης (π.χ., μονόδρομη λειτουργία) υπολογιστικά, για παράδειγμα, με την επανάληψη μιας απλούστερης λειτουργίας. Με την έξοδο της i επανάληψης χρησιμοποιείται για επανάληψη i + 1. Ο συνολικός αριθμός των επαναλήψεων πρέπει να είναι περιορίζεται ούτως ώστε να μην επιβάλει μια αισθητή ή αδικαιολόγητη καθυστέρηση των νόμιμων χρηστών. Επίσης, η λειτουργία πρέπει να είναι τέτοια ώστε όταν επαναλαμβάνεται η χαρτογράφηση να μην οδηγεί σε ένα αποτέλεσμα, του οποίου η εντροπία έχει σημαντικά αποδεκατιστεί.

*(v) Οι Salting κωδικοί πρόσβασης*
Για να γίνουν οι επιθέσεις λεξικών λιγότερο αποτελεσματικές, κάθε κωδικός πρόσβασης, κατά την αρχική καταχώρηση, μπορεί να αυξηθεί με t-bit σε τυχαία σειρά. Αυτή η διαδικασία ονομάζεται salt (μεταβάλλει τη "γεύση" από τον κωδικό πρόσβασης πριν από την εφαρμογή της λειτουργίας σε μονόδρομο). Τόσο οι διαγραμμένοι κωδικοί πρόσβασης και οι salt καταγράφονται στο αρχείο κωδικών. Όταν ο χρήστης εισάγει στη συνέχεια έναν κωδικό πρόσβασης, το σύστημα αναζητά τον αλλαγμένο, και εφαρμόζει τη λειτουργία μονόδρομο εγγράφοντας τον κωδικό πρόσβασης, όπως τροποποιείται ή ενισχύεται από τον

salt. Η δυσκολία της εξαντλητικής έρευνα σε κάποιο συγκεκριμένο κωδικό χρήστη παραμένει αμετάβλητη (από τον salt δίνεται σε απλό κείμενο στο αρχείο κωδικών). Ωστόσο, αυξάνει την πολυπλοκότητα μιας επίθεσης σε ένα μεγάλο σύνολο των κωδικών πρόσβασης ταυτοχρόνως, απαιτώντας από το λεξικό να περιέχει 2t παραλλαγές κάθε κωδικού πρόσβασης δοκιμής. Αυτό συνεπάγεται με απαίτηση για μεγαλύτερη μνήμη για την αποθήκευση των κρυπτογραφημένο λεξικών, και αντίστοιχα περισσότερος χρόνος για την προετοιμασία της. Σημειώστε ότι με αυτή τη λειτουργία, δύο χρήστες που επιλέγουν τον ίδιο κωδικό έχουν διαφορετικές εγγραφές στο αρχείο κωδικών του συστήματος. Σε κάποια συστήματα, μπορεί να ενδείκνυται να χρησιμοποιούνται userid μιας οντότητας η ίδια όπως με τον salt.

*(vi) Φράσεις κλειδιά*
Για να επιτραπεί μεγαλύτερη εντροπία χωρίς ενίσχυση πέρα από την ικανότητα μνήμης των ανθρωπίνων χρηστών, οι κωδικοί πρόσβασης μπορούν να επεκταθούν και σε φράσεις κλειδιά. Στην περίπτωση αυτή, ο χρήστης πληκτρολογεί σε μια φράση ή μια πρόταση παρά μια σύντομη "λέξη". Η φράση κλειδί κατακερματίζεται κάτω σε μια τιμή σταθερού μεγέθους, η οποία διαδραματίζει τον ίδιο ρόλο με έναν κωδικό πρόσβασης, είναι σημαντικό όμως ότι η φράση δεν είναι απλώς κατατετμημένη από το σύστημα, όπως οι κωδικοί πρόσβασης σε ορισμένα συστήματα. Η ιδέα είναι ότι οι χρήστες μπορούν να θυμηθούν φράσεις ευκολότερα από τυχαίες ακολουθίες χαρακτήρων. Αν οι κωδικοί πρόσβασης μοιάζουν με κείμενο, δεδομένου ότι κάθε χαρακτήρας περιέχει μόνο 1,5 bits της εντροπίας , μια συνθηματική φράση παρέχει μεγαλύτερη ασφάλεια μέσω αυξημένης εντροπίας από ένα σύντομο κωδικό πρόσβασης. Ένα μειονέκτημα είναι η πρόσθετη απαίτηση της πληκτρολόγησης.

## 2.2.2 Σταθερά συστήματα κωδικών πρόσβασης: επιθέσεις

Μια αδυναμία των σχεδίων που χρησιμοποιούν τους σταθερούς, επαναχρησιμοποιήσιμους κωδικούς πρόσβασης, είναι η δυνατότητα ότι ένας αντίπαλος μαθαίνει τον κωδικό πρόσβασης ενός χρήστη με την παρατήρηση του καθώς δακτυλογραφείται. Ένα δεύτερο πρόβλημα ασφαλείας είναι ότι οι χρήστης με κωδικό πρόσβασης διαβιβάζονται με καθαρά κείμενα πέρα από τη γραμμή επικοινωνιών μεταξύ του χρήστη και του συστήματος, και είναι επίσης διαθέσιμοι προσωρινά κατά τη διάρκεια της επαλήθευσης συστημάτων. Ένας αντίπαλος που «κρυφακούει» μπορεί να καταγράψει αυτό το στοιχείο, που επιτρέπει την επόμενη προσωποποίηση.

Τα σταθερά σχέδια κωδικού πρόσβασης είναι χρήσιμα όταν διαβιβάζεται ο κωδικός πρόσβασης πέρα από το εμπιστευμένο χρηματοκιβώτιο γραμμών επικοινωνιών από τον έλεγχο, αλλά δεν είναι κατάλληλα στην περίπτωση που οι κωδικοί πρόσβασης διαβιβάζονται πέρα από τα ανοικτά δίκτυα επικοινωνιών. Παραδείγματος χάριν, ο ενάγων Α μπορεί να είναι ένας χρήστης που συνδέεται από το σπίτι μέσο ενός τηλεφωνικού αποδιαμορφωτή, και σε μια περιοχή χιλιάδες μιλίων σε ένα γραφείο Β ο cleartext κωδικός πρόσβασης, μπορεί να ταξιδέψει πέρα από ένα ακάλυπτο τηλεφωνικό δίκτυο (που περιλαμβάνει ενδεχομένως μια ασύρματη σύνδεση), υπό τον όρο να κρυφακούσει.
Στην περίπτωση που η μακρινή επαλήθευση ταυτότητας χρησιμοποιείται για την πρόσβαση σε έναν τοπικό πόρο, π.χ., ένας αυτοματοποιημένος διανομέας μετρητών με την σε απευθείας σύνδεση επαλήθευση ταυτότητας, η απάντηση συστημάτων πρέπει να προστατευθεί εκτός από τον υποβληθέντα κωδικό πρόσβασης, και πρέπει να περιλάβει τη μεταβλητή για να αποτρέψει την επανάληψη μιας χρονικής σταθεράς ν να δεχτεί την

απάντηση.

*(i)Επανάληψη κωδικών πρόσβασης*
Μια αδυναμία των σχεδίων που χρησιμοποιούν τους σταθερούς, επαναχρησιμοποιήσιμους κωδικούς πρόσβασης, είναι η δυνατότητα ότι ένας αντίπαλος μαθαίνει τον κωδικό πρόσβασης ενός χρήστη με την παρατήρηση του καθώς δακτυλογραφείται. Ένα δεύτερο πρόβλημα ασφαλείας είναι ότι οι χρήστης με κωδικό πρόσβασης διαβιβάζονται με καθαρά κείμενα πέρα από τη γραμμή επικοινωνιών μεταξύ του χρήστη και του συστήματος, και είναι επίσης διαθέσιμοι προσωρινά κατά τη διάρκεια της επαλήθευσης συστημάτων. Ένας αντίπαλος που «κρυφακούει» μπορεί να καταγράψει αυτό το στοιχείο, που επιτρέπει την επόμενη προσωποποίηση.

Τα σταθερά σχέδια κωδικού πρόσβασης είναι χρήσιμα όταν διαβιβάζεται ο κωδικός πρόσβασης πέρα από το εμπιστευμένο χρηματοκιβώτιο γραμμών επικοινωνιών από τον έλεγχο, αλλά δεν είναι κατάλληλα στην περίπτωση που οι κωδικοί πρόσβασης διαβιβάζονται πέρα από τα ανοικτά δίκτυα επικοινωνιών. Παραδείγματος χάριν, ο ενάγων Α μπορεί να είναι ένας χρήστης που συνδέεται από το σπίτι μέσο ενός τηλεφωνικού αποδιαμορφωτή, και σε μια περιοχή χιλιάδες μιλίων σε ένα γραφείο Β ο cleartext κωδικός πρόσβασης, μπορεί να ταξιδέψει πέρα από ένα ακάλυπτο τηλεφωνικό δίκτυο (που περιλαμβάνει ενδεχομένως μια ασύρματη σύνδεση), υπό τον όρο να κρυφακούσει.
Στην περίπτωση που η μακρινή επαλήθευση ταυτότητας χρησιμοποιείται για την πρόσβαση σε έναν τοπικό πόρο, π.χ., ένας αυτοματοποιημένος διανομέας μετρητών με την σε απευθείας σύνδεση επαλήθευση ταυτότητας, η απάντηση συστημάτων πρέπει να προστατευθεί εκτός από τον υποβληθέντα κωδικό πρόσβασης, και πρέπει να περιλάβει τη μεταβλητή για να αποτρέψει την επανάληψη μιας χρονικής σταθεράς ν να δεχτεί την απάντηση.

*(ii) Εξαντλητική αναζήτηση κωδικού πρόσβασης*
Μια πολύ αφελής επίθεση περιλαμβάνει έναν αντίπαλο που δοκιμάζει απλά (τυχαία ή συστηματικά) τους κωδικούς πρόσβασης, ένα σε έναν χρόνο, στον πραγματικό ελεγκτή, με την ελπίδα ότι ο σωστός κωδικός πρόσβασης θα βρεθεί. Αυτό μπορεί να αντιμετωπιστεί με την εξασφάλιση ότι οι κωδικοί πρόσβασης επιλέγονται από ένα αρκετά μεγάλο εύρος, που ο αριθμός άκυρων (σε απευθείας σύνδεση) προσπαθειών που επιτρέπονται μέσα στις σταθερές χρονικές περιόδους, και που επιβραδύνει η ίδια τη χαρτογράφηση ή την σύνδεση-διαδικασία κωδικού πρόσβασης. Οι μη απευθείας σύνδεση επιθέσεις, που περιλαμβάνουν έναν μεγάλο υπολογισμό χαρακτήρων που δεν απαιτεί με τον πραγματικό ελεγκτή μια τελική φάση, προκαλούν μεγαλύτερη ανησυχία και εξετάζονται
εδώ.

Λαμβάνοντας υπόψη ένα αρχείο κωδικού πρόσβασης που περιέχει μονόδρομα hashes των κωδικών πρόσβασης χρηστών, ένας αντίπαλος μπορεί να προσπαθήσει να νικήσει το σύστημα με τη δοκιμή των κωδικών πρόσβασης σε έναν χρόνο, και τη σύγκριση μονόδρομου hash με κάθε ένα από τους κωδικούς πρόσβασης στο κρυπτογραφημένο αρχείο κωδικού πρόσβασης. Αυτό είναι θεωρητικά δυνατό δεδομένου ότι και η μονόδρομη χαρτογράφηση και ( το υποτιθέμενο) απλό κείμενο είναι γνωστά. Η δυνατότητα πραγματοποίησης της επίθεσης εξαρτάται από τον αριθμό κωδικών πρόσβασης που χρειάζονται να ελεγχθούν προτού να ανατεθεί μια αντιστοιχία (που ο ίδιος εξαρτάται από τον αριθμό πιθανών κωδικών πρόσβασης), και ο χρόνος που απαιτείται για να εξεταστεί κάθε ένας. Το τελευταίο εξαρτάται από τη χαρτογράφηση κωδικού πρόσβασης χρησιμοποιούμενη, την εφαρμογή του, το χρόνο εκτέλεσης των οδηγιών του επεξεργαστή του χρήστη, και τον αριθμό επεξεργαστών των διαθέσιμων κωδικών.

Ο χρόνος που απαιτείται για να συγκρίνει την πραγματική εικόνα κάθε δοκιμαστικού κωδικού πρόσβασης με όλους τους κωδικούς πρόσβασης σε ένα αρχείο κωδικού πρόσβασης είναι αμελητέος.

Παράδειγμα(εντροπία κωδικού πρόσβασης) υποθέστε ότι οι κωδικοί πρόσβασης αποτελούνται από τις σειρές των επτάμπιτων characters ASCII. Κάθε ένας έχει μια αριθμητική αξία στη σειρά 0-127. (Όταν οι οκτάμπιτοι χαρακτήρες χρησιμοποιούνται, αξίας 128-255 συνθέτουν τον εκτεταμένο χαρακτήρα - θέστε, γενικά απρόσιτο από τους τυποποιημένους κώδικες 0-31 ASCII keyboards.) Είναι διατηρημένος για τους χαρακτήρες ελέγχου 32 και είναι διαστημικός χαρακτήρας 33¬126 είναι πληκτρολογημένοι προσιτοί εκτυπώσιμοι χαρακτήρες και 127 είναι πρόσθετοι χαρακτήρες.

Ο πίνακας 2.2.2.1 δίνει τον αριθμό ευδιάκριτων κωδικών πρόσβασης ν-χαρακτήρων που αποτελούνται από τους συνδυασμούς χαρακτήρων, δείχνοντας έναν ανώτερο που δεσμεύεται στην ασφάλεια τέτοιων διαστημάτων κωδικού πρόσβασης.

Πίνακας 2.2.2.1

| → c<br>↓ n | 26<br>(lowercase) | 36 (lowercase<br>alphanumeric) | 62 (mixed case<br>alphanumeric) | 95 (keyboard<br>characters) |
|---|---|---|---|---|
| 5 | 23.5 | 25.9 | 29.8 | 32.9 |
| 6 | 28.2 | 31.0 | 35.7 | 39.4 |
| 7 | 32.9 | 36.2 | 41.7 | 46.0 |
| 8 | 37.6 | 41.4 | 47.6 | 52.6 |
| 9 | 42.3 | 46.5 | 53.6 | 59.1 |
| 10 | 47.0 | 51.7 | 59.5 | 65.7 |

(Handbook of Applied Cryptography by A. Menezes, P. van Oorschot and S. Vanstone, Ch. 10 Identification and Entity Authentication, page 392)

Μέγεθος Bit χώρου κωδικών πρόσβασης για διάφορους συνδυασμούς χαρακτήρων. Ο αριθμός των n χαρακτήρων κωδικών πρόσβασης, με δεδομένα Γ ανά χαρακτήρα, είναι cn. Ο πίνακας 2.2.2.2 δίνει τη βάση 2 του λογαρίθμου για κωδικούς πρόσβασης.

Πίνακας 2.2.2.2

| → c<br>↓ n | 26<br>(lowercase) | 36 (lowercase<br>alphanumeric) | 62 (mixed case<br>alphanumeric) | 95 (keyboard<br>characters) |
|---|---|---|---|---|
| 5 | 0.67 hr | 3.4 hr | 51 hr | 430 hr |
| 6 | 17 hr | 120 hr | 130 dy | 4.7 yr |
| 7 | 19 dy | 180 dy | 22 yr | 440 yr |
| 8 | 1.3 yr | 18 yr | 1400 yr | 42000 yr |
| 9 | 34 yr | 640 yr | 86000 yr | $4.0 \times 10^6$ yr |
| 10 | 890 yr | 23000 yr | $5.3 \times 10^6$ yr | $3.8 \times 10^8$ yr |

(Handbook of Applied Cryptography by A. Menezes, P. van Oorschot and S. Vanstone, Ch. 10 Identification and Entity Authentication,page 392)

Απαιτούμενος χρόνος για την αναζήτηση ολόκληρου διαστήματος κωδικού πρόσβασης. Ο πίνακας δίνει το χρόνο T (σε ώρες, ημέρες ή έτη) που απαιτείται για την αναζήτηση ή προ-υπολογίζουν πάνω από τον προβλεπόμενο χώρο χρησιμοποιώντας έναν επεξεργαστή. T = cn τ .. γ, όπου t ο αριθμός των υπερβάσεων της χαρτογράφησης κωδικός πρόσβασης επαναλαμβάνεται, και γ το χρόνο ανά επανάληψη, για t = 25, γ = 1 / (125 000) sec.

(iii) Οι κωδικοί πρόσβασης μαντεύουν τις επιθέσεις λεξικών

Για να βελτιωθεί η αναμενόμενη πιθανότητα επιτυχίας μιας εξαντλητικής αναζήτησης, παρά την έρευνα μέσω του διαστήματος όλων των πιθανών κωδικών πρόσβασης, ένας αντίπαλος μπορεί να ψάξει την κατά σειρά μικρότερη πιθανότητα. Ενώ οι αυθαίρετες σειρές των χαρακτήρων ν θα ήταν ίσων πιθανοτήτων ως χρήστης επιλεγμένων κωδικών πρόσβασης, οι περισσότεροι (απεριόριστοι) χρήστες επιλέγουν τα passwords από ένα μικρό υποσύνολο του πλήρους διαστήματος κωδικού πρόσβασης (π.χ., σύντομοι κωδικοί

πρόσβασης, λέξεις λεξικών, κατάλληλα ονόματα, πεζές σειρές). Τέτοιοι αδύνατοι κωδικοί πρόσβασης με τη χαμηλή εντροπία υποθέτονται εύκολα πράγματι, οι μελέτες δείχνουν ότι ένα μεγάλο μέρος των επιλεγμένων κωδικών πρόσβασης βρίσκεται στα χαρακτηριστικά λεξικά μόνο 150 000 λέξεων, ενώ ακόμη και ένα μεγάλο λεξικό 250000 λέξεων αντιπροσωπεύει μόνο ένα μικροσκοπικό μέρος όλων των πιθανών κωδικών πρόσβασης ν-χαρακτήρων.

Οι κωδικοί πρόσβασης που βρίσκονται σε οποιαδήποτε απευθείας σύνδεση ή διαθέσιμο κατάλογο λέξεων μπορούν να αποκαλυφθούν από έναν «εχθρό» ο ποίος δοκιμάζει όλες τις λέξεις σε αυτόν τον κατάλογο, χρησιμοποιώντας μια αποκαλούμενη επίθεση λεξικών. Εκτός από τα λεξικά, τα σε απευθείας σύνδεση λεξικά των ξένων γλωσσών, ή στα εξειδικευμένα θέματα όπως η μουσική, η ταινία, κ.λπ. είναι διαθέσιμα. Για την αποδοτικότητα σε επαναλαμβανόμενη χρήση από έναν αντίπαλο, ένας «κρυπτογραφημένος» κατάλογος λεξικού ή κωδικού πρόσβασης δημιουργούνται πιθανότητες να αποθηκευτεί σε δίσκο ή ταινία εικόνες του κωδικού πρόσβασης από τα αρχεία κωδικού πρόσβασης συστημάτων τα οποία μπορούν έπειτα να συλλεχθούν, να διαταχτούν (χρησιμοποιώντας έναν αλγόριθμο ταξινόμησης ή συμβατικό hashing), και να συγκριθούν έπειτα με τα λήμματα στο κρυπτογραφημένο λεξικό. Οι επιθέσεις λεξικού δεν είναι συνήθως επιτυχείς στην εύρεση του κωδικού πρόσβασης ενός ιδιαίτερου χρήστη, αλλά βρίσκουν πολλούς κωδικούς πρόσβασης στα περισσότερα συστήματα.

### 2.2.3 κωδικοί πρόσβασης UNIX

Το λειτουργικό σύστημα UNIX παρέχει ένα ευρέως γνωστό, ιστορικά σημαντικό παράδειγμα ενός σταθερού συστήματος κωδικού πρόσβασης. Ένα αρχείο κωδικού πρόσβασης UNIX περιέχει μια μονόδρομη λειτουργία των κωδικών πρόσβασης χρηστών που υπολογίζονται ως εξής: κάθε κωδικός πρόσβασης χρηστών χρησιμεύει ως το κλειδί για να κρυπτογραφήσει γνωστό απλό κείμενο (64 μηδενικών bit). Αυτό παράγει μια μονόδρομη λειτουργία του κλειδιού, από μόνο ο χρήστης (εκτός από το σύστημα) ξέρει τον κωδικό πρόσβασης. Για τον αλγόριθμο κρυπτογράφησης, μια δευτερεύουσα τροποποίηση DES χρησιμοποιείται, όπως περιγράφεται κατωτέρω και οι παραλλαγές μπορούν να εμφανιστούν στα προϊόντα έξω από τις ΗΠΑ. Η τεχνική που περιγράφεται στηρίζεται στην υποτιθέμενη ιδιότητα ότι ο DES είναι ανθεκτικός στις γνωστές επιθέσεις απλού κειμένου με δεδομένο το αρχικό κείμενο και το αντίστοιχο κρυπτογράφημα, τότε παραμένει δύσκολο να βρεθεί το κλειδί.
Η συγκεκριμένη τεχνική κάνει την επαναλαμβανόμενη χρήση DES, επαναλαμβάνοντας την κρυπτογράφηση t= 25 φορές .Λεπτομερώς, ένας κωδικός πρόσβασης χρηστών είναι περικομένος στους πρώτους 8 χαρακτήρες του κώδικα ASCII. Κάθε ένας από αυτούς παρέχει 7 bit για ένα 56bit κλειδί DES (που γεμίζεται με 0 bit εάν περιέχει λιγότερο από 8 χαρακτήρες). Το κλειδί χρησιμοποιείται για να κρυπτογραφήσει την εξηντατετράμπιτη σταθερά 0 του DES, με την παραγωγή που ανατροφοδοτείται ως επαναληπτικοί χρόνοι εισαγωγής τ. Το εξηντατετράμπιτο αποτέλεσμα είναι σε 11 εκτυπώσιμους χαρακτήρες (εξηντατετράμπιτη παραγωγή και 12 salt παραγωγές κομματιών 76 bit, 11 οι χαρακτήρες ASCII επιτρέπουν 77). Επιπλέον, μια μεταβλητή της μεθόδου salt χρησιμοποιείται, προορισμένη να περιπλέξει ταυτόχρονα τις επιθέσεις λεξικών και να αποκλείσει τη χρήση του υλικού DES για τις επιθέσεις:

1. *Salt κωδικοί πρόσβασης*: Συνδέει ένα τυχαίο 12bit που λαμβάνεται από το ρολόι συστημάτων στο χρόνο της δημιουργίας κωδικού πρόσβασης με κάθε επιλεγμένο κωδικό πρόσβασης από το χρήστη. Τα 12bit χρησιμοποιούνται για να αλλάξουν την τυποποιημένη λειτουργία Ε επέκτασης DES mapping (παρέχοντας τη μια από 4096 παραλλαγές). (Η επέκταση Ε δημιουργεί έναν φραγμό 48 bit αμέσως μετά, τα salt κομμάτια καθορίζουν συλλογικά τη μια από 4096 μεταλλαγές. Το κάθε bit συνδέεται με το καθορισμένο ζεύγος

του φραγμού των 48 bit , π.χ., το κομμάτι 1 και 25, το κομμάτι 2 2 και 26, κ.λπ. Εάν το salt κομμάτι είναι 1, τα κομμάτια φραγμών ανταλλάσσονται, και ειδάλλως δεν είναι. Και ο κομματιασμένος κωδικός πρόσβασης και το άλας καταγράφονται στο αρχείο κωδικού πρόσβασης συστημάτων. Η ασφάλεια του κωδικού πρόσβασης οποιουδήποτε ιδιαίτερου χρήστη είναι αμετάβλητη με τη μετατροπή αλλά μια επίθεση λεξικών απαιτεί τώρα 212 = δοκιμαστικούς κωδικούς πρόσβασης 4096 παραλλαγών

2. *Παρεμπόδιση της χρήσης του από το DES*: Επειδή η επέκταση DES E εξαρτάται από το salting, το πρότυπο DES δεν μπορεί πλέον να χρησιμοποιηθεί για την εφαρμογή του αλγόριθμου UNIX. Ένας αντίπαλος που επιθυμεί να χρησιμοποιήσει το υλικό για την επιτάχυνση μιας επίθεσης πρέπει να χρησιμοποιήσει προσαρμοσμένα υλικού και όχι τα κοινά εμπορικά από τις διαθέσιμες μάρκες. Αυτό μπορεί να αποτρέψει τους αντιπάλους με περιορισμένους πόρους. Η τιμή που αποθηκεύεται για ένα δεδομένο userid σε ένα απλό αρχείο προστατεύεται από κωδικό πρόσβασης .Έτσι, επαναλαμβάνεται η κρυπτογράφηση 0 υπό τον κωδικό πρόσβασης του χρήστη, χρησιμοποιώντας την τροποποίηση του DES. Η συνεχής 0 εδώ θα μπορούσε να αντικατασταθεί από άλλες αξίες, αλλά τυπικά δεν γίνεται. Ο αλγόριθμος καλείται UNIX crypt αλγόριθμος με κωδικό πρόσβασης.

## 2.2.4 Οι κωδικοί αριθμοί PIN's και οι κωδικοί πρόσβασης

(i)PIN's
Οι προσωπικοί αριθμοί αναγνώρισης (PINs) εμπίπτουν στην κατηγορία σταθερών (αμετάβλητων στο χρόνο) κωδικών πρόσβασης. Συχνότερα χρησιμοποιούνται από ένα φυσικό σημείο όπως μια πλαστική τραπεζική κάρτα με μια μαγνητικό λωρίδα, ή μια κάρτα chip. Για να αποδείξει την ταυτότητά κάποιος ως εξουσιοδοτημένος χρήστης, και να αποκτήσει πρόσβαση στα προνόμια που συνδέονται με αυτό, απαιτείται η εισαγωγή του σωστού PIN. Αυτό παρέχει ένα δεύτερο επίπεδο ασφάλειας εάν το σημείο χάνεται ή κλέβεται. Τα PINs μπορούν επίσης να χρησιμεύσουν ως το δεύτερο επίπεδο ασφάλειας της εισόδου στα κτήρια που έχουν ένα ανεξάρτητο πρώτο επίπεδο ασφάλειας (π.χ., μια φρουρά ασφάλειας ή μια κάμερα ελέγχου).

Για την διευκόλυνση των χρηστών και διάφορους ιστορικούς λόγους, τα PINs είναι σχετικά μικρά (σε σχέση με τα σταθερά σχέδια κωδικού πρόσβασης) και αριθμητικά, π.χ., 4 έως 8 ψηφία. Για να αποτρέψουν την εξαντλητική αναζήτηση μέσω του διαστήματος όπως το μικρό κλειδί (π.χ.,10.000 τιμές για μια τετραψήφια αριθμητική ΚΑΡΦΙΤΣΑ), οι πρόσθετοι διαδικαστικοί περιορισμοί είναι απαραίτητοι. Παραδείγματος χάριν, μερικές αυτοματοποιημένες μηχανές διανομέων μετρητών που σχετίζονται με την κατάθεση, έχουν ως βασική λειτουργία μια κάρτα να κατάσχεται εάν εισαχθούν διαδοχικά τρία ανακριβή PINs. Η ανακριβής είσοδος διάφορων διαδοχικών PINs μπορεί να αναγκάσει την κάρτα για "να κλειδωθεί" και να απενεργοποιηθεί, απαιτώντας έκτοτε ένα μεγαλύτερο Pin (π.χ., 8 ψηφία) για την απενεργοποίηση μετά από τέτοιες ύποπτες περιστάσεις. Σε ένα σύστημα ανοικτής γραμμής που χρησιμοποιεί PINs ή τους επαναχρησιμοποιήσιμους κωδικούς πρόσβασης, μια απαιτημένη ταυτότητα που συνοδεύεται από ένα χρήστη με εισαγμένο κωδικό PIN μπορεί να ελεγχθεί σε σύγκριση με το PIN που αποθηκεύεται για εκείνη την ταυτότητα σε μια βάση δεδομένων. Μια εναλλακτική λύση είναι να χρησιμοποιηθεί το PIN ως κλειδί για τη MAC. Σε ένα σύστημα με μη απευθείας σύνδεση χωρίς πρόσβαση σε μια κεντρική βάση δεδομένων, οι πληροφορίες που διευκολύνουν την επαλήθευση των PINS πρέπει να αποθηκευτούν για το ίδιο το σημείο. Εάν το PIN δεν χρειάζεται να επιλεγεί από το χρήστη, αυτό μπορεί να γίνει με τον καθορισμό PIN για τη δημιουργία ενός βασικού χρήστη και της ταυτότητας του που συνδέεται με το σημείο PIN και επαληθεύεται από οποιοδήποτε μακρινό σύστημα ξέροντας αυτό το κύριο κλειδί. Σε ένα σύστημα με μη απευθείας σύνδεση, μπορεί επίσης να είναι επιθυμητό να επιτραπεί το PIN για να είναι

επιλέξιμο από το χρήστη, ώστε να είναι ευκολότερη η αποστήθιση των PINS από τους χρήστες. Σε αυτήν την περίπτωση, το PIN μπορεί να κρυπτογραφηθεί κάτω από ένα κύριο κλειδί και να αποθηκευτεί στο σημείο, με το κύριο κλειδί που είναι γνωστό σε όλα τα σε μη απευθείας σύνδεση τερματικά. Ένα προτιμητέο σχέδιο είναι να αποθηκευτεί μια μονόδρομη λειτουργία το PIN, η ταυτότητα των χρηστών, και το κύριο κλειδί.

(ii) Τα δύο στάδια ελέγχου ταυτότητας και κωδικού πρόσβασης που προέρχονται από τα κλειδιά
Οι ανθρώπινοι χρήστες αντιμετωπίζουν δυσκολία απομνημόνευσης των μυστικών κλειδιών που έχουν την ικανοποιητική εντροπία για να παρέχουν την επαρκή ασφάλεια. Παρακάτω περιγράφονται δύο τεχνικές που αντιμετωπίζουν αυτό το ζήτημα.
Όταν τα σημεία χρησιμοποιούνται με επαλήθευση πολλών γραμμών PINS, μια κοινή τεχνική είναι για να χρησιμεύσει το PIN, να ελέγξει δηλαδή το χρήστη στο σημείο, ενώ το σημείο περιέχει τις πρόσθετες ανεξάρτητες πληροφορίες που επιτρέπουν στο σημείο για να επικυρωθεί στο σύστημα (ως έγκυρο σημείο που αντιπροσωπεύει έναν νόμιμο χρήστη). Ο χρήστης με αυτόν τον τρόπο επικυρώνεται έμμεσα στο σύστημα με μια δύο σταδίων διαδικασία. Αυτό δηλώνει ότι ο χρήστης έχει στην κατοχή το σημείο αλλά και θυμάται μόνο ένα μικρό PIN, ενώ ένα πιο μακροχρόνιο κλειδί (που περιέχει την επαρκή εντροπία) παρέχει την κρυπτογραφική ασφάλεια για την επικύρωση πέρα από μια ακάλυπτη σύνδεση. Μια δεύτερη τεχνική είναι για έναν κωδικό πρόσβασης χρηστών να χαρτογραφείται από μια μονόδρομη hash λειτουργία σε ένα κρυπτογραφικό κλειδί (π.χ., ένα κλειδί 56-κομματιών DES). Τέτοιοι κωδικοί πρόσβασης και παραγόμενα κλειδιά καλούνται passkeys. Το passkey χρησιμοποιείται έπειτα για να εξασφαλίσει μια σύνδεση επικοινωνιών μεταξύ του χρήστη και ενός συστήματος που ξέρει επίσης τον κωδικό πρόσβασης χρηστών. Πρέπει να εξασφαλιστεί ότι η εντροπία του κωδικού πρόσβασης του χρήστη είναι αρκετά μεγάλη και ότι η εξαντλητική αναζήτηση του διαστήματος κωδικού πρόσβασης δεν είναι αποδοτικότερη από την εξαντλητική αναζήτηση του διαστήματος passkey (δηλ., που υποθέτει τους κωδικούς πρόσβασης δεν είναι ευκολότερη από την υπόθεση 56-bit DES κλειδιών).

Μια εναλλακτική λύση της κατοχής passkeys, είναι να παραμένει σταθερό έως ότου αλλαχθεί ο κωδικός πρόσβασης και να κρατηθεί ένας τρέχοντας αριθμός ακολουθίας από την πλευρά συστημάτων μαζί με τον κωδικό πρόσβασης κάθε χρήστη, για τη χρήση ως time-variant που κοινοποιείται στο χρήστη και που αυξάνεται μετά από κάθε χρήση.
Το Passkey πρέπει να αντιμετωπισθεί ως μακροπρόθεσμο κλειδί, με τη χρήση του να περιορίζεται στην επικύρωση και τη βασική διαχείριση (παρά επίσης για τη μαζική κρυπτογράφηση των στοιχείων χρηστών). Ένα μειονέκτημα της χρήσης ενός κωδικού πρόσβασης και των παραγόμενων του κλειδιών είναι ότι η αποθήκευση του κωδικού πρόσβασης κάθε χρήστη μέσα στο σύστημα απαιτεί κάποιο μηχανισμό για να προστατεύσει την εμπιστευτικότητα των αποθηκευμένων κωδικών πρόσβασης.

## 2.2.5 One-time κωδικοί πρόσβασης (ισχυρής αυθεντικοποίησης)

Μια φυσική πρόοδος από τα σταθερά σχέδια κωδικού πρόσβασης στα πρωτόκολλα προσδιορισμού πρόκλησης απάντησης μπορεί να παρατηρηθεί με την εξέταση των onetime σχεδίων κωδικού πρόσβασης. Μια σημαντική ανησυχία ασφάλειας των σταθερών σχεδίων κωδικού πρόσβασης κρυφακούει και μια επόμενη επανάληψη του κωδικού πρόσβασης. Μια μερική λύση είναι οι one-time κωδικοί πρόσβασης: Κάθε κωδικός πρόσβασης χρησιμοποιείται μόνο μια φορά. Τέτοια σχέδια είναι ασφαλή από τους παθητικούς αντιπάλους που κρυφακούνε. Οι παραλλαγές περιλαμβάνουν:
1. *κοινή λίστα των one-time passwords*: Ο χρήστης και το σύστημα χρησιμοποιεί μια ακολουθία με μυστικούς κωδικούς πρόσβασης (κάθε άδεια ισχύει για ένα μόνο έλεγχο ταυτότητας), το οποίο διανέμεται με κοινή λίστα. Ένα μειονέκτημα είναι η συντήρηση του κοινού καταλόγου. Εάν η λίστα δεν χρησιμοποιείται διαδοχικά, το σύστημα μπορεί να ελέγξει τις εγγραφές κωδικού πρόσβασης από όλες τους υπόλοιπους αχρησιμοποίητους κωδικούς πρόσβασης. Μια μεταβολή συνεπάγεται τη χρήση ενός πίνακα πρόκλησης απάντησης, με την οποία ο χρήστης και το σύστημα μοιράζεται ζεύγη πρόκλησης-απάντησης, με ιδανική περίπτωση κάθε ζεύγος να ισχύει το πολύ μία φορά.
2. *διαδοχική ενημέρωση one-time passwords*: Αρχικά μόνο ένας ενιαίος μυστικός κωδικός πρόσβασης μοιράζεται. Κατά τη διάρκεια της επικύρωσης χρησιμοποιεί τον κωδικό πρόσβασης ι, ο χρήστης δημιουργεί και διαβιβάζει στο σύστημα έναν νέο κωδικό πρόσβασης (κωδικός πρόσβασης ι + 1) κρυπτογραφημένο κάτω από ένα κλειδί που προέρχεται από τον κωδικό πρόσβασης I. Αυτή η μέθοδος γίνεται δύσκολη εάν προκύψουν αποτυχίες επικοινωνίας.

3. *one-time* ακολουθίες με κωδικό πρόσβασης που βασίζεται σε μια μονόδρομη συνάρτηση: Αυτή η μέθοδος είναι πιο αποτελεσματική (σε σχέση με το εύρος ζώνης) από τα one-time passwords, και μπορεί να θεωρηθεί ως ένα πρωτόκολλο πρόκλησης-απάντησης, όπου η πρόκληση ορίζεται από την τρέχουσα θέση, κατά την ακολουθία του κωδικού πρόσβασης.

## 2.3 Πρόκληση-απάντηση αναγνώρισης (ισχυρή αυθεντικοποίηση)

Η ιδέα των κρυπτογραφικών πρωτοκόλλων πρόκλησης-απάντησης είναι ότι μια οντότητα (ο ενάγων)"αποδεικνύει" ένα κλειδί που είναι γνωστό για να συνδέεται με εκείνη την οντότητα, χωρίς να αποκαλύψει το ίδιο το μυστικό στον ελεγκτή κατά τη διάρκεια του πρωτοκόλλου. Αυτό γίνεται όταν δώσει μια απάντηση σε μια time-variant πρόκληση, όπου η απάντηση εξαρτάται από το μυστικό της οντότητας και την πρόκληση. Η πρόκληση είναι χαρακτηριστικά ένας αριθμός που επιλέγεται από μια οντότητα (τυχαία και κρυφά) στην έναρξη του πρωτοκόλλου. Εάν η γραμμή επικοινωνιών ελέγχεται, η απάντηση από μια εκτέλεση του πρωτοκόλλου προσδιορισμού δεν πρέπει να παρέχει σε έναν αντίπαλο τις χρήσιμες πληροφορίες για έναν επόμενο προσδιορισμό, δεδομένου ότι οι επόμενες προκλήσεις θα διαφέρουν. (Σε μερικούς μηχανισμούς, το μυστικό είναι γνωστό στον ελεγκτή, και χρησιμοποιείται για να ελέγξει την απάντηση για άλλους, το μυστικό δεν χρειάζεται να μαθευτεί πραγματικά από τον ελεγκτή).

## 2.3.1 Time-variant παράμετροι

Οι time-variant παράμετροι μπορούν να χρησιμοποιηθούν στα πρωτόκολλα προσδιορισμού για να αντιδράσουν στις επιθέσεις επανάληψης και παρεμβολής λευκών σελίδων, παρέχοντας τις εγγυήσεις μοναδικότητας ή επικαιρότητας, και για να αποτρέψει ορισμένες επιθέσεις επιλεγμένων κειμένων. Μπορούν ομοίως να χρησιμοποιηθούν στα επικυρωμένα βασικά πρωτόκολλα καθιερώσεων, αλλά και για να παρέχουν τις εγγυήσεις μοναδικότητας από κοινού με την επικύρωση μηνυμάτων.
Οι time-variant παράμετροι που διακρίνουν μια περίπτωση πρωτοκόλλου από άλλη καλούνται μερικές φορές nonces, μοναδικές τιμές μη-επανάληψης αριθμών , ή οι ορισμοί αυτών των όρων είναι παραδοσιακά χαλαροί, όπως οι συγκεκριμένες ιδιότητες που εξαρτώνται από την χρήση και το πρωτόκολλο.
Ορισμός: Nonce είναι μια αξία που χρησιμοποιείται λιγότερος από μιά φορά για τον ίδιο σκοπό. Χρησιμεύει χαρακτηριστικά να αποτρέψει (τη μη ανιχνεύσιμη) επανάληψη.Ο όρος nonce χρησιμοποιείται για να αναφερθεί σε έναν "τυχαίο" αριθμό πρωτόκολλου, και οι απαραίτητες ιδιότητες ποικίλλουν. Παρακάτω θα εξετάσουμε τρεις κατηγορίες time-variant παραμέτρων: τυχαίοι αριθμοί, αριθμοί ακολουθίας, και time-stamps. Συχνά, για να εξασφαλιστεί η ασφάλεια πρωτοκόλλου, πρέπει να εγγυηθεί η ακεραιότητα τέτοιων παραμέτρων (π.χ., κρυπτογραφικά να δεσμεύσει με άλλα στοιχεία μια ακολουθία πρόκλησης-απάντησης). Αυτό ισχύει ιδιαίτερα για τα πρωτόκολλα στα οποία η μόνη απαίτηση μιας time-variant παραμέτρου είναι η μοναδικότητα.Παρακάτω εξετάζονται ορισμένες διαφορές για τις time-variant παραμέτρους.

1. Η επαληθεύσιμη επικαιρότητα μπορεί να παρασχεθεί μέσω της χρήσης των τυχαίων αριθμών στους μηχανισμούς πρόκλησης-απάντησης, οι timestamps από κοινού με διανεμημένα timeclocks, ή οι αριθμοί ακολουθίας από κοινού με τη συντήρηση pairwise (ενάγων, ελεγκτής) δηλώνοντας τις πληροφορίες.
2. Για να παρέχει τις εγγυήσεις επικαιρότητας ή μοναδικότητας, ο ελεγκτής στο πρωτόκολλο ελέγχει τη time-variant παράμετρο, είτε άμεσα (μέσω της επιλογής ενός τυχαίου αριθμού) είτε έμμεσα (μέσω των πληροφοριών που διατηρούνται σχετικά με μια κοινή ακολουθία, ή λογικά μέσω ενός κοινού χρονικού ρολογιού).
3. Για να προσδιορίσουν μεμονωμένα ένα μήνυμα ή μια ακολουθία μηνυμάτων (περίπτωση πρωτοκόλλου), τα nonces που προέρχονται από μια μονοτονική αυξανόμενη ακολουθία μπορούν να χρησιμοποιηθούν (π.χ., ακολουθία ή αύξοντες αριθμοί, και timestamps, εάν εγγυάται τη μοναδικότητα), ή τυχαίοι αριθμοί ικανοποιητικού μεγέθους. Η μοναδικότητα απαιτείται συχνά μόνο μέσα σε ένα δεδομένο βασικό παράθυρο διάρκειας ζωής ή χρόνου.
4. Μπορούν να χρησιμοποιηθούν συνδυασμοί time-variant παραμέτρων, π.χ., τυχαίοι αριθμοί που συνδέονται με timestamps ή με αριθμούς ακολουθίας. Αυτό μπορεί να εγγυηθεί ότι ένας ψευδοτυχαίος αριθμός δεν αναπαράγεται.

(i) *Τυχαίοι αριθμοί*
Οι τυχαίοι αριθμοί μπορούν να χρησιμοποιηθούν στους μηχανισμούς πρόκλησης-απάντησης, για να παρέχουν τις διαβεβαιώσεις μοναδικότητας και επικαιρότητας, και για να αποκλείσουν ορισμένες επιθέσεις επανάληψης και παρεμβολής λευκών σελίδων (συμπεριλαμβανομένων των τυχαίων αριθμών παρατήρησης). Μπορεί επίσης να μην είναι προβλέψιμοι, παραδείγματος χάριν, για να αποκλείσει τις επιθέσεις κειμένων. Οι τυχαίοι αριθμοί όρου, όταν χρησιμοποιούνται στα πλαίσια των πρωτοκόλλων προσδιορισμού και επικύρωσης, περιλαμβάνουν τους ψευδοτυχαίους αριθμούς που είναι απρόβλεπτοι σε έναν αντίπαλο αυτό διαφέρει από το τυχαίο υπό την παραδοσιακή στατιστική έννοια. Στις περιγραφές πρωτοκόλλου, η επιλογή τυχαίου αριθμού συνήθως σημαίνει την επιλογή ενός αριθμού με την ομοιόμορφη διανομή από ένα διευκρινισμένο διάστημα δειγμάτων. Οι

τυχαίοι αριθμοί χρησιμοποιούνται στα πρωτόκολλα πρόκλησης-απάντησης ως εξής. Μια οντότητα περιλαμβάνει έναν (νέο) τυχαίο αριθμό σε ένα εξερχόμενο μήνυμα. Ένα εισερχόμενο μήνυμα λαμβανόμενο στη συνέχεια (π.χ. το επόμενο μήνυμα πρωτοκόλλου της ίδιας περίπτωσης πρωτοκόλλου), του οποίου η κατασκευή απαιτεί τη γνώση αυτού του nonce και στο οποίο αυτό το nonce είναι αχώριστα συνδεδεμένο, πρέπει να είναι νέο βάσει στο ότι ο τυχαίος αριθμός συνδέει τα δύο μηνύματα. Απαιτείται η μη απευθείας σύνδεση για να αποτρέψει την επισύναψη ενός nonce σε ένα παλαιό μήνυμα. Οι τυχαίοι αριθμοί που χρησιμοποιούνται με αυτόν τον τρόπο καθορίζουν ένα σχετικό σημείο εγκαίρως για τα ενδιαφερόμενα μέρη, ανάλογα με το κοινό timeclock. Ο μέγιστος επιτρεπόμενος χρόνος μεταξύ των μηνυμάτων πρωτοκόλλου περιορίζεται μέχρι μια περίοδο διαλείμματος, χρησιμοποιώντας τα τοπικά, ανεξάρτητα χρονόμετρα αντίστροφης μέτρησης.

Παρατηρήσεις:
1. Στα πλαίσια της πρόκληση-απάντησης τα πρωτόκολλα, νέα χαρακτηριστικά σημαίνουν πρόσφατο, από την άποψη της δημιουργίας μετά από την αρχή της τρέχουσας περίπτωσης πρωτοκόλλου. Σημειώστε ότι έτσι δεν αποκλείονται οι επιθέσεις παρεμβολής λευκών σελίδων χρησιμοποιώντας τις παράλληλες συνόδους
2. Οι επαναλήψεις γενεθλίων στους τυχαίους αριθμούς κατά την παραγωγή των ψευδοτυχαίων αριθμών για χρήση ως time-variant παραμέτρων, αρκεί η πιθανότητα ενός επαναλαμβανόμενου αριθμού να είναι χαμηλή και οι αριθμοί να μην επαναχρησιμοποιούνται σκόπιμα. Αυτό μπορεί να επιτευχθεί με την επιλογή της τυχαίας αξίας από ένα αρκετά μεγάλο διάστημα δειγμάτων, λαμβάνοντας υπόψη τις συμπτώσεις που προκύπτουν από το παράδοξο γενεθλίων. Τα τελευταία μπορούν να εξεταστούν είτε με την επιλογή ενός μεγαλύτερου διαστήματος δειγμάτων, είτε με τη λειτουργία μιας διαδικασίας παραγωγής που εγγυάται την αποφυγή της επανάληψης, όπως η χρήση του μετρητή είτε του OFB cipher φραγμών.

3. Στα μειονεκτήματα των τυχαίων αριθμών βλέπουμε ότι πολλά πρωτόκολλα που περιλαμβάνουν τυχαίους αριθμούς απαιτούν την ασφάλεια της κρυπτογράφησης τυχαίων αριθμών. Εάν χρησιμοποιούνται ψευδοτυχαίες γεννήτριες αριθμού, απαιτούνται νέες με αρχική ταχύτητα ικανοποιητικής εντροπίας. Όταν οι τυχαίοι αριθμοί χρησιμοποιούνται στους μηχανισμούς πρόκλησης-απάντησης αντί των timestamps, το πρωτόκολλο περιλαμβάνει ένα πρόσθετο μήνυμα, και ο αμφισβητίας πρέπει προσωρινά να διατηρήσει τις κρατικές πληροφορίες, αλλά μόνο έως ότου ελέγχει η απάντηση.

(ii) *Αριθμοί ακολουθίας*
Ένας αριθμός ακολουθίας (αύξων αριθμός, ή αντίθετη αξία) χρησιμεύει ως ένας μοναδικός αριθμός που προσδιορίζει ένα μήνυμα, και χρησιμοποιείται χαρακτηριστικά για να ανιχνεύσει την επανάληψη μηνυμάτων. Για τα αποθηκευμένα αρχεία, οι αριθμοί ακολουθίας μπορούν να χρησιμεύσουν ως αριθμοί έκδοσης για το εν λόγω αρχείο. Οι αριθμοί ακολουθίας είναι συγκεκριμένοι για ένα ζευγάρι οντοτήτων, και πρέπει ρητά ή σιωπηρά να συνδεθούν και με το δημιουργό και με τον παραλήπτη ενός μηνύματος. Οι ακολουθίες είναι συνήθως απαραίτητες για τα μηνύματα από το A στο B και από το B στο A.

Τα συμβαλλόμενα μέρη ακολουθούν μια προκαθορισμένη πολιτική για την αρίθμηση μηνυμάτων. Ένα μήνυμα γίνεται αποδεκτό μόνο εάν ο αριθμός ακολουθίας εκεί μέσα δεν έχει χρησιμοποιηθεί προηγουμένως (ή δεν έχει χρησιμοποιηθεί προηγουμένως εντός ενός καθορισμένου χρονικού διαστήματος), και ικανοποιεί τη συμφωνηθείσα πολιτική. Η

απλούστερη πολιτική είναι ότι μια ακολουθία αριθμών ξεκινάει στο μηδέν, αυξάνεται διαδοχικά, και κάθε διαδοχικό μήνυμα έχει έναν αριθμό μεγαλύτερο από τον προηγούμενο . Μια λιγότερο περιοριστική πολιτική είναι ότι οι αριθμοί ακολουθίας χρειάζεται (μόνο) να αυξάνονται μονοτονικά. Έτσι τα χαμένα μηνύματα μπορεί να περνάνε λόγω των δύσκολων επικοινωνιών, αλλά αποκλείεται η ανίχνευση των μηνυμάτων που χάνονται λόγω της εκατέρωθεν επέμβασης.

Στα μειονεκτήματα των αριθμών ακολουθίας είναι ότι η χρήση των αριθμών ακολουθίας απαιτεί ο κάθε ενάγων να καταγράψει και να διατηρήσει τη μακροπρόθεσμη δήλωση pairwise, οι πληροφορίες για κάθε πιθανό ελεγκτή δηλαδή, να είναι επαρκείς για να καθορίσει τους προηγουμένως χρησιμοποιημένους ή/και έγκυρους αριθμούς ακολουθίας. Οι ειδικές διαδικασίες (π.χ., για την επαναρύθμιση των αριθμών ακολουθίας) μπορεί να είναι απαραίτητες μετά από τις περιστάσεις που αναστατώνουν την κανονική αλληλουχία (π.χ., διακοπές του συστήματος). Οι αναγκασμένες καθυστερήσεις δεν είναι ανιχνεύσιμες γενικά. Συνεπώς, οι αριθμοί ακολουθίας είναι οι πιο κατάλληλοι για τις μικρότερες, κλειστές ομάδες.

*(iii) Timestamps*

Τα Timestamps μπορούν να χρησιμοποιηθούν για να παρέχουν τις εγγυήσεις επικαιρότητας και μοναδικότητας, για να ανιχνεύσουν την επανάληψη μηνυμάτων. Μπορούν επίσης να χρησιμοποιηθούν για να εφαρμόσουν τα περιορισμένα προνόμια πρόσβασης, και για να ανιχνεύσουν τις αναγκασμένες καθυστερήσεις. Λειτουργούν ως εξής: Το συμβαλλόμενο μέρος λαμβάνει ένα μήνυμα timestamp από το τοπικό ρολόι και το δεσμεύει κρυπτογραφικά σε ένα μήνυμα. Κατά τη λήψη ενός σφραγισμένου μηνύματος, το δεύτερο συμβαλλόμενο μέρος λαμβάνει τον τρέχοντα χρόνο από το ρολόι και αφαιρεί το timestamp που λαμβάνει. Για το λαμβανόμενο μήνυμα ισχύει:

**1**. η διαφορά είναι μέσα στο παράθυρο αποδοχής (ένα χρονικό διάστημα καθορισμού μεγέθους, π.χ., 10 χιλιοστά του δευτερολέπτου ή 20 δευτερόλεπτα, που επιλέγονται για να αποτελέσουν το μέγιστο χρόνο διέλευσης και επεξεργασίας μηνυμάτων, συν τη λοξή κίνηση ρολογιών) και
**2**. (προαιρετικά) κανένα μήνυμα με ίδιο timestamp δεν έχει παραληφθεί από τον ίδιο δημιουργό. Αυτός ο έλεγχος μπορεί να γίνει από τον ελεγκτή που διατηρεί έναν κατάλογο με όλα τα timestamps που παραλαμβάνονται από κάθε οντότητα πηγής μέσα στο τρέχον παράθυρο αποδοχής. Μια άλλη μέθοδος είναι να καταγραφεί το πιο πρόσφατο (έγκυρο) timestamp που χρησιμοποιείται από κάθε πηγή (σε αυτήν την περίπτωση ο ελεγκτής δέχεται μόνο τις αυστηρά αυξανόμενες χρονικές τιμές).

Η ασφάλεια της timestamp επαλήθευσης στηρίζεται στη χρήση μιας κοινής χρονικής αναφοράς . Αυτό απαιτεί ότι τα ρολόγια οικοδεσποτών είναι διαθέσιμα και συγχρονίζονται αόριστα και είναι ασφαλή λόγω της τροποποίησης. Ο συγχρονισμός είναι απαραίτητος για να αντιμετωπίσει την κλίση ρολογιών, και πρέπει να είναι κατάλληλα προσαρμοσμένος στο παράθυρο αποδοχής που χρησιμοποιείται. Ο βαθμός κίνησης ρολογιών που επιτρέπεται ο έλεγχος, και το παράθυρο αποδοχής, πρέπει να είναι κατάλληλα μικρός για να αποκλείσουν την επανάληψη μηνυμάτων εάν ο ανωτέρω προαιρετικός παραλείπεται. Το timeclock πρέπει να είναι ασφαλές για να αποτρέψει την εκατέρωθεν επαναρύθμιση ενός ρολογιού ώστε να αποκατασταθεί προς τα πίσω η ισχύς των παλαιών μηνυμάτων, ή τη ρύθμιση ενός ρολογιού για να προετοιμάσει προς τα εμπρός ένα μήνυμα για κάποιο μελλοντικό σημείο.

Τα timestamp πρωτόκολλα απαιτούν ότι τα ρολόγια είναι και συγχρονισμένα και εξασφαλισμένα. Ο αποκλεισμός της εκατέρωθεν τροποποίησης των τοπικών timeclocks είναι δύσκολο να εγγυηθεί σε πολλά διανεμημένα περιβάλλοντα και η ασφάλεια πρέπει να επαναξιολογηθεί προσεκτικά. Η διατήρηση των καταλόγων των χρησιμοποιημένων timestamps μέσα στο τρέχον παράθυρο μειονεκτεί σε μια ενδεχομένη μεγάλη απαίτηση αποθήκευσης. Ενώ οι τεχνικές λύσεις υπάρχουν για το συγχρονισμό των διανεμημένων ρολογιών, εάν ο συγχρονισμός ολοκληρώνεται μέσω των πρωτοκόλλων δικτύων (τέτοια πρωτόκολλα πρέπει να είναι ασφαλή), απαιτούνται χαρακτηριστικά για την επικύρωση οδηγώντας σε ένα κυκλικό επιχείρημα ασφάλειας εάν η επικύρωση είναι βασισμένη στο ίδιο timestamps.

Συγκρίνοντας τα timestamps στα πρωτόκολλα δεν προσφέρουν το πλεονέκτημα λιγότερων μηνυμάτων και δεν υπάρχει καμία απαίτηση να διατηρηθούν οι μακροπρόθεσμες κρατικές πληροφορίες ή οι βραχυπρόθεσμες κρατικές πληροφορίες ανά σύνδεση. Η ελαχιστοποίηση των κρατικών πληροφοριών είναι ιδιαίτερα σημαντική για τους κεντρικούς υπολογιστές στις εφαρμογές πελατών εξυπηρετητών. Το κύριο μειονέκτημα των timestamps είναι η απαίτηση ασφάλειας, που συγχρονίζεται σε χωριστά timeclocks. Τα timestamps στα πρωτόκολλα μπορούν να αντικατασταθούν από μια τυχαία πρόκληση αριθμού συν ένα μήνυμα επιστροφής.

## 2.3.2 Πρόκληση-απόκριση με τεχνικές συμμετρικού κλειδιού

Οι μηχανισμοί πρόκλησης-απάντησης βασίζονται στις βασικές τεχνικές που απαιτούν τον ενάγοντα και τον ελεγκτή για να μοιραστούν ένα συμμετρικό κλειδί. Για τα κλειστά συστήματα με έναν μικρό αριθμό χρηστών, κάθε ζευγάρι των χρηστών μπορεί να μοιραστεί ένα κλειδί στα μεγαλύτερα συστήματα που υιοθετούν, τα πρωτόκολλα προσδιορισμού περιλαμβάνουν συχνά τη χρήση ενός εμπιστευμένου σε απευθείας σύνδεση κεντρικού υπολογιστή με τον οποίο κάθε συμβαλλόμενο μέρος μοιράζεται ένα κλειδί. Ο κεντρικός υπολογιστής που συνδέεται απευθείας ενεργεί αποτελεσματικά, παρέχοντας ένα κοινό κλειδί συνόδου σε δύο συμβαλλόμενα μέρη κάθε φορά που ζητά επικύρωση με άλλο. Η προφανής απλότητα των τεχνικών είναι παραπλανητική. Το σχέδιο τέτοιων τεχνικών είναι περίπλοκο και η ασφάλεια είναι εύθραυστη.

(i)Πρόκληση-απάντηση βασισμένη στο συμμετρικό κλειδί κρυπτογράφησης
Και τα δύο πρωτόκολλα. το Kerberos και το Needham-Schroeder το οποίο έχει μοιραζόμενο κλειδί παρέχουν την επικύρωση οντοτήτων βασισμένη στη συμμετρική κρυπτογράφηση και περιλαμβάνουν τη χρήση ενός σε απευθείας σύνδεση εμπιστευμένου τρίτου. Παρακάτω περιγράφονται τρεις απλές τεχνικές βασισμένες στο ISO/ IEC9798-2. Υποθέτουν την προγενέστερη ύπαρξη ενός κοινού μυστικού κλειδιού (και καμίας περαιτέρω απαίτησης για έναν σε απευθείας σύνδεση κεντρικό υπολογιστή). Σε αυτήν την περίπτωση, δύο συμβαλλόμενα μέρη μπορούν να πραγματοποιήσουν μονομερή επικύρωση οντοτήτων σε ένα πέρασμα χρησιμοποιώντας timestamps ή τους αριθμούς ακολουθίας, ή δύο περάσματα χρησιμοποιώντας τους τυχαίους αριθμούς. Η αμοιβαία επικύρωση απαιτεί, αντίστοιχα, δύο και τρία περάσματα. Ο ενάγων επιβεβαιώνει την ταυτότητά του με την επίδειξη της γνώσης του κοινού κλειδιού με την κρυπτογράφηση μιας πρόκλησης (και των ενδεχομένως πρόσθετων στοιχείων) χρησιμοποιώντας το κλειδί.

Όταν η κρυπτογράφηση χρησιμοποιείται στα πρωτόκολλα επικύρωσης οντοτήτων, η ακεραιότητα στοιχείων πρέπει χαρακτηριστικά επίσης να εγγυηθεί για να εξασφαλίσει την ασφάλεια. Παραδείγματος χάριν, για τα μηνύματα που εκτείνονται με περισσότερους από

έναν φραγμούς, η αναδιοργάνωση των φραγμών κρυπτογραφημάτων δεν μπορεί να ανιχνευθεί στον τρόπο ECB κρυπτογράφησης φραγμών, και ακόμη και η κρυπτογράφηση CBC μπορεί να παρέχει μόνο μια μερική λύση. Τέτοια ακεραιότητα στοιχείων πρέπει να παρασχεθεί μέσω της χρήσης ενός αποδεκτού μηχανισμού ακεραιότητας στοιχείων.

Οι μηχανισμοί 9798-2: Το tA και rA, αντίστοιχα, χαρακτηρίζουν έναν τυχαίο αριθμό και μια χρονική σήμανση, που παράγεται από το A. (Σε αυτούς τους μηχανισμούς, τα tA timestamp μπορούν να αντικατασταθούν από ένα nA αύξων αριθμό, που παρέχει ελαφρώς διαφορετικές εγγυήσεις.) Το EK δείχνει έναν συμμετρικό αλγόριθμο κρυπτογράφησης, με ένα βασικό K κοινό στο A και το β εναλλακτικά, τα ευδιάκριτα κλειδιά KAB και το BA K μπορούν να χρησιμοποιηθούν για την ομοιοκατευθυνόμενη επικοινωνία. Υποτίθεται ότι αμφότερα τα συμβαλλόμενα μέρη γνωρίζουν την άλλη ταυτότητα, είτε από το πλαίσιο είτε από τους πρόσθετους cleartext τομείς στοιχείων. Οι προαιρετικοί τομείς μηνυμάτων δείχνονται από έναν αστερίσκο(*), ενώ ένα κόμμα() στο πλαίσιο του ε K δείχνει την αλληλουχία.

1.*Μονομερής επικύρωση βασισμένη στο timestamp:*

$$A - B : EK(tA,B^*) \qquad (1)$$

Επάνω στην υποδοχή και την αποκρυπτογράφηση, το B ελέγχει αν το timestamp είναι αποδεκτό, και προαιρετικά εξετάζει το λαμβανόμενο προσδιοριστικό. Το προσδιοριστικό B αποτρέπει έναν αντίπαλο από να επαναχρησιμοποιήσει το μήνυμα αμέσως στο A, στην περίπτωση που ένα ενιαίο αμφίδρομο βασικό K χρησιμοποιείται.
2.*Μονομερής επικύρωση, που χρησιμοποιεί τους τυχαίους αριθμούς:*
Για να αποφευχθεί η εξάρτηση από τα timestamps, το timestamp μπορεί να αντικατασταθεί από έναν τυχαίο αριθμό, το κόστος είναι ένα επιπλέον μήνυμα:

$$A <- B : rB \ (1) \ A - B : EK \ (rB \ , B^*) \qquad (2)$$

Το B αποκρυπτογραφεί το λαμβανόμενο μήνυμα και ελέγχει ότι οι τυχαίες αντιστοιχίες αριθμού που έστειλαν (1). Προαιρετικά, το B ελέγχει ότι το προσδιοριστικό (2) είναι δικό του αποτρέποντας μια επίθεση αντανάκλασης στην περίπτωση ενός αμφίδρομου βασικού K. Για να αποτρέψει τις επιθέσεις κειμένων, το A μπορεί να ενσωματώσει έναν πρόσθετο τυχαίο αριθμό σε (2) ή διαδοχικά, η μορφή των προκλήσεων μπορεί να περιοριστεί στην κρίσιμη απαίτηση της απαγόρευσης της επανάληψης.
*3. Αμοιβαία επικύρωση, που χρησιμοποιεί τους τυχαίους αριθμούς:*

$$A < - \beta : \rho \ B \ (1) \ A — \beta : E \ K \ (\rho \ ENA \ , r \ B \ , B \ ^* \ ) \ (2) \ A < \_ \ \beta : E \ K \ (\rho \ B \ , r \ A) \ (3)$$

Κατά την παραλαβή του (2), το B πραγματοποιεί τους ελέγχους όπως ορίζονται ανωτέρω και, επιπλέον, ανακτά το αποκρυπτογραφημένο rA συμπεριλαμβάνοντας το στη σχέση (3). Μετά την αποκρυπτογράφηση (3),το A ελέγχει ότι οι δύο τυχαίοι αριθμοί ταιριάζουν με αυτές που χρησιμοποιήθηκαν προηγουμένως. Ο δεύτερος τυχαίο rA αριθμός στο (2) λειτουργεί ως μια πρόκληση και για την πρόληψη επιθέσεων κειμένων.
Ενώ η αμοιβαία επικύρωση μπορεί να ληφθεί με το να τρέξει σε οποιουσδήποτε από τους ανωτέρω μονομερείς μηχανισμούς επικύρωσης δύο φορές (μιά φορά σε κάθε κατεύθυνση), ένας τέτοιος ειδικός συνδυασμός υφίσταται το μειονέκτημα ότι οι δύο μονομερείς επικυρώσεις, που δεν συνδέονται, δεν μπορούν λογικά να συνδεθούν με ένα ενιαίο τρέξιμο πρωτοκόλλου.

*(ii) Πρόκλησης-απάντηση βασισμένη στις μονόδρομες συναρτήσεις*
Ο αλγόριθμος κρυπτογράφησης στους ανωτέρω μηχανισμούς μπορεί να αντικατασταθεί από μια μονόδρομη ή μη αναστρέψιμη λειτουργία του κοινόχρηστου κλειδιού και της πρόκλησης, π.χ., έχοντας τις ιδιότητες παρόμοιες με το aMAC . Αυτό μπορεί να είναι προτιμητέο στις καταστάσεις όπου οι αλγόριθμοι κρυπτογράφησης είναι μη διαθέσιμοι ή ανεπιθύμητοι (π.χ., λόγω των περιορισμών εξαγωγής ή των υπολογιστικών δαπανών). Οι τροποποιήσεις που απαιτούνται στους 9798-2 μηχανισμούς (παράγοντας τους ανάλογους μηχανισμούς ISO/IEC 9798-4) είναι οι ακόλουθες:
**1**. η λειτουργία EK κρυπτογράφησης αντικαθίσταται από έναν αλγόριθμο hK της MAC
**2.** παρά την αποκρυπτογράφηση και την επαλήθευση ότι οι τομείς ταιριάζουν, ο παραλήπτης τώρα ανεξάρτητα υπολογίζει την αξία της MAC από τις γνωστές ποσότητες, και δέχεται τις υπολογισμένες αντιστοιχίες της MAC λαμβάνοντας υπ'όψιν αξία της MAC και
**3**. για να επιτρέψει τον ανεξάρτητο υπολογισμό της MAC από τον παραλήπτη, το πρόσθετο cleartext tA πρέπει να στείλει στο μήνυμα (1) του μηχανισμού ένα πέρασμα. Το r A πρέπει να σταλεί ως πρόσθετος cleartext τομέας στο μήνυμα (2) του μηχανισμού τρειών περασμάτων.

Ο αναθεωρημένος μηχανισμός πρόκλησης-απάντησης τριών περασμάτων βασισμένος στη MAC hk, με τις ενέργειες όπως σημειώνονται ανωτέρω, παρέχει τον αμοιβαίο προσδιορισμό. Ουσιαστικά το ίδιο πρωτόκολλο, αποκαλούμενο SKID3, έχει τα μηνύματα ως εξής:

*A <- B : rB (1) A — B : rA,hK(rA,rB,B)(2) A <- B : hK (rB ,rA,A) (3)*

Σημειώστε ότι ο πρόσθετος τομέας A συμπεριλαμβάνεται στο μήνυμα (3). Το πρωτόκολλο SKID2, που λαμβάνεται με την παράλειψη του τρίτου μηνύματος, παρέχει τη μονομερή επικύρωση οντοτήτων.

*(iii) Εφαρμογή με χρήση φορητών γεννητριών κωδικό πρόσβασης*
Η απάντηση μιας πρόκλησης στα πρωτόκολλα πρόκλησης-απάντησης απαιτεί κάποιο τύπο συσκευής υπολογισμού και ασφαλούς αποθήκευσης για το μακροπρόθεσμο υλικό διαμόρφωσης (π.χ., ένα αρχείο σε εμπιστευμένο τοπικό δίσκο, ίσως που εξασφαλίζεται κάτω από ένα τοπικό κωδικό πρόσβασης και το παραγόμενο κλειδί). Για την πρόσθετη ασφάλεια, μια συσκευή όπως ένα chipcard (και ο αντίστοιχος αναγνώστης καρτών) μπορεί να χρησιμοποιηθεί και για τη βασική αποθήκευση και για τον υπολογισμό απάντησης. Σε μερικές περιπτώσεις, μια λιγότερο ακριβή επιλογή είναι μια passcode γεννήτρια.
Οι Passcode γεννήτριες είναι φορητές συσκευές, που μοιάζουν με λεπτούς υπολογιστές και στο μέγεθος και στην επίδειξη, και που παρέχουν τους time-variant κωδικούς πρόσβασης ή passcodes. Η γεννήτρια περιέχει μια συσκευή με συγκεκριμένο μυστικό κλειδί. Όταν ένας χρήστης παρουσιάζεται με μια πρόκληση (π.χ., από ένα σύστημα που το επιδεικνύει σε ένα τερματικό υπολογιστών), η πρόκληση κλειδώνεται στη γεννήτρια. Η γεννήτρια επιδεικνύει το passcode, που υπολογίζεται ως λειτουργία μυστικού του βασικού και η πρόκληση μπορεί να είναι είτε μια ασυμμετρική λειτουργία, είτε μια συμμετρική λειτουργία (π.χ., κρυπτογράφηση ή MAC). Ο χρήστης επιστρέφει την απάντηση (π.χ., κλειδώνει το passcode μέσα στο τερματικό του), που το σύστημα ελέγχει σε σύγκριση με μια ανεξάρτητη υπολογισμένη απάντηση, χρησιμοποιώντας τις ίδιες πληροφορίες που αποθηκεύονται από την πλευρά συστημάτων. Για την περαιτέρω προστασία ενάντια στις τοποθετημένες σε λάθος μέρος γεννήτριες, η απάντηση μπορεί επίσης να εξαρτηθεί από ένα PIN.
Οι απλούστερες passcode γεννήτριες παραλείπουν το αριθμητικό πληκτρολόγιο χρηστών, και τη χρήση ως υπονοούμενη πρόκληση μιας χρονικής αξίας που καθορίστηκε από ένα timeclock ,συγχρονίζοντας αόριστα αυτόματα μεταξύ τους το σύστημα και την passcode γεννήτρια.

Μια περιπλοκότερη συσκευή συνδυάζει τον υπονοούμενο συγχρονισμό με τις ρητές προκλήσεις, που παρουσιάζουν μια ρητή πρόκληση μόνο όταν χάνεται ο συγχρονισμός. Ένα μειονέκτημα των συστημάτων που χρησιμοποιούν τις passcode γεννήτριες είναι η απαίτηση να παρασχεθεί η εμπιστευτικότητα για τους κωδικούς πρόσβασης χρηστών που αποθηκεύονται από την πλευρά συστημάτων.

### 2.3.3 Πρόκληση-απάντηση με τεχνικές δημόσιου κλειδιού

Τεχνικές δημόσιων κλειδιών μπορούν να χρησιμοποιηθούν για την πρόκληση-απόκρισης με βάση την αναγνώριση, με τον ενάγοντα να αποδεικνύει ότι γνωρίζει το ιδιωτικό κλειδί με έναν από τους δύο τρόπους:

i. ο αιτών αποκρυπτογραφεί μια πρόκληση που κρυπτογραφείται κάτω από το δημόσιο κλειδί του
ii. ο αιτών υπογράφει ψηφιακά μια πρόκληση

Ιδανικά, το δημόσιος βασικό ζευγάρι που χρησιμοποιείται σε τέτοιους μηχανισμούς δεν πρέπει να χρησιμοποιηθεί για άλλους λόγους, δεδομένου ότι η συνδυασμένη χρήση μπορεί να συμβιβάσει την ασφάλεια. Μια δεύτερη προσοχή είναι ότι το δημόσιος βασικό σύστημα χρησιμοποιούμενο δεν πρέπει να είναι ευαίσθητο στις επιθέσεις κρυπτογραφημάτων, όπως ένας αντίπαλος μπορεί να προσπαθήσει να εξαγάγει τις πληροφορίες με έναν ελεγκτή και την επιλογή των στρατηγικών παρά τυχαίων προκλήσεων.

*Με βάση συμπράξεις αποκρυπτογράφησης δημόσιου κλειδιού*
Ταυτοποίηση με βάση την αποκρυπτογράφηση PK και των μαρτύρων. Ας εξετάσουμε το ακόλουθο πρωτόκολλο:
*A <- B : H(V),B,PA(r,B A — B : r)  (1)*
Το B επιλέγει ένα τυχαίο r, υπολογίζει το μάρτυρα x = h (r) (x αποδεικνύει τη γνώση της r χωρίς να τη γνωστοποιήσει και υπολογίζει το e πρόκληση = PA (r, B). Εδώ το PA δείχνει το δημόσιο κλειδί κρυπτογράφησης (π.χ., RSA) του αλγόριθμου της A, και σημαίνει μια λειτουργία one-way hash. Το B στέλνει (1) για την A. Αποκρυπτογραφεί την ανάκτηση r' και B', υπολογίζει x '= h (r'), και κλείνει αν x '= x (που συνεπάγεται r' = r) εάν το B »δεν είναι ίσο με το δικό του αναγνωριστικό. Σε αντίθετη περίπτωση,το A στέλνει r=r' στο B. Το B πετυχαίνει με (μονομερή) έλεγχο γνησιότητας μιας οντότητας του A αφού ελέγξει την προέλευση του r και αν συμφωνεί με αυτή που στάλθηκε νωρίτερα. Η χρήση του μάρτυρα απαγορεύει τις επιθέσεις κειμένου.
Το τροποποιημένο Needham-Schroeder πρωτόκολλο δημόσιου κλειδιού παρέχει βασικές μεταφορές των διακριτών κλειδιών ki, k2 από το A στο B και από το B στο A, αντίστοιχα, καθώς και αμοιβαίο έλεγχο ταυτότητας. Αν το κύριο χαρακτηριστικό εγκατάστασης δεν απαιτείται, τα k1 και k2 είναι δυνατόν να παραλείπονται. Με τον αλγόριθμο PB που δηλώνει το δημόσιο κλειδί κρυπτογράφησης για το B (π.χ., RSA), τα μηνύματα στο τροποποιημένο πρωτόκολλο για την αναγνώριση, γίνονται ως εξής:

*A - B : PB(ri,A)(1) A <_ B : PA(ri ,r2 )  (2)*

*A - B : r2  (3)*

(ii) με βάση τις ψηφιακές υπογραφές
X.509 μηχανισμοί βασισμένοι στις ψηφιακές υπογραφές. Το ITU-T (στο παρελθόν CCITT)

X.509 πρωτόκολλο διπλής και τριπλής κατεύθυνης, ισχυρού ελέγχου ταυτότητας, ορίζει τεχνικές αναγνώρισης που βασίζονται στις ψηφιακές υπογραφές και, αντιστοίχως, timestamps με τυχαίο αριθμό προκλήσεων.

*9798-3 μηχανισμοί:* Τρεις μηχανισμοί προσδιορισμού πρόκλησης-απάντησης βασισμένοι στις υπογραφές , και την συμμετρική βασική κρυπτογράφηση, αλλά και στις τεχνικές του ISO/to IEC9798-3. Το r A και TA, αντίστοιχα, δείχνει έναν τυχαίο αριθμό και ένα timestamp που παράγεται από το A. S.A και δείχνει το μηχανισμό υπογραφών A's εάν αυτός ο μηχανισμός παρέχει την αποκατάσταση μηνυμάτων, μερικοί από τους cleartext τομείς που απαριθμούνται είναι περιττοί και μπορούν να παραλειφθούν. Το certA δείχνει το δημόσιο βασικό πιστοποιητικό που περιέχει το δημόσιο κλειδί υπογραφών A's. (Σε αυτούς τους μηχανισμούς, εάν ο ελεγκτής έχει το αυθεντικό δημόσιο κλειδί του ενάγοντος, τα πιστοποιητικά μπορούν να παραλειφθούν, ειδάλλως, υποτίθεται ότι ο ελεγκτής έχει τις σωστές πληροφορίες για να ελέγξει την ισχύ του δημόσιου κλειδιού που περιλαμβάνεται σε ένα λαμβανόμενο πιστοποιητικό.

i. μονομερής επικύρωση με timestamps:

$$A - B : cert\ A,iA,B,SA(iA,B) \qquad (1)$$

Επάνω στην υποδοχή, το B ελέγχει αν το timestamp είναι αποδεκτό, το λαμβανόμενο προσδιοριστικό B είναι δικό του, και (χρησιμοποιώντας το δημόσιο κλειδί A που εξάγεται από το cert A μετά τον έλεγχο) ελέγχει ότι η υπογραφή πέρα από αυτούς τους δύο τομείς είναι σωστή.

ii. μονομερής επικύρωση με τους τυχαίους αριθμούς: Η εμπιστοσύνη timestamps μπορεί να αντικατασταθεί από έναν τυχαίο αριθμό, με κόστος ενός πρόσθετου μηνύματος:

$$A <- B : rB \qquad (1)$$

$$A — B : certA,rA,B,SA(rA,rB,B) \qquad (2)$$

Το β ελέγχει ότι το cleartext προσδιοριστικό είναι δικό του και χρησιμοποιώντας μια έγκυρη υπογραφή δημόσιου κλειδιού για το A (π.χ., από το certA), ελέγχει ότι υπογραφή A ισχύει πέρα από το cleartext τυχαίο αριθμό rA, ο ίδιος αριθμός rB όπως δίνει η σχέση (1), και αυτό το αναγνωριστικό. Το υπογεγραμμένο rA αποτρέπει ρητά τις επιθέσεις κειμένων.

iii. αμοιβαία αναγνώριση με τυχαίους αριθμούς:

$$A <- B : rB \qquad (1)$$
$$A — B : certA,rA,B,SA(rA,rB,B) \qquad (2)$$
$$A <- B : certB,A,SB(rB,rA,A) \qquad (3)$$

Η επεξεργασία των (1) και (2),μας δίνει τη σχέση (3) όπου εκεί δίνεται η επεξεργασία ενός ενός αρχείου καταγραφής της διαφοράς που μας δίνει η σχέση (2).

## 2.4 Πρωτόκολλα ταυτοποίησης προσαρμοσμένης και μηδενικής γνώσης

Αυτό το τμήμα εξετάζει τα πρωτόκολλα που έχουν σκοπό να επιτύχουν τον προσδιορισμό, τα οποία χρησιμοποιούν τις ασύμμετρες τεχνικές αλλά δεν στηρίζονται στις ψηφιακές υπογραφές ή την κρυπτογράφηση δημόσιων κλειδιών, και που αποφεύγουν τη χρήση chipers φραγμών, των αριθμών ακολουθίας, και τα timestamps. Είναι παρόμοιοι με τα πρωτόκολλα πρόκλησης απάντησης, αλλά είναι βασισμένοι στις ιδέες των διαλογικών συστημάτων απόδειξης και των αποδείξεων μηδενικής γνώσης, υιοθετώντας τους τυχαίους αριθμούς όχι μόνο ως προκλήσεις, αλλά και ως υποχρεώσεις αποτρέποντας την εξαπάτηση.

### 2.4.1 Επισκόπηση της μηδενικής γνώσης εννοιών

Ένα μειονέκτημα των απλών πρωτοκόλλων κωδικού πρόσβασης είναι ότι όταν δίνει ένας ενάγων Α (αποκαλούμενο prover στα πλαίσια των πρωτοκόλλων μηδενικής γνώσης) στον ελεγκτή Β τον κωδικό πρόσβασής, το Β μπορεί έκτοτε να υποδυθεί το πρωτόκολλο Α. Το Α ανταποκρίνεται στην πρόκληση Β για να καταδείξει τη γνώση του μυστικού Α με χρονική παραλλαγή, που παρέχει πληροφορίες όχι άμεσα επαναχρησιμοποιήσιμες από το Β. Έτσι μπορεί να αποκαλυφθούν ορισμένες πληροφορίες για το μυστικό του ενάγοντος, ένας εκατέρωθεν ελεγκτής όμως είναι σε θέση να επιλέξει στρατηγικά τις προκλήσεις για να λάβει τις απαντήσεις που παρέχουν τέτοιες πληροφορίες.

Τα πρωτόκολλα μηδενικής γνώσης (ZK) σχεδιάζονται για να εξετάσουν αυτές τις ανησυχίες, με την βοήθειας ενός μέρους που μπορεί να αποδείξει τη γνώση ενός μυστικού, χωρίς να αποκαλύψει καμία πληροφορία (πέρα από αυτό που ο ελεγκτής ήταν σε θέση να συναγάγει πριν από το πρωτόκολλο που οργανώθηκε) της χρήσης στον ελεγκτή, κατά τη μεταβίβαση αυτής της επίδειξης της γνώσης σε άλλους. Το σημείο είναι ότι μόνο ένα ενιαίο κομμάτι των πληροφοριών χρειάζεται να μεταβιβαστεί - συγκεκριμένα, μόνο ένας πραγματικά ξέρει το μυστικό.

Γενικότερα, ένα πρωτόκολλο μηδενικής γνώσης επιτρέπει μια απόδειξη της αλήθειας ενός ισχυρισμού, χωρίς να μεταβιβάζει καμία πληροφορία (αυτή η έννοια μπορεί να υπολογιστεί υπό μια αυστηρή έννοια) ο ίδιος για τον ισχυρισμό εκτός από την πραγματική αλήθειά του. Από αυτή την άποψη, μια απόδειξη μηδενικής γνώσης είναι παρόμοια με μια απάντηση που λαμβάνεται από έναν (εμπιστευμένο) χρησμό.

*(i) Διαδραστικά συστήματα απόδειξης και μηδενικές γνώσεις πρωτοκόλλων*
Τα πρωτόκολλα ZK είναι περιπτώσεις διαλογικών συστημάτων απόδειξης, όπου ένα μέλος που γνωρίζει(prover) και ένας ελεγκτής ανταλλάσσουν τα πολλαπλάσια μηνύματα (προκλήσεις και απαντήσεις), χαρακτηριστικά εξαρτώμενα από τους τυχαίους αριθμούς (ιδανικά: οι εκβάσεις των δίκαιων εκτινάξεων νομισμάτων) που μπορούν να κρατήσουν μυστικά. Ο στόχος των prover είναι να πειστεί ο ελεγκτής την αλήθεια ενός ισχυρισμού, π.χ., απαιτημένη γνώση ενός μυστικού. Ο ελεγκτής είτε δέχεται είτε απορρίπτει την

απόδειξη. Την παραδοσιακή μαθηματική έννοια μιας απόδειξης, εντούτοις, αλλάζουν σε ένα διαλογικό παιχνίδι όπου οι αποδείξεις είναι πιθανολογικές παρά απόλυτες, μια απόδειξη σε αυτό το πλαίσιο χρειάζεται να είναι σωστή μόνο με την οριακή πιθανότητα, αν και ενδεχομένως είναι αυθαίρετα κοντά στο 1. Για αυτόν τον λόγο, μια διαλογική απόδειξη καλείται μερικές φορές απόδειξη από το πρωτόκολλο.

Οι διαλογικές αποδείξεις που χρησιμοποιούνται για τον προσδιορισμό μπορούν να διατυπωθούν ως αποδείξεις της γνώσης. Το α κατέχει κάποιο μυστικό s, και προσπαθεί να πείσει το Β που έχει τη γνώση s να αποκριθεί σωστά στις ερωτήσεις (που περιλαμβάνουν τις δημόσιες γνωστές εισαγωγές σύμφωνες με τις λειτουργίες) που απαιτούν τη γνώση s για να απαντήσουν. Σημειώστε ότι η απόδειξη του s ως γνωστό διαφέρει από την παρουσίαση αποδείξεων ότι το s υπάρχει - παραδείγματος χάριν, η παρουσίαση αποδείξεων των πρωταρχικών παραγόντων του ν διαφέρει από την παρουσίαση αποδείξεων ότι το ν είναι σύνθετο.

Μια διαλογική απόδειξη λέγεται ότι είναι μια απόδειξη της γνώσης εάν έχει και τις ιδιότητες της πληρότητας και της υγείας. Η πληρότητα μπορεί να αντιμετωπισθεί ως συνήθης απαίτηση ότι ένα πρωτόκολλο λειτουργεί κατάλληλα.

Μια διαλογική απόδειξη (πρωτόκολλο) είναι πλήρης εάν, λαμβάνοντας υπόψη ένα τίμιο prover και έναν τίμιο ελεγκτή, το πρωτόκολλο πετυχαίνει με τη συντριπτική πιθανότητα (δηλ., ο ελεγκτής δέχεται την αξίωση των prover). Ο καθορισμός να συντρίψει εξαρτάται από την εφαρμογή, αλλά γενικά υπονοεί ότι η πιθανότητα της αποτυχίας δεν είναι πρακτικής σημασίας.

Μια διαλογική απόδειξη (πρωτόκολλο) είναι πλήρης εάν, λαμβάνοντας υπόψη ένα τίμιο prover και έναν τίμιο ελεγκτή, το πρωτόκολλο πετυχαίνει με τη συντριπτική πιθανότητα (δηλ., ο ελεγκτής δέχεται την αξίωση των prover). Ο καθορισμός να συντρίψει εξαρτάται από την εφαρμογή, αλλά γενικά υπονοεί ότι η πιθανότητα της αποτυχίας δεν είναι πρακτικής σημασίας.

Μια διαλογική απόδειξη (πρωτόκολλο) είναι υγιής εάν υπάρχει ένας αναμενόμενος πολυωνυμικός χρονικός αλγόριθμος μ με την ακόλουθη ιδιοκτησία: εάν ένα ανέντιμο prover ( Α) μπορεί με την μη αμελητέα πιθανότητα να εκτελέσει επιτυχώς το πρωτόκολλο με το Β , το μ μπορεί να χρησιμοποιηθεί για να εξαγάγει από τον prover το μυστικό (ουσιαστικά αντίτιμο με το μυστικό του Α ) που με τη συντριπτική πιθανότητα επιτρέπει τις επιτυχείς επόμενες εκτελέσεις πρωτοκόλλου.

Μια εναλλάσσομαι εξήγηση του όρου είναι η ακόλουθη: Το μυστικό s
των prover μαζί με τα δημόσια στοιχεία ικανοποιούν κάποιο πολυωνυμικό χρονικό κατηγόρημα, και μια άλλη λύση αυτού του κατηγορήματος μπορεί να εξαχθεί, επιτρέποντας την επιτυχή εκτέλεση των επόμενων περιπτώσεων πρωτοκόλλου. Δεδομένου ότι οποιοδήποτε συμβαλλόμενο μέρος πρέπει να ξέρει το αντίτιμο της μυστικής γνώσης Α, οι εγγυήσεις υγείας ότι το πρωτόκολλο πράγματι χορηγεί μια απόδειξη της γνώσης - γνώση ισοδύναμη με αυτήν που ρωτιέται απαιτούνται για να πετύχει. Η υγεία αποτρέπει έτσι ένα ανέντιμο prover να πείσει έναν τίμιο ελεγκτή (αλλά όχι από την εγγύηση ότι η απόκτηση του μυστικού από τον prover είναι δύσκολη). Μια τυποποιημένη μέθοδος για να καθιερώσει την υγεία ενός ιδιαίτερου πρωτοκόλλου είναι να υποτεθεί η ύπαρξη ενός ανέντιμου prover που γνωρίζει το πρωτόκολλο, και να επιδειχθεί πώς αυτό επιτρέπει να υπολογίσει το πραγματικό μυστικό του prover .

Ένα πρωτόκολλο είναι μια απόδειξη ότι γνωρίζει την μηδενική γνώση εάν είναι προσομοιωμένο υπό την ακόλουθη έννοια: υπάρχει ένας αναμενόμενος πολυωνυμικός χρονικός αλγόριθμος (προσομοιωτής) που μπορεί να παραχθεί, επάνω στην εισαγωγή του ισχυρισμού αλλά χωρίς αλληλεπίδραση με τον πραγματικό prover, αντίγραφα όμοια με τα αποτέλεσμα της αλληλεπίδρασης με το πραγματικό prover. Η μηδενική γνώση υπονοεί ότι ένα prover που εκτελεί το πρωτόκολλο (ακόμα και που αλληλεπιδρά με έναν κακόβουλο ελεγκτή) δεν δημοσιεύει οποιεσδήποτε πληροφορίες εκτός από τις υπολογίσιμες στον πολυωνυμικό χρόνο δημόσιες πληροφορίες. Κατά συνέπεια, η συμμετοχή δεν αυξάνει τις πιθανότητες της επόμενης προσωποποίησης.

Ένα πρωτόκολλο είναι υπολογιστικά μηδενικής γνώση εάν ένας παρατηρητής που περιορίζεται στις πιθανολογικές πολυωνυμικές χρονικές δοκιμές δεν μπορεί να διακρίνει το πραγματικό από τα μιμούμενα αντίγραφα. Για την τέλεια μηδενική γνώση, οι διανομές πιθανότητας των αντιγράφων πρέπει να είναι ίδιες. Από τη σύμβαση, όταν είναι κατάλληλη, η μηδενική γνώση σημαίνει την υπολογιστική μηδενική γνώση.

Στην περίπτωση της υπολογιστικής μηδενικής γνώσης, τα πραγματικά και μιμούμενα αντίγραφα θεωρούνται πολυωνιμικά όμοια (όμοιοι χρησιμοποιώντας πολυωνυμικό-χρονικό αλγόριθμο). Οποιεσδήποτε πληροφορίες που εξάγονται από έναν ελεγκτή μέσω της αλληλεπίδρασης με ένα prover δεν παρέχουν κανένα πλεονέκτημα στον ελεγκτή μέσα στον πολυωνυμικό χρόνο.

Η κατοχύρωση της μηδενικής γνώσης δεν εγγυάται ότι ένα πρωτόκολλο είναι ασφαλές. Ομοίως, η ιδιοκτησία υγείας δεν εγγυάται ότι ένα πρωτόκολλο είναι ασφαλές. Καμία ιδιοκτησία δεν έχει πολλή αξία εκτός αν το ελλοχεύον πρόβλημα που αντιμετωπίζεται από έναν αντίπαλο είναι υπολογιστικά σκληρό.

*(ii) Διαφορές της μηδενικής γνώσης σε σχέση με άλλα ασύμμετρες*
Οι ακόλουθες παρατηρήσεις μπορούν να γίνουν σχετικά με τις τεχνικές μηδενικής γνώσης (ZK), συγκρινόμενες με άλλες δημόσιες βασικές τεχνικές (BT).
1. *καμία υποβάθμιση με τη χρήση*: τα πρωτόκολλα που αποδεικνύονται ότι έχουν την ZK δεν υφίστανται την υποβάθμιση της ασφάλειας με την επαναλαμβανόμενη χρήση, και αντιστέκονται στις επιθέσεις κειμένων. Αυτό είναι ίσως το πιο ελκυστικό πρακτικό χαρακτηριστικό γνώρισμα των τεχνικών ZK. Μια τεχνική ZK που δεν είναι αποδεδειγμένα ασφαλής μπορεί να αντιμετωπισθεί καλύτερα ή να απορριφθεί από μια τεχνική του BT που είναι ευαπόδεικτα ασφαλής .
**2.** *κρυπτογράφηση που αποφεύγεται*: πολλές τεχνικές ZK αποφεύγουν τη χρήση των ρητών αλγορίθμων κρυπτογράφησης. Αυτό μπορεί να προσφέρει τα πολιτικά πλεονεκτήματα (π.χ., όσον αφορά τους ελέγχους εξαγωγής).
**3.** *αποδοτικότητα:* ενώ μερικές ZK βασισμένες τεχνικές είναι εξαιρετικά αποδοτικές, τα πρωτόκολλα που έχουν τυπικά την ιδιοκτησία μηδενικής γνώσης έχουν χαρακτηριστικά τις υψηλότερες επικοινωνίες ή/και τα υπολογιστικά γενικά έξοδα από τα πρωτόκολλα των BT . Η υπολογιστική αποδοτικότητα των πρακτικότερων ZK βασισμένων σχεδίων προκύπτει από τη φύση τους ως διαλογικές αποδείξεις, παρά από τη μηδενική γνώσης τους.
**4.** *μη αποδεδειγμένες υποθέσεις*: πολλά πρωτόκολλα ZK έχουν τις ίδιες μη αποδεδειγμένες υποθέσεις με τις τεχνικές των BT (π.χ., η δυσκολία εντοπισμού του παράγοντα).

*(iii) Παράδειγμα απόδειξης μηδενικής γνώσης: Fiat-Shamir πρωτόκολλο ταυτοποίησης*
Η γενική ιδέα μιας απόδειξης μηδενικής γνώσης (ZK) εμφανίζεται στη βασική έκδοση του πρωτοκόλλου Fiat-Shamir. Η βασική έκδοση παρουσιάζεται εδώ για ιστορικούς και επεξηγηματικούς λόγους.
Ο στόχος είναι το A να προσδιοριστεί από τη γνώση παρουσιάσεων αποδείξεων του μυστικού s (που συνδέεται με το A μέσω των αυθεντικών δημόσιων στοιχείων) σε οποιοδήποτε ελεγκτή B, χωρίς να αποκαλυφθεί οποιαδήποτε πληροφορία για το s πριν από την εκτέλεση του πρωτοκόλλου.

***Πρωτόκολλο ταυτοποίησης Fiat-Shamir (βασική έκδοση)***
Το A αποδεικνύει τη γνώση s στο B στις εκτελέσεις t ενός πρωτοκόλλου 3 περασμάτων.

***1. One-time οργάνωση.***
(α) ένα εμπιστευμένο κέντρο t επιλέγει και δημοσιεύει έναν συντελεστή v = pq
(β) κάθε ενάγων A επιλέγει το μυστικό s στο v, 1 < s < v — 1, υπολογίζει β = s 2 mod v, και καταχωρεί το B με T ως δημόσιο κλειδί του.
***2. Μηνύματα πρωτοκόλλου***. Κάθε ένας από τους κύκλους t έχει τρία μηνύματα με τη μορφή

*A — B : x = r2 mod n (1) A <- B : e G(0, 1} (2) A — B : y = r * se mod n (3)*

***3. Ενέργειες πρωτοκόλλου***. Το B δέχεται την απόδειξη εάν όλοι οι κύκλοι t πετυχαίνουν
(α) το A επιλέγει ένα τυχαίο ρ (υποχρέωσης ), ένα ) r, 1 < r < n — 1, και στέλνει το x = r2 mod n στο B.
(β) το B επιλέγει τυχαία ένα bit (πρόκληση) e = 0 ή e = 1, και στέλνει το e στο A.
(γ) υπολογίζει και στέλνει στον B το y, οπότε y = r (αν e = 0) ή y = n mod rs (αν e = 1).
(δ) B απορρίπτει την απόδειξη, εφόσον y = 0, και δέχεται διαφορετικά μετά από έλεγχο y2 Ξ x ve(n mod). (Ανάλογα με το e, y2 = x ή y2 xv = n mod, αφού v = s2 mod n. Να σημειωθεί ότι ο έλεγχος για y = 0 αποκλείει την περίπτωση r = 0.)

Το πρωτόκολλο μπορεί να εξηγηθεί και να δικαιολογηθεί ανεπίσημα ως εξής. Η πρόκληση (ή διαγωνισμός) e απαιτεί ότι το A είναι σε θέση δύο ερωτήσεων, μια από τις οποίες καταδεικνύει τη γνώση του μυστικού s, και άλλης μια εύκολης ερώτησης (για τα τίμια provers) για να αποτρέψει την εξαπάτηση. Ένας αντίπαλος που το A θα προσπαθήσει να εξαπατήσει με την επιλογή οποιουδήποτε r και τη ρύθμιση X = r 2 / B, απαντώντας έπειτα στην πρόκληση e = 1 με ένα "σωστό" Y = r αλλά θα ήταν ανίκανος να απαντήσει στο e = 0 που απαιτεί μια τετραγωνική ρίζα mod n*X. Ένας prover A που ξέρει το s μπορεί να απαντήσει και στις δύο ερωτήσεις, ειδάλλως μπορεί στην καλύτερη περίπτωση να απαντήσει σε μια από τις δύο ερωτήσεις, και έχει έτσι πιθανότητα μόνο 1/2 της διαφυγής της ανίχνευσης. Για να μειώσει την πιθανότητα να εξαπατήσει αυθαίρετα σε μια κατά αποδεκτό τρόπο μικρή αξία 2 - τ (π.χ., τ = 20 ή το τ = 40), το πρωτόκολλο επαναλαμβάνεται σε χρόνοι t, με την αποδοχή B. Τερματίζει επιτυχώς , βρίσκοντας την ταυτότητα, μόνο εάν όλες οι απαντήσεις του s δείχνουν τη σωστή απάντηση.

*(iv) Γενική διάρθρωση μηδενικής γνώσης πρωτοκόλλων*
Το πρωτόκολλο αυτό επεξηγεί τη γενική δομή μιας μεγάλης κατηγορίας πρωτοκόλλων μηδενικής γνώσης σε 3 βήματα:

***A — B : μάρτυρας A «— B : πρόκληση A — B : απόκριση***

Το prover που υποστηρίζει ότι είναι A επιλέγει ένα τυχαίο στοιχείο από ένα

προκαθορισμένο σύνολο ως μυστική υποχρέωσή του (η παροχή της κρυμμένης τυχαιοποίησης υπολογίζει ένα μάρτυρα. Αυτό παρέχει το αρχικό τυχαίο για την παραλλαγή από άλλα τρεξίματα πρωτοκόλλου, και καθορίζει ουσιαστικά ένα σύνολο ερωτήσεων που το prover υποστηρίζει για να είναι σε θέση να απαντήσει, με αυτόν τον τρόπο περιορίζοντας την προσεχή απάντησή της. Από το σχέδιο πρωτοκόλλου, μόνο το νόμιμο συμβαλλόμενο μέρος Α, με τη γνώση μυστικού Α είναι σε θέση να απαντήσει σε όλες τις ερωτήσεις, και η απάντηση σε οποιαδήποτε από αυτές δεν παρέχει καμία πληροφορία για ένα μακροπρόθεσμο μυστικό του s. Η επόμενη πρόκληση Β επιλέγει μια από αυτές τις ερωτήσεις. Το Α δίνει την απάντησή του, την οποία το Β ελέγχει για την ακρίβεια. Το πρωτόκολλο επαναλαμβάνεται, εφόσον κρίνεται απαραίτητο, για το βέλτιστο περιορισμό τη πιθανότητας της επιτυχούς εξαπάτησης.

Τα διαλογικά πρωτόκολλα μηδενικής γνώσης συνδυάζουν έτσι τις ιδέες της περικοπής και επιλογής (αυτή η ορολογία προκύπτει από την τυποποιημένη μέθοδο με την οποία δύο παιδιά μοιράζονται ένα κομμάτι του κέικ: κάποιο κόβει, άλλο επιλέγει) και τα πρωτόκολλα πρόκλησης-απάντησης. Το Α ανταποκρίνεται το πολύ σε μια πρόκληση (ερώτηση) για έναν δεδομένο μάρτυρα, και δεν πρέπει να επαναχρησιμοποιήσει οποιοδήποτε μάρτυρα σε άλλα πρωτόκολλα, η ασφάλεια (ενδεχομένως του μακροπρόθεσμου υλικού διαμόρφωσης) μπορεί να συμβιβαστεί εάν κάποιος όρος παραβιάζεται.

## 2.4.2 Πρωτόκολλο ταυτοποίησης Feige-Fiat-Shamir

Η βασική έκδοση του πρωτοκόλλου Fiat- Shamir παρουσιάζεται παραπάνω. Αυτό μπορεί να γενικευτεί, ως (fss) πρωτόκολλο προσδιορισμού Feige-Fiat- Shamir ως μια δευτερεύουσα παραλλαγή μιας τέτοιας γενίκευσης. Το πρωτόκολλο FFS περιλαμβάνει μια οντότητα προσδιορισμένη από τη γνώση παρουσιάσεων αποδείξεων ενός μυστικού χρησιμοποιώντας μια απόδειξη μηδενικής γνώσης δεν αποκαλύπτει καμία πληροφορία σχετικά με τη μυστική αξία προσδιορισμού (s) του Α. Αυτό απαιτεί τον περιορισμένο υπολογισμό και ταιριάζει για τις εφαρμογές με τους χαμηλής ισχύος επεξεργαστές (π.χ., οκτάμπιτοι μικροεπεξεργαστές chipcard).

***Πρωτόκολλο ταυτοποίησης Feige-Fiat-Shamir***

Το Α αποδεικνύει την ταυτότητά του στο Β στο πρωτόκολλο 3 περασμάτων εκτελέσεων t.

<u>1. *παράμετροι επιλογής συστήματος.*</u> Ένα εμπιστευμένο κέντρο t δημοσιεύει ένα κοινό συντελεστή n = pq για όλους τους χρήστες, μετά επιλέγει ένα από τα δύο μυστικά το p και το q αν είναι σύμφωνα με 3mod4, έτσι ώστε το n να είναι υπολογιστικά απραγματοποίητο στον παράγοντα. (Συνεπώς, το n είναι ένας ακέραιος αριθμός Blum, και -1 είναι τετραγωνικό modn με το σύμβολο Jacobi + 1.) Οι ακέραιοι αριθμοί K και t ορίζονται ως παράμετροι ασφάλειας.

<u>2. *επιλογή μυστικού προς το φορέα*</u>. Κάθε οντότητα Α ακολουθεί την παρακάτω διαδικασία:

- επίλεκτοι τυχαίοι ακέραιοι αριθμοί K s ι,s 2...,s K στη σειρά 1 < s " < v —1, και το K τυχαίο (για τεχνικούς λόγους, gcd (s j,n) = 1 απαιτείται, αλλά
είναι σχεδόν σίγουρα εγγυημένο δεδομένου ότι η αποτυχία της επιτρέπει την παραγοντοποίηση του v.)

- υπολογισμός B = (—( s 2)-1mod* v για 1 < ι < K. (αυτό επιτρέπει στο Β να

κυμανθεί σε όλους τους ακέραιους αριθμούς στο ν με το σύμβολο Jacobi + 1, ένας τεχνικός όρος που απαιτείται για να αποδείξει ότι καμία μυστική πληροφορία δεν είναι ακριβώς μια υπογεγραμμένη επιλογή για το Β με τετραγωνική ρίζα.)

- το Α προσδιορίζεται με μη-κρυπτογραφικά μέσα (π.χ., ταυτότητα φωτογραφιών) στο t, το οποίο καταχωρεί έκτοτε το δημόσιο κλειδί Α (β 1,n K N), ενώ μόνο το Α ξέρει το ιδιωτικό κλειδί του (s 1... ,s K) και το n. (για να εγγυηθεί την οριακή πιθανότητα της επίθεσης που διευκρινίζεται ανά σημείωση10,28. Το t μπορεί να επιβεβαιώσει ότι κάθε Β πράγματι έχει το σύμβολο Jacobi + 1 σχετικά με το ν.) Αυτό ολοκληρώνει τη one-time φάση οργάνωσης.

*3. μηνύματα πρωτοκόλλου*. Κάθε ένας από τους κύκλους t έχει τρία μηνύματα με τη μορφή ως εξής:

*A — B : x (= ±r2 mod n)(1) A <- B :(e1,...,efc),ei G{0, 1} (2) A — B : y (= r * Πe, =1 sj mod n)(3)*

Το πρωτόκολλο Feige-Fiat-Shamir είναι αποδεδειγμένα ασφαλές ενάντια στην επιλεγμένη επίθεση μηνυμάτων υπό την ακόλουθη έννοια: υπό τον όρο ότι η πρακτόρευση n είναι δύσκολη, η καλύτερη επίθεση έχει μια πιθανότητα 2 - kt της επιτυχούς προσωποποίησης. Η ασφάλεια στηρίζεται στη δυσκολία εξαγωγής της τετραγωνικής ρίζας μεγάλων σύνθετων αριθμών άγνωστης παραγοντοποίησης. Αυτό είναι ισοδύναμο με την πρακτόρευση n. Το πρωτόκολλο αυτό είναι, σχετικά με έναν εμπιστευμένο κεντρικό υπολογιστή, μια (υγιής) απόδειξη μηδενικής γνώσης της γνώσης που χορηγείται k = O(loglog n) και το t = 9(log n) σχετικά με την πρακτική σημασία τέτοιων περιορισμών. Μια απλοϊκή άποψη για το σταθερό k είναι ότι ο ελεγκτής, ευνοεί το μεγαλύτερο t (περισσότερες επαναλήψεις) για μια μειωμένη πιθανότητα της απάτης ενώ το prover, ενδιαφερόμενο για τη μηδενική γνώση, ευνοεί το μικρότερο t. Η επιλογή της παραμέτρου k και t έτσι ώστε αν έχουμε kt = 20 επιτρέπουν μια πιθανότητα ενός εκατομμυρίου της προσωποποίησης, η οποία αρκεί στην περίπτωση που μια προσπάθεια προσδιορισμού απαιτεί μια προσωπική εμφάνιση από έναν δυνάμει μιμητή. Η μνήμη, και επικοινωνία canbe που ανταλλάσσεται υπολογίζεται ως 1 < k < 18 ανάλογα με την περίπτωση. Οι συγκεκριμένες επιλογές παραμέτρου είναι, για την ασφάλεια 2-20: k= 5,t= 4 για 2-30: k = 6, t= 5. Τόσο ο υπολογισμός όσο και η επικοινωνία ίσως μειωθεί κατά την ανταλλαγή των παραμέτρων ασφαλείας για να παραγάγει μια επανάληψη (t = 1), κρατώντας το kt ως προϊόν με σταθερό και αυξανόμενο k και με παράλληλη μείωση των t. Ωστόσο, σε αυτή την περίπτωση το πρωτόκολλο δεν είναι πλέον μια απόδειξη μηδενική γνώσης.

Ως εναλλακτική λύση στο βήμα 1 του πρωτοκόλλου Feige-Fiat-Shamir, κάθε χρήστης μπορεί να πάρει το δικό του n. Το t εξακολουθεί να είναι απαραίτητο για να συνδέσει κάθε χρήστη με το συντελεστή του. Η πολυπλοκότητα επικοινωνίας μπορεί να μειωθεί εάν το Α στέλνει στο Β (π.χ.,128 bit) μια hash αξία h (X) αντί του X στο μήνυμα (1), με επαλήθευση του Β τροποποιημένη αναλόγως.

Μετατρέποντας τον προσδιορισμό στο σχέδιο υπογραφών: Η ακόλουθη γενική τεχνική μπορεί να χρησιμοποιηθεί για να μετατρέψει ένα σχέδιο προσδιορισμού που περιλαμβάνει μια ακολουθία μάρτυρας-πρόκλησης-απάντησης σε ένα σχέδιο υπογραφών: αντικαταστήστε την τυχαία πρόκληση e του ελεγκτή από μονόδρομο hash e = h (x||m), της αλληλουχίας του μάρτυρα x και του μηνύματος m που υπογράφεται (το h διαδραματίζει ουσιαστικά το ρόλο του ελεγκτή). Δεδομένου ότι αυτό μετατρέπει ένα διαλογικό σχέδιο προσδιορισμού σε ένα μη διαλογικό σχέδιο υπογραφών, της πρόκλησης e πρέπει χαρακτηριστικά να αυξηθεί για να αποκλείσει τις σε μη απευθείας σύνδεση

επιθέσεις στη hash λειτουργία.

### 2.4.3 Πρωτόκολλο ταυτοποίησης GQ(Guillou-Quisquater)

Το Guillou-Quisquater (GQ) σύστημα αναγνώρισης είναι μια επέκταση του πρωτοκόλλου Fiat-Shamir. Επιτρέπει τη μείωση τόσο στον αριθμό των μηνυμάτων που ανταλλάσσονται και τις απαιτήσεις μνήμης για τα μυστικά των χρηστών και, όπως και η Fiat-Shamir, είναι κατάλληλο για εφαρμογές στις οποίες ο αιτών έχει περιορισμένη ισχύ και μνήμη. Περιλαμβάνει τρία μηνύματα μεταξύ του διεκδικούντος Α του οποίου η ταυτότητα επιβεβαιώνεται, καθώς και ένα επιθεωρητή Β. Το Α αποδεικνύει την ταυτότητά του (μέσω της γνώσης της Α.Ε.) στο Β, σε ένα πρωτόκολλο 3 περασμάτων.

1. Επιλογή των παραμέτρων του συστήματος.
(α) Μια αρχή Τ, είναι αποδεκτή από όλα τα μέρη όσον αφορά τις δεσμευτικές ταυτότητες για τα δημόσια κλειδιά, επιλέγει τυχαία ένα μυστικό RSA-όπως p για τους primes και q για την παραγωγή ενός συντελεστή n = pq. (Όσο για το RSA, πρέπει να είναι υπολογιστικά ανέφικτο να παραγοντοποιήσει το n.)
(β) Το Τ ορίζει ένα δημόσιο εκθέτη v> 3 με gcd (v, ϕ) = 1, όπου ϕ = (p-1) (q-1), και υπολογίζει τον εκθέτη του ϕ = v-1 mod.
(γ) οι παράμετροι του συστήματος (v, n) που διατίθενται (με εγγύηση αυθεντικότητας) για όλους τους χρήστες.

2. Επιλογή ανά χρήστη παραμέτρους.
(α) Κάθε οντότητα Α δίνει μια μοναδική ταυτότητα IA, από την οποία έχουμε JA = f (IA), πληρώντας τη σχέση 1 <JA <n, και χρησιμοποιώντας μια γνωστή συνάρτηση f. Υποθέτοντας ότι το n είναι δύσκολο να συνεπάγεται με gcd (JA ^) = 1.)
(β) Το Τ δίνει στον Α το μυστικό (στοιχεία διαπίστευσης) SA = (JA) mod-s n.

3. Πρωτόκολλο μηνύματα. Κάθε ένα από τους t γύρους έχει τρία μηνύματα ως εξής (συχνά t =1).

A — B : IA ,x = rv mod n (1) A — B : e (όπου 1 < e < v)(2) A — B : y = r * sAE mod n (3)

4. Πρωτόκολλο δράσεων. Το Α αποδεικνύει την ταυτότητά της σε Β από t εκτελέσεις από τα ακόλουθα Β αποδέχεται την ταυτότητα μόνο εάν όλες οι t εκτελέσεις είναι επιτυχημένες.
Ασφάλεια του πρωτοκόλλου ταυτοποίησης GQ
*(i) πιθανότητα πλαστογραφίας*. Στο πρωτόκολλο GQ, καθορίζεται το επίπεδο ασφάλειας, ορισμένες αξίες, όπως η v = 216+1 μπορεί να προσφέρει ένα υπολογιστικό πλεονεκτήματα. Ένας απατημένος αιτών μπορεί να νικήσει το πρωτόκολλο με την ευκαιρία να μαντέψει σωστά το e εκ των προτέρων (και στη συνέχεια σχηματίζει x = Jae YV ). Η συνιστώμενη διάρκεια bit του v εξαρτάται συνεπώς από το περιβάλλον στο οποίο οι επιθέσεις θα μπορούσαν να τοποθετηθούν.
*(ii) ανάληψη απαιτούμενης ασφάλειας*. Εξάγοντας τις vth ρίζες ενός σύνθετου ακέραιου n(δηλαδή, την επίλυση του προβλήματος RSA), κρίνεται αναγκαίο να νικήσουμε το πρωτόκολλο αυτό το οποίο δεν είναι δυσκολότερο από , τον παράγοντα v παρόλο που φαίνεται δυσεπίλυτο υπολογιστικά αγνοώντας τους παράγοντες του n.
*(iii) αρτιότητα*. Στην πράξη, GQ με t = 1και ενός k-bit prime v είναι συχνά προτείνονται. Για γενικευμένους παραμέτρους (n, v, t), η πιθανότητα της πλαστογραφίας είναι κατά v-t.If σταθερή, τότε τεχνικά για την αρτιότητα, τα t πρέπει να αυξηθούν ασυμπτωτικά ταχύτερα από το log logn. (Για αρτιότητα, vt = O (e-kt) πρέπει να είναι μικρότερες από αντιστρόφου πολυωνύμου σε n log. Μόνο το πολυώνυμο παρέχει εγγύηση για μια σταθερά c, vt = O((log n)c).

*(iv) ιδιοκτησία μηδενικής γνώσης*. Σε αντίθεση με την απαίτηση ευρωστία (ορθότητα), για να είναι μηδενικής γνώσης το GQ προφανώς απαιτεί tv = O ((log n), c) για σταθερά c, επιβάλλοντας ένα άνω όριο στο t, για την κατά συνεχή, t δεν πρέπει να είναι μεγαλύτερο από το πολυώνυμο log n.

Οι ασυμπτωτικές προϋποθέσεις για σταθερότητα έχουν μικρή σημασία στην πράξη, για παράδειγμα, επειδή τα μεγάλα-Ο είναι ένας συμβολισμός που δεν μπορεί να εφαρμοστεί όταν οι σταθερές τιμές θα αποδοθούν στις παραμέτρους. Πράγματι,η μηδενική γνώση είναι μια θεωρητική έννοια, ενώ η πολυπλοκότητα της θεωρίας προσφέρει καθοδήγηση για την επιλογή των πρακτικών παραμέτρων ασφάλειας και η σημασία τους μειώνεται όταν οι παράμετροι είναι σταθερές.

Το πρωτόκολλο είναι μια ταυτότητα με βάση την έκδοση όπου το δημόσιο κλειδί του A ανακατασκευάστηκε από το αναγνωριστικό IA στέλνοντας το μήνυμα στο (1). Εναλλακτικά, ένα πιστοποιημένο δημόσιο κλειδί μπορεί να χρησιμοποιηθεί, αφού διανεμηθεί σε ένα πιστοποιητικό. Ένα παράδειγμα της λειτουργίας f είναι η χαρτογράφηση της προεπεξεργασίας ISO / IEC 9796. Ένα δεύτερο παράδειγμα είναι μια μεμονωμένη τιμή συνάρτηση f, για μια κατάλληλη τιμή i.

Ο σκοπός είναι να εμποδίζει έναν αντίπαλο υπολογιστών με ψευδή στοιχεία διαπίστευσης που αντιστοιχεί σε μια ταυτότητα, κάτι που ισοδυναμεί με σφυρηλάτηση ενός πιστοποιητικού με βάση τα συστήματα.

## 2.4.4 Πρωτόκολλο ταυτοποίησης Schnorr

Το πρωτόκολλο προσδιορισμού Schnorr είναι μια εναλλακτική λύση στα πρωτόκολλα Fiat-Shamir και του GQ. Η ασφάλειά του είναι βασισμένη στη δυσκολία εντοπισμού του ιδιαίτερου λογαρίθμου. Το σχέδιο επιτρέπει τον προϋπολογισμό, μειώνει το ο σε πραγματικό χρόνο υπολογισμού για τον ενάγων με ένα πολλαπλασιασμό κι ένα πρωταρχικό q. Είναι έτσι ιδιαίτερα κατάλληλο για τους ενάγοντες της περιορισμένης υπολογιστικής δυνατότητας. Ένας περαιτέρω σημαντικός υπολογισμός της αποδοτικότητας προκύπτει από το χρήση. Μια υποομάδα διατάζει το q σαν πολλαπλασιαστική ομάδα ενός αριθμού p, όπου q | (p—1). Επίσης μειώνεται ο απαραίτητος αριθμός που διαβιβάζει το κομμάτι. Τέλος, το πρωτόκολλο σχεδιάστηκε για να απαιτήσει μόνο τρία περάσματα, και ένα χαμηλό εύρος ζώνης επικοινωνιών (π.χ., έναντι Fiat- Shamir).
Η βασική ιδέα είναι ότι το A αποδεικνύει τη γνώση ενός μυστικού (χωρίς αποκάλυψη του) κατά τρόπο time-variant (ανάλογα με μια πρόκληση e), που προσδιορίζει το A μέσω της ένωσης του με το δημόσιο κλειδί B μέσω του επικυρωμένου πιστοποιητικού A.
Το A αποδεικνύει την ταυτότητά του στο B σε ένα πρωτόκολλο 3 περασμάτων.

1. παράμετροι επιλογής συστήματος.
(a) ένας κατάλληλος πρωταρχικός p επιλέγεται έτσι ώστε p —1 ο οποίος είναι διαιρετός από ένα πρωταρχικό q.
(b) ένα στοιχείο B επιλέγεται, 1 < β < p —1, έχοντας το πολλαπλασιαστικό παράδειγμα διαταγής q
(c) κάθε συμβαλλόμενο μέρος λαμβάνει ένα αυθεντικό αντίγραφο των παραμέτρων συστημάτων (p, q, B) και το ρόλο επαλήθευσης (δημόσιο κλειδί) του εμπιστευμένου συμβαλλόμενου μέρους t, επιτρέποντας την επαλήθευση. Υπογραφές t e;inais t (m) στα μηνύματα m. (S t περιλαμβάνουν μια κατάλληλη γνωστή hash λειτουργία πριν από την υπογραφή, και μπορεί να είναι οποιοσδήποτε μηχανισμός υπογραφών.)
(d) μια παράμετρος t (π.χ., t > 40), 2 t < q, είναι επιλεγμένη (καθορίζοντας ένα επίπεδο ασφάλειας 2 t).

2. Επιλογή παραμέτρων ανά χρήστη.
(a) σε κάθε ενάγοντα A δίνεται μια μοναδική ταυτότητα.
(b) το A επιλέγει ένα ιδιωτικό βασικό A, 0 < A < q —1, και υπολογίζει v = β-α mod p.
(c) το A προσδιορίζεται με τα συμβατικά μέσα στο t, μεταφέρει το v στο T με την ακεραιότητα, και λαμβάνει ένα πιστοποιητικό certA = (IA,v, ST(IA,v) από το τ που δεσμεύει tolA με το v.

3. μηνύματα πρωτοκόλλου. Το πρωτόκολλο περιλαμβάνει τρία μηνύματα.
A — B : certA,X = β7* modp (1) A — B : e (where 1 < e < 2t <q)(2) A — B : y = ae + r mod q (3)

4. ενέργειες πρωτοκόλλου. Το A προσδιορίζεται στον ελεγκτή B ως εξής.
(a) το A επιλέγει ένα τυχαίο r, 1 < r < q —1, υπολογίζει (ο μάρτυρας) το x = β7 mod p, και το στέλνει στο B.
(b) το B επικυρώνει το δημόσιο κλειδί του A με την επαλήθευση της υπογραφής t στο cert A, έπειτα στέλνει στο A ένα (ποτέ προηγουμένως χρησιμοποιημένο) τυχαίο e (η πρόκληση), 1 < e < 2 t.
(c) οι έλεγχοι 1 < e < 2 t στέλνουν στο β (η απάντηση) y = ae + r mod q
(a) το B υπολογίζει z = ve mod p, και δέχεται ότι ταυτότητα του A είναι z = x.

*Ασφάλεια του πρωτοκόλλου ταυτοποίησης Schnorr*

*(i) πιθανότητα της πλαστογραφίας*. Στο πρωτόκολλο Schnorr, το t πρέπει να είναι αρκετά μεγάλο για να κάνει την πιθανότητα 2 - τ σωστά να υποθέσει την πρόκληση e ως αμελητέα. Τα t= 40, q > 22t = 2 80 προτάθηκαν αρχικά στην περίπτωση που μια απάντηση απαιτείται εντός δευτερολέπτων και είναι μεγαλύτερο το q μπορεί να είναι απαραίτητο για να αποκλείσει τις χρόνου/μνήμης ανταλλαγές, και το q > 2160 προτείνεται για να αποκλείσει άλλες σε μη απευθείας σύνδεση ιδιαίτερες επιθέσεις. Σωστά το e επιτρέπει σε έναν αντίπαλο να υποδυθεί το A με την επιλογή οποιουδήποτε y στέλνοντας x = ve modp ε στο B στην (1), στέλνοντας έπειτα το y στην (3).

*(ii) αρτιότητα*. Μπορεί να αποδειχθεί ότι το πρωτόκολλο είναι μια απόδειξη της γνώσης, δηλαδή, κάθε ενδιαφερόμενο μέρος που συμπληρώνει το πρωτόκολλο ως Α πρέπει να είναι σε θέση να υπολογίζει το Α. Ανεπίσημα, το πρωτόκολλο αποκαλύπτει μη χρήσιμες πληροφορίες ηγούμενο ενός x τυχαίου αριθμό, και y είναι η ενόχλησή από τον τυχαίο αριθμό r. (Ωστόσο, αυτό δεν αποδεικνύει ότι η αντιδικία της ανακάλυψης ενός είναι δύσκολη.)

*(iii) ιδιοκτησίας μηδενικής γνώσης*. Το πρωτόκολλο δεν έχει μηδενική γνώση για τα μεγάλα e, διότι μέσω της αλληλεπίδρασης, το Β αποκτά τη λύση (x, y, e) με την εξίσωση x = ve mod p, όπου το Β να μην είναι σε θέση να την υπολογίσει (π.χ., εάν ε αυτές επιλέξει να εξαρτάται από την x).

***Σημείωση:*** Ο αριθμός των bits που διαβιβάζονται στο πρωτόκολλο μπορεί να μειωθεί με την αντικατάσταση x στο μήνυμα (1) από t προκαθορισμένο bits του x (π.χ., τα λιγότερο σημαντικά bits t), και έχοντας το Β το συγκρίνουμε με αυτό που αντιστοιχούν τα κομμάτια του z.

## 2.4.5 Σύγκριση: Fiat-Shamir, GQ, και Schnorr

Τα πρωτόκολλα Feige-Fiat-Shamir, Guillou-Quisquater, και Schnorr παρέχουν τις λύσεις στο πρόβλημα προσδιορισμού. Κάθε ένα έχει τα σχετικά πλεονεκτήματα και τα μειονεκτήματα όσον αφορά τα διάφορα κριτήρια απόδοσης για τις συγκεκριμένες εφαρμογές. Για να συγκρίνει τα πρωτόκολλα, ένα χαρακτηριστικό σύνολο επιλεγμένων παραμέτρων πρέπει να επιλεχτεί για κάθε επίπεδο παρέχοντας συγκρίσεις ασφάλειας. Τα πρωτόκολλα μπορούν έπειτα να συγκριθούν βάση των ακόλουθων κριτηρίων:

1. επικοινωνίες: αριθμός μηνυμάτων που ανταλλάσσονται, και τα συνολικά κομμάτια που μεταφέρονται

2. υπολογισμοί: αριθμός των πολλαπλασιασμών για κάθε ένα από τους prover και τον ελεγκτή (σημειώνοντας τους σε απευθείας σύνδεση και σε μη απευθείας σύνδεση υπολογισμούς)

3. μνήμη: απαιτήσεις αποθήκευσης για τα μυστικά κλειδιά (και το μέγεθος υπογραφών, στην περίπτωση των σχεδίων υπογραφών)

4. εγγυήσεις ασφάλειας: οι συγκρίσεις πρέπει να εξετάσουν την ασφάλεια ενάντια στην παραποίηση από την εικασία (υγεία), την πιθανή κοινοποίηση των μυστικών πληροφοριών (ιδιοκτησία μηδενικής γνώσης), και τη θέση σχετικά με την αποδεδειγμένη ασφάλεια και

5. εμπιστοσύνη που απαιτείται στον τρίτο: οι παραλλαγές των πρωτοκόλλων μπορούν να απαιτήσουν τις διαφορετικές υποθέσεις εμπιστοσύνης στο εμπιστευμένο ενδιαφερόμενο μέρος.

Ο αριθμός κριτηρίων και πιθανών επιλογών παραμέτρου αποκλείει μια σύγκριση που είναι και οριστική και συνοπτική. Γενικευμένα όμως παρατηρούμε:

*1. υπολογιστική αποδοτικότητα*. Το Fiat-Shamir απαιτεί μεταξύ ενός και δύο τάξεων μεγέθους πλήρεις πολλαπλασιασμούς (βήματα) από τον υποδεικνύων από ένα ιδιωτικό RSA-κλειδί λειτουργία. Όταν kt = 20 και n είναι 512 bits, το Fiat-Shamir χρησιμοποιείται από περίπου 11 σε περίπου 30 μέτρα (k = 20, t = 1 και k = 1, t =20). Το GQ απαιτεί περίπου 60 μέτρα (για t = 1, m = 20 = log2 (v)), ή κάπως λιγότερα, εάν έχει χαμηλό βάρος κατά Hamming και την πλήρη ύψωση σε δύναμη σε μη βελτιωμένο RSA παίρνει 768μέτρα.

*2. υπολογισμούς χωρίς σύνδεση*. Η Schnorr αναγνώριση έχει το πλεονέκτημα ότι απαιτεί μόνο μία σύνδεση πολλαπλασιασμού από τον ενάγοντα, υπό την προϋπόθεση ύψωσης σε δύναμη ι ως προεπεξεργασία. (Μια τέτοια εμπορική, μακρινή απευθείας σύνδεση υπολογισμού γραμμής είναι δυνατή σε ορισμένες εφαρμογές. Σε άλλες, ο συνολικός υπολογισμός πρέπει να ληφθούν υπόψη.)Ωστόσο, είναι σημαντική η μέθοδος του υπολογισμού που απαιτείται από τον επιθεωρητή σε σχέση με τη Fiat-Shamir και GQ.

*3. εύρος ζώνης και μνήμης για τα μυστικά*. Το GQ επιτρέπει την ταυτόχρονη μείωση και των δύο, μνήμης (παράμετρος k) και εύρους ζώνης μετάδοσης (παράμετρος t) με k = t = 1, με την εισαγωγή του κοινού εκθέτη > 2 με την πρόθεση ότι η πιθανότητα επιτυχούς εξαπάτησης γίνεται v-kt, όπου αυτή η ταυτόχρονη μείωση δεν είναι δυνατή από το πρωτόκολλο Fiat-Shamir, που απαιτεί μυστικό και χρήστη k και t επαναλήψεις με ασφάλεια (πιθανότητα εξαπάτησης) 2-kt.

*4. Τα πρωτόκολλα που απαιτούν οι παραδοχές που χρησιμοποιούνται τα ακόλουθα βασικά δυσεπίλυτα προβλήματα είναι , για ένα σύνθετο(RSA) ακέραιο n*: Fiat-Shamir-εξάγει τετραγωνικές ρίζες modn. Το GQ εξάγει τις VTH ρίζες modn(δηλαδή, το πρόβλημα RSA). Το Schnorr αναγνώρισης συνδέεται με ένα υπολογιστικό διακριτό υπολογισμό ενός προνομιακού p.

## 2.5 Επιθέσεις σε πρωτόκολλα αναγνώρισης

Οι μέθοδοι που ένας αντίπαλος μπορεί να υιοθετήσει σε μία προσπάθεια να νικηθούν τα πρωτόκολλα προσδιορισμού είναι ένα υποσύνολο για την επικυρωμένη βασική καθιέρωση, και οι τύποι αντιπάλων μπορούν να ταξινομηθούν ομοίως (π.χ., ενεργητικός εναντίον ενεργού, μέλος εναντίον του ξένου) για μια συζήτηση των επιθέσεων σχετικά με τα απλά σχέδια κωδικού πρόσβασης. Είναι, εντούτοις, λιγότερο σύνθετοι από την επικυρωμένη βασική καθιέρωση, δεδομένου ότι δεν υπάρχει κανένα ζήτημα ενός αντιπάλου που μαθαίνει ένα προηγούμενο κλειδί συνόδου, ή που αναγκάζει ένα παλαιό κλειδί για να επαναχρησιμοποιηθεί.

Περιεκτικά, δίνονται οι ορισμοί:

1. *προσωποποίηση*: μια εξαπάτηση με το οποίο μια οντότητα ισχυρίζεται να είναι άλλη.
2. *επίθεση επανάληψης*: μια προσωποποίηση ή άλλη εξαπάτηση που περιλαμβάνει τη χρήση των πληροφοριών από μια ενιαία προηγούμενη εκτέλεση πρωτοκόλλου, για έναν ίδιο ή διαφορετικό ελεγκτή. Για τα αποθηκευμένα αρχεία, το ανάλογο μιας επίθεσης επανάληψης είναι η αποκατάσταση της επίθεσης, με το οποίο ένα αρχείο αντικαθίσταται από μια προηγούμενη έκδοση.

3. *επίθεση παρεμβολής λευκών σελίδων*: μια προσωποποίηση ή άλλη εξαπάτηση που περιλαμβάνει τον εκλεκτικό συνδυασμό πληροφοριών από μια ή περισσότερες προηγούμενες ή ταυτόχρονα τρέχουσες εκτελέσεις πρωτοκόλλου (παράλληλες σύνοδοι), συμπεριλαμβανομένης της πιθανής αρχικής σύνταξης μιας ή περισσότερων εκτελέσεων πρωτοκόλλου από τον ίδιο αντίπαλο.
4. *επίθεση αντανάκλασης*: μια επίθεση παρεμβολής λευκών σελίδων που στέλνει τις πληροφορίες από μια τρέχουσα εκτέλεση πρωτοκόλλου πίσω στο δημιουργό τέτοιων πληροφοριών.
5. *αναγκασμένη καθυστέρηση*: μια αναγκασμένη καθυστέρηση εμφανίζεται όταν παρεμποδίζει ένας αντίπαλος ένα μήνυμα (χαρακτηριστικά περιέχει έναν αριθμό ακολουθίας), και το αναμεταδίδει σε κάποιο πιο πρόσφατο χρονικό σημείο. Σημειώστε ότι το καθυστερημένο μήνυμα δεν είναι μια επανάληψη.
6. *επίθεση επιλεγμένων κειμένων*: μια επίθεση σε ένα πρωτόκολλο πρόκλησης-απάντησης όπου ένας αντίπαλος επιλέγει στρατηγικά τις προκλήσεις σε μία προσπάθεια να εξαχθούν οι πληροφορίες για το μακροπρόθεσμο κλειδί του ενάγοντος.

Οι επιθέσεις επιλεγμένων κειμένων αναφέρονται μερικές φορές ως χρησιμοποιήσεις του ενάγοντος ως χρησμός, δηλ., για να λάβουν πληροφορίες μη υπολογίσιμες από τη γνώση του δημόσιου κλειδιού ενός ενάγοντος μόνο. Η επίθεση μπορεί να περιλάβει επιλεγμένα κείμενα εάν ο ενάγων πρέπει για να υπογράψει μια κρυπτογράφηση, ή MAC πρόκληση, ή να επιλέξει το κρυπτογράφημα, αν η απαίτηση είναι να αποκρυπτογραφήσει μια πρόκληση. Πιθανές απειλές για τα πρωτόκολλα ταυτοποίησης περιλαμβάνουν πλαστοπροσωπία από οποιαδήποτε από τις ακόλουθες επιθέσεις: αναπαραγωγή, προβληματισμό μεταξύ της εξόδου, ή αναγκαστική καθυστέρηση. Η μίμηση είναι επίσης τετριμμένη, αν ένας αντίπαλος είναι σε θέση να ανακαλύψουν το μακροπρόθεσμο (μυστικό ή ιδιωτικό) υλικό μιας οντότητας κλειδώματος, για παράδειγμα, χρησιμοποιώντας μια επίθεση επιλεγμένου κειμένου. Αυτό μπορεί να είναι δυνατό σε πρωτόκολλα που δεν έχουν τη μηδενική γνώση ,διότι ο ενάγων χρησιμοποιεί το ιδιωτικό κλειδί του για να υπολογίσει την απάντησή της, συνεπώς, μια απάντηση μπορεί να αποκαλύψει μερικές πληροφορίες. Σε περίπτωση που η δράση του αντιπάλου, οι ενδέχεται να περιλαμβάνουν την επίθεση με ένα ή περισσοτέρους ίδιους τρόπους τρεξίματος του πρωτόκολλου, δημιουργούνται, ή αλλιώς να μεταβάλλονται τα νέα ή προηγούμενη μηνύματα.

Χρειάζεται προσοχή εάν οποιοδήποτε κρυπτογραφικό κλειδί χρησιμοποιείται για περισσότερους από έναν σκοπούς. Παραδείγματος χάριν, η χρησιμοποίηση ενός κλειδιού RSA για την επικύρωση και για τις υπογραφές οντοτήτων μπορεί να συμβιβάσει την ασφάλεια με την άδεια μιας επίθεσης επιλεγμένων κειμένων. Υποθέτουμε ότι η επικύρωση αποτελείται εδώ από το Β που προκαλεί το Α με έναν τυχαίο αριθμό rB RSA που κρυπτογραφείται κάτω από το δημόσιο κλειδί Α , και το Α απαιτείται για να αποκριθεί με τον αποκρυπτογραφημένο τυχαίο αριθμό. Εάν το Β προκαλεί το Α με το with rB = h(x), τότε η απάντηση του Α σε αυτό το αίτημα επικύρωσης μπορεί (ασυναίσθητα) να παρέχει στο Β την υπογραφή RSA της hash αξίας (άγνωστος Α) στο μήνυμα Χ. Σε οποιοδήποτε πρωτόκολλο προσδιορισμού μεταξύ του Α και του Β, ένα αντίπαλο Γ μπορεί να περπατήσει στην πορεία επικοινωνιών και να αναμεταδώσει απλά (χωρίς αλλαγή) τα μηνύματα μεταξύ των νόμιμων συμβαλλόμενων μέρων Α και Β, που ενεργούν ως μέρος της σύνδεσης επικοινωνιών. Χαρακτηριστικά στην πράξη, αυτό δεν θεωρείται αληθινή "επίθεση", δεν αλλάζει όμως τη διαβεβαίωση ζωτικότητας που παραδίδεται από το πρωτόκολλο εντούτοις, ενώ σε μερικές ειδικές εφαρμογές, αυτό μπορεί να είναι μια ανησυχία. Η ταυτοποίηση πρωτόκολλων δεν παρέχει εγγυήσεις σχετικά με την φυσική τοποθεσία του επικυρωμένο κόμματος. Ως εκ τούτου, μια ανησυχία μπορεί να προκύψει κατά την ειδική περίπτωση όπου: ο Γ αντίπαλος προσπαθεί να μιμηθεί το Β, όπου τίθεται

υπό αμφισβήτηση (για να αποδείξει ότι είναι Β) από το Α, και είναι σε θέση να (σε πραγματικό χρόνο, χωρίς ανίχνευση ή την αισθητή καθυστερήσει, και προσποιείται ότι είναι Α) προκαλέσει τον πραγματικό Β, ώστε να πάρει μια σωστή απάντηση από το Β, και να περάσει αυτή η απάντηση κατά μήκος στο Α. Στην περίπτωση αυτή, τα πρόσθετα μέτρα είναι αναγκαία να αποφύγουν την αμφισβήτηση της οντότητα αποκλείοντας ενισχύσεις στις απαντήσεις των υπολογιστών. Αυτό σχετίζεται με το λεγόμενο πρόβλημα grandmaster ταχυδρομικού σκακιού, σύμφωνα με την οποία η βαθμολόγηση σκάκι ερασιτεχνών μπορεί άδικα να βελτιωθεί με τη συμμετοχή σε δύο ταυτόχρονες αγώνες σκακιού με διακριτά grandmasters, παίζοντας ως μαύρος σε ένα παιχνίδι και λευκός στο δεύτερο, και χρησιμοποιώντας κινήσεις του grandmaster του από το ένα παιχνίδι στο άλλο. Είτε δύο ισοπαλίες, είτε μια νίκη και μια απώλεια, είναι εγγυημένα, τα οποία θα βελτιώσουν την βαθμολογία τους ερασιτέχνες του.

*(i) διατηρώντας την αυθεντικότητα*
Τα πρωτόκολλα προσδιορισμού παρέχουν τις διαβεβαιώσεις που επιβεβαιώνουν την ταυτότητα μιας οντότητας μόνο σε μια δεδομένη στιγμή εγκαίρως. Εάν η συνοχή μιας τέτοιας διαβεβαίωσης απαιτείται, οι πρόσθετες τεχνικές είναι απαραίτητες για να αντιδράσουν στους ενεργούς αντιπάλους. Παραδείγματος χάριν, εάν ο προσδιορισμός πραγματοποιείται στην αρχή μιας συνόδου επικοινωνιών για να χορηγήσει τις άδειες επικοινωνιών, μια πιθανή απειλή είναι αντίπαλος που "κόβει" μετά από τον επιτυχή προσδιορισμό του νόμιμου συμβαλλόμενου μέρους. Οι προσεγγίσεις για να αποτρέψουν αυτό περιλαμβάνουν:

1. εκτελώντας την επαναληπτική επικύρωση περιοδικά, ή για κάθε ιδιαίτερο πόρο ζητούμενο (π.χ., κάθε πρόσβαση αρχείων). Μια υπόλοιπη απειλή είναι εδώ αντίπαλος που κάθε φορά που εκτελείται η επαναληπτική επικύρωση, επιτρέποντας στο νόμιμο συμβαλλόμενο μέρος για να εκτελέσει αυτόν τον στόχο, πρίν καταγράφει εκ νέου.
2. σύνδεση της διαδικασίας προσδιορισμού σε μια τρέχουσα υπηρεσία ακεραιότητας.
Σε αυτήν την περίπτωση, η διαδικασία προσδιορισμού πρέπει να ενσωματωθεί με σε έναν βασικό μηχανισμό καθιερώσεων, έτσι ώστε ένα υποπροϊόν του επιτυχούς προσδιορισμού είναι ένα κλειδί συνόδου κατάλληλο για τη χρήση σε έναν επόμενο τρέχοντα μηχανισμό ακεραιότητας.

*(ii) επίπεδο ασφαλείας που απαιτείται για on-line εναντίον off-line επιθέσεις*
Το επίπεδο ασφάλειας που απαιτείται για τα πρωτόκολλα προσδιορισμού εξαρτάται από το περιβάλλον και τη συγκεκριμένη εφαρμογή προσιτά. Η πιθανότητα της επιτυχίας "της εικασίας των επιθέσεων" εξετάζεται, και διακρίνεται από το ποσό υπολογισμού που απαιτήθηκε για να τοποθετήσει τις σε απευθείας σύνδεση ή σε μη απευθείας σύνδεση επιθέσεις (που χρησιμοποιούν τις καλύτερες τεχνικές γνωστές). Μερικές επεξηγηματικές σημειώσεις ακολουθούν
1. *τοπικές επιθέσεις*. Η επιλογή των παραμέτρων ασφάλειας που περιορίζουν την πιθανότητα της επιτυχούς προσωποποίησης μιας επίθεσης εικασίας (ένας αντίπαλος υποθέτει απλά το μυστικό ενός νόμιμου συμβαλλόμενου μέρους) σε ένα 1 στην πιθανότητα 2 20 (20 bit της ασφάλειας) μπορεί να αρκέσει εάν, για κάθε αποπειραθείσα προσωποποίηση, μια τοπική εμφάνιση απαιτείται από τον εν δυνάμει μιμητή και υπάρχει μια ποινική ρήτρα για τις αποτυχημένες προσπάθειες. Ανάλογα με την πιθανή απώλεια που οδηγεί σχετικά με την ποινική ρήτρα, 10 έως 30 bits ή μπορεί να απαιτηθεί μεγαλύτερη ασφάλεια.

2. *μακρινές επιθέσεις*. Ένα πιο υψηλό επίπεδο ασφάλειας απαιτείται στα περιβάλλοντα όπου απεριόριστες προσπάθειες προσδιορισμού, που περιλαμβάνουν την ελάχιστη υπολογιστική προσπάθεια, είναι δυνατές από τις μακρινές ηλεκτρονικές επικοινωνίες, από έναν ανώνυμο ενάγοντα που αλληλεπιδρά με ένα σύστημα ανοικτής γραμμής, χωρίς τις ποινικές ρήτρες για τις αποτυχημένες προσπάθειες. 20 έως 40 bit της ασφάλειας ή περισσότερα μπορούν να απαιτηθούν εδώ, εκτός αν ο αριθμός αλληλεπιδράσεων μπορεί να περιοριστεί κάπως.

3. *σε μη απευθείας σύνδεση ή μη-διαλογικές επιθέσεις*. Η επιλογή των παραμέτρων ασφάλειας έτσι ώστε μια επίθεση απαιτεί 240 υπολογισμούς στον πραγματικό χρόνο (κατά τη διάρκεια μιας εκτέλεσης πρωτοκόλλου) μπορεί να είναι αποδεκτή, αλλά ένα όριο 260 έως 2 80 υπολογισμών (τα τελευταία πρέπει να είναι επαρκή σε όλα περίπτωση) μπορεί να απαιτηθεί εάν οι υπολογισμοί μπορούν να πραγματοποιηθούν offline, και η επίθεση είναι επαληθεύσιμη (δηλ., ο αντίπαλος μπορεί να επιβεβαιώσει, πριν αλληλεπιδράσει με το σύστημα ανοικτής γραμμής, ότι η πιθανότητα επιτυχούς προσωποποίησής του είναι κοντά στο 1 ή μπορεί να ανακτήσει ένα μακροπρόθεσμο μυστικό από τους σε μη απευθείας σύνδεση υπολογισμούς σε μια επόμενη αλληλεπίδραση).

# Κεφάλαιο 3ο

# Ψηφιακές υπογραφές

## 3.1 Εισαγωγή

Στο κεφάλαιο αυτό θεωρούμε τεχνικές που έχουν σχεδιαστεί για να παράσχουν το ψηφιακό αντίστοιχο μιας χειρόγραφης υπογραφής. Ψηφιακή υπογραφή ενός μηνύματος είναι ένας αριθμός που εξαρτάται από κάποιο μυστικό το οποίο είναι γνωστό μόνο στον υπογράφοντα και, επιπρόσθετα, από το περιεχόμενο του προς υπογραφή μηνύματος. Οι υπογραφές πρέπει να είναι επαληθεύσιμες αν προκύψει διαφωνία για το κατά πόσον ένα μέλος υπέγραψε ένα έγγραφο (η οποία προκαλείται από έναν ψευδόμενο υπογράφοντα που προσπαθεί να απαρνηθεί την υπογραφή που δημιούργησε, ή από έναν δόλιο παράγοντα που προβάλλει αξίωση ή διεκδίκηση), ένα αμερόληπτο τρίτο μέλος θα πρέπει να είναι σε θέση να επιλύσει το ζήτημα δίκαια, χωρίς την απαίτηση πρόσβασης στη μυστική πληροφορία του υπογράφοντα (ιδιωτικό κλειδί).
Οι ψηφιακές υπογραφές έχουν πολλές εφαρμογές στην ασφάλεια πληροφοριών, συμπεριλαμβανομένης της πιστοποίησης αυθεντικότητας, της ακεραιότητας δεδομένων και της μη απάρνησης. Μια από τις σημαντικότερες εφαρμογές των ψηφιακών υπογραφών είναι η πιστοποίηση των δημόσιων κλειδιών σε μεγάλα δίκτυα. Η πιστοποίηση είναι ένα μέσο για ένα έμπιστο τρίτο μέλος (TTP) προκειμένου να δεσμεύσει την ταυτότητα ενός χρήστη με ένα δημόσιο κλειδί, έτσι ώστε σε κάποια μεταγενέστερη χρονική στιγμή, άλλες οντότητες να μπορούν να πιστοποιήσουν την αυθεντικότητα ενός δημόσιου κλειδιού χωρίς τη βοήθεια ενός έμπιστου τρίτου μέλους.
Η έννοια και η χρησιμότητα της ψηφιακής υπογραφής είχε αναγνωριστεί μερικά χρόνια πριν γίνει διαθέσιμη οποιαδήποτε πρακτική υλοποίηση. Η πρώτη μέθοδος που ανακαλύφθηκε ήταν το σχήμα υπογραφών RSA, η οποία παραμένει μέχρι σήμερα μία από τις πιο πρακτικές και γόνιμες διαθέσιμες μεθόδους. Η έρευνα που ακολούθησε είχε ως αποτέλεσμα πολλές εναλλακτικές τεχνικές ψηφιακών υπογραφών. Μερικές προσφέρουν σημαντικά πλεονεκτήματα ως προς τη λειτουργικότητα και την υλοποίηση. Το κεφάλαιο αυτό είναι μια περιγραφή πολλών αποτελεσμάτων που έχουν προκύψει μέχρι σήμερα, με έμφαση σε εκείνες τις αναπτύξεις που είναι πρακτικές.

## 3.2 Ένα πλαίσιο για μηχανισμούς ψηφιακών υπογραφών

### 3.2.1 Βασικοί ορισμοί

1. *Ψηφιακή υπογραφή* είναι μια συμβολοσειρά δεδομένων η οποία συσχετίζει ένα μήνυμα (σε ψηφιακή μορφή) με κάποια δημιουργό οντότητα.
2. *Αλγόριθμος παραγωγής ψηφιακών υπογραφών* (ή αλγόριθμος παραγωγής υπογραφών) είναι μια μέθοδος παραγωγής μιας ψηφιακής υπογραφής.
3. *Αλγόριθμος επαλήθευσης ψηφιακών υπογραφών* (ή αλγόριθμος επαλήθευσης) είναι μια μέθοδος για την επιβεβαίωση ότι μια ψηφιακή υπογραφή είναι αυθεντική (δηλ. ότι όντως δημιουργήθηκε από την καθορισμένη οντότητα).
4. *Ένα σχήμα ψηφιακών υπογραφών* (ή μηχανισμός) συνίσταται σε έναν αλγόριθμο

παραγωγής υπογραφών και έναν αντίστοιχο αλγόριθμο επαλήθευσης.
5. Μια *διεργασία υπογραφής ψηφιακών υπογραφών* (ή διαδικασία) συνίσταται σε έναν (μαθηματικό) αλγόριθμο παραγωγής ψηφιακών υπογραφών, μαζί με μια μέθοδο μορφοποίησης των δεδομένων σε μηνύματα τα οποία μπορούν να υπογραφούν.
6. Μια *διεργασία επαλήθευσης ψηφιακών υπογραφών* (ή διαδικασία) συνίσταται σε έναν αλγόριθμο επαλήθευσης, μαζί με μια μέθοδο ανάκτησης δεδομένων από το μήνυμα.
Στο κεφάλαιο αυτό, στο μεγαλύτερο μέρος, ενδιαφερόμαστε απλά για τα σχήματα ψηφιακών υπογραφών. Για να χρησιμοποιήσουμε στην πράξη ένα σχήμα ψηφιακών υπογραφών είναι αναγκαίο να έχουμε μια διεργασία ψηφιακών υπογραφών. Έχουν εμφανιστεί στο προσκήνιο αρκετές διεργασίες συνδεδεμένες με διάφορα σχήματα ως σχετικά εμπορικά πρότυπα δύο τέτοιες διεργασίες, συγκεκριμένα η ISO/IEC 9796 και η PKCS#1, περιγράφονται στην §3.3.5 και την §3.3.6, αντίστοιχα. Στον πίνακα 3.1 παρέχονται οι συμβολισμοί που χρησιμοποιούνται στο υπόλοιπο αυτού του κεφαλαίου. Τα σύνολα και οι συναρτήσεις που αναφέρονται στον Πίνακα παρακάτω είναι όλα δημόσια γνωστά.

*Συμβολισμοί για τους μηχανισμούς ψηφιακών υπογραφών*

Πίνακας 3.1

| Συμβολισμός | Σημασία |
|---|---|
| M | ένα σύνολο στοιχείων που λέγεται χώρος μηνυμάτων |
| MS | ένα σύνολο στοιχείων που λέγεται χώρος υπογραφής (signing space) |
| S | ένα σύνολο στοιχείων που λέγεται χώρος υπογραφών (signature space) |
| R | μια 1-1 απεικόνιση από το M στο MS που λέγεται συνάρτηση περίσσειας |
| MR | η εικόνα της R (δηλ. MR = Im(R)) |
| R1 | η αντίστροφη της R (δηλ. R1 : MR — M) |
| R | ένα σύνολο στοιχείων που λέγεται σύνολο δεικτοδότησης για υπογραφή |
| h | μια μονόδρομη συνάρτηση με πεδίο ορισμού M .Η εικόνα της h (δηλ. h : M — MH)^ το MH c MS λέγεται χώρος τιμών διασποράς. |

Σχόλια για τον πίνακα:

(i) (μηνύματα) Το M είναι το σύνολο των στοιχείων στα οποία ο υπογράφων μπορεί να επισυνάψει μια ψηφιακή υπογραφή.
(ii) (χώρος υπογραφής) Το MS είναι το σύνολο των στοιχείων στα οποία εφαρμόζονται οι μετασχηματισμοί υπογραφών. Οι μετασχηματισμοί υπογραφών δεν εφαρμόζονται απευθείας στο σύνολο M.
(iii) (χώρος υπογραφών) Το S είναι το σύνολο των στοιχείων που συσχετίζονται με τα μηνύματα στο M. Τα στοιχεία αυτά χρησιμοποιούνται για να δεσμεύσουν τον υπογράφοντα με το μήνυμα.

(iv) (σύνολο δεικτοδότησης) Το R χρησιμοποιείται για την ταυτοποίηση συγκεκριμένων μετασχηματισμών υπογραφής

***Μια κατάταξη των σχημάτων ψηφιακών υπογραφών***

Στη συνέχεια θα περιγράφουν δύο γενικές κλάσεις σχημάτων ψηφιακών υπογραφών οι οποίες μπορούν συνοπτικά να συνοψιστούν ως εξής:
1. Τα σχήματα ψηφιακών υπογραφών με παράρτημα απαιτούν το πρωτότυπο μήνυμα ως είσοδο στον αλγόριθμο επαλήθευσης
2. Τα σχήματα ψηφιακών υπογραφών με ανάκτηση μηνύματος δεν απαιτούν το πρωτότυπο μήνυμα ως είσοδο στον αλγόριθμο επαλήθευσης. Στην περίπτωση αυτή το πρωτότυπο μήνυμα ανακτάται από την ίδια την υπογραφή.
Αυτές οι κλάσεις μπορούν να υποδιαιρεθούν περαιτέρω σύμφωνα με το εάν ισχύει ή όχι η |R| = 1.

**Ορισμός:** Ένα σχήμα ψηφιακών υπογραφών (με ανάκτηση μηνύματος είτε με παράρτημα), λέγεται ότι είναι ένα τυχαιοκρατικό σχήμα ψηφιακών υπογραφών αν |R| > 1 διαφορετικά, το σχήμα ψηφιακών υπογραφών λέγεται ότι είναι αιτιοκρατικό.

## 3.2.2 Σχήματα ψηφιακών υπογραφών με παράρτημα

Τα σχήματα ψηφιακών υπογραφών με παράρτημα, όπως περιγράφονται στην ενότητα αυτή, είναι αυτά που συνήθως χρησιμοποιούνται στην πράξη. Βασίζονται σε κρυπτογραφικές συναρτήσεις διασποράς αντί των ειδικά προσαρμοσμένων συναρτήσεων περίσσειας και είναι λιγότερο επιρρεπείς σε επιθέσεις υπαρξιακής πλαστογράφησης .
Ορισμός :Τα σχήματα ψηφιακών υπογραφών τα οποία απαιτούν το μήνυμα ως είσοδο στον αλγόριθμο επαλήθευσης λέγονται σχήματα ψηφιακών υπογραφών με παράρτημα.
Παραδείγματα μηχανισμών που παρέχουν ψηφιακές υπογραφές με παράρτημα είναι τα σχήματα υπογραφών DSA, ElGamal και Schnorr .

***Αλγόριθμος Παραγωγής κλειδιών για σχήματα ψηφιακών υπογραφών με παράρτημα***

Κάθε οντότητα δημιουργεί ένα ιδιωτικό κλειδί για την υπογραφή μηνυμάτων και ένα αντίστοιχο δημόσιο κλειδί προκειμένου να χρησιμοποιηθεί από άλλες οντότητες για την επαλήθευση υπογραφών.

1. Κάθε οντότητα A θα πρέπει να επιλέξει ένα ιδιωτικό κλειδί το οποίο ορίζει ένα σύνολο μετασχηματισμών βA = [SAk : k e R}. Κάθε SAk είναι μια 1-1 απεικόνιση από το Mh στο S και λέγεται μετασχηματισμός υπογραφής.

2. Το ορίζει μια αντίστοιχη απεικόνιση VA από το Mh χ S στο {αληθές, ψευδές}
τέτοια ώστε
Va (m, S*\ j^il^ αν SA,k (m) = s" [ψευδές, διαφορετικά
για κάθε m e Mh, s* e S εδώ, m = h (m) για m e M. Η απεικόνιση VA λέγεται μετασχηματισμός επαλήθευσης και κατασκευάζεται έτσι ώστε να μπορεί να υπολογιστεί χωρίς τη γνώση του ιδιωτικού κλειδιού του υπογράφοντα.

3. Το δημόσιο κλειδί της A είναι η VA το ιδιωτικό κλειδί της A είναι το σύνολο SA.

***Αλγόριθμος Παραγωγής και Επαλήθευσης υπογραφών (σχήματα ψηφιακών υπογραφών με παράρτημα)***

Η οντότητα Α παράγει μια υπογραφή s e S για ένα μήνυμα m eM, η οποία μπορεί αργότερα να επαληθευτεί από οποιαδήποτε οντότητα Β.

*1. Παραγωγή υπογραφής.* Η οντότητα Α θα πρέπει να κάνει τα εξής:
(i) Να επιλέξει ένα στοιχείο k e R.
(ii) Να υπολογίσει τα m = h (m) και s" = SAk (m).
(iii) Η υπογραφή της Α για το m είναι s*. Τα m και s* γίνονται διαθέσιμα σε οντότητες οι οποίες μπορεί να θελήσουν να επαληθεύσουν την υπογραφή.

*2. Επαλήθευση.* Η οντότητα Β θα πρέπει να κάνει τα εξής:
(i) Να προμηθευτεί το αυθεντικό δημόσιο κλειδί VA της Α.
(ii) Να υπολογίσει τα m = h(m) και u = VA (m,s*).
(iii) Να αποδεχτεί την υπογραφή, αν και μόνο αν u = αληθές.

Οι ακόλουθες ιδιότητες είναι απαραίτητες για τους μετασχηματισμούς υπογραφής και επαλήθευσης:
(i) Για κάθε k e R, θα πρέπει να είναι αποδοτικός ο υπολογισμός της SAk
(ii) Θα πρέπει να είναι αποδοτικός ο υπολογισμός της VA και
(iii) Θα πρέπει να είναι υπολογιστικά ανέφικτο για μια οντότητα άλλη από την Α να βρει ένα m eM και ένα s* e Sτέτοια, ώστε VA (m,s*) = αληθές, όπου m = h(m).

Χρήση συναρτήσεων διασποράς: Τα περισσότερα σχήματα ψηφιακών υπογραφών με ανάκτηση μηνύματος εφαρμόζονται σε μηνύματα συγκεκριμένου μήκους, ενώ οι ψηφιακές υπογραφές με παράρτημα εφαρμόζονται σε μηνύματα οποιουδήποτε μήκους. Η μονόδρομη συνάρτηση h στον επιλέγεται τυπικά να είναι μια ελεύθερη-συμπτώσεων συνάρτηση διασποράς. Αντί για διασπορά μπορεί να γίνει διαχωρισμός του μηνύματος σε τμήματα (μπλοκ) συγκεκριμένου μήκους τα οποία είναι δυνατό να υπογραφούν μεμονωμένα χρησιμοποιώντας ένα σχήμα υπογραφών με ανάκτηση μηνύματος. Αφού η παραγωγή υπογραφών είναι σχετικά αργή για πολλά σχήματα και αφού η αναδιάταξη πολλαπλών υπογεγραμμένων τμημάτων παρουσιάζουν ένα ρίσκο ασφάλειας, η προτιμητέα μέθοδος είναι η διασπορά.

## 3.2.3 Σχήματα ψηφιακών υπογραφών με ανάκτηση μηνύματος

Τα σχήματα ψηφιακών υπογραφών που περιγράφουμε στην ενότητα αυτή έχουν το χαρακτηριστικό ότι το υπογεγραμμένο μήνυμα μπορεί να ανακτηθεί από την ίδια την υπογραφή. Στην πράξη, το χαρακτηριστικό αυτό χρησιμεύει για σύντομα μηνύματα . Σχήμα ψηφιακών υπογραφών με ανάκτηση μηνύματος είναι ένα σχήμα ψηφιακών υπογραφών για το οποίο δεν απαιτείται εκ των προτέρων γνώση του μηνύματος για τον αλγόριθμο επαλήθευσης.

Παραδείγματα μηχανισμών που παρέχουν ψηφιακές υπογραφές με ανάκτηση μηνύματος είναι τα σχήματα υπογραφών δημόσιου κλειδιού RSA , Rabin και Nyberg-Rueppel .

***Αλγόριθμος Παραγωγή κλειδιών για σχήματα ψηφιακών υπογραφών με ανάκτηση μηνύματος***

Κάθε οντότητα δημιουργεί ένα ιδιωτικό κλειδί προκειμένου να χρησιμοποιηθεί για την υπογραφή μηνυμάτων και ένα αντίστοιχο δημόσιο κλειδί προκειμένου να χρησιμοποιηθεί από άλλες οντότητες για την επαλήθευση υπογραφών.

1. Κάθε οντότητα A θα πρέπει να επιλέξει ένα σύνολο μετασχηματισμών = {SA k: k eR}. Κάθε SAik είναι μια 1-1 απεικόνιση από το MS στο S και λέγεται μετασχηματισμός υπογραφής.

2. Το ορίζει μια αντίστοιχη απεικόνιση VA με την ιδιότητα ότι η VA ο SAk είναι η ταυτοτική απεικόνιση στο MS για κάθε k e R. Η VA λέγεται μετασχηματισμός επαλήθευσης και κατασκευάζεται έτσι, ώστε να μπορεί να υπολογιστεί χωρίς τη γνώση του ιδιωτικού κλειδιού του υπογράφοντα.

3. Το δημόσιο κλειδί της A είναι η VA το ιδιωτικό κλειδί της A είναι το σύνολο .

***Αλγόριθμος Παραγωγή και επαλήθευση υπογραφών για σχήματα με ανάκτηση μηνύματος***

Η οντότητα A παράγει μια υπογραφή s e S για ένα μήνυμα m e M, η οποία μπορεί αργότερα να επαληθευτεί από οποιαδήποτε οντότητα B. Το μήνυμα m ανακτάται από το s.

*1. Παραγωγή υπογραφής.* Η οντότητα A θα πρέπει να κάνει τα εξής:
(i) Να επιλέξει ένα στοιχείο k e R.
(ii) Να υπολογίσει τα m = R (m) και s* = SAk (m). (R είναι μια συνάρτηση περίσσειας
(iii) Η υπογραφή της A είναι £* αυτή γίνεται διαθέσιμη σε οντότητες που μπορεί να επιθυμούν να επαληθεύσουν την υπογραφή και να ανακτήσουν το m από αυτή.

*2. Επαλήθευση.* Η οντότητα B θα πρέπει να κάνει τα εξής:
(i) Να προμηθευτεί το αυθεντικό δημόσιο κλειδί VA της A.
(ii) Να υπολογίσει το m = VA (s*) .
(iii) Να επαληθεύσει ότι m e MR . (Αν m ί MR , τότε να απορρίψει την υπογραφή.)
(iv) Να ανακτήσει το m από το m υπολογίζοντας το R1 (m).

Οι ακόλουθες ιδιότητες είναι απαραίτητες για τους μετασχηματισμούς υπογραφής και επαλήθευσης:
(i) Για κάθε k e R, θα πρέπει να είναι εφικτός ο υπολογισμός της SA:k-
(ii) Θα πρέπει να είναι αποδοτικός ο υπολογισμός της VA και
(iii) Θα πρέπει να είναι υπολογιστικά ανέφικτο για μια οντότητα άλλη από την A να βρει ένα s* e S τέτοιο, ώστε VA (s*) e MR.

Η συνάρτηση περίσσειας R και η αντίστροφή της R1 είναι δημόσια γνωστές. Η επιλογή της κατάλληλης R είναι κρίσιμη για την ασφάλεια του συστήματος. Για να γίνει κατανοητό αυτό, ας υποθέσουμε ότι MR = MS. Υποθέτουμε ότι οι R και Saik είναι 1-1 και επί από το M στο MR και από το MS στο S, αντίστοιχα. Αυτό συνεπάγεται ότι τα M και S έχουν το ίδιο πλήθος στοιχείων. Τότε για s* e S, είναι VA (s*) e MR και είναι εύκολο να βρούμε μηνύματα m και

τις αντίστοιχες υπογραφές s* που θα γίνουν αποδεκτά από τον αλγόριθμο επαλήθευσης ως εξής:

1. Επιλογή τυχαίου k e R και τυχαίου s* e S.

2. Υπολογισμός του m = VA (s *).

3. Υπολογισμός του m

Το στοιχείο s* είναι μια έγκυρη υπογραφή για το μήνυμα m και δημιουργήθηκε χωρίς τη γνώση του συνόλου των μετασχηματισμών υπογραφής.

Παράδειγμα
Ας υποθέσουμε ότι M = {m : m e {0, 1}"} για κάποιον συγκεκριμένο ακέραιο " και MS = {t : t e {0, 1}2"}. Ορίζουμε την R : M — MS με R(m) = m||m, όπου το || συμβολίζει συνένωση δηλαδή, MR = {m||m : m e M} c MS. Για μεγάλες τιμές του ", η ποσότητα | MR |/| MS | = (1/2)" είναι ένα πάρα πολύ μικρό κλάσμα. Αυτή η συνάρτηση περίσσειας είναι κατάλληλη με την προϋπόθεση ότι καμιά συνετή επιλογή του s* από τη μεριά του αντίπαλου δεν θα έχει μια μη αμελητέα πιθανότητα να δίνει VA(s*) e MR.

Αν και η συνάρτηση περίσσειας R είναι δημόσια γνωστή και η R1 είναι εύκολο να την υπολογίσουμε, η επιλογή της R είναι κρίσιμη και δεν θα πρέπει να γίνει ανεξάρτητα από την επιλογή των μετασχηματισμών υπογραφής του S^i. Το παράδειγμα παρέχει ένα συγκεκριμένο παράδειγμα μιας συνάρτησης περίσσειας η οποία θέτει σε κίνδυνο την ασφάλεια του σχήματος υπογραφών. Αυτή η συνάρτηση περίσσειας δεν είναι κατάλληλη για όλα τα σχήματα ψηφιακών υπογραφών με ανάκτηση μηνύματος, αλλά εφαρμόζεται στα σχήματα ψηφιακών υπογραφών RSA και Rabin .

Υπογραφές με παράρτημα από σχήματα που παρέχουν ανάκτηση μηνύματος. Ένα σχήμα ψηφιακών υπογραφών με ανάκτηση μηνύματος μπορεί να μετατραπεί σε σχήμα ψηφιακών υπογραφών με παράρτημα κάνοντας απλώς διασπορά του μηνύματος και στη συνέχεια υπογράφοντας την τιμή διασποράς. Το μήνυμα είναι τώρα απαιτούμενο ως είσοδος στον αλγόριθμο επαλήθευσης. Η συνάρτηση περίσσειας R δεν είναι πλέον κρίσιμη για την ασφάλεια του σχήματος υπογραφών και μπορεί να είναι μια οποιαδήποτε συνάρτηση 1-1 από το Mh στο MS.

## 3.2.4 Τύποι επιθέσεων σε σχήματα υπογραφών

Ο σκοπός ενός αντιπάλου είναι η πλαστογράφηση των υπογραφών η παραγωγή δηλαδή υπογραφών οι οποίες θα γίνουν αποδεκτές ως υπογραφές κάποιας άλλης οντότητας. Τα ακόλουθα παρέχουν ένα σύνολο κριτηρίων για το τι σημαίνει ότι κάποιος παραβιάζει ένα σχήμα υπογραφών.

1. *ολική παραβίαση*. Ένας αντίπαλος είτε είναι σε θέση να υπολογίσει τις πληροφορίες ιδιωτικού κλειδιού του υπογράφοντα, είτε βρίσκει έναν αποδοτικό αλγόριθμο υπογραφής λειτουργικά ισοδύναμο με τον έγκυρο αλγόριθμο υπογραφής.
2. *επιλεκτική πλαστογράφηση*. Ένας αντίπαλος είναι σε θέση να δημιουργήσει μια έγκυρη υπογραφή για ένα συγκεκριμένο μήνυμα ή για μια κλάση μηνυμάτων επιλεγμένων

εκ των προτέρων. Η δημιουργία της υπογραφής δεν εμπλέκει άμεσα τον νόμιμο υπογράφοντα.
3. *υπαρξιακή πλαστογράφηση*. Ένας αντίπαλος είναι σε θέση να πλαστογραφήσει μια υπογραφή για ένα τουλάχιστο μήνυμα. Ο αντίπαλος έχει λίγο ή καθόλου έλεγχο επί του μηνύματος του οποίου έχει αποσπάσει την υπογραφή, και ο νόμιμος υπογράφων μπορεί να εμπλέκεται στην εξαπάτηση.
Υπάρχουν δύο βασικές επιθέσεις εναντίον των σχημάτων ψηφιακών υπογραφών δημόσιου κλειδιού.

*επιθέσεις κλειδιού*. Στις επιθέσεις αυτές, ένας αντίπαλος γνωρίζει μόνο το δημόσιο κλειδί του υπογράφοντα.

*επιθέσεις μηνύματος*. Εδώ ένας αντίπαλος είναι σε θέση να εξετάσει υπογραφές που αντιστοιχούν είτε σε γνωστά είτε σε επιλεγμένα μηνύματα. Οι επιθέσεις μηνύματος μπορούν να υποδιαιρεθούν παραπέρα σε τρεις κλάσεις:

*(i) επίθεση γνωστού μηνύματος*. Ένας αντίπαλος έχει υπογραφές για ένα σύνολο μηνυμάτων τα οποία είναι γνωστά στον αντίπαλο αλλά δεν έχουν επιλεγεί από τον ίδιο.
*(ii) επίθεση επιλεγμένου μηνύματος*. Ένας αντίπαλος λαμβάνει έγκυρες υπογραφές από μια επιλεγμένη λίστα μηνυμάτων πριν προσπαθήσει να παραβιάσει το σχήμα υπογραφών. Η επίθεση αυτή είναι μη προσαρμόσιμη (non-adaptive) με την έννοια ότι τα μηνύματα επιλέγονται πριν ειδωθούν οποιεσδήποτε υπογραφές. Οι επιθέσεις επιλεγμένου μηνύματος εναντίον σχημάτων υπογραφών είναι ανάλογες με τις επιθέσεις επιλεγμένου κρυπτοκειμένου εναντίον σχημάτων κρυπτογράφησης δημόσιου κλειδιού.
*(iii) προσαρμόσιμη επίθεση επιλεγμένου μηνύματος*. Επιτρέπεται στον αντίπαλο να χρησιμοποιήσει τον υπογράφοντα ως μαντείο ο αντίπαλος μπορεί να ζητά υπογραφές μηνυμάτων που εξαρτώνται από το δημόσιο κλειδί του υπογράφοντα και μπορεί να ζητά υπογραφές μηνυμάτων που εξαρτώνται από υπογραφές ή μηνύματα που ελήφθησαν προηγουμένως.

Προσαρμόσιμη επίθεση επιλεγμένου μηνύματος: Κατ' αρχήν, μια προσαρμόσιμη επίθεση επιλεγμένου μηνύματος αποτελεί τον πλέον δύσκολο τύπο επίθεσης να αποτραπεί. Είναι πιθανό ότι δεδομένων αρκετών μηνυμάτων και των αντίστοιχων υπογραφών, ένας αντίπαλος θα μπορούσε να συναγάγει ένα πρότυπο (μοτίβο) και μετά να πλαστογραφήσει μια υπογραφή της επιλογής του. Ενώ μια προσαρμόσιμη επίθεση επιλεγμένου μηνύματος μπορεί να είναι ανέφικτο να εξαπολυθεί στην πράξη, ένα καλά σχεδιασμένο σχήμα υπογραφών θα πρέπει μολαταύτα να είναι σχεδιασμένο έτσι, ώστε να παρέχει προστασία έναντι αυτής της δυνατότητας.

Ζητήματα ασφάλειας: Το επίπεδο ασφάλειας που απαιτείται σε ένα σχήμα ψηφιακών υπογραφών μπορεί να διαφέρει ανάλογα με την εφαρμογή. Παραδείγματος χάρη, σε καταστάσεις όπου ο αντίπαλος είναι σε θέση να εξαπολύσει μόνο επίθεση κλειδιού, μπορεί να αρκεί να σχεδιάσουμε το σχήμα ώστε να εμποδίζει τον αντίπαλο από το να επιτυγχάνει επιλεκτική πλαστογράφηση. Σε καταστάσεις όπου ο αντίπαλος είναι ικανός για επίθεση μηνύματος, είναι ενδεχομένως αναγκαία η προφύλαξη ενάντια στη δυνατότητα υπαρξιακής πλαστογράφησης.

Συναρτήσεις διασποράς και διεργασίες ψηφιακών υπογραφών : Όταν μια συνάρτηση διασποράς h χρησιμοποιείται σε ένα σχήμα ψηφιακών υπογραφών (όπως συμβαίνει συχνά), η h θα πρέπει να αποτελεί τμήμα της διεργασίας υπογραφών έτσι ώστε να μην μπορεί ο αντίπαλος να πάρει μια έγκυρη υπογραφή, να αντικαταστήσει την h με μια

ασθενή συνάρτηση διασποράς και στη συνέχεια να εξαπολύσει μια επίθεση επιλεκτικής πλαστογράφησης.

## 3.3 RSA και συναφή σχήματα υπογραφών

Στην ενότητα αυτή περιγράφουμε το σχήμα υπογραφών RSA όπως και άλλες συναφείς μεθόδους. Η ασφάλεια των σχημάτων που παρουσιάζουμε εδώ βασίζεται σε μεγάλο βαθμό στο δυσεπίλυτο του προβλήματος της παραγοντοποίησης ακεραίων. Τα σχήματα που παρουσιάζουμε περιλαμβάνουν τις ψηφιακές υπογραφές με ανάκτηση μηνύματος και με παράρτημα.

### 3.3.1 Το σχήμα υπογραφών RSA

Ο χώρος μηνυμάτων και ο χώρος κρυπτοκειμένων για το σχήμα κρυπτογράφησης δημόσιου κλειδιού RSA είναι και στις δύο περιπτώσεις το σύνολο $Z_n = \{0, 1, 2, ..., n - 1\}$, όπου $n = pq$ είναι το γινόμενο δύο τυχαία επιλεγμένων διαφορετικών πρώτων αριθμών. Επειδή ο μετασχηματισμός κρυπτογράφησης είναι μια 1-1 και επί συνάρτηση, οι ψηφιακές υπογραφές μπορούν να δημιουργηθούν αντιστρέφοντας τους ρόλους κρυπτογράφησης και αποκρυπτογράφησης. Το σχήμα υπογραφών RSA είναι ένα αιτιοκρατικό σχήμα ψηφιακών υπογραφών το οποίο παρέχει ανάκτηση μηνύματος. Ο χώρος υπογραφής MS και ο χώρος υπογραφών S είναι το σύνολο Zn. Επιλέγεται μια συνάρτηση περίσσειας $R: M \rightarrow Z_n$ και είναι δημόσια γνωστή.

***Αλγόριθμος Παραγωγή κλειδιών για το σχήμα υπογραφών RSA***

Κάθε οντότητα δημιουργεί ένα δημόσιο κλειδί RSA και ένα αντίστοιχο ιδιωτικό κλειδί. Κάθε οντότητα A θα πρέπει να κάνει τα εξής:

1. Να παραγάγει δύο μεγάλους διαφορετικούς τυχαίους πρώτους p και q του ιδίου περίπου μεγέθους
2. Να υπολογίσει τα $n = pq$ και $\phi = (p - 1)(q - 1)$.
3. Να επιλέξει έναν τυχαίο ακέραιο e, $1 < e < \phi$, τέτοιον ώστε $\gcd(e, \phi) = 1$.
4. Να χρησιμοποιήσει τον διευρυμένο Ευκλείδειο αλγόριθμο (Αλγόριθμος 2.107) για να υπολογίσει τον μοναδικό ακέραιο d, $1 < d < \phi$, τέτοιον ώστε $ed = 1 \pmod{\phi}$.
5. Το δημόσιο κλειδί της A είναι το (n, e) το ιδιωτικό κλειδί της A είναι το d.

***Αλγόριθμος Παραγωγή και επαλήθευση υπογραφών RSA***

Η οντότητα A υπογράφει ένα μήνυμα m e M. Οποιαδήποτε οντότητα B μπορεί να επαληθεύσει την υπογραφή της A και να ανακτήσει το μήνυμα m από την υπογραφή.

1. *Παραγωγή υπογραφής*. Η οντότητα A θα πρέπει να κάνει τα εξής:
(i) Να υπολογίσει το in = R (m) , έναν ακέραιο στο διάστημα [0, n - 1].
(ii) Να υπολογίσει το s = fhd mod n.
(iii) Η υπογραφή της A για το m είναι s.

2. *Επαλήθευση*. Για να επαληθεύσει την υπογραφή s της A και να ανακτήσει το

μήνυμα m,
η οντότητα B θα πρέπει:
(i) Να προμηθευτεί το αυθεντικό δημόσιο κλειδί (n, e) της A.
(ii) Να υπολογίσει το m = se mod n.
(iii) Να επαληθεύσει ότι m e MR αν όχι, να απορρίψει την υπογραφή.
(iv) Να ανακτήσει το m = R 1 (m).

Απόδειξη ότι η επαλήθευση της υπογραφής λειτουργεί. Αν s είναι μια υπογραφή για το μήνυμα m, τότε s = md mod n, όπου m = R (m). Αφού ed = 1 (mod ϕ), είναι se = med = m (mod n). Τελικά, R- (m) = R 1 (R (m)) = m.

Παράδειγμα (παραγωγή υπογραφής RSA με τεχνηέντως μικρές παραμέτρους):
*Παραγωγή κλειδιών*. Η οντότητα A επιλέγει δύο πρώτους p = 7927, q = 6997 και υπολογίζει n = pq = 55465219 και ϕ = 7926x6996 = 55450296. Η A επιλέγει e = 5 και λύνει την ed = 5d = 1 (mod 55450296), βρίσκοντας d = 44360237. Το δημόσιο κλειδί της A είναι (n = 55465219, e = 5) το ιδιωτικό κλειδί της A είναι d = 44360237.
*Παραγωγή υπογραφής*. Χάριν απλότητας , υποθέτουμε ότι M = Zn και ότι η συνάρτηση περίσσειας R: M — Z„ είναι η ταυτοτική απεικόνιση R(m) = m για κάθε m e M. Για να υπογράψει το μήνυμα m = 31229978, η A υπολογίζει m = R(m) = 31229978 και μετά υπολογίζει την υπογραφή s = md mod n = 3122997844360237 mod 55465219 = 30729435.
*Επαλήθευση υπογραφής*. Η οντότητα B υπολογίζει m = se mod n = 307294355 mod 55465219 = 31229978. Τελικά ο B αποδέχεται την υπογραφή επειδή το m έχει την απαιτούμενη περίσσεια (δηλ., m e MR) και ανακτά το m = R 1 (ι) = 31229978.

## 3.3.2 Πιθανές επιθέσεις στις υπογραφές RSA

**Παραγοντοποίηση ακεραίων**
Αν ένας αντίπαλος είναι σε θέση να παραγοντοποιήσει το δημόσιο modulus n μιας οντότητας A, τότε ο αντίπαλος αυτός μπορεί να υπολογίσει το ϕ και στη συνέχεια, χρησιμοποιώντας τον διευρυμένο Ευκλείδειο αλγόριθμο, να συναγάγει το ιδιωτικό κλειδί d από το ϕ και τον δημόσιο εκθέτη e λύνοντας την ed = 1 (mod ϕ). Αυτό συνιστά μια ολική παραβίαση του συστήματος. Για να προφυλαχτεί από κάτι τέτοιο η A πρέπει να επιλέξει τα p και q έτσι ώστε η παραγοντοποίηση του n να είναι μια υπολογιστικά ανέφικτη αποστολή.

**Πολλαπλασιαστική ιδιότητα του RSA**
Το σχήμα υπογραφών RSA (όπως επίσης και η μέθοδος κρυπτογράφησης) έχει την ακόλουθη πολλαπλασιαστική ιδιότητα, η οποία μερικές φορές αναφέρεται ως ομομορφική ιδιότητα. Αν s1 = m1d modn και s2 = m2l modn είναι υπογραφές στα μηνύματα m1 και m2, αντίστοιχα (ή πιο σωστά σε μηνύματα στα οποία έχει προστεθεί περίσσεια), τότε το s = s1s2 mod n έχει την ιδιότητα ότι s = (m1m2)d mod n. Αν το m = m1m2 έχει την ενδεδειγμένη περίσσεια (δηλ., m e MR), τότε το s θα είναι μια έγκυρη υπογραφή γι' αυτό. Άρα, είναι σημαντικό το ότι η συνάρτηση περίσσειας R δεν είναι πολλαπλασιαστική, δηλ., για όλα ουσιαστικά τα ζεύγη a, b e M, R(a * b) Φ R(a)R(b). Η συνθήκη αυτή στην R είναι αναγκαία αλλά όχι και ικανή για την ασφάλεια.

## 3.3.3 Οι υπογραφές RSA στην πράξη

*(i) Πρόβλημα ανατμηματοποίησης*
Μια προτεινόμενη χρήση του RSA είναι να υπογράψουμε το μήνυμα και μετά να κρυπτογραφήσουμε την υπογραφή που προκύπτει. Θα πρέπει όμως να μας απασχολούν τα σχετικά μεγέθη των moduli που εμπλέκονται όταν υλοποιούμε τη διεργασία αυτή. Ας υποθέσουμε ότι η Α επιθυμεί να υπογράψει και στη συνέχεια να κρυπτογραφήσει ένα μήνυμα για τον Β. Έστω ότι τα δημόσια κλειδιά των Α και Β είναι (ηΑ, eA) και (ηΒ, eB), αντίστοιχα. Αν είναι ηΑ > ηΒ, τότε υπάρχει μια πιθανότητα να μη μπορεί να ανακτηθεί το μήνυμα από τον Β.

Παράδειγμα (πρόβλημα ανατμηματοποίησης):
Έστω ηΑ = 8387x7499 = 62894113, eA = 5 και dA = 37726937 και ηΒ = 55465219, eB = 5, dB = 44360237. Να σημειωθεί ότι ηΑ > ηΒ. Ας υποθέσουμε ότι το m = 1368797 είναι ένα μήνυμα με περίσσεια που πρόκειται να υπογραφεί με το ιδιωτικό κλειδί της Α και μετά να κρυπτογραφηθεί χρησιμοποιώντας το δημόσιο κλειδί του Β. Η Α υπολογίζει τα εξής:
1. s = mdA modηA = 13 6 8 7 9 737726937 mod62894113 = 59847900.
2. c = seB modηB = 5 984 7 9 005 mod55465219 = 38842235.
Για να ανακτήσει το μήνυμα και να επαληθεύσει την υπογραφή, ο Β υπολογίζει τα εξής:
1. s = cdB modηB = 3 8 8 4 2 2 3 5 44360237mod55465219 = 4382681.
2. m = seA modηA = 43826815 mod62894113 = 54383568.

Παρατηρούμε ότι m Φ m. Ο λόγος γι' αυτό είναι ότι το s είναι μεγαλύτερο από το modulus ηΒ. Εδώ, η πιθανότητα εμφάνισης αυτού του προβλήματος είναι (ηΑ - ηΒ )/ηΑ « 0.12. ? Υπάρχουν διάφοροι τρόποι για να ξεπεράσουμε το πρόβλημα ανατμηματοποίησης.

1. αναδιάταξη. Το πρόβλημα της εσφαλμένης αποκρυπτογράφησης δεν θα εμφανιστεί ποτέ αν εκτελεστεί πρώτα η πράξη στην οποία χρησιμοποιείται το μικρότερο modulus. Δηλαδή, αν ηΑ > ηΒ, η οντότητα Α θα πρέπει πρώτα να κρυπτογραφήσει το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του Β και μετά να υπογράψει το προκύπτον κρυπτοκείμενο χρησιμοποιώντας το ιδιωτικό κλειδί της Α. Η προτιμητέα σειρά των πράξεων, όμως, είναι πάντοτε να υπογράφεται πρώτα το μήνυμα και μετά να κρυπτογραφείται η υπογραφή γιατί αν η Α πρώτα κρυπτογραφήσει και μετά υπογράψει, ο αντίπαλος θα μπορούσε να αφαιρέσει την υπογραφή και να την αντικαταστήσει με τη δική του υπογραφή. Ακόμα κι αν ο αντίπαλος δεν γνωρίζει τι είναι υπογεγραμμένο, μπορεί να υπάρχουν καταστάσεις όπου αυτό να αποτελεί πλεονέκτημα για τον αντίπαλο. Άρα η αναδιάταξη δεν είναι η ενδεδειγμένη λύση.

2. δύο moduli ανά οντότητα. Κάθε οντότητα πρέπει να παράγει ξεχωριστά moduli για κρυπτογράφηση και υπογραφή. Αν το modulus υπογραφής κάθε χρήστη είναι μικρότερο απ' όλα τα πιθανά moduli κρυπτογράφησης, τότε δεν θα εμφανιστεί ποτέ εσφαλμένη αποκρυπτογράφηση. Αυτό μπορούμε να το εγγυηθούμε απαιτώντας να είναι τα moduli κρυπτογράφησης αριθμοί των (t + 1) bit και τα moduli υπογραφής αριθμοί των t bit.

3. προκαθορισμός της μορφής του modulus. Στη μέθοδο αυτή επιλέγουμε τους πρώτους p και q έτσι ώστε το modulus η να έχει μια ειδική μορφή: το υψηλότερης τάξης bit είναι 1 και τα επόμενα k bit είναι όλα 0. Ένα modulus η των t bit αυτής της μορφής μπορεί να βρεθεί ως εξής. Για να έχει το η την απαιτούμενη μορφή πρέπει να ισχύει, 2t-1 < η < 2t-1 + 2t- k-1. Επιλέγουμε έναν τυχαίο πρώτο p των \tj2] bit και αναζητούμε έναν πρώ¬το q στο διάστημα μεταξύ των |~2t-1/p] και [(2t-1 + 2t-k-1)/p J τότε το η = pq είναι ένα modulus του ζητούμενου τύπου . Αυτή η επιλογή του modulus η δεν αποτρέπει τελείως το πρόβλημα της

εσφαλμένης αποκρυπτογράφησης, αλλά μπορεί να ελαττώσει την πιθανότητα εμφάνισής του σε έναν πολύ μικρό αριθμό.
Ας υποθέσουμε ότι ο ηA είναι ένα τέτοιο modulus και ότι ο s = mdA modηA είναι μια υπογραφή στο m. Ας υποθέσουμε επιπλέον ότι ο s έχει ένα 1 σε μια από τις k + 1 υψηλής τάξης θέσεις bit, άλλη από την υψηλότερη. Τότε ο s, αφού είναι μικρότερος του ηA, πρέπει να έχει ένα 0 στην υψηλότερης τάξης θέση bit και έτσι είναι αναγκαστικά μικρότερος από οποιοδήποτε άλλο modulus παρόμοιας μορφής. Η πιθανότητα ότι ο s δεν έχει κάποιο 1 στις k + 1 υψηλής τάξης θέσεις bit, άλλη από την υψηλότερη, είναι μικρότερη από (1/2)k, αριθμός που είναι πολύ μικρός αν επιλέξουμε το k να είναι περίπου 100.

Παράδειγμα (προκαθορισμός της μορφής του modulus):
Ας υποθέσουμε ότι θέλουμε να κατασκευάσουμε ένα modulus η των 12 bit τέτοιο, ώστε το υψηλής τάξης bit να είναι 1 και τα επόμενα k = 3 bit να είναι 0. Αρχίζουμε επιλέγοντας έναν πρώτο των 6 bit, p = 37.
Επιλέγουμε έναν πρώτο q στο διάστημα μεταξύ των |~211/pJ = 56 και |_(211 + 28 )/pJ = 62. Οι δυνατότητες για το q είναι 59 και 61. Αν επιλέξουμε q = 61, τότε n = 37 x 61 = 2257, που έχει δυαδική αναπαράσταση 100011010001.

(ii) Συναρτήσεις περίσσειας
Για να αποφύγουμε μια επίθεση υπαρξιακής πλαστογράφησης στο σχήμα υπο¬γραφών RSA, απαιτείται μια κατάλληλη συνάρτηση περίσσειας R. Η συνετή επιλογή μιας συνάρτησης περίσσειας είναι ένα κρίσιμο ζήτημα για την ασφάλεια του συστήματος .
Το σχήμα ψηφιακών υπογραφών RSA με παράρτημα
Αν χρησιμοποιήσουμε τον MD5 για να διασπείρουμε μηνύματα οποιουδήποτε δυαδικού μήκους σε δυαδικές συμβολοσειρές μήκους 128 για να υπογράφουμε αυτές τις τιμές διασποράς. Αν το n είναι ένα modulus RSA των k bit, τότε απαιτείται μια κατάλληλη συνάρτηση περίσσειας R για να αντιστοιχίζουμε ακεραίους των 128 bit σε ακεραίους των k bit.

(iv) Χαρακτηριστικά επιδόσεων της π αραγωγής και επαλήθευσης υπογραφών
Έστω n = pq ένα modulus RSA των 2k bit, όπου p και q είναι πρώτοι των k bit ο καθένας. Ο υπολογισμός μιας υπογραφής, s = md mod η, για ένα μήνυμα m απαιτεί O(k3) πράξεις bit (όσον αφορά τον πολλαπλασιασμό στην αριθμητική υπολοίπων και για την ύψωση σε δύναμη στην αριθμητική υπολοίπων,). Αφού ο υπογράφων τυπικά γνωρίζει τα p και q, μπορεί να υπολογίσει τα s1 = m d mod p, s2 = m d mod q, και να προσδιορίσει το s χρησιμοποιώντας το Κινέζικο θεώρημα υπολοίπων. Παρόλο που η πολυπλοκότητα της διαδικασίας αυτής παραμένει O(k3), είναι αισθητά πιο αποδοτική σε ορισμένες περιπτώσεις.

Η επαλήθευση των υπογραφών είναι σημαντικά πιο γρήγορη από την υπογραφή αν ο δημόσιος εκθέτης επιλέγεται να είναι ένας μικρός αριθμός. Αν γίνει αυτό, η επαλήθευση απαιτεί O(k ) πράξεις bit. Προτεινόμενες τιμές για το e, στην πράξη, είναι 3 ή 216 + 1 φυσικά, τα p και q πρέπει να επιλέγονται έτσι, ώστε να είναι gcd(e, (p - 1)(q - 1)) = 1.
Το σχήμα υπογραφών RSA, συνεπώς, ταιριάζει ιδεατά στις περιπτώσεις που η επαλήθευση υπογραφών είναι η δεσπόζουσα πράξη η οποία εκτελείται. Παραδείγματος χάρη, όταν ένα έμπιστο τρίτο μέλος δημιουργεί ένα πιστοποιητικό δημόσιου κλειδιού για μια οντότητα A, αυτό απαιτεί μόνο μία παραγωγή υπογραφής και η υπογραφή αυτή μπορεί να επαληθευτεί πολλές φορές από διάφορες άλλες οντότητες.

(v) Επιλογή παραμέτρων
Κατά το 1996, για τα moduli υπογραφών RSA συστήνεται ένα ελάχιστο των 768 bit. Ένα modulus τουλάχιστο των 1024 bit συστήνεται για υπογραφές οι οποίες απαιτούν πολύ μεγαλύτερους χρόνους ζωής ή οι οποίες είναι κρίσιμες για τη συνολική ασφάλεια ενός μεγάλου δικτύου. Είναι ενδεδειγμένο να παραμένουμε ενήμεροι για την πρόοδο που σημειώνεται στην παραγοντοποίηση ακεραίων και να είμαστε προετοιμασμένοι για την προσαρμογή των παραμέτρων ανάλογα.
Δεν έχουν αναφερθεί αδυναμίες του σχήματος υπογραφών RSA όταν επιλέγεται ο δημόσιος εκθέτης e να είναι ένας μικρός αριθμός όπως ο 216 + 1. Δεν συστήνεται να περιορίζουμε το μέγεθος του ιδιωτικού εκθέτη d προκειμένου να βελτιώσουμε την αποδοτικότητα της παραγωγής υπογραφών .

(vi) Αποδοτικότητα εύρους ζώνης
Η αποδοτικότητα εύρους ζώνης (bandwidth efficiency) για ψηφιακές υπογραφές με ανάκτηση μηνύματος αναφέρεται στον λόγο του λογαρίθμου (βάση 2) του μεγέθους του χώρου υπογραφής MS προς τον λογάριθμο (βάση 2) του μεγέθους του MR, του χώρου εικόνας της συνάρτησης περίσσειας. Συνεπώς, η αποδοτικότητα εύρους ζώνης προσδιορίζεται από την περίσσεια R. Για το RSA (και για το σχήμα ψηφιακών υπογραφών Rabin, η συνάρτηση περίσσειας που καθορίζεται από το ISO/IEC 9796 δέχεται μηνύματα των k bit και τα κωδικοποιεί σε στοιχεία των 2k bit στο MS από τα οποία σχηματίζεται μια υπογραφή των 2k bit. Η αποδοτικότητα εύρους ζώνης στην περίπτωση αυτή είναι Ά. Παραδείγματος χάρη, με ένα modulus μεγέθους 1024 bit, το μέγιστο μέγεθος ενός μηνύματος το οποίο μπορεί να υπογραφεί είναι 512 bit.

(vii) Παράμετροι καθολικής εφαρμογής
Κάθε οντότητα πρέπει να έχει ένα διαφορετικό modulus RSA- δεν είναι ασφαλές να χρησιμοποιούμε ένα modulus καθολικής εφαρμογής (system-wide)). Ο δημόσιος εκθέτης e μπορεί να είναι μια παράμετρος καθολικής εφαρμογής, και είναι σε πολλές εφαρμογές ).

(viii) Σύντομα και μακροσκελή μηνύματα
Ας υποθέσουμε ότι το η είναι ένα modulus RSA των 2k bit για την υπογραφή μηνυμάτων των k bit (δηλ. η αποδοτικότητα εύρους ζώνης είναι Ά). Ας υποθέσουμε ότι η οντότητα A επιθυμεί να υπογράψει ένα μήνυμα m των k bit. Μια προσέγγιση είναι να διαμερίσουμε το m σε τμήματα των k bit τέτοια, ώστε m = m1\\m2\\...\\mt και να υπογράψουμε κάθε τμήμα μεμονωμένα. Η απαίτηση εύρους ζώνης γι' αυτό είναι 2kt bit. Εναλλακτικά, η A θα μπορούσε να διασπείρει το μήνυμα m σε μια συμβολοσειρά μήκους l < k και να υπογράψει την τιμή διασποράς. Η απαίτηση εύρους ζώνης για την υπογραφή αυτή είναι kt + 2k, όπου ο όρος kt προέρχεται από την αποστολή του μηνύματος m. Αφού kt + 2k < 2kt όταν t > 2, έπεται ότι η πλέον αποδοτική μέθοδος εύρους ζώνης είναι να χρησιμοποιήσουμε ψηφιακές υπογραφές RSA με παράρτημα. Για ένα μήνυμα μεγέθους το πολύ k bit είναι προτιμότερο το RSA με ανάκτηση μηνύματος.

## 3.3.4 Το σχήμα υπογραφών δημόσιου κλειδιού Rabin

Το σχήμα υπογραφών δημόσιου κλειδιού Rabin είναι παρόμοιο με το RSA, αλλά χρησιμοποιεί έναν άρτιο δημόσιο εκθέτη e. Χάριν απλότητας, θα υποθέσουμε ότι e = 2. Ο χώρος υπογραφής MS είναι το Qn (το σύνολο των τετραγωνικών καταλοίπων modulo η) και οι υπογραφές είναι τετραγωνικές ρίζες των στοιχείων του. Επιλέγεται μια συνάρτηση περίσσειας R από τον χώρο μηνυμάτων M στο MS και αποτελεί δημόσια γνώση.

***Αλγόριθμος Παραγωγή κλειδιών για το σχήμα υπογραφών δημόσιου κλειδιού Rabin***

Κάθε οντότητα δημιουργεί ένα δημόσιο κλειδί και το αντίστοιχο ιδιωτικό κλειδί.
Κάθε οντότητα Α θα πρέπει να κάνει τα εξής:
1. Να δημιουργήσει δύο μεγάλους διαφορετικούς τυχαίους πρώτους p και q του αυτού περίπου μεγέθους.
2. Να υπολογίσει το η = pq.
3. Το δημόσιο κλειδί της Α είναι το η το ιδιωτικό κλειδί της Α είναι το ζεύγος (p, q).

***Αλγόριθμος Παραγωγή και επαλήθευση υπογραφών Rabin***

Η οντότητα Α υπογράφει ένα μήνυμα m e M. Η οποιαδήποτε οντότητα Β μπορεί να επαληθεύσει την υπογραφή της Α και να ανακτήσει το μήνυμα m από την υπογραφή.

1. Παραγωγή υπογραφής. Η οντότητα Α θα πρέπει να κάνει τα εξής:
i) Να υπολογίσει το m = R (m) .
ii) Να υπολογίσει μια τετραγωνική ρίζα s του in mod n (
iii) Η υπογραφή του Α για το m είναι s.

2. Επαλήθευση. Για να επαληθεύσει την υπογραφή s της Α και να ανακτήσει το μήνυμα m, η οντότητα Β θα πρέπει να κάνει τα εξής:
i) Να προμηθευτεί το αυθεντικό δημόσιο κλειδί η της Α.
ii) Να υπολογίσει το in = s2 mod n .
iii) Να επαληθεύσει ότι rh e MR αν όχι, να απορρίψει την υπογραφή.
iv) Να ανακτήσει το μήνυμα m = R 1 (m).

Παράδειγμα (παραγωγή υπογραφής Rabin με τεχνηέντως μικρές παραμέτρους)

*Παραγωγή κλειδιών.* Η οντότητα Α επιλέγει πρώτους p = 7, q = 11 και υπολογίζει το η = 77, το δημόσιο κλειδί της Α είναι (p = 7, q = 11). Ο χώρος υπογραφής είναι MS = Q77 = {1, 4, 9, 15, 16, 23, 25, 36, 37, 53, 58, 60, 64, 67, 71}. Χάριν απλότητας θεωρούμε ότι M = MS και τη συνάρτηση περίσσειας R να είναι η ταυτοτική απεικόνιση (δηλ., m = R (m) = m).
Παραγωγή υπογραφής. Για να υπογράψει το μήνυμα m = 23, η Α υπολογίζει R (m) = m = 23 και στη συνέχεια βρίσκει μια τετραγωνική ρίζα του m modulo 77. Αν s συμβολίζει μια τέτοια τετραγωνική ρίζα, τότε s = ±3 (mod 7) και s = ±1 (mod 11), απ' όπου προκύπτει ότι s = 10, 32, 45 ή 67. Η υπογραφή για το m επιλέγεται να είναι s = 45. (Η υπογραφή θα μπορούσε να είναι μία από τις τέσσερις τετραγωνικές ρίζες.)

*Επαλήθευση υπογραφής.* Ο Β υπολογίζει m = s2 mod 77 = 23. Αφού m = 23 e MR, ο Β αποδέχεται την υπογραφή και ανακτά το m = R (m) = 23.

***Σημείωση*** (περίσσεια)
i) Όπως και με το σχήμα υπογραφών RSA, η κατάλληλη επιλογή μιας συνάρτησης περίσσειας R είναι κρίσιμη για την ασφάλεια του σχήματος υπογραφών Rabin. Παραδείγματος χάρη, ας υποθέσουμε ότι M = MS = Qn και R(m) = m για κάθε m e M. Αν ο αντίπαλος επιλέξει έναν ακέραιο s e Z*n και τον υψώσει στο τετράγωνο για να πάρει m = s2 mod n, τότε το s είναι μια έγκυρη υπογραφή για το m και λαμβάνεται χωρίς γνώση του ιδιωτικού κλειδιού. (Εδώ, ο αντίπαλος έχει λίγο έλεγχο πάνω στο ποιο θα είναι το μήνυμα.) Στην περίπτωση αυτή, η υπαρξιακή πλαστογράφηση είναι τετριμμένη.

ii) Στις περισσότερες εφαρμογές των σχημάτων ψηφιακών υπογραφών με ανάκτηση μηνύματος, ο χώρος μηνυμάτων M αποτελείται από συμβολοσειρές κάποιου συγκεκριμένου μήκους. Για το σχήμα Rabin, αποτελεί πρόκληση ο προσδιορισμός μιας συνάρτησης περίσσειας R. Παραδείγματος χάρη, αν το μήνυμα m είναι μια συμβολοσειρά, η R μπορεί να το αντιστοιχίσει στον ακέραιο του οποίου η δυαδική αναπαράσταση είναι το μήνυμα. Δεν υπάρχει, όμως, εγγύηση ότι ο ακέραιος που προκύπτει είναι ένα τετραγωνικό κατάλοιπο modulo n και επομένως ο υπολογισμός μιας τετραγωνικής ρίζας μπορεί να είναι αδύνατος. Κάποιος μπορεί να προσπαθήσει να προσαρτήσει στο m ένα μικρό πλήθος τυχαίων bit και να εφαρμόσει την R πάλι με την ελπίδα ότι R(m) e Qn. Κατά μέσο όρο, δύο τέτοιες προσπάθειες θα αρκούσαν, αλλά θα ήταν προτιμότερη μια αιτιοκρατική μέθοδος.

***Τροποποιημένο σχήμα υπογραφών Rabin***

Για να αντιμετωπίσουμε το πρόβλημα, παρέχουμε μια τροποποιημένη εκδοχή του βασικού σχήματος υπογραφών Rabin. Η τεχνική που παρουσιάζουμε είναι παρόμοια με αυτήν που χρησιμοποιείται στο πρότυπο ψηφιακών υπογραφών ISO/IEC 9796. Παρέχει μια αιτιοκρατική μέθοδο συσχέτισης των μηνυμάτων με στοιχεία του χώρου υπογραφής MS, τέτοια, ώστε ο υπολογισμός μιας τετραγωνικής ρίζας (ή ενός αριθμού κοντά σ' αυτή) να είναι πάντα δυνατή. Η κατανόηση της μεθόδου αυτής θα κάνει ευκολότερη την ανάγνωση της.

Έστω p και q δύο διαφορετικοί πρώτοι με τον καθένα να είναι ισότιμος του 3 modulo 4, και έστω η = pq.
i) Αν gcd(x, n) = 1, τότε x(p-1)(q-1)/2 = 1 (mod n).
ii) Αν χ e Q„, τότε το χ(" p-q+5)/8 mod η είναι μια τετραγωνική ρίζα του χ modulo η.
iii) Έστω χ ακέραιος που έχει σύμβολο Jacobi ^-j = 1 και έστω d = (η - p - q + 5)/8. Τότε
2d d \ X αν X e Qn
χ mod η = <
[η - χ, αν χ £ Qn
iv) Αν p ΐ q (mod 8), τότε (—) = -1. Άρα, ο πολλαπλασιασμός ενός ακεραίου χ με το 2 ή με το 2-1 mod η αντιστρέφει το σύμβολο Jacobi του χ. (Ακέραιοι της μορφής η = pq, όπου p = q = 3 (mod 4) και p ΐ q (mod 8), λέγονται μερικές φορές ακέραιοι Williams.)

***Αλγόριθμος Παραγωγή κλειδιών για το τροποποιημένο σχήμα υπογραφών Rabin***

Ορισμός συνόλων και συναρτήσεων

Πίνακας 3.3.4.1

| **Σύμβολο** | **Όρος** | **Περιγραφή** |
|---|---|---|
| M | χώρος μηνυμάτων | {m e Zη: m < ί(η - 6)/16_\|} |
| MS | χώρος υπογραφής | {m e Zη: m = 6 (mod 16)} |
| S | χώρος υπογραφών | {s e Zη: (s2 mod η) e MS} |
| R | συνάρτηση περίσσειας | R(m) = 16m + 6 για κάθε m e M |
| MR | εικόνα της R | { m e Zη: m = 6 (mod 16)} |

Η οντότητα Α υπογράφει ένα μήνυμα m e M. Μια οντότητα Β μπορεί να επαληθεύσει την υπογραφή της Α και να ανακτήσει το μήνυμα m από την υπογραφή.

ii) Να υπολογίσει το σύμβολο Jacobi J = [—J ]
iii) Αν J = 1, τότε υπολογίζει το s = md mod n.
iv) Αν J = -1, τότε υπολογίζει το s = (fhj2)d mod n.4
v) Η υπογραφή της Α για το m είναι s.

*Επαλήθευση.* Για να επαληθεύσει την υπογραφή s της Α και να ανακτήσει το μήνυμα m, η οντότητα Β θα πρέπει να κάνει τα εξής:

i) Να προμηθευτεί το αυθεντικό δημόσιο κλειδί n της Α.
ii) Να υπολογίσει το m' = s2 mod n. (Να σημειωθεί ότι το ίδιο το αρχικό μήνυμα m δεν είναι απαραίτητο.)
iii) Αν m' = 6(mod8), να πάρει m = m'.
iv) Αν m' = 3(mod 8), να πάρει m = 2m'.
v) Αν m' = 7(mod 8), να πάρει m = n - m'.
vi) Αν m' = 2(mod8), να πάρει m = 2(n - m').
vii) Να επαληθεύσει ότι m e MR αν όχι, να απορρίψει την υπογραφή

Γεγονός για το (iv) ένα ακριβώς από τα m , m /2 έχει σύμβολο Jacobi 1. Η τιμή υ που υπογράφεται είναι τέτοια, ώστε υ = 3 ή 6 (mod 8). Από το Γεγονός 11.28(iii), είναι s2 mod n = υ ή n - υ ανάλογα με το αν ισχύει, ή όχι, ότι υ e Qn. Αφού n = 5 (mod 8), οι περιπτώσεις αυτές μπορούν να διακριθούν μονοσήμαντα.

**Παράδειγμα** (τροποποιημένο σχήμα υπογραφών Rabin με τεχνηέντως μικρές παραμέτρους) Παραγωγή κλειδιών. Η Α επιλέγει p = 19, q = 31 και υπολογίζει n = pq = 589 και d = (n - p -q + 5)/8 = 68. Το δημόσιο κλειδί της Α είναι n = 589, ενώ το ιδιωτικό κλειδί της Α είναι d = 68. Ο χώρος υπογραφής MS δίνεται στον πίνακα που ακολουθεί, μαζί με το σύμβολο Jacobi κάθε στοιχείου.

viii) Να ανακτήσει το m = R_1(m) = (m - 6)/16.

Πίνακας 3.3.4.2

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | G | 22 | ii | 70 | 36 | 102 | 118 | 134 | 1E0 | 1Θ6 |
| | -1 | 1 | -1 | -1 | 1 | 1 | 1 | 1 | -1 | 1 |
| m | 182 | 198 | 21 i | 230 | 246 | 262 | 278 | 294 | 326 | 3£8 |
| (™) | -1 | 1 | 1 | 1 | 1 | -1 | 1 | -1 | -1 | -1 |
| ιπ | 374 | 390 | dDG | 422 | | 454 | 470 | 4BG | £02 | 513 |
| | -1 | -1 | -1 | 1 | 1 | 1 | -1 | -1 | 1 | -1 |
| m | E3d | £50 | 5Θ6 | ES2 | | | | | | |

*Παραγωγή υπογραφής.* Για να υπογράψει το μήνυμα m = 12, η Α υπολογίζει τα m = R(12) = 198, glj = ggj = 1 και s = 19 868 mod 589 = 102. Η υπογραφή της Α για το m = 12 είναι s =102. Επαλήθευση υπογραφής. Ο Β υπολογίζει το m' = s2 mod n = 1022 mod 589 = 391. Αφού m'= 7 (mod 8), ο Β παίρνει m = n - m' = 589 - 391 = 198. Τελικά, ο Β υπολογίζει το m = R_1( m) = (198 - 6)/16 = 12 και δέχεται την υπογραφή.

***Σημείωση*** (ασφάλεια του τροποποιημένου σχήματος υπογραφών Rabin)
i) Όταν χρησιμοποιούμε τον αλγόριθμο αυτό δεν θα πρέπει ποτέ να υπογράψουμε μια τιμή υ που έχει σύμβολο Jacobi -1, διότι κάτι τέτοιο οδηγεί σε παραγοντοποίηση του n. Για να το δούμε αυτό, παρατηρούμε ότι το y = υ2ά = s2 πρέπει να έχει σύμβολο Jacobi 1 αλλά είναι y2 = (υ2)M = υ2 (mod n). Επομένως, (υ - y) (υ + y)= 0 (mod n). Αφού τα υ και y έχουν αντίθετα σύμβολα Jacobi, υ ΐ y (mod n) και συνεπώς gcd(υ - y, n) = p ή q.

ii) Η υπαρξιακή πλαστογράφηση επιτυγχάνεται εύκολα για το τροποποιημένο σχήμα Rabin όπως επιτυγχάνονταν για το αρχικό σχήμα Rabin. Κάποιος χρειάζεται να βρει μόνο ένα s, 1 < s < n - 1, τέτοιο, ώστε το s2 ή το n - s2 ή το 2s2 ή το 2(n - s2) mod n να είναι ισότιμο με το 6 modulo 16. Σε οποιαδήποτε από τις περιπτώσεις αυτές, το s είναι μια έγκυρη υπογραφή για το m = s2 mod n.

***Σημείωση*** (χαρακτηριστικά επιδόσεων του σχήματος υπογραφών Rabin) Ο αλγόριθμος απαιτεί μια συνάρτηση περίσσειας από το M στο MS = Qn, η οποία τυπικά περιλαμβάνει τον υπολογισμό ενός συμβόλου Jacobi . Η παραγωγή μιας υπογραφής τότε περιλαμβάνει τον υπολογισμό τουλάχιστο ενός συμβόλου Jacobi και μιας τετραγωνικής ρίζας modulo n. Ο υπολογισμός της τετραγωνικής ρίζας είναι συγκρίσιμος με μια ύψωση σε δύναμη modulo n. Αφού ο υπολογισμός του συμβόλου Jacobi είναι ισοδύναμος με λίγους πολλαπλασιασμούς της αριθμητικής υπολοίπων, η παραγωγή υπογραφής δεν είναι αισθητά διεξοδικότερη από μια παραγωγή υπογραφής RSA με το ίδιο μέγεθος του modulus. Η επαλήθευση μιας υπογραφής είναι πολύ γρήγορη αν e = 2 απαιτεί μόνο έναν πολλαπλασιασμό της αριθμητικής υπολοίπων. Η ύψωση στο τετράγωνο μπορεί να πραγματοποιηθεί ελαφρώς πιο αποδοτικά απ' ότι ένας γενικός πολλαπλασιασμός της αριθμητικής υπολοίπων. Αυτό επίσης συγκρίνεται ευνοϊκά με την επαλήθευση υπογραφών RSA ακόμα κι όταν ο δημόσιος εκθέτης RSA είναι e = 3.
Το τροποποιημένο σχήμα Rabin καθορίζει τον χώρο μηνυμάτων και
τη συνάρτηση περίσσειας. Η παραγωγή μιας υπογραφής απαιτεί τον υπολογισμό ενός συμβόλου Jacobi και μια ύψωση σε δύναμη της αριθμητικής υπολοίπων.

***Σημείωση*** (αποδοτικότητα εύρους ζώνης) Το σχήμα ψηφιακών υπογραφών Rabin είναι παρόμοιο με το σχήμα RSA σε σχέση με την αποδοτικότητα εύρους ζώνης.

## 3.3.5 Τυποποίηση ISO/IEC 9796

Το ISO/IEC 9796 δημοσιεύθηκε το 1991 από τον Διεθνή Οργανισμό Προτύπων (International Standards Organization - ISO) ως το πρώτο διεθνές πρότυπο για ψηφιακές υπογραφές. Καθορίζει μια διεργασία ψηφιακών υπογραφών η οποία χρησιμοποιεί έναν μηχανισμό ψηφιακών υπογραφών που παρέχει ανάκτηση μηνύματος.
Τα κύρια χαρακτηριστικά του ISO/IEC 9796 είναι:
(i) βασίζεται στην κρυπτογραφία δημόσιου κλειδιού
(ii) ο συγκεκριμένος αλγόριθμος υπογραφών δεν καθορίζεται αλλά πρέπει να απεικονίζει k bit σε k bit
(iii) χρησιμοποιείται για την υπογραφή μηνυμάτων περιορισμένου μήκους και δεν απαιτεί κρυπτογραφική συνάρτηση διασποράς
(iv) παρέχει ανάκτηση μηνύματος και
(v) καθορίζει το "παραγέμισμα" (padding) μηνύματος, όπου απαιτείται.

Παραδείγματα μηχανισμών κατάλληλων για το πρότυπο είναι ο RSA και ο τροποποιημένος Rabin. Οι συγκεκριμένες μέθοδοι που χρησιμοποιούνται για "παραγέμισμα", περίσσεια και αποκοπή ή σύντμηση (truncation) στο ISO/IEC 9796 εμποδίζουν διάφορα μέσα να πλαστογραφούν υπογραφές.

***Παράδειγμα*** (δειγματοληπτικές τιμές παραμέτρων για το ISO/IEC 9796) Ο πίνακας που ακολουθεί παρουσιάζει δειγματοληπτικές τιμές των παραμέτρων στη διεργασία υπογραφής για ένα μήνυμα των 150 bit και μια υπογραφή των 1024 bit.

**Συμβολισμός του ISO/IEC 9796**

Πίνακας 3.3.5.1

| Σύμβολο | Σημασία |
|---|---|
| k | το δυαδικό μήκος της υπογραφής |
| d | το δυαδικό μήκος του προς υπογραφή μηνύματος• απαιτείται να είναι d < 8 \|_(k + 3)/16 J. |
| z | το πλήθος των byte στο "παραγεμισμένο" μήνυμα z = \dj 8]. |
| r | ένα παραπάνω από τα bit "παραγεμίσματος" r = 8z - d + 1. |
| t | ο μικρότερος ακέραιος τέτοιος, ώστε μια συμβολοσειρά των 2t byte να περιλαμβάνει τουλάχιστο k - 1 bit t = \|~(k -1)/16]. |

***Διεργασία υπογραφής για το ISO/IEC 9796***

Η διεργασία υπογραφής αποτελείται από 5 βήματα

*1. παραγέμισμα*. Αν m είναι το μήνυμα, σχηματίζουμε το "παραγεμισμένο" μήνυμα MP = 0r-1||m, όπου 1 < r < 8, τέτοιο ώστε το πλήθος των bit στο MP να είναι πολλαπλάσιο του 8. Το πλήθος των byte στο MP είναι z: MP = mz||mz-1||...m2||m1, όπου κάθε mi είναι ένα byte.

*2. επέκταση μηνύματος*. Το επεκταμένο μήνυμα, συμβολικά ΜΕ, προκύπτει από το MP με επανειλημμένη συνένωση στα αριστερά του MP με τον εαυτό του μέχρι να υπάρξουν t byte στη συμβολοσειρά: ΜΕ = MEt||MEt-1||...||ME2||ME1 (κάθε ΜΕ, είναι ένα byte). Αν το t δεν είναι πολλαπλάσιο του z, τότε τα τελευταία byte που είναι να συνενωθούν είναι ένα μερικό σύνολο από byte από το MP, όπου αυτά τα byte είναι διαδοχικά byte του MP από τα δεξιά. Ακριβέστερα, MEi+1 = m(i mod z)+1 για 0 < i < t - 1.

*3. περίσσεια μηνύματος*. Προστίθεται περίσσεια στο ΜΕ για να πάρουμε τη συμβολοσειρά των byte MR = MR2t|\MR2t-1||^||MR2||MR1 ως εξής. Το MR προκύπτει "ανακατεύοντας" (interleaving) τα t byte του ΜΕ με t byte περίσσειας και στη συνέχεια προσαρμόζοντας το byte MR2z της προκύπτουσας συμβολοσειράς. Ακριβέστερα, MR2i-1 = MEi και MR2i = S(MEi) για 1 < i < t, όπου S(u) λέγεται συνάρτηση σκίασης του byte u και ορίζεται ως εξής. Αν u = u2||u1, όπου u1 και u2 είναι συμβολοσειρές δυαδικού μήκους 4, τότε S(u) = π(^)|| π(u1), όπου π είναι η μετάθεση

_ / 0 1 2 3 4 5 G 7S 9 A E € Ω E F \
= \ E 3 E 6 7 A C 1 J'

(Για συντομία, η μετάθεση π γράφεται με συμβολοσειρές δυαδικού μήκους 4 που αναπαρίστανται με δεκαεξαδικούς χαρακτήρες.) Τελικά, το MR προκύπτει αντικαθιστώντας το MR2z με r θ MR2z.

*4. αποκοπή και forcing*. Σχηματίζουμε τον ενδιάμεσο ακέραιο IR των k bit από τον MR ως
εξής:
α) στα λιγότερο σημαντικά k - 1 bit του MR προσαρτούμε στα αριστερά ένα bit 1β, τροποποιούμε το λιγότερο σημαντικό byte u2||u1 του αποτελέσματος, αντικαθιστώντας το με u1||0110. (Αυτό γίνεται για να εξασφαλίσουμε ότι IR = 6 (mod 16).)

*5. παραγωγή υπογραφής*. Χρησιμοποιείται ένας μηχανισμός υπογραφών ο οποίος απεικονίζει ακεραίους των k bit σε ακεραίους των k bit (και επιτρέπει ανάκτηση μηνύματος). Το IR υπογράφεται χρησιμοποιώντας τον μηχανισμό αυτό έστω ότι s συμβολίζει την προκύπτουσα υπογραφή.

***Σημείωση*** (RSA, Rabin) Το ISO/IEC 9796 προορίζονταν για χρήση με τους μηχανισμούς ψηφιακών υπογραφών RSA και Rabin. Για αυτά τα συγκεκριμένα σχήματα, η παραγωγή υπογραφής διατυπώνεται σαφέστερα. Έστω e ο δημόσιος εκθέτης για τους αλγορίθμους του RSA ή του Rabin, n το modulus και d ο ιδιωτικός εκθέτης. Αρχικά σχηματίζουμε το αντιπροσωπευτικό στοιχείο RR το οποίο είναι:

(i) IR αν το e είναι περιττός, ή αν το e είναι άρτιος και το σύμβολο Jacobi του IR (θεωρώντας το ως ακέραιο) ως προς το modulus n είναι 1

(ii) IR / 2 αν το e είναι άρτιος και το σύμβολο Jacobi του IR ως προς n είναι -1. Η υπογραφή για το m είναι s = (RR)d mod n. Το ISO/IEC 9796 καθορίζει ότι η υπογραφή s θα πρέπει να είναι η μικρότερη των (RR)d mod n και n - ((RR)d mod n).

(ii) Διεργασία επαλήθευσης για το ISO/IEC 9796
Η διεργασία υπογραφής για μια ψηφιακή υπογραφή του ISO/IEC 9796 μπορεί να χωριστεί σε τρία στάδια.

*1. άνοιγμα υπογραφής*. Έστω ότι s είναι η υπογραφή. Τότε εκτελούνται τα εξής βήματα.
(α) Εφαρμόζουμε τον δημόσιο μετασχηματισμό επαλήθευσης στην s για να ανακτήσουμε έναν ακέραιο IR'.
(β) Απορρίπτουμε την υπογραφή αν το IR' δεν είναι μια συμβολοσειρά των k bit με το πιο σημαντικό bit να είναι 1, ή αν η λιγότερο σημαντική συμβολοσειρά των 4 bit δεν έχει την τιμή 0110.

2. *ανάκτηση μηνύματος*. Μια συμβολοσειρά MR' των 2t byte κατασκευάζεται από το IR' εκτελώντας τα εξής βήματα.

(α) Έστω X τα λιγότερο σημαντικά k - 1 bit του IR'.

(β) Αν u4||u3||u2||0110 είναι οι τέσσερις λιγότερο σημαντικές συμβολοσειρές των 4 bit του X, αντικαθιστούμε το λιγότερο σημαντικό byte του X με π _1(u4)||u2. (γ) το MR' λαμβάνεται με "παραγέμισμα" του X με (από) 0 έως 15 μηδενικά bit έτσι ώστε η προκύπτουσα συμβολοσειρά να έχει 2t byte. Οι τιμές z και r υπολογίζονται ως εξής.

(α) Από τα 2t byte του MR' υπολογίζουμε τα t αθροίσματα MR2 i θ S (MR2 i-1) ,1< i < t. Αν όλα τα αθροίσματα είναι 0, απορρίπτουμε την υπογραφή.

(β) Έστω z η μικρότερη τιμή του i για την οποία MR2i θ S (MR2i-1) Φ 0.

(γ) Έστω r η λιγότερο σημαντική συμβολοσειρά των 4 bit του αθροίσματος που βρέθηκε στο
βήμα (β). Απορρίπτουμε την υπογραφή αν η δεκαεξαδική τιμή του r δεν είναι μεταξύ των 1 και 8.

Από το MR', η συμβολοσειρά των z byte MP' κατασκευάζεται ως εξής:

(α) MP2'i = MR2i-1, για 1 < i < z.

(β) Απορρίπτουμε την υπογραφή αν τα r - 1 πιο σημαντικά bit του MP' δεν είναι όλα 0.

(γ) Έστω M' τα 8z - r + 1 λιγότερο σημαντικά bit του MP'.

3. *έλεγχος περίσσειας*. Η υπογραφή s επαληθεύεται ως εξής.

(α) Από το M' κατασκευάζουμε μια συμβολοσειρά MR" εφαρμόζοντας τα βήματα "παραγεμίσματος" του μηνύματος, επέκτασης του μηνύματος και περίσσειας του μηνύματος της διεργασίας υπογραφής,

(β) Αποδεχόμαστε την υπογραφή, αν και μόνο αν τα k - 1 λιγότερο σημαντικά bit του MR" είναι ίσα με τα τα k - 1 λιγότερο σημαντικά bit του MR'.

## 3.3.6 Μορφοποίηση PKCS #1

Τα πρότυπα κρυπτογραφίας δημόσιου κλειδιού (PKCS - public-key cryptography standards) είναι ένα σύνολο ομοειδών προδιαγραφών οι οποίες περιλαμβάνουν τεχνικές για κρυπτογράφηση και υπογραφές RSA. Στην υποενότητα αυτή περιγράφουμε τη διεργασία ψηφιακών υπογραφών που καθορίζεται στο PKCS #1 ("Πρότυπο Κρυπτογράφησης RSA"). Ο μηχανισμός ψηφιακών υπογραφών στο PKCS #1 δεν χρησιμοποιεί το χαρακτηριστικό της ανάκτησης μηνύματος του σχήματος υπογραφών RSA. Απαιτεί μια συνάρτηση διασποράς (MD2 ή MD5) και, επομένως, είναι ένα σχήμα ψηφιακών υπογραφών με παράρτημα. Ο Πίνακας 3.3.6.1 παρουσιάζει τον συμβολισμό που χρησιμοποιούμε στην υποενότητα αυτή. Τα κεφαλαία γράμματα αναφέρονται σε συμβολοσειρές οκτάδων. Αν X είναι μια συμβολοσειρά οκτάδων τότε Xi είναι η οκτάδα i μετρώντας από τα αριστερά.

Πίνακας 3.3.6.1

| Σύμβολο | Σημασία | Σύμβολο | Σημασία |
|---|---|---|---|
| K | το μήκος του n σε οκτάδες (k > 11) | EB | τμήμα κρυπτογράφησης |
| n | το modulus, 28(k-1) < n < 28k | ED | κρυπτογραφημένα δεδομένα |
| p q | οι πρώτοι παράγοντες του | n | οκτάδα συμβολοσειρά μήκους 8 |
| e | ο δημόσιος εκθέτη ς | ab | δεκαεξαδική τιμή οκτάδας |
| d | ο ιδιωτικός εκθέτης | BT | τύπος τμήματος |
| M | μήνυμα | PS | συμβολοσειρά παραγεμίσματος |
| MD | σύνοψη μνηύματος | S | υπογραφή |
| MD' | συγκριτική σύνοψη μηνύματος | \|X\|\| | μήκος του X σε οκτάδες |

***Μορφοποίηση δεδομένων PKCS #1***

Τα δεδομένα είναι μια συμβολοσειρά οκτάδων D, όπου ||D|| < k - 11. BT είναι μια μεμονωμένη οκτάδα της οποίας η δεκαεξαδική αναπαράσταση είναι 00 ή 01. PS είναι μια συμβολοσειρά οκτάδων με ||PS|| = k - 3 - ||D||. Αν BT = 00, τότε όλες οι οκτάδες στην PS είναι ff. Το μορφοποιημένο τμήμα δεδομένων (που λέγεται τμήμα κρυπτογράφησης) είναι το EB =00||BT||PS||00||D.

***Σημείωση*** (σκεπτικό μορφοποίησης δεδομένων)

(i) Το τμήμα 00 των πρώτων θέσεων εξασφαλίζει ότι η συμβολοσειρά οκτάδων EB, όταν ερμηνευτεί ως ακέραιος, είναι μικρότερη από το modulus n.

(ii) Αν ο τύπος τμήματος είναι BT = 00, τότε η D πρέπει να αρχίζει με μια μη μηδενική οκτάδα ή το μήκος της πρέπει να είναι γνωστό προκειμένου να επιτρέπει μη διφορούμενη συντακτική ανάλυση (parsing) του EB.

(iii) Αν BT = 01, τότε είναι πάντοτε δυνατή μη διφορούμενη συντακτική ανάλυση.

(iv) Για τον λόγο που δίνεται στο (iii) και για την αποτροπή ορισμένων ενδεχόμενων επιθέσεων στον μηχανισμό υπογραφών, συστήνεται BT = 01.
Παράδειγμα (μορφοποίηση δεδομένων PKCS #1 για συγκεκριμένες τιμές) Ας υποθέσουμε Ότι το n είναι ένα modulus των 1024 bit (οπότε k = 128). Αν ||D|| = 20 οκτάδες, τότε ||PS||=105 οκτάδες και ||EB|| = 128 οκτάδες.

(ii) Διεργασία υπογραφών για το PKCS #1
Η διεργασία υπογραφών περιλαμβάνει τα παρακάτω βήματα
Η είσοδος στη διεργασία υπογραφών είναι το μήνυμα M, και ο ιδιωτικός εκθέτης d και το

modulus n του υπογράφοντα.

1. *διασπορά μηνύματος*. Διασπείρουμε το μήνυμα M χρησιμοποιώντας τον επιλεγμένο αλγόριθμο μηνύματος-σύνοψης για να πάρουμε τη συμβολοσειρά οκτάδων MD.
2. *κωδικοποίηση σύνοψης μηνύματος*. Η MD και το αναγνωριστικό του αλγόριθμου διασποράς συνδυάζονται σε μια τιμή ASN.1 (abstract syntax notation - αφηρημένος συμβολισμός σύνταξης) και μετά BER-κωδικοποιούνται (basic encoding rules - βασικοί κανόνες κωδικοποίησης) προκειμένου να δώσουν μια συμβολοσειρά οκτάδων D.
3. *μορφοποίηση τμήματος δεδομένων*. Με συμβολοσειρά δεδομένων εισόδου D, χρησιμοποιούμε τη μορφοποίηση δεδομένων για τον σχηματισμό της συμβολοσειράς οκτάδων EB.
4. *μετατροπή συμβολοσειράς οκτάδων σε ακέραιο*. Έστω ότι οι οκτάδες της EB είναι EB1||EB2||...||EBk. Ορίζουμε EBi να είναι ο ακέραιος του οποίου η δυαδική αναπαράσταση είναι η οκτάδα EBi (το λιγότερο σημαντικό bit είναι στα δεξιά). Ο ακέραιος που αναπαριστά την EB είναι m = Σ k=128(k-i) EBi.
5. *υπολογισμός RSA*. Υπολογίζουμε s = md mod n.
μετατροπή ακεραίου σε συμβολοσειρά οκτάδων. Μετατρέπουμε το s σε μια συμβολοσειρά οκτάδων ED = ED1||ED2||...||EDk, όπου οι οκτάδες EDi ικανοποιούν την ισότητα s = Z!=128(k-i)EDi. Η υπογραφή είναι S = ED.

(iii) Διεργασία επαλήθευσης για το PKCS #1
Η διεργασία επαλήθευσης περιλαμβάνει τα ακόλουθα βήματα. Η είσοδος στη διεργασία επαλήθευσης είναι το μήνυμα M, η υπογραφή S, ο δημόσιος εκθέτης e και το modulus n.

1. *μετατροπή συμβολοσειράς οκτάδων σε ακέραιο*.
(α) Απορρίπτουμε την S, αν το δυαδικό μήκος της S δεν είναι πολλαπλάσιο του 8.
(β) Μετατρέπουμε την S σε έναν ακέραιο s όπως στο βήμα 4 της διεργασίας υπογραφών.
(γ) Απορρίπτουμε την υπογραφή αν s > n.
2. *υπολογισμός RSA*. Υπολογίζουμε το m = se mod n.
3. μετατροπή ακεραίου σε συμβολοσειρά οκτάδων. Μετατρέπουμε το m σε μια συμβολοσειρά οκτάδων EB μήκους k οκτάδων όπως στο βήμα 6 της διεργασίας υπογραφών.
4. *ανάλυση (parsing)*. Αναλύουμε συντακτικά την EB σε έναν τύπο τμήματος BT, μια συμβολοσειρά παραγεμίσματος PS και τα δεδομένα D.
(α) Απορρίπτουμε την υπογραφή αν η EB δεν μπορεί να αναλυθεί αναμφίβολα.
(β) Απορρίπτουμε την υπογραφή αν ο BT δεν είναι ένας εκ των 00 ή 01.
(γ) Απορρίπτουμε την υπογραφή αν η PS αποτελείται από < 8 οκτάδες ή είναι ασυμβίβαστη με τον BT.
5. *κωδικοποίηση δεδομένων*.
(α) BER-κωδικοποιούμε τα δεδομένα D προκειμένου να πάρουμε μια σύνοψη μηνύματος MD και ένα αναγνωριστικό αλγόριθμου διασποράς.
(β) Απορρίπτουμε την υπογραφή αν το αναγνωριστικό αλγόριθμου διασποράς δεν ταυτοποιεί μία από τις MD2 ή MD5.
6. *σύνοψη μηνύματος και σύγκριση*.
(α) Διασπείρουμε το μήνυμα M με τον επιλεγμένο αλγόριθμο μηνύματος-σύνοψης για να πάρουμε την MD'.
(β) Αποδεχόμαστε την υπογραφή S στο M, αν και μόνο αν MD' = MD.

## 3.4 Τα σχήματα υπογραφών Fiat-Shamir

Ένα σχήμα ταυτοποίησης που περιλαμβάνει μια ακολουθία αποκρίσεων πρόκλησης-μαρτυρίας (witness-challenge response) μπορεί να μετατραπεί σε ένα σχήμα υπογραφών αντικαθιστώντας την τυχαία πρόκληση του μέλους που κάνει την επαλήθευση με μια μονόδρομη συνάρτηση διασποράς. Στην ενότητα αυτή περιγράφουμε δύο μηχανισμούς υπογραφών οι οποίοι προκύπτουν με αυτόν τον τρόπο. Η βάση αυτής της μεθοδολογίας είναι το πρωτόκολλο ταυτοποίησης Fiat-Shamir .

### 3.4.1 Το σχήμα ψηφιακών υπογραφών Feige-Fiat-Shamir

Το σχήμα ψηφιακών υπογραφών Feige-Fiat-Shamir είναι μια τροποποίηση ενός πρωθύστερου σχήματος υπογραφών των Fiat και Shamir, και απαιτεί μια μονόδρομη συνάρτηση διασποράς h : {0, 1}* — {0, 1}k για κάποιον συγκεκριμένο θετικό ακέραιο k. Εδώ το {0, 1}k συμβολίζει το σύνολο των δυαδικών συμβολοσειρών δυαδικού μήκους k και το {0, 1}* συμβολίζει το σύνολο όλων των δυαδικών συμβολοσειρών (αυθαίρετων δυαδικών μηκών). Η μέθοδος παρέχει μια ψηφιακή υπογραφή με παράρτημα και είναι ένας τυχαιοκρατικός μηχανισμός.

***Αλγόριθμος Παραγωγής κλειδιών για το σχήμα Feige-Fiat-Shamir***

Κάθε οντότητα δημιουργεί ένα δημόσιο κλειδί και το αντίστοιχο ιδιωτικό κλειδί.
Κάθε οντότητα Α θα πρέπει να κάνει τα εξής:
1. Να παραγάγει τυχαίους διαφορετικούς πρώτους p, q και να σχηματίσει το n = pq.
2. Να επιλέξει έναν θετικό ακέραιο k και διαφορετικούς τυχαίους πρώτους s1, s2, ..., sk , e, Z*,n.
3. Να υπολογίσει vj = s j2 mod n,1 < j < k.
4. Το δημόσιο κλειδί της Α είναι η k-άδα (v1,v2,...,vk) και το modulus ή το ιδιωτικό κλειδί της Α είναι η k-άδα (s1,s2,...,sk).

***Αλγόριθμος Παραγωγής και επαλήθευσης υπογραφών Feige-Fiat-Shamir***

Η οντότητα Α υπογράφει ένα δυαδικό μήνυμα m οποιουδήποτε μήκους. Μια οντότητα Β μπορεί να επαληθεύσει την υπογραφή αυτή χρησιμοποιώντας το δημόσιο κλειδί της Α.

1. *Παραγωγή υπογραφής*. Η οντότητα Α θα πρέπει να κάνει τα εξής:
(i) Να επιλέξει έναν τυχαίο ακέραιο r, 1 < r < n - 1.
(ii) Να υπολογίσει u = r2 mod n.
(iii) Να υπολογίσει e = (e1, e2, ek) = h(m\\u) κάθε ei e {0, 1}.
(iv) Να υπολογίσει s = r ¦ Πkj=1 se- mod n.
(v) Η υπογραφή της Α για το m είναι (e, s).

2. *Επαλήθευση*. Για να επαληθεύσει την υπογραφή της Α στο m, ο Β θα πρέπει να κάνει τα εξής:
(i) Να προμηθευτεί το αυθεντικό δημόσιο κλειδί (v1,v2,...,vk)της Α και το n.
(ii) Να υπολογίσει w = s2 ¦ Πk=1 v/ mod n.
(iii) Να υπολογίσει e' = h(m\\w).
(iv) Να αποδεχτεί την υπογραφή, αν και μόνο αν e = e'.
Απόδειξη ότι η επαλήθευση υπογραφής λειτουργεί.
w = s2 ¦ Π v/ - r2 ¦ ins2ej Π v/ - r2 - Π (s2vj )ej = r2 - u (mod n).
Άρα, w = u και επομένως e = e'.

*Παραγωγή υπογραφής*. Ας υποθέσουμε ότι h : {0, 1}* — {0, 1}5 είναι μια συνάρτηση διασποράς. Η Α επιλέγει έναν τυχαίο ακέραιο r = 23181 και υπολογίζει u = r2 mod n = 4354872. Για να υπογράψει το μήνυμα m, η Α υπολογίζει, e = h(m\\u) = 10110 (έχουμε επινοήσει την τιμή διασποράς για το παράδειγμα αυτό). Η Α σχηματίζει το s = rs1s3s4 mod n = (23181)(42)(85) (101) mod n = 7978909 η υπογραφή για το m είναι (e = 10110, s = 7978909). Επαλήθευση υπογραφής. Ο Β υπολογίζει s2 mod n = 2926875 και v1v3v4 mod n = (503594) (7104483)(1409171) mod n = 15668174. Ο Β μετά υπολογίζει, w2 = s2 VV3V4 mod n = 4354872. Αφού είναι w = u, έπεται ότι e' = h(m\\w) = h(m\\u) = e και συνεπώς, ο Β αποδέχεται την υπογραφή.

***Σημείωση*** (ασφάλεια του σχήματος υπογραφών Feige-Fiat-Shamir)

(i) Αντίθετα με το σχήμα υπογραφών RSA, όλες οι οντότητες μπορούν να χρησιμοποιήσουν το ίδιο modulus n. Σ' αυτό το σενάριο, ένα έμπιστο τρίτο μέλος (TTP) θα πρέπει να παραγάγει τους πρώτους p και q όπως επίσης το δημόσιο και το ιδιωτικό κλειδί για κάθε οντότητα.

(ii) Η ασφάλεια του σχήματος Feige-Fiat-Shamir βασίζεται στο δυσεπίλυτο του υπολογισμού τετραγωνικών ριζών modulo n. Έχει αποδειχθεί ότι είναι ασφαλές έναντι μιας προσαρμόσιμης επίθεσης επιλεγμένου μηνύματος, με την προϋπόθεση ότι η παραγοντοποίηση είναι δυσεπίλυτο πρόβλημα, η h είναι μια τυχαία συνάρτηση, και τα si είναι διαφορετικά μεταξύ τους.
Σημείωση 2 (επιλογή παραμέτρων και απαιτήσεις αποθήκευσης κλειδιών) Αν n είναι ένας ακέραιος των t bit, το ιδιωτικό κλειδί που κατασκευάζεται είναι μεγέθους kt bit. Αυτό μπορεί να μειωθεί επιλέγοντας τις τυχαίες τιμές sj, 1 < j < k, ως αριθμούς δυαδικού μήκους t < t ΤΟ t', όμως, δεν θα πρέπει να επιλεγεί τόσο μικρό έτσι ώστε να είναι εφικτή η πρόβλεψη των sj. Το δημόσιο κλειδί είναι μεγέθους (k + 1) bit. Παραδείγματος χάρη, αν t = 768 και k = 128, τότε το ιδιωτικό κλειδί απαιτεί 98304 bit και το δημόσιο κλειδί απαιτεί 99072 bit.

***Σημείωση*** (υπογραφές Feige-Fiat-Shamir βασισμένες σε ταυτότητα) Ας υποθέσουμε ότι ένα TTP κατασκευάζει τους πρώτους p και q και το modulus n το modulus είναι κοινό σε όλες τις οντότητες του συστήματος. Ο αλγόριθμος μπορεί να τροποποιηθεί έτσι ώστε να είναι το σχήμα βασισμένο σε ταυτότητα. Η δυαδική συμβολοσειρά IA της οντότητας A περιέχει πληροφορίες οι οποίες ταυτοποιούν την A. Το TTP υπολογίζει τα Vj = f (IA\j), 1 < j < k, όπου f είναι μια μονόδρομη συνάρτηση διασποράς από το {0, 1}* στο Qn και το j αναπαρίσταται στο δυαδικό σύστημα, και υπολογίζει επίσης μια τετραγωνική ρίζα sj του v-1 modulo n, 1 < j < k. Το δημόσιο κλειδί της A είναι απλά η πληροφορία ταυτότητας IA, ενώ το ιδιωτικό κλειδί της A (διαβιβασμένο με ασφάλεια και μυστικά από το TTP στην A) είναι η k-άδα (s1, s2, ..., sk). Οι συναρτήσεις h, f και το modulus n είναι ποσότητες καθολικής εφαρμογής.
Η διαδικασία αυτή έχει το πλεονέκτημα ότι το δημόσιο κλειδί που παράγεται μπορεί να παραχθεί από μια μικρότερη ποσότητα IA, δυνητικά ελαττώνοντας το κόστος αποθήκευσης και διαβίβασης. Έχει τα μειονεκτήματα ότι τα ιδιωτικά κλειδιά των οντοτήτων είναι γνωστά στο TTP και το modulus n είναι καθολικής εφαρμογής, καθιστώντας το έναν περισσότερο ελκυστικό στόχο.

***Σημείωση*** (παραλλαγή μικρού πρώτου των υπογραφών Feige-Fiat-Shamir) Η βελτίωση αυτή βοηθά στην ελάττωση του μεγέθους του δημόσιου κλειδιού και αυξάνει την αποδοτικότητα της επαλήθευσης υπογραφών. Αντίθετα με την τροποποίηση, κάθε οντότητα A παράγει το δικό της modulus nA και ένα σύνολο από k μικρούς πρώτους v1, v2, ..., vk e Qn (κάθε πρώτος θα απαιτεί περίπου 2 byte για να αναπαρασταθεί). Η οντότητα A επιλέγει μία από τις τετραγωνικές ρίζες sj του v-1 modulo n, για κάθε j, 1 < j <k αυτές σχηματίζουν το ιδιωτικό κλειδί. Το δημόσιο κλειδί αποτελείται από το nA και τις τιμές v1, V2, ..., vk. Η επαλήθευση των υπογραφών διεξάγεται πιο αποδοτικά αφού οι υπολογισμοί γίνονται με πολύ μικρότερους αριθμούς.

***Σημείωση*** (χαρακτηριστικά επιδόσεων των υπογραφών Feige-Fiat-Shamir) Με το σχήμα RSA και ένα modulus μήκους t = 768, η παραγωγή υπογραφών με χρήση απλοϊκών τεχνικών απαιτεί, κατά μέσο όρο, 1152 πολλαπλασιασμούς της αριθμητικής υπολοίπων (ακριβέστερα, 768 τετραγωνισμούς και 384 πολλαπλασιασμούς). Η παραγωγή υπογραφών για το σχήμα Feige-Fiat-Shamir απαιτεί, κατά μέσο όρο, k/2 πολλαπλασιασμούς της αριθμητικής υπολοίπων. Για την υπογραφή ενός μηνύματος με αυτό το σχήμα, ένα modulus μήκους t = 768 και k = 128 απαιτεί, κατά μέσο όρο, 64 πολλαπλασιασμούς της αριθμητικής υπολοίπων, ή λιγότερο από 6% του έργου που απαιτείται από μια απλοϊκή υλοποίηση του RSA. Η επαλήθευση υπογραφών απαιτεί μόνον ένα πολλαπλασιασμό της αριθμητικής υπολοίπων για το RSA αν ο δημόσιος εκθέτης είναι e = 3, και 64 πολλαπλασιασμούς της αριθμητικής υπολοίπων, κατά μέσο όρο, για το Feige-Fiat-Shamir. Για εφαρμογές όπου η παραγωγή υπογραφών πρέπει να εκτελείται γρήγορα και ο χώρος αποθήκευσης κλειδιών δεν είναι περιορισμένος, το σχήμα Feige-Fiat-Shamir (ή σχήματα τύπου DSA) μπορεί να είναι προτιμότερο από το RSA.

## 3.4.2 Το σχήμα υπογραφών GQ

Το πρωτόκολλο ταυτοποίησης Guillou-Quisquater (GQ) μπορεί να μετατραπεί σε έναν μηχανισμό ψηφιακών υπογραφών αν η πρόκληση αντικατασταθεί με μια μονόδρομη συνάρτηση διασποράς. Έστω h : {0, 1}* — Zn μια συνάρτηση διασποράς, όπου n είναι ένας θετικός ακέραιος.
Κάθε οντότητα παράγει ένα δημόσιο κλειδί (n, e, JA) και το αντίστοιχο ιδιωτικό κλειδί a.

***Αλγόριθμος Παραγωγής κλειδιών για το σχήμα υπογραφών Feige-Fiat-Shamir***

Η οντότητα Α θα πρέπει να κάνει τα εξής:

1. Να επιλέξει τυχαίους διαφορετικούς μυστικούς πρώτους p, q και να σχηματίσει το n=pq.

2. Να επιλέξει έναν ακέραιο e e {1, 2, ., n - 1} τέτοιον, ώστε gcd(e, (p - 1)(q - 1)) = 1.

3. Να επιλέξει έναν ακέραιο JA, 1 < JA < n, ο οποίος χρησιμεύει ως αναγνωριστικό για την Α και είναι τέτοιος, ώστε gcd(JA, n) = 1. (Η δυαδική αναπαράσταση του JA θα μπορούσε να κομίσει πληροφορίες για την Α όπως όνομα, διεύθυνση, αριθμό αδείας οδήγησης, κτλ.)
4. Να προσδιορίσει έναν ακέραιο a e 7Ln τέτοιον, ώστε JAae = 1 (mod n) ως εξής:

4.1 Να υπολογίσει το JA-1 mod n.
4.2 Να υπολογίσει τα d1 = e mod (p - 1) και d2 = e mod (q - 1).
4.3 να υπολογίσει τα a1 = (J~A)d mod p και a2 = (JA-1)d2 mod q.
4.4 Να βρει μια κοινή λύση a των ισοτιμιών a = a1 (mod p) και a = a2 (mod q).

5. Το δημόσιο κλειδί της Α είναι (n, e, JA) το ιδιωτικό κλειδί της Α είναι το a.

***Αλγόριθμος Παραγωγής και επαλήθευσης υπογραφών GQ***

Η οντότητα Α υπογράφει ένα δυαδικό μήνυμα m οποιουδήποτε μήκους. Μια οντότητα Β μπορεί να επαληθεύσει την υπογραφή αυτή χρησιμοποιώντας το δημόσιο κλειδί της Α.

*1. Παραγωγή υπογραφής*. Η οντότητα Α θα πρέπει να κάνει τα εξής:
(i) Να επιλέξει έναν τυχαίο ακέραιο k και να υπολογίσει το r = ke mod n.
(ii) Να υπολογίσει το l = h(m\\r).
(iii) Να υπολογίσει το s = ka mod n.
(iv) Η υπογραφή της Α για το m είναι το ζεύγος (s, /).
2. *Επαλήθευση*. Για να επαληθεύσει την υπογραφή της Α, ο Β θα πρέπει να κάνει τα εξής:
(i) Να προμηθευτεί το αυθεντικό δημόσιο κλειδί (n, e, JA) της Α.
(ii) Να υπολογίσει τα u = seJA mod n και V =h(m\\u).
(iii) Να αποδεχτεί την υπογραφή, αν και μόνο αν l = /'.
Απόδειξη ότι η επαλήθευση υπογραφής λειτουργεί. Παρατηρούμε ότι
u = seJA' = (kal )eJA' = ke (aeJA)l = ke = r (mod n). Άρα, u = r και επομένως l = /'.
Παράδειγμα (παραγωγή υπογραφής GQ με τεχνητώς μικρές παραμέτρους)
Η οντότητα Α επιλέγει τους πρώτους p = 20849, q = 27457 και υπολογίζει το n = pq = 572450993. Η Α επιλέγει έναν ακέραιο e = 47, ένα αναγνωριστικό JA= 1091522 και λύνει την ισοτιμία JAae = 1 (mod n) για να πάρει a = 214611724. Το δημόσιο κλειδί της Α είναι (n = 572450993, e = 47, JA = 1091522), ενώ το ιδιωτικό κλειδί της Α είναι α= 214611724.

*Παραγωγή υπογραφής*. Για να υπογράψει το μήνυμα m = 1101110001, η Α επιλέγει έναν τυχαίο ακέραιο k = 42134 και υπολογίζει το r = ke mod n = 297543350.

**Σημείωση** (ασφάλεια του σχήματος υπογραφών GQ) Στον αλγόριθμο GQ το e πρέπει να

είναι αρκούντως μεγάλο προκειμένου να αποκλείσουμε τη δυνατότητα πλαστογράφησης που βασίζεται στο παράδοξο των γενεθλίων. Η δυνητική επίθεση εκτυλίσσεται ως εξής. Ο αντίπαλος επιλέγει ένα μήνυμα m και υπολογίζει το I = h(m\\JAI) για αρκούντως πολλές τιμές του t μέχρι I = t (mod e)- αυτό αναμένεται να πραγματοποιηθεί σε O(4Z) δοκιμές. Έχοντας προσδιορίσει ένα τέτοιο ζεύγος (I, t), ο αντίπαλος προσδιορίζει έναν ακέραιο x τέτοιον, ώστε t = xe + I και υπολογίζει το s = JAx mod n. Παρατηρούμε ότι seJA' = (JAx)e JAI = JAxe+I = JAt (mod n), και συνεπώς, h(m\\JAt) = I. Έτσι, το (s, I) είναι μια έγκυρη (πλαστογραφημένη) υπογραφή για το μήνυμα m.

***Σημείωση*** (επιλογή παραμέτρων). Οι τρέχουσες μέθοδοι (μέχρι το 1996) παραγοντοποίησης ακεραίων συνιστούν ότι ενδείκνυται ένα modulus n των 768 bit. Το μέγεθος του e θα πρέπει να είναι τουλάχιστο 128 bit. Τυπικές τιμές για τα δεδομένα εξόδου ασφαλών συναρτήσεων διασποράς είναι 128 ή 160 bit. Με ένα modulus των 768 bit και ένα e των 128 bit, το δημόσιο κλειδί για το σχήμα GQ είναι μεγέθους 896 + u bit, όπου u είναι το πλήθος των bit που χρειάζονται για την αναπαράσταση του JA. Το μέγεθος του ιδιωτικού κλειδιού a είναι 768 bit.

***Σημείωση*** (χαρακτηριστικά επιδόσεων για υπογραφές GQ). Η παραγωγή υπογραφής για το GQ απαιτεί δύο υψώσεις σε δύναμη και δύο πολλαπλασιασμούς της αριθμητικής υπολοίπων. Χρησιμοποιώντας ένα modulus n των 768 bit, μια τιμή e των 128 bit και μια συνάρτηση διασποράς με έξοδο I των 128 bit, η παραγωγή υπογραφής (χρησιμοποιώντας απλοϊκές τεχνικές για ύψωση σε δύναμη) απαιτεί κατά μέσο όρο 384 πολλαπλασιασμούς της αριθμητικής υπολοίπων (128 τετραγωνισμούς και 64 πολλαπλασιασμούς για καθένα από τα e και I). Η επαλήθευση υπογραφής απαιτεί μια παραπλήσια ποσότητα έργου.

Συγκρίνετέ το αυτό με το RSA (απλοϊκά 1152 πολλαπλασιασμούς της αριθμητικής υπολοίπων) και με το Feige-Fiat-Shamir (64 πολλαπλασιασμούς της αριθμητικής υπολοίπων) για την παραγωγή υπογραφών. Το GQ είναι υπολογιστικά πιο εντατικό από το Feige-Fiat-Shamir αλλά απαιτεί σημαντικά μικρότερο χώρο αποθήκευσης κλειδιών.

***Σημείωση*** (παραλλαγή ανάκτησης μηνύματος των υπογραφών GQ). Ο GQ μπορεί να τροποποιηθεί ως ακολούθως προκειμένου να παρέχει ανάκτηση μηνύματος. Έστω ότι ο χώρος υπογραφής είναι MS = Zn, και έστω m e MS. Στην παραγωγή υπογραφών, επιλέγουμε έναν τυχαίο k τέτοιον, ώστε gcd(k, n) = 1 και υπολογίζουμε τα r =ke mod n και I = mr mod n. Η υπογραφή είναι s = kaI mod n. Η επαλήθευση δίνει seJAI = keaeIJAI = ke = r (mod n). Το μήνυμα m ανακτάται από το Ir -1 mod n. Όπως συμβαίνει σε όλα τα σχήματα ψηφιακών υπογραφών με ανάκτηση μηνύματος, απαιτείται μια κατάλληλη συνάρτηση περίσσειας R για προφύλαξη από μια υπαρξιακή πλαστογράφηση.

## 3.5 Ο DSA και τα σχετικά σχήματα υπογραφών

Στην ενότητα αυτή παρουσιάζουμε τον Αλγόριθμο Ψηφιακών Υπογραφών (DSA - Digital Signature Algorithm) και ορισμένα σχετικά σχήματα υπογραφών. Τα περισσότερα απ' αυτά τα παρουσιάζουμε επί του Z*p για κάποιον μεγάλο πρώτο, αλλά όλοι αυτοί οι μηχανισμοί μπορούν να γενικευτούν σε οποιαδήποτε πεπερασμένη κυκλική ομάδα αυτό επιδεικνύεται με σαφήνεια για το σχήμα υπογραφών ElGamal. Όλες οι μέθοδοι που παρουσιάζουμε στην ενότητα αυτή είναι τυχαιοκρατικά σχήματα ψηφιακών υπογραφών. Όλες δίνουν ψηφιακές υπογραφές με παράρτημα και μπορούν να παράσχουν ψηφιακές υπογραφές με ανάκτηση μηνύματος. Μια αναγκαία συνθήκη για την ασφάλεια όλων των σχημάτων υπογραφών

που εξετάζουμε στην ενότητα αυτή είναι ότι ο υπολογισμός λογαρίθμων στο Z*p είναι υπολογιστικά ανέφικτος. Η συνθήκη αυτή, όμως, δεν είναι απαραίτητα ικανή για την ασφάλεια των σχημάτων αυτών ανάλογα, παραμένει αναπόδεικτο ότι οι ψηφιακές υπογραφές είναι ασφαλείς ακόμα κι αν η παραγοντοποίηση ακεραίων είναι δύσκολη.

### 3.5.1 Ο Αλγόριθμος Ψηφιακών Υπογραφών (DSA-Digital Signature Algorithm)

Τον Αύγουστο του 1991 το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST - National Institute of Standards and Technology) των ΗΠΑ πρότεινε έναν αλγόριθμο ψηφιακών υπογραφών (DSA). Ο DSA έχει γίνει ένα Ομοσπονδιακό Πρότυπο Επεξεργασίας Πληροφοριών των ΗΠΑ (FIPS 186 - Federal Information Processing Standard), που λέγεται Πρότυπο Ψηφιακών Υπογραφών (DSS - Digital Signature Standard ) και είναι το πρώτο σχήμα ψηφιακών υπογραφών που αναγνωρίζεται από οποιαδήποτε κυβέρνηση. Ο αλγόριθμος είναι μια παραλλαγή του σχήματος ElGamal και είναι ένα σχήμα ψηφιακών υπογραφών με παράρτημα.
Ο μηχανισμός υπογραφών απαιτεί μια συνάρτηση διασποράς h: {0, 1}* — Zq για κάποιον ακέραιο q. Το DSS απαιτεί ρητά τη χρήση του Ασφαλούς Αλγορίθμου Διασποράς (SHA-1 - Secure Hash Algorithm).

***Αλγόριθμος Παραγωγής κλειδιών για τον DSA***

Κάθε οντότητα δημιουργεί ένα δημόσιο κλειδί και το αντίστοιχο ιδιωτικό κλειδί.
Κάθε οντότητα Α θα πρέπει να κάνει τα εξής:
1. Να επιλέξει έναν πρώτο αριθμό q τέτοιον, ώστε 2159 < q < 2160.
2. Να διαλέξει ένα t έτσι ώστε 0 < t < 8 και να επιλέξει έναν πρώτο αριθμό p, όπου 2511+64t < p < 2512+64t, με την ιδιότητα ότι ο q διαιρεί τον (p - 1).
3. (Να επιλέξει έναν γεννήτορα α της μοναδικής κυκλικής ομάδας τάξεως q της Z*p .)
3.1 Να επιλέξει ένα στοιχείο g e lip και να υπολογίσει το α = gp - 1)/q mod p.
3.2 Αν α = 1 τότε να πάει στο βήμα 3.1.
4. Να επιλέξει έναν τυχαίο ακέραιο a τέτοιον, ώστε 1 < a < q - 1.
5. Να υπολογίσει το y = aa mod p.
6. Το δημόσιο κλειδί της Α είναι (p, q, α, y)- το ιδιωτικό κλειδί της Α είναι το a.
***Σημείωση*** (παραγωγή των πρώτων p και q του DSA) Πρέπει να επιλέξουμε πρώτα τον πρώτο q και μετά να προσπαθήσουμε να βρούμε έναν πρώτο p τέτοιον, ώστε ο q να διαιρεί τον (p-1).

***Αλγόριθμος Παραγωγής και επαλήθευση υπογραφών DSA***

Η οντότητα Α υπογράφει ένα δυαδικό μήνυμα m οποιουδήποτε μήκους. Μια οντότητα Β μπορεί να επαληθεύσει την υπογραφή αυτή χρησιμοποιώντας το δημόσιο κλειδί της Α.

1. *Παραγωγή υπογραφής*. Η οντότητα Α θα πρέπει να κάνει τα εξής:
i) Να επιλέξει έναν τυχαίο μυστικό ακέραιο k, 0 < k < q .
ii) Να υπολογίσει το r = (α*" mod p) mod q iii) Να υπολογίσει το k 1 mod q
iv) Να υπολογίσει το s = k_1 {h(m) + ar} mod q.
v) Η υπογραφή της Α για το m είναι το ζεύγος (r, s).

2. *Επαλήθευση*. Για να επαληθεύσει την υπογραφή (r, s) της Α στο μήνυμα m, ο Β θα πρέπει να κάνει τα εξής:

i) Να προμηθευτεί το αυθεντικό δημόσιο κλειδί (p, q, α, y) της Α.
ii) Να επαληθεύσει ότι 0 < r < q και 0 < s < q- αν όχι, τότε να απορρίψει την υπογραφή.
iii) Να υπολογίσει τα w = s 1 mod q και h(m).
iv) Να υπολογίσει τα u1 = w ¦ h(m) mod q και u2 = rw mod q.
v) Να υπολογίσει το υ = (α"1 y"2 mod p) mod q.
vi) Να αποδεχτεί την υπογραφή, αν και μόνο αν υ = r.

Απόδειξη ότι η επαλήθευση της υπογραφής λειτουργεί. Αν (r, s) είναι μια γνήσια υπογραφή της οντότητας Α στο μήνυμα m, τότε η h(m) = -ar + ks (mod q) πρέπει να ισχύει. Πολλαπλασιάζοντας και τα δύο μέλη αυτής της ισοτιμίας με w και αναδιατάσσοντας τους όρους, προκύπτει

w : h(m) + arw = k (mod q). Αυτό όμως είναι απλώς u1 + au2 = k (mod q). Υψώνοντας το α και στα δύο μέλη αυτής της εξίσωσης προκύπτει
(α^ yu2 mod p) mod q = (αk mod p) mod q. Άρα, υ = r, που είναι το ζητούμενο.

Παράδειγμα (παραγωγή υπογραφής DSA με τεχνηέντως μικρές παραμέτρους)
Η Α επιλέγει πρώτους p = 124540019 και q = 17389 τέτοιους, ώστε ο q
να διαιρεί τον (p - 1) εδώ (p - 1)/q = 7162. Η Α επιλέγει ένα τυχαίο στοιχείο g = 110217528 e lip και υπολογίζει το α = g7162 modp = 10083255. Αφού α Φ 1, το α είναι ένας γεννήτορας της μοναδικής υποομάδας τάξεως q της Zp . Στη συνέχεια η Α επιλέγει έναν τυχαίο ακέραιο a = 12496 που ικανοποιεί τις 1 < a < q - 1 και υπολογίζει το y = α" mod p = 1008325512496 mod 124540019 = 119946265. Το δημόσιο κλειδί της Α είναι (p = 124540019, q = 17389, α = 10083255, y = 119946265), ενώ το ιδιωτικό κλειδί της Α είναι a = 12496.
*Παραγωγή υπογραφής*. Για να υπογράψει το μήνυμα m η Α επιλέγει έναν τυχαίο ακέραιο k =9557 και υπολογίζει το r = (O1 modp) mod q = (100832559557 mod 124540019) mod 17389=27039929 mod 17389 = 34. Η Α μετά υπολογίζει τα k 1 mod q 7631, h(m) = 5246 (έχουμε επινοήσει την τιμή διασποράς για το παράδειγμα αυτό) και τελικά
s = (7631){5246 + (12496)(34)} mod q = 13049. Η υπογραφή για το m είναι το ζεύγος
(r = 34, s = 13049).

*Επαλήθευση υπογραφής*.
Ο Β υπολογίζει τα
w = s -1 mod q = 1799, u1 = w ¦ h(m) mod q =(5246)(1799) mod 17389 = 12716 και u2 = rw mod q = (34)(1799) mod q = (34)(1799) mod 17389 = 8999.
Ο Β στη συνέχεια υπολογίζει το

υ = (α*yu2 mod p) mod q = (1008325512716

1199462658999 mod 124540019) mod 17389 = 27039929 mod 17389 = 34.
Επειδή,

υ = r, ο Β

αποδέχεται την υπογραφή.

***Σημείωση*** (ασφάλεια του DSA) Η ασφάλεια του DSA εναπόκειται σε δύο διαφορετικά αλλά σχετιζόμενα προβλήματα διακριτού λογαρίθμου. Το ένα είναι το πρόβλημα λογαρίθμου όπου εφαρμόζεται η ισχυρή μέθοδος του λογισμού δεικτών (index calculus) το άλλο είναι το πρόβλημα λογαρίθμου στην κυκλική υποομάδα τάξεως q, όπου οι καλύτερες

τρέχουσες μέθοδοι εκτελούνται σε χρόνο "τετραγωνικής ρίζας". Για περαιτέρω λεπτομέρειες δείτε την §3.6.6. Αφού ο DSA είναι ειδική περίπτωση των υπογραφών ElGamal όσον αφορά την εξίσωση για το s, πρέπει να λάβουμε υπόψη εδώ το ζήτημα της ασφάλειας για τις τελευταίες.

***Σημείωση*** (συνιστώμενα μεγέθη παραμέτρων) Το μέγεθος του q είναι συγκεκριμένο από τον αλγόριθμο (σύμφωνα με το FIPS 186) στα 160 bit, ενώ το μέγεθος του p μπορεί να είναι ένα οποιοδήποτε πολλαπλάσιο του 64 μεταξύ των 512 και 1024 bit, συμπεριλαμβανομένων.
Ένας πρώτος p των 512 bit παρέχει μικρού βαθμού ασφάλεια εναντίον μιας συντονισμένης επίθεσης. Μέχρι το 1996, συνιστάται ένα modulus των 768 bit τουλάχιστο. Το FIPS 186 δεν επιτρέπει πρώτους p μεγαλύτερους από 1024 bit.

***Σημείωση*** (χαρακτηριστικά επιδόσεων του DSA) Για να είμαστε συγκεκριμένοι, ας υποθέσουμε ότι ο p είναι ένας ακέραιος των 768 bit. Η παραγωγή υπογραφών απαιτεί μια ύψωση σε δύναμη της αριθμητικής υπολοίπων, απαιτώντας κατά μέσο όρο (με χρήση απλοϊκών τεχνικών ύψωσης σε δύναμη) 240 πολλαπλασιασμούς της αριθμητικής υπολοίπων, έναν αντίστροφο της αριθμητικής υπολοίπων με ένα modulus των 160 bit, δύο πολλαπλασιασμούς των 160 bit της αριθμητικής υπολοίπων και μία πρόσθεση. Οι πράξεις των 160 bit είναι ίσης σημασίας συγκρινόμενες με την ύψωση σε δύναμη. Ο DSA έχει το πλεονέκτημα ότι η ύψωση σε δύναμη μπορεί να προ-υπολογιστεί και δεν χρειάζεται να γίνει κατά τη διάρκεια της παραγωγής της υπογραφής. Σε αντιδιαστολή, ο προϋπολογισμός δεν είναι δυνατός με το σχήμα υπογραφών RSA. Το κύριο τμήμα της εργασίας για την επαλήθευση υπογραφής είναι δύο υψώσεις σε δύναμη modulo p, κάθε μία με εκθέτη των 160 bit. Κατά μέσο όρο, κάθε μία απ' αυτές απαιτεί 240 πολλαπλασιασμούς της αριθμητικής υπολοίπων ή 480 στο σύνολο. Κάποιες εξοικονομήσεις μπορούν να πραγματοποιηθούν κάνοντας τις δύο υψώσεις σε δύναμη συγχρόνως το κόστος, κατά μέσο όρο, είναι τότε 280 πολλαπλασιασμοί της αριθμητικής υπολοίπων.

***Σημείωση*** (παράμετροι καθολικής εφαρμογής) Δεν είναι αναγκαίο για κάθε οντότητα να επιλέγει τους δικούς της πρώτους p και q. Το DSS επιτρέπει τα p, q και α να είναι παράμετροι καθολικής εφαρμογής. Αυτό όμως παρουσιάζει έναν ελκυστικότερο στόχο για τον αντίπαλο.

***Σημείωση*** (πιθανότητα αποτυχίας) Η επαλήθευση απαιτεί τον υπολογισμό του s_1 mod q. Αν s = 0, τότε το s-1 δεν υπάρχει. Για να αποφύγει την κατάσταση αυτή ο υπογράφων μπορεί να ελέγξει ότι s Φ 0 αλλά αν υποθέσουμε ότι το s είναι ένα τυχαίο στοιχείο του Zq, τότε η πιθανότητα να είναι s = 0 είναι (Λ)160. Στην πράξη, κάτι τέτοιο είναι εξαιρετικά απίθανο να πραγματοποιηθεί. Ο υπογράφων μπορεί επίσης να ελέγξει ότι r Φ 0. Αν ο υπογράφων παρατηρήσει ότι r = 0 ή s = 0, θα πρέπει να παραχθεί μια νέα τιμή του k.

## 3.5.2 Το σχήμα υπογραφών ElGamal

Το σχήμα υπογραφών ElGamal είναι ένας τυχαιοκρατικός μηχανισμός υπογραφών. Παράγει ψηφιακές υπογραφές με παράρτημα σε δυαδικά μηνύματα οποιουδήποτε μήκους και απαιτεί μια συνάρτηση διασποράς h: {0, 1}* — Zp, όπου p είναι ένας μεγάλος πρώτος αριθμός. Ο DSA είναι μια παραλλαγή του μηχανισμού υπογραφών ElGamal.

Αλγόριθμος Παραγωγή κλειδιών για το σχήμα υπογραφών ElGamal
Κάθε οντότητα δημιουργεί ένα δημόσιο κλειδί και το αντίστοιχο ιδιωτικό κλειδί.
Κάθε οντότητα Α θα πρέπει να κάνει τα εξής:

1. Να παραγάγει έναν μεγάλο τυχαίο πρώτο p και έναν γεννήτορα α της πολλαπλασιαστικής ομάδας Z*p).
2. Να επιλέξει έναν τυχαίο ακέραιο a, 1 < a < p - 2.
3. Να υπολογίσει το y = α"2 modp
4. Το δημόσιο κλειδί της Α είναι (p, α, y) το ιδιωτικό κλειδί της Α είναι το a.
Η οντότητα Α υπογράφει ένα δυαδικό μήνυμα m οποιουδήποτε μήκους. Μια οντότητα Β μπορεί να επαληθεύσει την υπογραφή αυτή χρησιμοποιώντας το δημόσιο κλειδί της Α.

1. *Παραγωγή υπογραφής*. Η οντότητα Α θα πρέπει να κάνει τα εξής:

i) Να επιλέξει έναν τυχαίο μυστικό ακέραιο k, 1 < k < p - 2, με gcd(k, p - 1) = 1.
ii) Να υπολογίσει το r = αι modp (π.χ., χρησιμοποιώντας τον Αλγόριθμο 2.143).
iii) Να υπολογίσει το k 1 mod (p - 1) (π.χ., χρησιμοποιώντας τον Αλγόριθμο 2.142).
iv) Να υπολογίσει το s = k-1 {h(m) - ar} mod (p - 1).
v) Η υπογραφή της Α για το m είναι το ζεύγος (r, s).
Αλγόριθμος Παραγωγή και επαλήθευση υπογραφών ElGamal

2. *Επαλήθευση*. Για να επαληθεύσει την υπογραφή (r, s) της Α στο m, ο Β θα πρέπει να κάνει τα εξής:
i) Να προμηθευτεί το αυθεντικό δημόσιο κλειδί (p, α, y) της Α.
ii) Να επαληθεύσει ότι 1 < r <p - 1 αν όχι, τότε να απορρίψει την υπογραφή.
iii) Να υπολογίσει το υ1 = y rr s mod p.
iv) Να υπολογίσει τα h(m) και υ2 = α h(m) mod p.
Απόδειξη ότι η επαλήθευση της υπογραφής λειτουργεί. Αν η υπογραφή δημιουργήθηκε από την Α, τότε s = k 1 {h(m) - ar} (mod p-1). Πολλαπλασιάζοντας και τα δύο μέλη με k προκύπτει ks = h(m) - ar (modp-1) και αναδιατάσσοντας τους όρους προκύπτει h(m) = ar + ks (modp-1). Αυτό συνεπάγεται ότι α h(m) = α ar+ks = ^fr" (mod p). Επομένως, υ1 = υ2, που είναι το ζητούμενο.

Παράδειγμα (παραγωγή υπογραφής ElGamal με τεχνηέντως μικρές παραμέτρους)
Παραγωγή κλειδιών. Η Α επιλέγει τον πρώτο p = 2357 και έναν γεννήτορα α = 2 της ομάδας Z2357. Η Α επιλέγει το ιδιωτικό κλειδί a = 1751 και υπολογίζει το y = α"* modp = 21751 mod2357 = 1185. Το δημόσιο κλειδί της Α είναι (p = 2357, α = 2, y = 1185).
Παραγωγή υπογραφής. Χάριν απλότητας, τα μηνύματα θα είναι ακέραιοι από το Zp και h(m)= m (δηλ. για το παράδειγμα αυτό θεωρούμε ότι η συνάρτηση h είναι η ταυτοτική συνάρτηση). Για να υπογράψει το μήνυμα m = 1463 η Α επιλέγει έναν τυχαίο ακέραιο k = 1529, υπο¬λογίζει το r = αk mod p = 21529 mod 2357 = 1490 και το k 1 mod (p - 1) = 245. Τελικά η Α υπολογίζει το s = 245{1463 - 1751(1490)} mod 2356 = 1777. Η υπογραφή της Α για το m =1463 είναι το ζεύγος (r = 1490, s = 1777).
*Επαλήθευση υπογραφής*. Ο Β υπολογίζει τα υ1 = 11851490 ¦ 14901777 mod 2357 = 1072, h(m) = 1463 και υ2 = 21463 mod 2357 = 1072. Επειδή υ1 = υ2, ο Β αποδέχεται την υπογραφή.

***Σημείωση*** (ασφάλεια των υπογραφών ElGamal)
(i) Ο αντίπαλος μπορεί να προσπαθήσει να πλαστογραφήσει την υπογραφή της Α στο

μήνυμα m επιλέγοντας έναν τυχαίο ακέραιο k και υπολογίζοντας το r = aiΓ mod p. Ο αντίπαλος πρέπει μετά να προσδιορίσει το s = k 1 {h(m) - ar}mod (p - 1). Αν το πρόβλημα διακριτού λογαρίθμου είναι υπολογιστικά ανέφικτο, ο αντίπαλος δεν μπορεί παρά να διαλέξει ένα s στην τύχη η πιθανότητα επιτυχίας είναι μόνο 1/p, η οποία είναι αμελητέα για μεγάλα p.

(ii) Για κάθε υπογεγραμμένο μήνυμα πρέπει να επιλέγεται διαφορετικό k διαφορετικά, το ιδιωτικό κλειδί μπορεί να προσδιοριστεί με μεγάλη πιθανότητα ως εξής. Υποθέτουμε ότι s1 = k _1{h(m1) - ar} mod (p - 1) και s2 = k -1{h(m2) - ar} mod (p - 1). Τότε (s1 - s2)k = (h(m1) - h(m2)) (modp - 1). Αν s1 - s2 ί 0 (modp - 1), τότε k = (s1 - s2) _1(h(m1) - h(m2)) mod (p - 1). Άπαξ και το k είναι γνωστό, το a βρίσκεται εύκολα.

(iii) Αν δεν γίνεται χρήση συνάρτησης διασποράς h, η εξίσωση υπογραφής είναι s = k _1{m -ar} mod (p - 1). Είναι τότε εύκολο για έναν αντίπαλο να εξαπολύσει μια επίθεση υπαρ-

v) Να αποδεχτεί την υπογραφή, αν και μόνο αν υ1 = υ2.
Επιλέγει ένα ζεύγος ακεραίων (u, υ) με gcd^, p - 1) = 1. Υπολογίζει r = α uyu mod p = O"^" mod p και s = - iv- mod (p - 1). Το ζεύγος (r, s) είναι μια έγκυρη υπογραφή για το μήνυμα m = su mod (p - 1), αφού (α"O-ar) = αuyv = r.

(iv) Το βήμα 2ii στον αλγόριθμο αυτό απαιτεί από αυτόν που κάνει την επαλήθευση να ελέγξει αν 0 < r < p. Αν δεν γίνει αυτός ο έλεγχος τότε ο αντίπαλος μπορεί να υπογράφει μηνύματα δικής του επιλογής, με την προϋπόθεση ότι έχει μια υπογραφή που έχει δημιουργηθεί από την οντότητα A, ως εξής. Υποθέτουμε ότι (r, s) είναι μια υπογραφή για το μήνυμα m η οποία έχει παραχθεί από την A. Ο αντίπαλος διαλέγει ένα μήνυμα m' δικής του επιλογής και υπολογίζει τα h(m') και u = h(m')-[h(m)] 1 mod (p - 1) (υποθέτοντας ότι υπάρχει το [h(m)] 1 mod (p - 1)). Υπολογίζει μετά το s' = su mod (p - 1) και το r' τέτοιο, ώστε r' = ru (mod p - 1) και r' = r (mod p). Το τελευταίο είναι πάντοτε δυνατό με βάση το Κινέζικο Θεώρημα Υπολοίπων (Γεγονός 2.120). Το ζεύγος (r', s') είναι μια υπογραφή για το μήνυμα m' η οποία θα γίνονταν αποδεκτή από τον αλγόριθμο επαλήθευσης αν αγνοούνταν το βήμα 2ii.

***Σημείωση*** (ασφάλεια βασισμένη στην επιλογή παραμέτρων)
(i) (επίθεση λογισμού δεικτών) Ο πρώτος p θα πρέπει να είναι αρκούντως μεγάλος για να παρεμποδίσει τη χρήση αποδοτικών μεθόδων του λογισμού δεικτών.

(ii) (επίθεση Pohlig-Hellman) Ο p - 1 θα πρέπει να διαιρείται με έναν πρώτο αριθμό q αρκούντως μεγάλο για να παρεμποδίσει μια επίθεση διακριτού λογαρίθμου Pohlig-Hellman

(iii) (ασθενείς γεννήτορες) Ας υποθέσουμε ότιp = 1 (mod 4) και ότι ο γεννήτορας α ικανοποιεί τις ακόλουθες συνθήκες:

(α) ο α διαιρεί τον (p - 1) και

(β) ο υπολογισμός λογαρίθμων στην υποομάδα S τάξεως α της Z*p μπορεί να γίνει αποδοτικά (παραδείγματος χάρη, αν μπορεί να εξαπολυθεί στην S μια επίθεση Pohlig-Hellman .
Είναι τότε δυνατό για τον αντίπαλο να κατασκευάσει υπογραφές (χωρίς τη γνώση του ιδιωτικού κλειδιού της A) οι οποίες θα γίνουν αποδεκτές από τον αλγόριθμο επαλήθευσης. Για να το δούμε αυτό, ας υποθέσουμε ότι p - 1 = oq.

Για να υπογράψει ένα μήνυμα m ο αντίπαλος κάνει τα εξής: (α) Υπολογίζει το t - (p - 3)/2 και θέτει r = q.

(γ) Προσδιορίζει το z τέτοιο, ώστε = yq (mod p), όπου y είναι το ιδιωτικό κλειδί της A. (Αυτό είναι δυνατό διότι τα α< καιyq είναι στοιχεία της ομάδας S και το aq είναι γεννήτορας της S.) (γ) Υπολογίζει το s = t ¦ {h(m) - qz} mod (p - 1).

(δ) Το ζεύγος (r, s) είναι μια υπογραφή στο m η οποία θα γίνει αποδεκτή
Η επίθεση αυτή λειτουργεί επειδή ικανοποιείται η εξίσωση επαλήθευσης fyr = aA(m) (mod p). Για να το δούμε αυτό, παρατηρούμε αρχικά ότι aq = -1 (modp), α = -q- (modp) και ότι q(p-1))2 = -1 (mod p). (Η τελευταία ισοτιμία προκύπτει από το γεγονός ότι το α είναι ένας γεννήτορας της ομάδας Z*p και q = α-1 (mod p).) Από τις ισοτιμίες αυτές προκύπτει ότι q' = q(p-1))2q-1 = - q- = a (mod p). Τώρα, rsyr = (q')[h(m)-qz]yq = ah(m)a-qzyq = ah(m)y-qyq =ah(-m) (modp). Να σημειωθεί ότι, στην περίπτωση που το α = 2 είναι ένας γεννήτορας, οι συνθήκες που καθορίζονται παραπάνω στο (iii) ικανοποιούνται τετριμμένα.Η επίθεση μπορεί να αποφευχθεί αν το α επιλεγεί ως γεννήτορας μιας υποομάδας της Z*p τάξεως έναν πρώτο, αντί ως γεννήτορας της ίδιας της Z*p .

***Σημείωση*** (χαρακτηριστικά επιδόσεων των υπογραφών ElGamal)
(i) Η παραγωγή υπογραφών είναι σχετικά γρήγορη, απαιτώντας μία ύψωση σε δύναμη της αριθμητικής υπολοίπων (α* mod p), τον διευρυμένο Ευκλείδειο αλγόριθμο (για τον υπολογισμό του k 1 mod (p - 1)) και δύο πολλαπλασιασμούς της αριθμητικής υπολοίπων. (Η αφαίρεση της αριθμητικής υπολοίπων είναι αμελητέα συγκρινόμενη με τον πολλαπλασιασμό αριθμητικής υπολοίπων.) Η ύψωση σε δύναμη και η εφαρμογή του διευρυμένου Ευκλείδειου αλγορίθμου μπορεί να γίνει off-line, οπότε η παραγωγή υπογραφής (σε στιγμιότυπα στα οποία είναι δυνατός ο προ-υπολογισμός) απαιτεί μόνο δύο (on-line) πολλαπλασιασμούς της αριθμητικής υπολοίπων.

(ii) Η επαλήθευση υπογραφών είναι πιο δαπανηρή, απαιτώντας τρεις υψώσεις σε δύναμη. Κάθε ύψωση σε δύναμη (χρησιμοποιώντας απλοϊκές τεχνικές) απαιτεί -\\gp~\ πολλαπλασιασμούς της αριθμητικής υπολοίπων, κατά μέσο όρο, για ένα συνολικό κόστος πολλαπλασιασμών. Οι υπολογιστικές δαπάνες μπορούν να μειωθούν τροποποιώντας ελαφρώς την επαλήθευση. Υπολογίζουμε το υ1 = OL'h(m)yrrs mod p και δεχόμαστε την υπογραφή ως έγκυρη, αν και μόνο αν υ1 = 1. Τώρα, το υ1 μπορεί να υπολογιστεί πιο αποδοτικά κάνοντας τις τρεις υψώσεις σε δύναμη συγχρόνως το συνολικό κόστος είναι τώρα περίπου 15 [lg p ] πολλαπλασιασμοί της αριθμητικής υπολοίπων, σχεδόν 2.5 φορές πιο αποδοτικό ως προς το κόστος απ' ότι προηγούμενα.

(iii) Οι υπολογισμοί της επαλήθευσης υπογραφών εκτελούνται όλοι modulo p, ενώ οι υπολογισμοί της παραγωγής υπογραφών γίνονται modulo (p - 1).
Σημείωση 4 (συνιστώμενα μεγέθη παραμέτρων) Δεδομένης της πρόσφατης προόδου που έχει σημειωθεί στο πρόβλημα διακριτού λογαρίθμου στο ΙΤp , ένα modulus p των 512 bit παρέχει μικρού μεγέθους ασφάλεια από μια συντονισμένη επίθεση. Στα 1996, συστήνεται modulus p των 768 bit τουλάχιστο. Για μακροχρόνια ασφάλεια θα πρέπει να χρησιμοποιούνται moduli των 1024 bit ή μεγαλύτερα.
***Σημείωση*** (παράμετροι καθολικής εφαρμογής) Όλες οι οντότητες μπορεί να προτιμήσουν να χρησιμοποιήσουν τον ίδιο πρώτο αριθμό p και γεννήτορα α, οπότε τα p και α δεν είναι απαραίτητο να είναι τμήμα του δημόσιου κλειδιού.

***Παραλλαγές του σχήματος ElGamal***

Έχουν προταθεί πολλές παραλλαγές του βασικού σχήματος υπογραφών ElGamal. Οι περισσότερες από αυτές αλλάζουν αυτό που συνηθίζεται να αναφέρεται ως εξίσωση υπογραφής. Μετά από κατάλληλη αναδιάταξη αυτή η εξίσωση υπογραφής μπορεί να γραφτεί ως u = αυ + kw mod (ρ - 1), όπου u = h(m), υ = r και w = s (δηλ., h(m) = ar + ks mod (ρ - 1)). Άλλες εξισώσεις υπογραφής μπορούν να ληφθούν επιτρέποντας στα u, υ και w να πάρουν τις τιμές s, r και h(m) με διαφορετική σειρά. Ο πίνακας παρουσιάζει τις 6 δυνατότητες.

***Σημείωση*** (σύγκριση παραλλαγών του σχήματος υπογραφών ElGamal)
Παραλλαγές της εξίσωσης υπογραφής ElGamal. Οι εξισώσεις υπογραφής υπολογίζονται modulo (ρ - 1) η επαλήθευση γίνεται modulo ρ.

Πίνακας 3.5.2.1

| | u | v | w | Εξίσωση υπογραφής | Επαλήθευση |
|---|---|---|---|---|---|
| | | | | | ah(m) = (aayrs |
| 1 | h(m) | T | s | h(m) — ar + ks | ah(m) = (a«)v |
| 2 | h(m) | S | r | him) = as + kr | |
| 3 | s | T | h(m) | s — ar + kh(m) | |
| 4 | s | h(m) | r | s = ah(m) + kr | aT = (a.a)srk(m) |
| 5 | T | s | h(m) | r = as + kh{m)<br>(a.a)srk(m) | |
| 6 | T | h(m) | s | r = ah(m) + ks | |

(i) Μερικές από τις εξισώσεις υπογραφής που παρουσιάζονται στον πίνακα είναι πιο αποδοτικές στον υπολογισμό απ' ότι η αρχική εξίσωση ElGamal. Παραδείγματος χάρη, οι εξισώσεις (3) και (4) του πίνακα δεν απαιτούν τον υπολογισμό του αντίστροφου για τον προσδιορισμό της υπογραφής s. Οι εξισώσεις (2) και (3) απαιτούν από τον υπογράφοντα τον υπολογισμό του a -1 mod (ρ - 1), αλλά αυτή η συγκεκριμένη ποσότητα χρειάζεται να υπολογιστεί μόνο μία φορά.

(ii) Οι εξισώσεις επαλήθευσης (2) και (4) περιλαμβάνουν την παράσταση rr. Μέρος της ασφάλειας των σχημάτων υπογραφών που βασίζονται σε αυτές τις εξισώσεις υπογραφής είναι το δυσεπίλυτο της εύρεσης λύσεων σε μια παράσταση της μορφής X = c (mod ρ) για συγκεκριμένο c. Το πρόβλημα αυτό εμφανίζεται να είναι δυσεπίλυτο για μεγάλες τιμές του ρ, αλλά δεν έχει τύχει της ίδιας προσοχής με το πρόβλημα διακριτού λογαρίθμου.

(ii) Το γενικευμένο σχήμα υπογραφών ElGamal
Το σχήμα ψηφιακών υπογραφών ElGamal, που αρχικά περιγράφηκε στα πλαίσια της πολλαπλασιαστικής ομάδας Z*ρ , μπορεί να γενικευτεί εύκολα προκειμένου να λειτουργεί σε μια πεπερασμένη αβελιανή ομάδα G(Στα Μαθηματικά, μια αβελιανή ομάδα (ή αντιμεταθετική ομάδα) είναι μια ομάδα (A,0) στην οποία ισχύει η ιδιότητα αοβ=βοα για κάθε α,β εA. Οι αβελιανές ομάδες πήραν την ονομασία τους από τον Νορβηγό μαθηματικό Νιλς Χένρικ Άμπελ (Nils Henrik Abel). Η χρήση της λέξης «αβελιανή» έχει γίνει τόσο κοινή στα Μαθηματικά, ώστε καθιερώθηκε να γράφεται με μικρό «α»). Ο Αλγόριθμος Παραγωγής και επαλήθευσης υπογραφών γενικευμένου ElGamal απαιτεί μια κρυπτογραφική συνάρτηση διασποράς
h: {0, 1}* —> Z
όπου n είναι το πλήθος των στοιχείων του G.
Υποθέτουμε ότι κάθε στοιχείο r e G μπορεί να αναπαρασταθεί στο δυαδικό σύστημα έτσι ώστε να ορίζεται το h(r).

***Αλγόριθμος Παραγωγή κλειδιών για το γενικευμένο σχήμα υπογραφών ElGamal***

Κάθε οντότητα επιλέγει μια πεπερασμένη ομάδα G- έναν γεννήτορα της G- τα δημόσια και ιδιωτικά κλειδιά.
Κάθε οντότητα A θα πρέπει να κάνει τα εξής:

1. Να επιλέξει μια κατάλληλη κυκλική ομάδα G τάξεως n, με γεννήτορα α.
(Υποθέτουμε
ότι η G γράφεται πολλαπλασιαστικά.)

2. Να επιλέξει έναν τυχαίο μυστικό ακέραιο a, 1 < a < n - 1. Να υπολογίσει το στοιχείο ομάδας y = α".

3. Το δημόσιο κλειδί της A είναι το (α, y), μαζί με μια περιγραφή του τρόπου πολλαπλασιασμού των στοιχείων στην ομάδα G το ιδιωτικό κλειδί της A είναι το a.

***Αλγόριθμος Παραγωγή και επαλήθευση υπογραιφών γενικευμένου ElGamal***

Η οντότητα A υπογράφει ένα δυαδικό μήνυμα m οποιουδήποτε μήκους. Μια οντότητα B μπορεί να επαληθεύσει την υπογραφή αυτή χρησιμοποιώντας το δημόσιο κλειδί της A.

1. *Παραγωγή υπογραφής*. Η οντότητα Α θα πρέπει να κάνει τα εξής:
i) Να επιλέξει έναν τυχαίο μυστικό ακέραιο k, 1 < k < n - 1, με gcd(k, n) = 1.
ii) Να υπολογίσει το στοιχείο ομάδας r = α k.
iii) Να υπολογίσει το k -1 mod n.
iv) Να υπολογίσει τα h(m) και h(r).
v) Να υπολογίσει το s = k-1 {h (m) - ah (r)} mod n.
vi) Η υπογραφή της Α για το m είναι το ζεύγος (r, s).

2. *Επαλήθευση*. Για να επαληθεύσει την υπογραφή (r, s) της Α στο m, ο Β θα πρέπει να κάνει τα εξής:
i) Να προμηθευτεί το αυθεντικό δημόσιο κλειδί (α, y) της Α.
ii) Να υπολογίσει τα h(m) και h(r).
iii) Να υπολογίσει το υ1 = yh(-r) ¦ VS .
iv) Να υπολογίσει το υ2 = αίί
v) Να αποδεχτεί την υπογραφή, αν και μόνο αν υ1 = υ2.

Παράδειγμα (υπογραφές γενικευμένου ElGamal με τεχνηέντως μικρές παραμέτρους)
*Παραγωγή κλειδιών*. Ας θεωρήσουμε το πεπερασμένο σώμα F25 που είναι κατασκευασμένο από το ανάγωγο πολυώνυμο f (x) = x5 + X2 + 1 επί του F2. Τα στοιχεία του σώματος αυτού είναι οι 31 δυαδικές 5-άδες, μαζί με την 00000. Το στοιχείο α =(00010) είναι γεννήτορας της ομάδας G = F*,, που είναι η πολλαπλασιαστική ομάδα του σώματος. Η τάξη αυτής της ομάδας G είναι n = 31. Έστω h: {0, 1}* — Z31 μια συνάρτηση διασποράς. Η οντότητα Α επιλέγει το ιδιωτικό κλειδί a = 19 και υπολογίζει y = α"2 = (00010)19 = (00110). Το δημόσιο κλειδί της Α είναι (α = (00010),y = (00110)).
*Παραγωγή υπογραφής*. Για να υπογράψει το μήνυμα m = 10110101, η Α επιλέγει έναν τυχαίο ακέραιο k = 24 και υπολογίζει τα r = α24 = (11110) και k 1 mod 31 = 22. Η Α μετά υπολογίζει, h(m) = 16 και h(r) = 7 (έχουμε επινοήσει τις τιμές διασποράς για το παράδειγμα αυτό) και s = 22 ¦ {16 - (19)(7)} mod 31 = 30. Η υπογραφή της Α για το μήνυμα m είναι (r = (11110), s= 30).
*Επαλήθευση υπογραφής*. Ο Β υπολογίζει, h(m) = 16, h(r) = 7, υ1 = yh(r)rs = (00110)7(11110)30 =(11011) και υ2 = υ2 = α16 = (11011). Ο Β αποδέχεται την υπογραφή αφού υ1 = υ2.

**Σημείωση** (ασφάλεια του γενικευμένου ElGamal) Ένα μεγάλο μέρος της ασφάλειας του Αλγορίθμου εναπόκειται στο δυσεπίλυτο του προβλήματος διακριτού λογαρίθμου στην ομάδα G. Τα περισσότερα από τα σχόλια για την ασφάλεια εφαρμόζονται στο γενικευμένο σχήμα ElGamal.

**Σημείωση**(πράξεις υπογραφής και επαλήθευσης) Η παραγωγή απαιτεί υπολογισμούς στην ομάδα G (δηλ., r = α1") και υπολογισμούς στο Zn. Η επαλήθευση υπογραφών απαιτεί υπολογισμούς μόνο στην ομάδα G.

**Σημείωση** (γενικευμένο ElGamal με χρήση ελλειπτικών καμπυλών) Μια από τις πιο πολλά υποσχόμενες υλοποιήσεις είναι η περίπτωση όπου η πεπερασμένη ομάδα G κατασκευάζεται από το σύνολο των σημείων μιας ελλειπτικής καμπύλης επί ενός πεπερασμένου σώματος Fq. Το πρόβλημα διακριτού λογαρίθμου σε ομάδες αυτού του τύπου εμφανίζεται να είναι δυσκολότερο από το πρόβλημα διακριτού λογαρίθμου στην

πολλαπλασιαστική ομάδα ενός πεπερασμένου σώματος. Αυτό συνεπάγεται ότι το q μπορεί να επιλεγεί μικρότερο απ' ότι για τις αντίστοιχες υλοποιήσεις σε ομάδες όπως η G = Fq*

### 3.5.3 Το σχήμα υπογραφών Schnorr

Μια γνωστή παραλλαγή του σχήματος ElGamal είναι το σχήμα υπογραφών του Schnorr. Όπως με τον DS), αυτή η τεχνική χρησιμοποιεί μια υποομάδα της ΊΤρ , τάξεως q, όπου ρ είναι κάποιος μεγάλος πρώτος αριθμός. Η μέθοδος απαιτεί επίσης μια συνάρτηση διασποράς h: {0, 1}* — Zq. Η παραγωγή κλειδιών για το σχήμα υπογραφών Schnorr είναι η ίδια με την παραγωγή κλειδιών του DSA με τη διαφορά ότι δεν υπάρχουν περιορισμοί για τα μεγέθη των ρ και q.
Αλγόριθμος Παραγωγή και επαλήθευση υπογραφών Schnorr
Η οντότητα Α υπογράφει ένα δυαδικό μήνυμα m οποιουδήποτε μήκους. Μια οντότητα Β μπορεί να επαληθεύσει την υπογραφή αυτή χρησιμοποιώντας το δημόσιο κλειδί της Α.

1. *Παραγωγή υπογραφής*. Η οντότητα Α θα πρέπει να κάνει τα εξής:
i) Να επιλέξει έναν τυχαίο μυστικό ακέραιο k, 1 < k < q - 1.
ii) Να υπολογίσει τα r = 0/ mod ρ, e = h(m\\r) και s = ae + k mod q.
iii) Η υπογραφή της Α για το m είναι το ζεύγος (s, e).

2. *Επαλήθευση*. Για να επαληθεύσει την υπογραφή (s, e) της Α στο m, ο Β θα πρέπει να κάνει τα εξής:

Απόδειξη ότι η επαλήθευση της υπογραφής λειτουργεί. Αν η υπογραφή δημιουργήθηκε από την Α, τότε υ = αsy~e = αsy~ae = αk = r (mod ρ). Επομένως, h(m\^) = h(m\\r) και e' = e.
Παράδειγμα (σχήμα υπογραφών του Schnorr με τεχνηέντως μικρές παραμέτρους)
*Παραγωγή κλειδιών*. Η Α επιλέγει τους πρώτους ρ = 129841 και q = 541 εδώ, (ρ - 1)/q = 240. Η Α μετά επιλέγει έναν τυχαίο ακέραιο g = 26346 e Z*ρ και υπολογίζει το α = 26346240 mod ρ = 26. Αφού α Φ 1, το α παράγει τη μοναδική κυκλική υποομάδα της Έ*ρ τάξεως 541. Στη συνέχεια η Α επιλέγει το ιδιωτικό κλειδί a = 423 και υπολογίζει το y = 26423 mod ρ = 115917. Το δημόσιο κλειδί της Α είναι (ρ = 129841, q = 541, α = 26, y = 115917).
*Παραγωγή υπογραφής*. Για να υπογράψει το μήνυμα m = 11101101, η Α επιλέγει έναν τυχαίο αριθμό k = 327 τέτοιον, ώστε 1 < k < 540, και υπολογίζει τα r = 26327 mod ρ = 49375 και e = h(m\\r) = 155 (έχουμε επινοήσει την τιμή διασποράς για το παράδειγμα αυτό). Τελικά, η Α υπολογίζει το s = 423 * 155 + 327 mod 541 = 431. Η υπογραφή για το m είναι (s = 431, e =155).
*Επαλήθευση υπογραφής*. Ο Β υπολογίζει, υ = 26431 115917~155 mod ρ = 49375 και e' = h(m\^) = 155. Ο Β αποδέχεται την υπογραφή διότι e = e'.

***Σημείωση*** (χαρακτηριστικά επιδόσεων για το σχήμα Schnorr) Η παραγωγή υπογραφών απαιτεί μία ύψωση σε δύναμη modulo ρ και έναν πολλαπλασιασμό modulo

i) Να προμηθευτεί το αυθεντικό δημόσιο κλειδί (ρ, q, α, y) της Α.

ii) Να υπολογίσει τα υ = αsy~e mod ρ και e' = h(m\^).

iii) Να αποδεχτεί την υπογραφή, αν και μόνο αν e' = e.
Η ύψωση σε δύναμη modulo ρ θα μπορούσε να γίνει off-line. Ανάλογα με τον αλγόριθμο διασποράς που χρησιμοποιείται, ο χρόνος υπολογισμού του h(m\\r) θα πρέπει να είναι σχετικά μικρός. Η επαλήθευση απαιτεί δύο υψώσεις σε δύναμη modulo ρ. Αυτές οι δύο υψώσεις σε δύναμη μπορούν να υπολογιστούν με ένα κόστος περίπου 1.17 υψώσεις σε δύναμη. Η χρήση της υποομάδας τάξεως q δεν βελτιώνει σημαντικά την υπολογιστική

αποδοτικότητα σε σχέση με το σχήμα ElGamal, αλλά παρέχει μικρότερες υπογραφές (για το ίδιο επίπεδο ασφάλειας) από εκείνες που παράγονται με τη μέθοδο ElGamal.

### 3.5.4 Το σχήμα υπογραφών ElGamal με ανάκτηση μηνύματος

Το σχήμα ElGamal και οι παραλλαγές του που εξετάσαμε μέχρι τώρα είναι όλα τυχαιοκρατικά σχήματα ψηφιακών υπογραφών με παράρτημα (δηλ. το μήνυμα είναι απαραίτητο στα δεδομένα εισόδου του αλγορίθμου επαλήθευσης). Αντίθετα, ο μηχανισμός υπογραφών έχει το χαρακτηριστικό ότι το μήνυμα μπορεί να ανακτηθεί από την ίδια την υπογραφή. Επομένως, η παραλλαγή αυτή του ElGamal παρέχει μια τυχαιοκρατική ψηφιακή υπογραφή με ανάκτηση μηνύματος.
Για το σχήμα αυτό, ο χώρος υπογραφής είναι MS = Ί , ρ πρώτος, και ο χώρος υπογραφών είναι S = Έ x % , q πρώτος, όπου ο q διαιρεί τον (ρ - 1). Έστω R μια συνάρτηση περίσσειας από το σύνολο μηνυμάτων M στο MS. Η παραγωγή κλειδιών είναι ή ίδια με την παραγωγή κλειδιών στον DSA, με τη διαφορά ότι δεν υπάρχουν περιορισμοί για τα μεγέθη των ρ και q.

*Αλγόριθμος Παραγωγής και επαλήθευσης υπογραφών Nyberg-Rueppel*

Η οντότητα Α υπογράφει ένα μήνυμα m e M. Μια οντότητα Β μπορεί να επαληθεύσει την υπογραφή της Α και να ανακτήσει το μήνυμα m από την υπογραφή.
Για να επαληθεύσει την υπογραφή (e, s) της Α στο m, ο Β θα πρέπει να κάνει τα εξής:

i) Να προμηθευτεί το αυθεντικό δημόσιο κλειδί (ρ, q, α, y) της Α.

ii) Να επαληθεύσει ότι 0 < e <ρ αν όχι, να απορρίψει την υπογραφή.

iii) Να επαληθεύσει ότι 0 < s < q αν όχι, να απορρίψει την υπογραφή.

iv) Να επαληθεύσει ότι υ = αsy e mod ρ και in = υe mod ρ.

v) Να επαληθεύσει ότι m e MR αν rh £ MR , τότε να απορρίψει την υπογραφή.

vi) Να ανακτήσει το μήνυμα m = R- (m).

Απόδειξη ότι η επαλήθευση της υπογραφής λειτουργεί. Αν η Α δημιούργησε την υπογραφή, τότε υ = αsy— = αs-ae = αk (mod ρ). Επομένως, υe = αkmα-k = m (mod ρ), που είναι το ζητούμενο

<u>Παράδειγμα</u> (παραγωγή υπογραφής Nyberg-Rueppel με τεχνηέντως μικρές παραμέτρους)

*Παραγωγή κλειδιών.* Η οντότητα Α επιλέγει τους πρώτους ρ = 1256993 και q = 3571, όπου ο q διαιρεί τον (ρ - 1) εδώ, (ρ - 1)/q = 352. Η Α μετά επιλέγει έναν τυχαίο αριθμό g = 4207 e Zp και υπολογίζει το α = 42077352 mod ρ = 441238. Αφού α Φ 1, το α παράγει τη μοναδική κυκλική υποομάδα της Zp τάξεως 3571. Τελικά, η Α επιλέγει έναν τυχαίο ακέραιο a = 2774 και υπολογίζει το y = α " mod ρ = 1013657. Το δημόσιο κλειδί της Α είναι (ρ = 1256993, q =3571, α = 441238,y = 1013657), ενώ το ιδιωτικό κλειδί της Α είναι το a = 2774.

*Παραγωγή υπογραφής.* Για να υπογράψει ένα μήνυμα m, η Α υπολογίζει το m = R(m) = 1147892 (έχουμε επινοήσει την τιμή R(m) για το παράδειγμα αυτό). Η Α μετά επιλέγει τυχαία k = 1001 και υπολογίζει, r = α- k mod ρ = 441238-1001 mod ρ = 1188935, e = m r mod ρ =138207 και s = (2774)(138207) + 1001 mod q = 1088. Η υπογραφή για το m είναι

(e=138207, s = 1088).

*Επαλήθευση υπογραφής*. Ο Β υπολογίζει, υ = 44123810SS 1013657-US20J mod 1256993 = 504308 και m = υ 138207 mod 1256993 = 1147892. Ο Β επαληθεύει ότι m e MR και ανακτά το m = R (ι).

**Σημείωση** (ασφάλεια του σχήματος υπογραφών Nyberg-Rueppel)

Αφού ο Αλγόριθμος είναι μια παραλλαγή του βασικού σχήματος ElGamal

(i) εφαρμόζονται οι εκτιμήσεις ασφάλειας. Όπως ο DSA, αυτός ο μηχανισμός ElGamal με ανάκτηση μηνύματος στηρίζεται στη δυσκολία δύο σχετικών αλλά διαφορετικών προβλημάτων διακριτού λογαρίθμου .

(ii) παρέχει ανάκτηση μηνύματος, απαιτείται μια κατάλληλη συνάρτηση περίσσειας R για προφύλαξη από μια υπαρξιακή πλαστογράφηση. Όπως και στην περίπτωση του RSA, πρέπει να θεωρήσουμε πολύ προσεκτικά την πολλαπλασιαστική φύση αυτού του σχήματος υπογραφών όταν επιλέγουμε μια συνάρτηση περίσσειας R. Πρέπει να έχουμε υπόψη την ακόλουθη πιθανή επίθεση. Ας υποθέσουμε ότι m e M, m = R(m) και ότι (e, s) είναι μια υπογραφή για το m. Τότε είναι e = ïα— mod ρ , για κάποιον ακέραιο k, και s = ae + k mod q. Έστω mh * = md mod ρ, για κάποιον ακέραιο I. Αν s* = s + I mod q και m* e MR , τότε (e, s") είναι μια έγκυρη υπογραφή για το m* = R (m*) . Για να το δούμε αυτό, ας θεωρήσου¬με τον αλγόριθμο. Είναι υ = αs y e = αs+1 α-ae = αk+ι (mod ρ) και υe = αk+1ïα-k = ïα = m* (mod ρ). Αφού m* e MR , η πλαστογραφημένη υπογραφή (e, s*) θα γίνει αποδεκτή ως μια έγκυρη υπογραφή για το m .

(iii) Η επαλήθευση ότι 0 < e < ρ που δίνεται είναι κρί¬σιμης σημασίας. Ας υποθέσουμε ότι (e, s) είναι η υπογραφή της Α για το μήνυμα m. Τότε, e = mr mod ρ και s = ae + k mod q. Ο αντίπαλος μπορεί να χρησιμοποιήσει τηνυπογραφή αυτή για να υπολογίσει μια υπογραφή σε ένα μήνυμα m* δικής του επιλογής. Προσδιορίζει ένα e* τέτοιο, ώστε e* = mr (mod ρ) και e* = e (mod q). (Αυτό είναι δυνατό από το Κινέζικο Θεώρημα Υπολοίπων ). (Το ζεύγος (e*, s) θα περάσει τον αλγόριθμο επαλήθευσης με την προϋπόθεση ότι δεν ελέγχεται αν 0 < e* <ρ.

***Σημείωση*** (μια γενίκευση των υπογραφών ElGamal με ανάκτηση μηνύματος) Η έκφραση e = mr mod ρ παρέχει έναν σχετικά απλό τρόπο κρυπτογράφησης του m με κλειδί r και θα μπορούσε να γενικευτεί σε οποιονδήποτε αλγόριθμο συμμετρικού κλειδιού. Έστω ότι E = {Er : r e Zρ] είναι το σύνολο των μετασχηματισμών κρυπτογράφησης, όπου κάθε Er δεικτοδοτείται με ένα στοιχείο r e Z*ρ και είναι μια αμφίδρομη σημαντική αντιστοιχία από το MS = Z*ρ στο Z*ρ . Για οποιοδήποτε m e M, επιλέγουμε έναν τυχαίο ακέραιο k, 1 < k < q - 1, υπολογίζουμε r = α k mod ρ, και s = ae + k mod q. Το ζεύγος (e, s) είναι μια υπογραφή για το m. Η θεμελιώδης εξίσωση υπογραφών s = ae + k mod q είναι ένα μέσο δέσμευσης του ιδιωτικού κλειδιού της οντότητας Α και του μηνύματος m με ένα συμμετρικό κλειδί το οποίο μπορεί στη συνέχεια να χρησιμοποιηθεί για την ανάκτηση του μηνύματος από οποιαδήποτε άλλη οντότητα σε κάποια μεταγενέστερη χρονική στιγμή.

## 3.6 Ψηφιακές υπογραφές μιας χρήσης

Τα σχήματα ψηφιακών υπογραφών μιας χρήσης είναι μηχανισμοί ψηφιακών υπογραφών οι οποίοι μπορούν να χρησιμοποιηθούν για την υπογραφή ενός, το πολύ, μηνύματος διαφορετικά οι υπογραφές μπορούν να πλαστογραφηθούν. Απαιτείται ένα νέο δημόσιο κλειδί για κάθε μήνυμα που υπογράφεται. Οι δημόσιες πληροφορίες που είναι αναγκαίες για την επαλήθευση υπογραφών μιας χρήσης αναφέρονται συχνά ως παράμετροι επικύρωσης. Όταν συνδυάζονται υπογραφές μιας χρήσης με τεχνικές πιστοποίησης αυθεντικότητας των παραμέτρων επικύρωσης, τότε καθίστανται δυνατές πολλαπλές υπογραφές.
Τα περισσότερα, αλλά όχι όλα, σχήματα ψηφιακών υπογραφών μιας χρήσης έχουν το πλεονέκτημα ότι η παραγωγή και η επαλήθευση υπογραφών είναι πολύ αποδοτικές. Τα σχήματα ψηφιακών υπογραφών μιας χρήσης είναι χρήσιμα σε εφαρμογές όπως είναι οι έξυπνες κάρτες, όπου απαιτείται χαμηλή υπολογιστική πολυπλοκότητα.

### 3.6.1 Το σχήμα υπογραφών μιας χρήσης Rabin

Το σχήμα υπογραφών μιας χρήσης του Rabin ήταν ένα από τα πρώτα που προτάθηκαν για ψηφιακή υπογραφή οποιουδήποτε είδους. Επιτρέπει την υπογραφή ενός μεμονωμένου μηνύματος. Η επαλήθευση μιας υπογραφής απαιτεί την αλληλεπίδραση μεταξύ του υπογράφοντα και αυτού που επαληθεύει. Αντίθετα από άλλα σχήματα ψηφιακών υπογραφών, η επαλήθευση μπορεί να γίνει μόνο μία φορά. Αν και δεν είναι πρακτικό, το παρουσιάζουμε εδώ για ιστορικούς λόγους. Ο συμβολισμός που χρησιμοποιούμε στην ενότητα αυτή δίνεται παρακάτω στον Πίνακα 3.6.1.1.

Πίνακας 3.6.1.1

| Σύμβολο | Σημασία |
|---|---|
| Mo | 0 = η συμβολοσειρά μήκους l που αποτελείται από μηδενικά. |
| Mo | (7) 0l-e\| \|be-1 .^b1b0, όπου be-1 .^b1b0 είναι η δυαδική αναπαράσταση του i. |
| K | ένα σύνολο συμβολοσειρών των l bit. |
| E | ένα σύνολο μετασχηματισμών κρυπτογράφησης δεικτοδοτημένο από ένα σύνολο κλειδιών K. |
| Et | είναι ένας μετασχηματισμός κρυπτογράφησης που ανήκει στο E με t e K. Κάθε Et απεικονίζει συμβολοσειρές των l bit σε συμβολοσειρές των l bit. |
| h | μια δημόσια γνωστή μονόδρομη συνάρτηση διασποράς από το {0, 1}* στο {0, l} . |
| n | ένας θετικός ακέραιος ο οποίος χρησιμεύει ως παράμετρος ασφάλειας. |

***Αλγόριθμος Παραγωγής κλειδιών για το σχήμα υπογραφών μιας χρήσης Rabin***

Κάθε οντότητα Α επιλέγει ένα σχήμα κρυπτογράφησης συμμετρικού κλειδιού Ε, παράγει 2n τυχαίες συμβολοσειρές και δημιουργεί ένα σύνολο παραμέτρων επικύρωσης. Κάθε οντότητα Α θα πρέπει να κάνει τα εξής:

1. Να επιλέξει ένα σχήμα κρυπτογράφησης συμμετρικού κλειδιού Ε (π.χ., το DES).

2. Να παραγάγει 2n τυχαίες μυστικές συμβολοσειρές k1, k2, ..., k2n e K, δυαδικού μήκους l η κάθε μία.

3. Να υπολογίσει τα yi = Ek (M0 (i)), 1 < i < 2n.

4. Το δημόσιο κλειδί της Α είναι (y1, y2, ..., y2n)- το ιδιωτικό κλειδί της Α είναι (k1, k2, ..., k2n).

***Αλγόριθμος Παραγωγής και επαλήθευσης υπογραφών μιας χρήσης Rabin***

Η οντότητα Α υπογράφει ένα δυαδικό μήνυμα m οποιουδήποτε μήκους. Η επαλήθευση υπογραφών είναι αλληλεπιδραστική με την Α.
Για να επαληθεύσει την υπογραφή s2, ..., s2n) της Α στο m, ο Β θα πρέπει:

i) Να προμηθευτεί το αυθεντικό κλειδί (y1, y2, ..., y2n) της Α.

ii) Να υπολογίσει το h(m).

iii) Να επιλέξει n διαφορετικούς τυχαίους αριθμούς η, 1 < η < 2n, για 1 < j < n.

iv) Να ζητήσει από την Α τα κλειδιά kr ,1 < j < n.

v) Να επαληθεύσει την αυθεντικότητα των κλειδιών που παρέλαβε, υπολογίζοντας το Zj = Ek (M0 (rj)) και ελέγχοντας ότι zj = yr , για κάθε 1 < j < n.

vi) Να επαληθεύσει ότι sr = Ek (h(m)), 1 < j < n.

***Σημείωση*** (μεγέθη κλειδιών για υπογραφές μιας χρήσης του Rabin) Αφού ο Ε( εξάγει l bit, το δημόσιο και το ιδιωτικό κλειδί αποτελείται το καθένα από 2nl bit. Για n = 80 και l = 64, τα κλειδιά είναι μήκους 1289 bit το καθένα.

***Σημείωση*** (επίλυση αντιδικιών) Για την επίλυση ενδεχόμενων αντιδικιών μεταξύ της οντότητας Α που υπογράφει και της οντότητας Β, θα πρέπει να ακολουθηθεί η εξής διαδικασία:

1. Ο Β παρέχει σε ένα τρίτο έμπιστο μέλος (TTP) το μήνυμα m και την υπογραφή s2,— , s2n).

2. Το TTP παραλαμβάνει τα k1, k2, ., k2n από την Α.

3. Το TTP επαληθεύει την αυθεντικότητα του ιδιωτικού κλειδιού υπολογίζοντας το zi= Eki (M0(i)) και ελέγχοντας αν είναι yi = zi, 1 < i < 2n. Αν ο έλεγχος αυτός αποτυγχάνει, το TTP αποφαίνεται υπέρ του Β (δηλ., η υπογραφή θεωρείται έγκυρη).

4. Το TTP υπολογίζει το ui = Ek (h(m)), 1 < i < 2n. Αν ui = si για το πολύ n τιμές του i, 1 < i < 2n, η υπογραφή δηλώνεται ότι είναι πλαστογραφημένη και το TTP αποφαίνεται υπέρ της Α (η οποία αρνείται ότι έχει δημιουργήσει την υπογραφή). Αν n + 1 ή περισσότερες τιμές του i δίνουν ui = si, η υπογραφή θεωρείται έγκυρη και το TTP αποφαίνεται υπέρ του Β. Σημείωση 3 (σκεπτικό για πρωτόκολλο επίλυσης αντιδικιών) Το σκεπτικό για την επιδίκαση αντιδικιών στο σχήμα υπογραφών μιας χρήσης του Rabin, έχει ως εξής. Αν ο Β έχει προσπαθήσει να πλαστογραφήσει την υπογραφή της Α σε ένα νέο μήνυμα m', ο Β είτε χρειάζεται να προσδιορίσει τουλάχιστο ένα παραπάνω κλειδί k έτσι ώστε τουλάχιστο n + 1 τιμές του i να δώσουν ui = si, είτε να προσδιορίσει το m' τέτοιο, ώστε h(m) = h(m'). Αυτό θα είναι ανέφικτο αν ο αλγόριθμος συμμετρικού κλειδιού και η συνάρτηση διασποράς επιλεγούν κατάλληλα. Αν η Α προσπαθήσει να δημιουργήσει μια υπογραφή την οποία μπορεί αργότερα να απαρνηθεί, η Α πρέπει να εξασφαλίσει ότι ui = si για n ακριβώς τιμές του i και να ελπίζει ότι ο Β επιλέγει αυτές τις n τιμές στο βήμα 2iii της διαδικασίας επαλήθευσης, η πιθανότητα του οποίου είναι μόνο 1.

## 3.6.2 Το σχήμα υπογραφών μιας χρήσης Merkle

Το σχήμα ψηφιακών υπογραφών μιας χρήσης του Merkle διαφέρει σημαντικά από εκείνο του Rabin ως προς το ότι η επαλήθευση υπογραφών δεν είναι αλληλεπιδραστική με τον υπογράφοντα. Ένα TTP ή κάποιο άλλο έμπιστο μέσο απαιτείται προκειμένου να πιστοποιεί την αυθεντικότητα των παραμέτρων επικύρωσης που κατασκευάζονται.
Για να υπογράψουμε ένα μήνυμα m των n bit, σχηματίζουμε μια συμβολοσειρά w = m||c, όπου c είναι η δυαδική αναπαράσταση για τον αριθμό των μηδενικών στο m. Το c υποθέτουμε ότι είναι μια δυαδική συμβολοσειρά δυαδικού μήκους | lg nj + 1 με τα υψηλής τάξεως bit "παραγεμισμένα" με μηδενικά, αν είναι αναγκαίο. Επομένως, το w είναι μια συμβολοσειρά δυαδικού μήκους t = n + | lg nj + 1.

***Αλγόριθμος Παραγωγής και επαλήθευσης υπογραφών μιας χρήσης Merkle***

Η οντότητα Α υπογράφει ένα μήνυμα m δυαδικού μήκους n. Μια οντότητα Β μπορεί να επαληθεύσει την υπογραφή αυτή χρησιμοποιώντας το δημόσιο κλειδί της Α.

1. *Παραγωγή υπογραφής*. Η οντότητα Α θα πρέπει να κάνει τα εξής:
i) Να υπολογίσει το c, τη δυαδική αναπαράσταση για τον αριθμό των 0 στο m.
ii) Να σχηματίσει το w = m||c = (a1a2_at).
iii) Να προσδιορίσει τις θέσεις συντεταγμένων i1 < i2 < ... < iu στο w τέτοιες, ώστε ai = 1, 1 < j < u.
iv) Έστω = k ,1 < j < u.
v) Η υπογραφή της Α για το m είναι (s1, s2, ., su).

2. *Επαλήθευση*. Για να επαληθεύσει την υπογραφή (s1, s2, ., s2n) της A στο m, ο B θα πρέπει:

i) Να προμηθευτεί το αυθεντικό κλειδί (υ1, υ2, ..., υt) της A.

ii) Να υπολογίσει το c, τη δυαδική αναπαράσταση για τον αριθμό των 0 στο m.

iii) Να σχηματίσει το w = m||c = (a1a2_at).

iv) Να προσδιορίσει τις θέσεις συντεταγμένων i1 < i2 < . < iu στο w τέτοιες, ώστε aij = 1, 1 < j < u.

v) Να αποδεχτεί την υπογραφή, αν και μόνο αν vi = h(s.), για κάθε 1 < j < u.

***Σημείωση*** (ασφάλεια του σχήματος υπογραφών μιας χρήσης του Merkle) Έστω ότι m είναι ένα μήνυμα, w = m||c η δυαδική συμβολοσειρά που σχηματίζει (s1, s2, ., su) μια υπογραφή για το m. Αν h είναι μια ανθιστάμενη προεικόνας συνάρτηση διασποράς, το ακόλουθο επιχείρημα δείχνει ότι δεν μπορεί να πλαστογραφηθεί μια υπογραφή για ένα μήνυμα m' Φ m. Έστω w' = m'||c', όπου c' είναι η συμβολοσειρά των (Llg nj + 1) bit η οποία είναι η δυαδική αναπαράσταση για τον αριθμό των μηδενικών στο m'. Αφού ένας αντίπαλος έχει πρόσβαση μόνο σε εκείνο το τμήμα του ιδιωτικού κλειδιού του υπογράφοντα το οποίο αποτελείται από τα (s1, s2, ., su), το σύνολο των συντεταγμένων θέσεων στο m που έχουν ένα 1 πρέπει να είναι υποσύνολο των συντεταγμένων θέσεων στο m που έχουν ένα 1 (διαφορετικά, το m θα έχει ένα 1 σε κάποια θέση όπου το m έχει ένα 0 και ο αντίπαλος θα χρειαστεί ένα στοιχείο του ιδιωτικού κλειδιού που δεν έχει αποκαλυφθεί από τον υπογράφοντα). Αλλά αυτό σημαίνει ότι το m' έχει περισσότερα μηδενικά από το m και ότι c' > c (όταν θεωρηθούν ως ακέραιοι). Στην περίπτωση αυτή, το c' θα έχει ένα 1 σε κάποια θέση όπου το c έχει ένα 0. Ο αντίπαλος θα χρειαζόταν ένα στοιχείο του ιδιωτικού κλειδιού, που αντιστοιχεί στη θέση αυτή, το οποίο δε έχει αποκαλυφθεί από τον υπογράφοντα.

**Σημείωση** (αποθηκευτικές και υπολογιστικές απαιτήσεις)
(i) Για να υπογράψει κάποιος ένα μήνυμα m των n bit το οποίο έχει k άσους χρειάζεται l ¦(n + Llg nj + 1) bit αποθηκευτικού χώρου για τις παραμέτρους επικύρωσης (δημόσιοκλειδί) και l ¦ (n + Llg nj + 1) bit για το ιδιωτικό κλειδί. Η υπογραφή απαιτεί l ¦ (k + k)bit αποθήκευσης, όπου k είναι ο αριθμός των άσσων στη δυαδική αναπαράσταση του n-k. Παραδείγματος χάρη, αν n = 128, l = 64 και k = 72, τότε το δημόσιο και το ιδιωτικό κλειδί απαιτούν 8704 bit (1088 byte) το καθένα. Η υπογραφή απαιτεί 4800 bit (600 byte).

(ii) Το ιδιωτικό κλειδί μπορεί να γίνει μικρότερο σχηματίζοντας τα ki από μία μόνο τιμή σπόρου (seed). Παραδείγματος χάρη, αν k* είναι μια συμβολοσειρά δυαδικού μήκους τουλάχιστο l, τότε σχηματίζουμε τα ki = h(k*||i), 1 < i < t. Αφού μόνο ο σπόρος k* χρειάζεται να αποθηκευτεί, το μέγεθος του ιδιωτικού κλειδιού ελαττώνεται δραστικά.

(iii) Η παραγωγή υπογραφών είναι πολύ γρήγορη, μη απαιτώντας υπολογισμό. Η επαλήθευση υπογραφών απαιτεί τον υπολογισμό της συνάρτησης διασποράς για λιγότερο από n + Llg nj + 1 τιμές.
***Σημείωση*** (βελτίωση της αποδοτικότητας του σχήματος μιας χρήσης του Merkle)
Ο αλγόριθμος απαιτεί l ¦ (n + Llg nj + 1) bit για καθένα από τα κλειδιά (ιδιωτικό και δημόσιο).

Το δημόσιο κλειδί πρέπει αναγκαστικά να είναι τόσο μεγάλο επειδή ο αλγόριθμος υπογραφής θεωρεί μεμονωμένα bit του μηνύματος. Το σχήμα μπορεί να γίνει πιο αποδοτικό αν ο αλγόριθμος υπογραφής θωρεί περισσότερα από ένα bit τη φορά. Ας υποθέσουμε ότι η οντότητα A επιθυμεί να υπογράψει ένα μήνυμα των kt bit. Γράφουμε m = m1||m2||_mt, όπου κάθε mi έχει δυαδικό μήκος k και το καθένα αναπαριστά έναν ακέραιο μεταξύ των 0 και 2k - 1 συμπεριλαμβανομένων. Ορίζουμε U = Σt=1(2k - mi) < 12k. Το U μπορεί να αναπαρασταθεί με lg U < Llg= u1||u2||_||ur, όπου κάθε ui έχει δυαδικό μήκος k. Σχηματίζουμε τη δυαδική συμβολοσειρά w = m1||m2||...mt||u1||u2||...||ur. Παράγουμε t + r τυχαίες δυαδικές συμβολοσειρές k1, k2, ..., kt+r 2k —1 και υπολογίζουμε τα vi = h (ki), 1 < i < t + r. Το ιδιωτικό κλειδί του τροποποιημένου σχήματος είναι (k1, k2, ..., kt+r) και το δημόσιο κλειδί είναι (υ,υ,...,vt+r). Η υπογραφή για το m είναι (S1,S2,...,st+r), όπου st = hmi (ki),1 < i < t, και si = hUi (kt+i), 1 < i < r. Εδώ, το hc συμβολίζει την c-πλή σύνθεση της h με τον εαυτό της.

Τα προσαρτημένα bit στο μήνυμα λειτουργούν σαν ένα άθροισμα ελέγχου (check¬sum) ως εξής. Δοθέντος ενός στοιχείου si = ha(k;), ένας αντίπαλος μπορεί εύκολα να υπολογίσει την τιμή ha+δ(^) για 0 < δ < 2k - a, αλλά δεν είναι σε θέση να υπολογίσει την τιμή ha-δ, για οποιοδήποτε δ > 0, αν η h είναι μια μονόδρομη συνάρτηση διασποράς. Για να πλαστογραφήσει μια υπογραφή σε ένα νέο μήνυμα, ο αντίπαλος μπορεί μόνο να ελαττώσει την τιμή του αθροίσματος ελέγχου, το οποίο θα καταστήσει αδύνατο για αυτόν, τον υπολογισμό των απαιτούμενων τιμών διασποράς στα προσαρτημένα kr bit.
Παράδειγμα (υπογραφή περισσοτέρων του ενός bit τη φορά) Στο παράδειγμα αυτό εξηγούμε την τροποποίηση του σχήματος Merkle . Έστω m = m1||m2||m3||m4, όπου m1 = 1011, m2 = 0111, m3 = 1010 και m4 = 1101. Τα m1, m2, m3, και m4 είναι οι δυαδικές αναπαραστάσεις των 11, 7, 10 και 13, αντίστοιχα. Είναι U = (16 - m1) + (16 - m2) + (16 - m3) + (16 - m4) = 5 + 9 + 6 +3 = 23. Στο δυαδικό σύστημα, U = 10111. Σχηματίζουμε το w = m||00010111.

Η υπογραφή είναι

*s2, s3, s4, s5, s6), όπου s1 = h11(k1), s2 =7 10 13 1 7*

*h (k2), s3 = h (k3), s4 = h (k4), s5 = h (k5) και s6 = h (k6).*

Αν ο αντίπαλος προσπαθήσει να μεταβάλλει το μήνυμα, μπορεί να εφαρμόσει τη συνάρτηση h σε μερικά si. Αυτό έχει ως συνέπεια να αυξηθεί το άθροισμα των χρησιμοποιούμενων εκθετών (δηλ. το Σ mi) και επομένως, να μειωθεί η διαφορά
12d — Σ mt. Ο αντίπαλος δεν θα είναι σε θέση να τροποποιήσει τα δύο τελευταία τμήματα διότι απαιτείται να ελαττώσει η h το άθροισμα.
Αλλά, αφού η heίναι ανθιστάμενη προεικόνιση, δεν είναι δυνατό να υπολογιστεί η h_1 από τον αντίπαλο.

## 3.6.3 Δέντρα πιστοποίησης αυθεντικότητας και υπογραφές μιας χρήσης

Στην ενότητα αυτή περιγράφουμε το πώς ένα δέντρο πιστοποίησης αυθεντικότητας μπορεί να χρησιμοποιηθεί σε συνδυασμό με ένα σχήμα υπογραφών μιας χρήσης προκειμένου να παράσχει ένα σχήμα το οποίο επιτρέπει πολλαπλές υπογραφές. Ένα μικρό παράδειγμα θα χρησιμεύσει ως επεξήγηση του πώς γίνεται αυτό.
Ένα δέντρο πιστοποίησης αυθεντικότητας για το σχήμα μιας χρήσης του Merkle.

Θεωρούμε το σχήμα υπογραφών μιας χρήσης για την υπογραφή μηνυμάτων των n bit. Έστω h : {0, 1}* — {0, 1} μια ανθιστάμενη προεικόνιση συνάρτηση διασποράς και t = n +Llg nj+ 1. Ένα δυαδικό δέντρο 5 κορυφών, που δημιουργήθηκε από μια οντότητα A κατά τη διάρκεια υπογραφής πέντε μηνυμάτων m0, m1, m2, m3, m4.

μήνυμα mi ιδιωτικές παράμετροι Xi, Ui, Wi

δημόσιες παράμετροι Yi, Vi, Zi

τιμές διασποράς h(Yi), h(V), h(Zi)

Ri h(h(Y)||h(V)||h(Z))

υπογραφή SA(mi, Xi)

παράμετροι επικύρωσης Yi

Στον Πίνακα3.6.3.1 συνοψίζουμε τις παραμέτρους και τις υπογραφές που σχετίζονται με κάθε ετικέτα κορυφής του δυαδικού δέντρου.
Για να περιγράψουμε το πώς χρησιμοποιείται το δέντρο για την επαλήθευση των υπογραφών, ας θεωρήσουμε το μήνυμα m4 και την υπογραφή SA(m4, X4). Η υπογράφουσα A πρώτα παρέχει στον B τις παραμέτρους επικύρωσης Y4. Ο B πρέπει μετά να πεισθεί ότι το Y4 είναι ένα αυθεντικό σύνολο παραμέτρων επικύρωσης που δημιουργήθηκε από την A.
Για να φέρει εις πέρας κάτι τέτοιο, η A παρέχει στον B μια ακολουθία τιμών που απαριθμούνται παρακάτω:

1. h(V4), h(Z4)- ο B υπολογίζει την h(Y4) και μετά την R4 = h(h(Y4)||h(V4)||h(Z4)).

2. SA(R4, W1) και Z1 ο B επαληθεύει την υπογραφή στην R4

3. h(Y1), h(V1)^ ο B υπολογίζει την h(Z1) και μετά την R1 = h(h(Y1)||h(V1)||h(Z1)).

4.SA(Ri, U0) και Vo ο B επαληθεύει την υπογραφή h(Y0), h(Z0)- ο B υπολογίζει την h(V0) και μετά την R0 = h(h(Yo)\\h(Vo)\\h(Z0)).

5. υπογραφή του TTP για την R0- ο B επαληθεύει την υπογραφή χρησιμοποιώντας έναν αλγόριθμο που αρμόζει στον μηχανισμό υπογραφών για το TTP.
Το δυαδικό δέντρο των 5 κορυφών θα μπορούσε να επεκταθεί απεριόριστα από οποιοδήποτε φύλλο καθώς δημιουργούνται περισσότερες υπογραφές από την A. Το μήκος της μακρύτερης διαδρομής πιστοποίησης αυθεντικότητας (ή ισοδύναμα, το βάθος του δέντρου) προσδιορίζει τη μέγιστη ποσότητα πληροφορίας την οποία πρέπει να παράσχει η A στον B προκειμένου ο B να επαληθεύσει την υπογραφή ενός μηνύματος που σχετίζεται με μια κορυφή.

| Μήνυμα | Ετικέτα κορυφής | Υπογραφή στην ετικέτα κορυφής | Παράμετροι Πιστοποίησης Αυθεντικότητας |
|---|---|---|---|
| m1 | R1 | Υπογραφή του TTP | - |
| m2 | R2 | SA(R1, *U0 )* | V0, *h(Y0)*, h(Z0) |
| m3 | R3 | *S A (R 2* , W0) | Z0, h(Y0), h(V0) |
| m4 | R4 | *SA(R*3, *U*1) | V1, h(Y1), h(Z1) |
| | | SA(R4, W1) | Z1, h(Y1), h(V1) |

Πίνακας 3.6.3.1

***Παράμετροι και υπογραφές σχετιζόμενες με κορυφές του δυαδικού δέντρου***

Το σχήμα των Godwasser, Micali και Rivest (GMR) είναι ένα σχήμα υπογραφών μιας χρήσης που απαιτεί ένα ελεύθερο-διχάλας (claw-free) ζεύγος μεταθέσεων. Όταν συνδυάζεται με ένα δέντρο της διαδικασίας πιστοποίησης αυθεντικότητας παρέχει έναν μηχανισμό για υπογραφή περισσοτέρων του ενός μηνύματος. Το σχήμα GMR είναι αξιοσημείωτο καθώς ήταν ο πρώτος μηχανισμός ψηφιακών υπογραφών που αποδείχθηκε ότι ήταν ασφαλής εναντίον μιας προσαρμόσιμης επίθεσης επιλεγμένου μηνύματος. Αν και το σχήμα GMR δεν είναι πρακτικό, έχουν προταθεί κάποιες παραλλαγές του οι οποίες υποδεικνύουν ότι η έννοια δεν είναι αμιγώς θεωρητικής σπουδαιότητας.

**Ορισμός** Έστω gi : X — X, i = 0, 1, δύο μεταθέσεις ορισμένες σε ένα πεπερασμένο σύνολο X. Οι g0 και g1 λέγονται ότι είναι ένα ελεύθερο-διχάλας ζεύγος (claw-free pair) μεταθέσεων αν είναι υπολογιστικά ανέφικτο να βρούμε x, y e X τέτοια, ώστε g0(x) = g1(y). Μια τριάδα (x, y, z) στοιχείων από το X με g0(x) = g1(y) = z λέγεται διχάλα (claw). Αν και οι δύο gi, i = 0, 1, έχουν την ιδιότητα ότι, δοθείσης επιπρόσθετης πληροφορίας, είναι υπολογιστικά εφικτό να υπολογίσουμε τις g-1, g-1, αντίστοιχα, οι μεταθέσεις λέγονται ελεύθερο-διχάλας ζεύγος μεταθέσεων κερκόπορτας.
Για να αποτελούν οι g0, g1 ένα ελεύθερο-διχάλας ζεύγος, ο υπολογισμός των g-1 για i = 0, 1, πρέπει να είναι υπολογιστικά ανέφικτος για όλα ουσιαστικά τα x e X. Διότι, αν ο υπολογισμός της g1-1 (και ομοίως της g0-1 ) ήταν εφικτός, θα μπορούσε κάποιος να επιλέξει ένα x e X, να υπολογίσει τις τιμές g0(x) = z και g-1(z) = y, για να λάβει μια διχάλα (x, y, z).

**Παράδειγμα** (ελεύθερο-διχάλας ζεύγος μεταθέσεων κερκόπορτας)
Έστω n = pq, όπου p = 3

*-1*

*n*

*(mod 8) και q = 7 (mod 8).*

*Για αυτή την επιλογή των p και q, είναι (—) = 1 αλλά - 1 i Qn*

*n*

*1 και 0 < x < — }.*

*Επίσης ορίζουμε,*

*g0: Dn — Dn και g1: Dn — Dn με 2*

*x mod n, αν x mod n < -2-*

*-x mod n, αν x mod n > -2-*

*και*

*2 2 n*

*4x mod n, αν 4x mod n < —g1(x):2 2 n- 4xmodn, αν 4xmodn> 2*

Αν η παραγοντοποίηση του n είναι δυσεπίλυτη, τότε οι g0, g1 σχηματίζουν ένα ελεύθερο-διχάλας ζεύγος μεταθέσεων κερκόπορτας αυτό μπορούμε να το δούμε ως εξής:

(i) (g0 και gi είναι μεταθέσεις στο Dn) Αν g0(x) = g0(y), τότε x = y (mod n) (x = -y (mod n) δεν είναι δυνατόν διότι - 1 ί Qn), οπότε x = ±y (mod n). Αφού 0 < x, y < n/2, τότε x = y και επομένως η g0 είναι μια μετάθεση στο Dn. Με παρόμοιο επιχείρημα δείχνουμε ότι η g1 είναι μια μετάθεση στο Dn.

(ii) (g0 και g1 είναι ελεύθερες-διχάλας) Ας υποθέσουμε ότι υπάρχει μια εφικτή μέθοδος εύρεσης των x, y e Dn τέτοιων, ώστε g0(x) = g1(y). Τότε x = 4y (mod n) (x = - 4y (modn) είναι αδύνατο, διότι - 1 ί Qn), οπότε (x - 2y)(x + 2y) = 0 (mod n). Αφού ) = 1 και (-±ny) = - 1, είναι x ΐ ± 2y (mod n) και συνεπώς, ο gcd(x - 2y, n) δίνει έναν μη τετριμμένο παράγοντα του n. Αυτό αντιφάσκει με την υπόθεση ότι η παραγοντοποίηση του n είναι δυσεπίλυτη.

(iii) (g0 και g1 είναι ελεύθερο-διχάλας ζεύγος κερκόπορτας) Η γνώση της παραγοντοποίησης του n μας επιτρέπει να υπολογίσουμε τις g-1 και g-1. Επομένως, οι g0, g1 αποτελούν ένα ελεύθερο-διχάλας ζεύγος μεταθέσεων κερκόπορτας. Ο παρακάτω πίνακας περιγράφει τις g0 και g1.
**Παράδειγμα** (ελεύθερο-διχάλας ζεύγος μεταθέσεων για τεχνηέντως μικρές παραμέτρους) Έστω p = 11, q = 7 και n = pq =77. D77 = {x: ) = 1 και 0 < x < 38} = {1, 4, 6, 9, 10, 13, 15, 16, 17, 19, 23, 24, 25, 36, 37}.

***Αλγόριθμος Παραγωγής κλειδιών για το σχήμα υπογραφών μιας χρήσης GMR***

Κάθε οντότητα A θα πρέπει να κάνει τα εξής:
1. Να επιλέξει ένα ελεύθερο-διχάλας ζεύγος μεταθέσεων κερκόπορτας σε κάποιο σύνολο X. (Είναι «κερκόπορτας» ως προς το ότι η A μπορεί από μόνη της να υπολογίσει τις g-1 και g-1.)

2. Να επιλέξει ένα τυχαίο στοιχείο r e X. (Το r λέγεται παράμετρος επικύρωσης.)

| *x* | *1* | *4* | *6* | *9* | *10* | *13* | *15* | *16* | *17* | *19* | *23* | *24* | *25* | *36* | *37* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *g0(x)* | *14* | *16* | *36* | *4 16* | *23* | *15* | *6* | *25* | *19 1* | *24* | *10* | *37 6* | *9* | *13* | |
| *g1(x)* | | *13* | *10* | | *15* | *17* | *24* | *23* | | *19* | *37* | | *36* | *25* | *9* |

Να σημειωθεί ότι οι $g_0$ και $g_1$ είναι μεταθέσεις στο $D_{77}$.

3. Το δημόσιο κλειδί της A είναι (g0, g1, r) το ιδιωτικό κλειδί της A είναι (g-1, g-1). Παρακάτω, ο συμβολισμός της σύνθεσης των συναρτήσεων g0, g1 που συνήθως γράφεται ως go ° g1, απλοποιείται σε g0g1. Επίσης, το (g0g\)(r) θα γράφεται ως gog1(r). Ο χώρος υπογραφής MS αποτελείται από δυαδικές συμβολοσειρές οι οποίες είναι ελεύθερες-προθέματος.

***Αλγόριθμος Παραγωγής και επαλήθευσης υπογραφών μιας χρήσης GMR***

Η Α υπογράφει μια δυαδική συμβολοσειρά m = m1m2...mt. Ο Β επαληθεύει χρησιμοποιώντας το δημόσιο κλειδί της Α.

*1. Παραγωγή υπογραφής*. Η οντότητα Α θα πρέπει να κάνει τα εξής:

(α) Να υπολογίσει την τιμή Sr (m) = Π;-0 gmn, . (r).

(β) Η υπογραφή της Α για το m είναι η Sr(m).

2. *Επαλήθευση*. Για να επαληθεύσει την υπογραφή Sr(m) της Α στο m, ο Β θα πρέπει να κάνει τα εξής:

(α) Να λάβει το αυθεντικό δημόσιο κλειδί (g0, g1, r) της Α.

(β) Να υπολογίσει την τιμή r' = Y['i=1 gmt (Sr (m)).

(γ) Να αποδεχτεί την υπογραφή, αν και μόνο αν r '= r.

Απόδειξη ότι η επαλήθευση της υπογραφής λειτουργεί.
tt t-1
r' = Π gmit (Sr (m)) = Π gmit Π gmlj (r)
i=1 i=1 j=0= g o g o•••o g o g1 o g1 o••. g1(r) = r
Άρα, r'= r, όπως απαιτείται.

***Σημείωση*** (κωδικοποίηση μηνύματος και ασφάλεια) Το σύνολο των μηνυμάτων τα οποία μπορούν να υπογραφούν πρέπει να προέρχεται από ένα σύνολο δυαδικών συμβολοσειρών οι οποίες είναι ελεύθερες-προθέματος (prefix-free). (Παραδείγματος χάρη, οι 101 και 10111 δεν μπορούν να είναι στον ίδιο χώρο διότι η 101 είναι πρόθεμα της 10111.) Μια μέθοδος για να πραγματοποιήσουμε κάτι τέτοιο είναι να κωδικοποιήσουμε μια δυαδική συμβολοσειρά b1b2...bl ως b1b1b2b2...blbl01. Για να δούμε το γιατί η απαίτηση «ελεύθερη προθέματος» είναι αναγκαία, ας υποθέσουμε ότι m = m1m2...mt είναι ένα μήνυμα του οποίου η υπογραφή είναι η Sr (m) = Π;-0 . (r).

Αν m '= m1m2... m„, u < t,

τότε ένας αντίπαλος μπορεί να βρει εύκολα μια έγκυρη υπογραφή για το m' από την Sr(m) υπολογίζοντας την
tu-1 1
Sr (m') = Π; gmj (Sr (m)) = Π; gmu-t (r).
j=u+1 z=0

***Σημείωση*** ( «μιας χρήσης») Για να δούμε ότι το σχήμα υπογραφών GMR είναι σχήμα μιας χρήσης, ας υποθέσουμε ότι δύο ελεύθερα προθέματος μηνύματα m = m1m2...mt και m'= n\n2...nu είναι υπογεγραμμένα και τα δύο με την ίδια παράμετρο επικύρωσης r.

Τότε είναι Sr (m) = Π 0gmit_i (r) και Sr (m') = Π=0 Sn]^ (r)

Επομένως, Y['i=\ Sm. (Sr (m)) = r = Πu=i gn. (Sr (m')).

Αφού ο χώρος μηνυμάτων είναι ελεύθερος-προθέματος, υπάρχει ένας μικρότερος όλων δείκτης h > 1 για τον οποίο είναι mh Φ nh. Επειδή κάθε gj είναι μια αμφίδρομη σημαντική αντιστοιχία, έπεται ότι

$$\prod_{i=h}^{u} g_{mi}(Sr(m)) = \prod_{i=h}^{} g_{ni}(Sr(m'))$$

ή

$$g_{mh} \prod_{i=h+1}^{} g_{mt}(Sr(m)) = g_{nh} \prod_{i=h+1}^{} g_{nt}(Sr(m'))$$

Παίρνοντας x = Π=h+1 gm (Sr (m)) και y = Π=h+1 g„. (Sr (m')), ο αντίπαλος έχει μια διχάλα (x,y, gmh (X)). Αυτό παραβιάζει τη βασική υπόθεση ότι είναι υπολογιστικά ανέφικτο να βρούμε μια διχάλα. Θα πρέπει να σημειωθεί ότι αυτό δεν σημαίνει κατ' ανάγκη ότι η υπογραφή για ένα νέο μήνυμα μπορεί να πλαστογραφηθεί. Η εύρεση μιας διχάλας παραγοντοποιεί το modulus n και επιτρέπει σε κάποιον να υπογράψει έναν απεριόριστο αριθμό νέων μηνυμάτων (δηλ. μια ολική κατάρρευση του συστήματος είναι δυνατή.)
Παράδειγμα (το GMR με τεχνηέντως μικρές παραμέτρους.)
Παραγωγή κλειδιών. Έστω ότι *n, p, q, g0, g1* είναι εκείνα που δίνονται στο Παράδειγμα
Η *A* επιλέγει την παράμετρο επικύρωσης *r = 15 e D77.*
Παραγωγή υπογραφής. Έστω *m = 1011000011* το προς υπογραφή μήνυμα. Τότε *Sr(m) = g{ 1 ° g{ 1 °g- 1 °g- 1 °g- 1 ° g0o1 ° g i i ° g i i °g-1 °g-i(15) = 23.*
Η υπογραφή της *A* για το μήνυμα *m* είναι *23.*
Επαλήθευση υπογραφής. Για να επαληθεύσει την υπογραφή, ο *B* υπολογίζει *r' = g1° g0 ° g1 ° g1 ° g0 ° g0 ° g0 ° g0 ° g1 ° g1(23) = 15.* Αφού *r = r',o B* αποδέχεται την υπογραφή.

*Σχήμα GMR με δέντρα πιστοποίησης αυθεντικότητας*

Για την υπογραφή πολλαπλών μηνυμάτων με τη βοήθεια του σχήματος υπογραφών μιας χρήσης GMR, απαιτούνται δέντρα πιστοποίησης αυθεντικότητας. Αν και εννοιολογικά είναι παρόμοια με τη μέθοδο , μόνο τα φύλλα χρησιμοποιούνται για την παραγωγή της υπογραφής. Πριν δώσουμε τις λεπτομέρειες, είναι αναγκαία μια επισκόπηση και κάποιος επιπρόσθετος συμβολισμός.

***Ορισμός***
_Πλήρες δυαδικό δέντρο με k επίπεδα είναι ένα δυαδικό δέντρο το οποίο έχει 2k+l - 1 κορυφές και 2k φύλλα. Τα φύλλα λέγεται ότι είναι στο επίπεδο k του δέντρου.
Έστω T ένα πλήρες δυαδικό δέντρο με k επίπεδα. Επιλέγουμε δημόσιες παραμέτρους Y1, Y2, ..., Yn, όπου n = 2k. Σχηματίζουμε ένα δέντρο πιστοποίησης αυθεντικότητας T * από το T με ετικέττα ρίζας R (βλ. παρακάτω). Η R πιστοποιείται από ένα TTP και τοποθετείται σε ένα δημόσια διαθέσιμο αρχείο. Το T * μπορεί τώρα να χρησιμοποιηθεί για την πιστοποίηση

αυθεντικότητας οποιασδήποτε από τις Yi παρέχοντας τις τιμές διαδρομής πιστοποίησης αυθεντικότητας που σχετίζονται με τη διαδρομή πιστοποίησης αυθεντικότητας για την Yi. Κάθε Yi μπορεί τώρα να χρησιμοποιηθεί ως η δημόσια παράμετρος r για το σχήμα GMR. Οι λεπτομέρειες για την κατασκευή του δέντρου αυθεντικότητας T* έπονται.
Το δέντρο T * κατασκευάζεται αναδρομικά. Για την κορυφή ρίζας επιλέγουμε μια τιμή r και δύο δυαδικές συμβολοσειρές rL και rR των t bit. Υπογράφουμε τη συμβολοσειρά rL\\rR με το σχήμα GMR χρησιμοποιώντας τη δημόσια τιμή r. Η ετικέτα για τη ρίζα αποτελείται από τις τιμές r, rL, rR και Sr(rL\\rR). Για την πιστοποίηση αυθεντικότητας των τέκνων της κορυφής ρίζας, επιλέγουμε δυαδικές συμβολοσειρές b0L, b1L, b0R και b1R των t bit. Η ετικέτα για το αριστερό τέκνο της ρίζας είναι το σύνολο των τιμών rL, b0L, b1L, SrL Φ0L \\ bn) και η ετικέτα για το δεξιό τέκνο της ρίζας είναι το σύνολο των τιμών rR, b0R, b1R, SrR (b0R \\ bm). Χρησιμοποιώντας τις συμβολοσειρές b0L, b1L, b0R και b1R ως δημόσιες τιμές για τον μηχανισμό υπογραφής, μπορεί κάποιος να κατασκευάσει ετικέτες για τα τέκνα των τέκνων της ρίζας. Συνεχίζοντας με τον τρόπο αυτό, κάθε κορυφή του T * μπορεί να σημανθεί με ετικέτα. Κάθε φύλλο του δέντρου πιστοποίησης αυθεντικότητας T * μπορεί να χρησιμοποιηθεί για την υπογραφή ενός διαφορετικού δυαδικού μηνύματος m. Η διαδικασία υπογραφής χρησιμοποιεί ένα ελεύθερο-διχάλας ζεύγος μεταθέσεων g0, g1. Αν m είναι το προς υπογραφή δυαδικό μήνυμα και x είναι η δημόσια παράμετρος στην ετικέτα ενός φύλλου που δεν έχει χρησιμοποιηθεί για την υπογραφή ενός άλλου μηνύματος, τότε η υπογραφή για το m αποτελείται από την Sx(m) και τις ετικέτες διαδρομής πιστοποίησης αυθεντικότητας.

## 3.7 Άλλα σχήματα υπογραφών

Τα σχήματα υπογραφών που περιγράφουμε στην ενότητα αυτή δεν εμπίπτουν φυσιολογικά (RSA και συναφή σχήματα υπογραφών, σχήματα υπογραφών Fiat-Shamir, DSA και συναφή σχήματα υπογραφών, ή ψηφιακές υπογραφές μιας χρήσης).

### 3.7.1 Επιτηδευόμενες ψηφιακές υπογραφές

Ορισμός Επιτηδευόμενο σχήμα ψηφιακών υπογραφών είναι ένας μηχανισμός ψηφιακών υπογραφών που απαιτεί ένα άνευ όρων έμπιστο τρίτο μέλος (TTP) ως μέρος της παραγωγής και επαλήθευσης των υπογραφών.
Ο αλγόριθμος απαιτεί έναν αλγόριθμο κρυπτογράφησης δημόσιου κλειδιού E = {Ek: k e K}, όπου K είναι ο κλειδοχώρος. Ας υποθέσουμε ότι τα δεδομένα εισόδου και εξόδου κάθε Ek είναι συμβολοσειρές των l bit και έστω h: {0, 1}* — {0, 1}l μια μονόδρομη συνάρτηση διασποράς. Το TTP επιλέγει ένα κλειδί kT e K το οποίο διατηρεί μυστικό.
Για να επαληθεύσει μια υπογραφή, μια οντότητα πρέπει να έχει από κοινού με το TTP ένα συμμετρικό κλειδί.

***Αλγόριθμος Παραγωγή κλειδιών για επιτηδευόμενες υπογραφές***

Κάθε οντότητα επιλέγει ένα κλειδί και το μεταβιβάζει μυστικά με αυθεντικότητα στο TTP. Κάθε οντότητα A θα πρέπει να κάνει τα εξής:
1. Να επιλέξει ένα τυχαίο μυστικό κλειδί kA e K.
2. Μυστικά και με κάποιο αυθεντικό μέσο, καθιστά το kA διαθέσιμο στο TTP.

***Αλγόριθμος Παραγωγής και επαλήθευση υπογραφών για επιτηδευόμενες υπογραφές.***

Η οντότητα Α παράγει υπογραφές χρησιμοποιώντας τον EkA . Μια οντότητα Β μπορεί να επαληθεύσει την υπογραφή της Α με τη συνεργασία του TTP.

1. *Παραγωγή υπογραφής*. Για να υπογράψει ένα μήνυμα m, η Α θα πρέπει να κάνει τα εξής:
(α) Η Α υπολογίζει την H = h(m).
(β) Η Α κρυπτογραφεί την Η με τον Ε για να πάρει u= EkA (H).
(γ) Η Α στέλνει το u μαζί με κάποια συμβολοσειρά ταυτοποίησης IA στο TTP.
(δ) Το TTP υπολογίζει την Ει (u) για να πάρει την Η.
(ε) Το TTP υπολογίζει την s = Ekj (H \\ I A ) και στέλνει την s στην Α.
(στ) Η υπογραφή της Α για το m είναι s.

2. *Επαλήθευση*. Μια οντότητα Β μπορεί να επαληθεύσει την υπογραφή s της Α στο m κάνοντας τα εξής:
(α) Ο Β υπολογίζει την υ = (s).
(β) Ο Β στέλνει την υ και κάποια συμβολοσειρά ταυτοποίησης IB στο TTP.
(γ) Το TTP υπολογίζει την Ε-1 (υ) για να πάρει την s.
(δ) Το TTP υπολογίζει την (s) για να πάρει την Η \\ IA.
(ε) Το TTP υπολογίζει την w = E^b (H \\ I A ) και στέλνει την w στον Β.
(στ) Ο Β υπολογίζει την Ε-1 (w) για να πάρει την Η \\ IA.
(ζ) Ο Β υπολογίζει την Η (m) από το m.
(η) Ο Β αποδέχεται την υπογραφή, αν και μόνο αν Η' = Η.

***Σημείωση*** ( για την ασφάλεια του σχήματος επιτηδευόμενων υπογραφών) Η ασφάλεια βασίζεται στο επιλεγμένο σχήμα κρυπτογράφησης συμμετρικού κλειδιού και τη δυνατότητα διανομής κλειδιών στους συμμετέχοντες κατά έναν αυθεντικό τρόπο.
Αφού οι αλγόριθμοι συμμετρικού κλειδιού είναι τυπικά πολύ ταχύτεροι από τις τεχνικές δημόσιου κλειδιού, η παραγωγή και επαλήθευση υπογραφής είναι (σχετικά) πολύ αποδοτικές. Ένα μειονέκτημα είναι το ότι απαιτείται η αλληλεπίδραση με ΤΟΥΤΤΡ, η οποία θέτει μια κατά πολύ υψηλότερη επιβάρυνση στο TTP και απαιτεί επιπρόσθετες ανταλλαγές μηνυμάτων μεταξύ οντοτήτων και του TTP.

## 3.7.2 ESIGN(Efficient digital SIGNature - αποδοτική ψηφιακή υπογραφή)

Το ESIGN (συντομογραφία του Efficient digital SIGNature - αποδοτική ψηφιακή υπογραφή) είναι ένα άλλο σχήμα ψηφιακών υπογραφών του οποίου η ασφάλεια εναπόκειται στη δυσκολία παραγοντοποίησης ακεραίων. Είναι ένα σχήμα υπογραφών με παράρτημα και απαιτεί μια μονόδρομη συνάρτηση διασποράς h: {0,1}* — Zn.

*Αλγόριθμος Παραγωγής κλειδιών για το ESIGN*

Κάθε οντότητα παράγει ένα δημόσιο κλειδί και το αντίστοιχο δημόσιο κλειδί. Κάθε οντότητα Α θα πρέπει να κάνει τα εξής:

1. Να επιλέξει πρώτους p και q τέτοιους, ώστε p > q και οι p, q να είναι περίπου του ίδιου δυαδικού μήκους.

2. Να υπολογίσει το n = pq.

3. Να επιλέξει έναν θετικό ακέραιο k > 4.

4. Το δημόσιο κλειδί είναι (n, k) το ιδιωτικό κλειδί είναι (p, q).

***Αλγόριθμος Παραγωγής και επαλήθευσης υπογραφών ESIGN***

Ο αλγόριθμος υπογραφής υπολογίζει έναν ακέραιο s τέτοιον, ώστε το sk mod n να κείται σε ένα ορισμένο διάστημα που προσδιορίζεται από το μήνυμα. Η επαλήθευση καταδεικνύει ότι το sk mod n κείται όντως στο καθορισμένο διάστημα.

*1. Παραγωγή υπογραφής.* Για να υπογράψει ένα μήνυμα m, το οποίο είναι μια συμβολοσειρά οποιουδήποτε μήκους, η οντότητα A θα πρέπει να κάνει τα εξής:
(α) Να υπολογίσει την τιμή υ = h(m).
(β) Να επιλέξει έναν τυχαίο μυστικό ακέραιο x, 0 < x < pq.
(γ) Να υπολογίσει τις τιμές w = ((υ- xk) mod n)/(pq)~^ και y = w ¦ (kxkmod p.
(δ) Να υπολογίσει την s = x + ypq mod n. (ε) η υπογραφή της A για το m είναι s.

*2. Επαλήθευση.* Για να επαληθεύσει την υπογραφή s της A στο m, ο B θα πρέπει να κάνει τα εξής:

(α) Να προμηθευτεί το αυθεντικό δημόσιο κλειδί (n, k) της A.

(β) Να υπολογίσει τις τιμές

u =sk mod n και z = h(m).

(γ) Αν z < u < z + 2 1, να αποδεχτεί την υπογραφή διαφορετικά να την απορρίψει

***Απόδειξη*** ότι η επαλήθευση υπογραφής λειτουργεί. Παρατηρούμε ότι sk = (χ + ypqf = Σ ί-ο ί k ~l (yPq)1 = X + kypqx k l (mod n). Αλλά kx k-1y = w (mod p) και, συνεπώς, kx k-1y = w + lp για κάποιο l e Z.
Επομένως,

$$sk = \chi k + pq(w + lp) = \chi k + pqw = \chi k + (h(m) - \chi) \bmod n:$$

$$\chi + pqh(m) - \chi + jn + \varepsilon \pmod n, \text{ όπου } \varepsilon = (X1 - h(m)) \bmod pq.$$

$$\text{Επομένως, } sk = \chi k + h(m) - X1 + \varepsilon \pmod n.$$

Αφού 0 < ε < pq, έπεται ότι h(m) < sk mod n < h(m) +It'8 nl

**Παράδειγμα** (ESIGN για τεχνηέντως μικρές παραμέτρους)
Θεωρούμε ότι τα μηνύματα είναι ακέραιοι m, 0 < m < n και ότι η συνάρτηση διασποράς h είναι h(m) = m.

Παραγωγή κλειδιών. Η A επιλέγει τους πρώτους p = 17389 και q = 15401, k = 4, και

υπολογίζει το n = p2q = 4656913120721. Το δημόσιο κλειδί της Α είναι (n = 4656913120721, k = 4) το ιδιωτικό κλειδί της Α είναι (p = 17389, q = 15401).
Παραγωγή υπογραφής. Για να υπογράψει το μήνυμα m = 3111527988477, η Α υπολογίζει την υ = h(m) = 3111527988477 και επιλέγει χ = 14222 τέτοιο, ώστε 0 < χ <pq. Η Α μετά υπολογίζει, w = {(υ — χ1" )mod n^(pq)] = [284818192180^267807989] = [10635.16414] = 10636 και y = w^k—1)—1modp = 10636(4χ 142223)-1 mod17389 = 9567. Τελικά, η Α υπολογίζει την υπογραφή s = χ + ypq mod n = 2562119044985.

*Επαλήθευση υπογραφής.* Ο Β προμηθεύεται το δημόσιο κλειδί (n = 4656913120721, k = 4) της Α και υπολογίζει την τιμή u = sk mod n = 3111751837675. Αφού, 3111527988477 < 3111751837675 < 3111527988477 + 229, ο Β αποδέχεται την υπογραφή (εδώ είναι, Γ -jig n ] =29).

***Σημείωση*** (*ασφάλεια του ESIGN*)

(i) Το modulus n = p2q διαφέρει από ένα modulus RSA στο ότι έχει έναν επαναλαμβανόμενο παράγοντα του p. Είναι άγνωστο εάν moduli αυτής της μορφής είναι ευκολότερο ή όχι να παραγοντοποιηθούν από ακεραίους οι οποίοι είναι απλά το γινόμενο δύο διαφορετικών πρώτων.

(ii) Δεδομένης μιας έγκυρης υπογραφής για ένα μήνυμα m, ένας αντίπαλος θα μπορούσε να πλαστογραφήσει μια υπογραφή για ένα μήνυμα m' αν η h(m') είναι τέτοια, ώστε|ylg n| kh(m') < u < h(m') + 2' 1 (όπου u = s mod n). Αν βρεθεί ένα m' με την ιδιότητα αυτή, τότε η s θα είναι η υπογραφή γι' αυτό. Αυτό θα εμφανιστεί αν οι h(m) και h(m') συμφωνούν στα υψηλής τάξης (lg n)/3 bit. Υποθέτοντας ότι η h συμπεριφέρεται σαν μια τυχαία συνάρτηση, θα μπορούσαμε να περιμένουμε τη δοκιμή 2(lg n)/3 διαφορετικών τιμών του m πριν το παρατηρήσουμε αυτό.

(iii) Μια άλλη δυνατή προσέγγιση για πλαστογράφηση είναι να βρούμε ένα ζεύγος μηνυμάτων m και m τέτοιων, ώστε οι h(m) και h(m ) να συμφωνούν στα υψηλής τάξης (lg n)/3 bit. Από το παράδοξο των γενεθλίων, μπορούμε να περιμένουμε την εύρεση ενός τέτοιου ζεύγους σε O(2(lgn)/6) δοκιμές. Αν ο αντίπαλος είναι σε θέση να καταφέρει να υπογράψει το m ο νόμιμος υπογράφων, η ίδια υπογραφή θα είναι μια υπογραφή για το m .
(iv) Για το μέγεθος του ακεραίου n που είναι απαραίτητος για να καταστήσει την παραγοντοποίηση του n ανέφικτη, οι παραπάνω περιπτώσεις (ii) και (iii) είναι εξαιρετικά απίθανες δυνατότητες.

***Σημείωση*** (*χαρακτηριστικά επιδόσεων για υπογραφές ESIGN*)
Η παραγωγή υπογραφής είναι πολύ αποδοτική. Για μικρές τιμές του k (π.χ k = 4), το πλέον υπολογιστικά εντατικό μέρος είναι η αντιστροφή αριθμητικής υπολοίπων που απαιτείται στο βήμα 1 γ. Ανάλογα με την υλοποίηση, αυτή αντιστοιχεί σε έναν μικρό αριθμό πολλαπλασιασμών αριθμητικής υπολοίπων με modulus p. Για k = 4 και ένα modulus n των 768 bit, η παραγωγή υπογραφής ESIGN μπορεί να είναι μεταξύ μίας ή δύο τάξεων μεγέθους (10 ή 100 φορές) ταχύτερη από την παραγωγή υπογραφής RSA με ένα ισοδύναμο μέγεθος του modulus. Η επαλήθευση υπογραφής είναι επίσης πολύ αποδοτική και είναι συγκρίσιμη της αντίστοιχης RSA με έναν μικρό δημόσιο εκθέτη.

## 3.8 Υπογραφές με επιπρόσθετη λειτουργικότητα

Οι μηχανισμοί που περιγράψαμε στην ενότητα αυτή παρέχουν λειτουργικότητα πέρα από την πιστοποίηση αυθεντικότητας και τη μη απάρνηση. Στις περισσότερες περιπτώσεις συνδυάζουν ένα βασικό σχήμα ψηφιακών υπογραφών (πχ., RSA) με ένα συγκεκριμένο πρωτόκολλο προκειμένου να επιτευχθούν επιπρόσθετα χαρακτηριστικά τα οποία δεν παρέχει η βασική μέθοδος.

### 3.8.1 Σχήματα τυφλών υπογραφών

Αντίθετα απ' ότι τα σχήματα υπογραφών, τα σχήματα τυφλών υπογραφών (blind signature schemes) είναι διμερή πρωτόκολλα μεταξύ ενός αποστολέα Α και ενός υπογράφοντα Β. Η βασική ιδέα είναι η ακόλουθη. Ο Α στέλνει ένα κομμάτι πληροφοριών στον Β το οποίο ο Β υπογράφει και το επιστρέφει στον Α. Από την υπογραφή αυτή, ο Α μπορεί να υπολογίσει την υπογραφή του Β σε ένα a priori μήνυμα m της επιλογής του Α. Κατά την ολοκλήρωση του πρωτοκόλλου ο Β δεν γνωρίζει ούτε το μήνυμα m ούτε την υπογραφή που συσχετίστηκε με αυτό.

Ο *σκοπός* μιας τυφλής υπογραφής είναι να εμποδίσει τον υπογράφοντα Β στο να παρατηρήσει το μήνυμα που υπογράφει και την υπογραφή έτσι δεν είναι σε θέση αργότερα να συσχετίσει το υπογεγραμμένο μήνυμα με τον αποστολέα Α.

**Παράδειγμα** (εφαρμογές των τυφλών υπογραφών). Τα σχήματα τυφλών υπογραφών έχουν εφαρμογές εκεί όπου ο αποστολέας Α (ο πελάτης) δεν θέλει να μπορεί ο υπογράφων Β (η τράπεζα) να συσχετίζει ένα μήνυμα m και μια υπογραφή SB(m) σε μια συγκεκριμένη στιγμή του πρωτοκόλλου. Αυτό μπορεί να είναι σημαντικό σε εφαρμογές ηλεκτρονικού χρήματος όπου το μήνυμα m μπορεί να αναπαριστά μια χρηματική τιμή την οποία μπορεί να ξοδέψει ο Α. Όταν παρουσιάζονται τα m και SB(m) στον Β για πληρωμή, ο Β δεν είναι σε θέση να συμπεράνει ποιο μέλος είχε δώσει αρχικά την υπογεγραμμένη τιμή. Αυτό επιτρέπει στον Α να παραμένει ανώνυμος και έτσι δεν είναι δυνατό να καταγράφονται καταναλωτικά πρότυπα.

Ένα πρωτόκολλο τυφλών υπογραφών απαιτεί τις εξής συνιστώσες:

1. Έναν μηχανισμό ψηφιακών υπογραφών για τον υπογράφοντα Β. SB^) συμβολίζει την υπογραφή του Β στο χ.

2. Δύο συναρτήσεις f και g (γνωστές μόνο στον αποστολέα) τέτοιες, ώστε g(SB(f (m))) = SB(m). Η f λέγεται συνάρτηση τύφλωσης (blinding function), η g συνάρτηση αποτύφλωσης ή επαναφοράς (unblinding function) και η τιμή fm) τυφλωμένο μήνυμα.

Η ιδιότητα 2 θέτει πολλούς περιορισμούς στην επιλογή των SB και g.

*Πρωτόκολλο τυφλών υπογραφών του Chaum*

Ο αποστολέας Α δέχεται μια υπογραφή του Β σε ένα τυφλωμένο μήνυμα. Από αυτό ο Α υπολογίζει την υπογραφή του Β σε ένα μήνυμα m επιλεγμένο a priori από τον Α, $0 < m < n-1$.
Ο Β δεν έχει γνώση του μηνύματος m ούτε της υπογραφής που συσχετίζεται με το m.

1. *Συμβολισμός.*

Το δημόσιο και το ιδιωτικό κλειδί RSA του Β είναι (n, e) και d, αντιστοίχως. Το k είναι ένας τυχαίος μυστικός ακέραιος επιλεγμένος από τον Α που ικανοποιεί τις $0 < k < n - 1$ και $\gcd(n, k) = 1$.

2. *Δράσεις πρωτοκόλλου.*

i) (τύφλωση) Ο Α υπολογίζει, $m^* = mk^e \bmod n$ και το στέλνει στον Β.
ii) (υπογραφή) Ο Β υπολογίζει, $s^* = (m^*)^d \bmod n$, την οποία στέλνει στον Α.
iii) (επαναφορά) Ο Α υπολογίζει, $s = k\_1 s^* \bmod n$, που είναι η υπογραφή του Β στο m.

Παράδειγμα **(συνάρτηση τύφλωσης βασισμένη στο RSA)**
Έστω n = pq το γινόμενο δύο τυχαίων μεγάλων πρώτων. Ο αλγόριθμος υπογραφής SB για την οντότητα Β είναι το σχήμα υπογραφών RSA με δημόσιο κλειδί (n, e) και ιδιωτικό κλειδί d. Έστω ότι k είναι ένας συγκεκριμένος ακέραιος με gcd(n, k) = 1. Η συνάρτηση τύφλωσης f: Z n — Z n ορίζεται από την fm) = mke mod n και η συνάρτηση επαναφοράς g: Z n — Z n από την g(m) = k-1m mod n. Για την επιλογή αυτή των f, g και SB, είναι g(SB(f(m))) = g(SB((mke mod n)) = g(mdk mod n) = md mod n = SB(m), όπως απαιτείται από την ιδιότητα 2.

## 3.8.2 Σχήματα αδιαμφισβήτητων υπογραφών

Τα σχήματα αδιαμφισβήτητων υπογραφών (undeniable signature schemes) διακρίνονται από τις ψηφιακές υπογραφές, ως προς το ότι το πρωτόκολλο επαλήθευσης υπογραφών απαιτεί τη συνεργασία του υπογράφοντα. Στο παρακάτω παράδειγμα περιγράφουμε δύο σενάρια όπου θα μπορούσε να εφαρμοστεί μια αδιαμφισβήτητη υπογραφή.
**Παράδειγμα** (σενάρια για αδιαμφισβήτητες υπογραφές)

i) Η οντότητα Α (ο πελάτης) επιθυμεί να αποκτήσει πρόσβαση σε μια ασφαλή περιοχή που ελέγχεται από την οντότητα Β (η τράπεζα). Η ασφαλής περιοχή μπορεί, για παράδειγμα, να είναι μια θυρίδα ασφαλούς κατάθεσης. Η Β ζητά από την Α να υπογράψει ένα έγγραφο με ημερομηνία και ώρα πριν να επιτραπεί η πρόσβαση. Αν η Α χρησιμοποιεί μια αδιαμφισβήτητη υπογραφή, τότε η Β δεν είναι σε θέση να αποδείξει (σε κάποια μεταγενέστερη ημερομηνία) σε οποιονδήποτε ότι η Α χρησιμοποίησε την υπηρεσία χωρίς την άμεση συμμετοχή της Α στη διεργασία επαλήθευσης υπογραφών.

ii) Υποθέτουμε ότι κάποια μεγάλη εταιρεία Α έχει δημιουργήσει ένα πακέτο λογισμικού. Η Α υπογράφει το πακέτο και το πουλά στην οντότητα Β η οποία αποφασίζει να κάνει αντίγραφα αυτού του πακέτου και να τα μεταπωλήσει σε ένα τρίτο μέλος Γ. Ο Γ δεν είναι σε θέση να επαληθεύσει την αυθεντικότητα του λογισμικού χωρίς τη συνεργασία της Α. Φυσικά, αυτό το σενάριο δεν εμποδίζει τη Β να υπογράψει ξανά το πακέτο με τη δική της υπογραφή αλλά χάνεται για τη Β το πλεονέκτημα στο μάρκετινγκ που σχετίζεται με το όνομα της εταιρείας Α. Θα είναι επίσης ευκολότερο να εξιχνιαστεί η απατηλή δραστηριότητα της Β.

***Αλγόριθμος Παραγωγής κλειδιών***

Κάθε οντότητα επιλέγει ένα ιδιωτικό κλειδί και το αντίστοιχο δημόσιο κλειδί. Κάθε οντότητα Α θα πρέπει να κάνει τα εξής:

1. Να επιλέξει έναν τυχαίο πρώτο p = 2q + 1, όπου q είναι επίσης πρώτος.

2. (επιλογή ενός γεννήτορα α για την υποομάδα τάξεως q της Z*p .)

   2.1 Να επιλέξει ένα τυχαίο στοιχείο β e Z*p και να υπολογίσει το α = β (p-1)/q mod p.

   2.2 Αν α = 1 τότε να ανατρέξει στο βήμα 2.1.

3. Να επιλέξει έναν τυχαίο ακέραιο a e {1, 2, ..., q-1} και να υπολογίσει το γ=αα mod p.

4. Το δημόσιο κλειδί της Α είναι (p, α, γ). Το ιδιωτικό κλειδί της Α είναι το α.

***Σχήμα αδιαμφισβήτητων υπογραφών Chaum-van Antwerpen***

Η οντότητα Α υπογράφει ένα μήνυμα m που ανήκει στην υποομάδα τάξεως q της Z*p. Μια οντότητα Β μπορεί να επαληθεύσει την υπογραφή αυτή με τη συνεργασία της Α.

1. *Παραγωγή υπογραφής*. Η Α θα πρέπει να κάνει τα εξής:
i) Να υπολογίσει το s = mk mod p.
ii) Η υπογραφή της Α στο μήνυμα m είναι s.

2. *Επαλήθευση*. Το πρωτόκολλο για τον Β προκειμένου να επαληθεύσει την υπογραφή S της Α στο μήνυμα m, είναι το εξής:
i) Ο Β προμηθεύεται το αυθεντικό δημόσιο κλειδί (p, α, γ) της Α.
ii) Ο Β επιλέγει τυχαίους μυστικούς ακεραίους x1, x2 e {1, 2, ..., q - 1}.
iii) Ο Β υπολογίζει το z = sX1 γX2 mod p και στέλνει το z στην Α.
iv) Η Α υπολογίζει το w = (z)α mod p (όπου αα 1 = 1 (mod q)) και στέλνει το w στον Β.
v) Ο Β υπολογίζει το w = mX1 αX2 mod p και αποδέχεται την υπογραφή, αν και μόνο αν w=w .

**Απόδειξη** ότι η επαλήθευση της υπογραφής λειτουργεί. Είναι w = (zf* = (sX1 γx2 J = (maX1 ααX2) ' = mX1 αX2 = W mod p, όπως απαιτείται να είναι. Υπάρχει λοιπόν υψηλή πιθανότητα, ένας αντίπαλος να μην είναι σε θέση να παρασύρει τον Β να αποδεχτεί μια δόλια υπογραφή. Διαπίστωση πλαστογραφιών για αδιαμφισβήτητες υπογραφές. Ας υποθέσουμε ότι s είναι μια πλαστογραφία της υπογραφής της Α για ένα μήνυμα m, δηλ. s Φ ma mod p.
Τότε η πιθανότητα να αποδεχτεί ο Β την υπογραφή είναι μόνο 1/q η πιθανότητα αυτή είναι ανεξάρτητη από τους πόρους του αντιπάλου.

***Σημείωση*** (αποκήρυξη υπογραφής)
Η υπογράφουσα Α θα μπορούσε να αποκηρύξει μια
(έγκυρη) υπογραφή που κατασκευάστηκε με έναν από τους τρεις τρόπους:
(i) αρνείται να συμμετάσχει στο πρωτόκολλο επαλήθευσης
(ii) εκτελεί το πρωτόκολλο επαλήθευσης λανθασμένα ή
(iii) ισχυρίζεται ότι μια υπογραφή είναι πλαστογραφημένη παρότι το πρωτόκολλο επαλήθευσης είναι επιτυχές.
Η αποκήρυξη μιας υπογραφής ακολουθώντας το (i) θα θεωρούνταν ως μια προφανής προσπάθεια (παράνομης) απάρνησης. Τα (ii) και (iii) είναι πιο δύσκολο να προφυλαχτούμε εναντίον τους και απαιτούν ένα πρωτόκολλο αποκήρυξης.

***Πρωτόκολλο αποκήρυξης για το σχήμα αδιαμφισβήτητων υπογραφών Shaumvan Antwerpen***

Το πρωτόκολλο αποκήρυξης για το σχήμα αδιαμφισβήτητων υπογραφών Shaum-van Antwerpen ουσιαστικά εφαρμόζει το πρωτόκολλο επαλήθευσης δύο φορές και μετά εκτελεί έναν έλεγχο για να επαληθεύσει ότι η Α έχει εκτελέσει το πρωτόκολλο σωστά.
Το πρωτόκολλο αυτό προσδιορίζει κατά πόσο ή όχι η υπογράφουσα Α προσπαθεί να αποκηρύξει μια έγκυρη υπογραφή s, ή κατά πόσο η υπογραφή είναι μια πλαστογραφία.

1. Ο Β προμηθεύεται το αυθεντικό δημόσιο κλειδί (p, α, γ).

2. Ο Β επιλέγει τυχαίους μυστικούς ακεραίους X1, X2 e {1, 2, ..., q - 1} και υπολογίζει, ζ = sX1 γX2 modp και στέλνει το ζ στην Α.

3. Η Α υπολογίζει, w = (ζ)a modp (όπου aa- = 1 (mod p)) και στέλνει το w στον Β.

4. Αν w = mxαX2 modp, ο Β αποδέχεται την υπογραφή s και το πρωτόκολλο τερματίζει.

5. Ο Β επιλέγει τυχαίους μυστικούς ακεραίους x', x'2 e {1, 2, ..., q - 1} και υπολογίζει, ζ'= sX1 γX2 modp και στέλνει το ζ' στην Α.

6. Η Α υπολογίζει, w' = (ζ')a modp και στέλνει το w'στον Β.

7. Αν w' = mx αX2 mod p, ο Β αποδέχεται την υπογραφή s και το πρωτόκολλο τερματίζει.
8. Ο Β υπολογίζει, c = (wa~X2)X1 modp και c' = (w'α-X2)X1 modp. Αν _____c = c', τότε ο Β συμπεραίνει ότι η c είναι μια πλαστογραφία διαφορετικά, ο Β συμπεραίνει ότι η υπογραφή είναι έγκυρη και η Α προσπαθεί να αποκηρύξει την υπογραφή s.

Έστω m ένα μήνυμα και ας υποθέσουμε ότι s είναι η (εμφανιζόμενη ως) υπογραφή της Α στο m.
(i) Αν s είναι μια πλαστογραφία, δηλ. s Φma mod p και αν οι Α και Β, τότε w = w (και συνεπώς, το συμπέρασμα του Β ότι η s είναι μια πλαστογραφία είναι σωστό).
(ii) Υποθέτουμε ότι η s είναι όντως η υπογραφή της Α για το m, δηλ. ότι s = ma mod p. Υποθέτουμε ότι ο Β ακολουθεί το πρωτόκολλο σωστά, αλλά η Α δεν το ακολουθεί. Τότε η πιθανότητα ότι w = w ' (και συνεπώς η Α πετυχαίνει στην αποκήρυξη της υπογραφής) είναι μόνο 1/q.

*Ασφάλεια των αδιαμφισβήτητων υπογραφών*

Η ασφάλεια βασίζεται στο δυσεπίλυτο του προβλήματος διακριτού λογαρίθμου στην κυκλική υποομάδα τάξης q της Zp.

Ας υποθέσουμε ότι ο επαληθεύων Β καταγράφει τα μηνύματα που ανταλλάσσονται και επίσης τις τυχαίες τιμές x1, x2 που χρησιμοποιούνται στο πρωτόκολλο. Ένα τρίτο μέλος C δεν θα πρέπει να δεχθεί αυτό το επικυρωμένο αντίγραφο από τον Β ως επαλήθευση της υπογραφής s. Για να δούμε γιατί είναι αυτή η περίπτωση, αρκεί να δείξουμε πώς θα μπορούσε ο Β να σκαρφιστεί ένα επιτυχές αντίγραφο χωρίς τη συμμετοχή της υπογράφουσας Α. Ο Β επιλέγει ένα μήνυμα m, ακεραίους x1, x2 και l στο διάστημα [1, q - 1] και υπολογίζει την s = ((mx αX2) y-X2)X1 mod p. Το μήνυμα πρωτοκόλλου από τον Β στην Α θα είναι το ζ = sX1 y%2 mod p και από την Α στον Β θα είναι w = ζ mod p. Ο αλγόριθμος θα δεχθεί την s ως μια έγκυρη υπογραφή της Α για το μήνυμα m. Το επιχείρημα αυτό δείχνει οι υπογραφές μπορούν να επαληθευτούν μόνο με αλληλεπίδραση απευθείας με τον υπογράφοντα.

## 3.8.3 Σχήματα υπογραφών αποτυχίας-τερματισμού (fail-stop)

Οι ψηφιακές υπογραφές αποτυχίας-τερματισμού είναι ψηφιακές υπογραφές οι οποίες επιτρέπουν σε μια οντότητα Α να αποδείξει ότι μια υπογραφή, η οποία φαινομενικά (αλλά όχι πραγματικά) είναι υπογεγραμμένη από την Α, είναι μια πλαστογραφία. Αυτό γίνεται δείχνοντας ότι η υποκείμενη υπόθεση στην οποία βασίζεται ο μηχανισμός υπογραφών έχει παραβιαστεί. Η δυνατότητα απόδειξης μιας πλαστογραφίας δεν εναπόκειται σε οποιαδήποτε κρυπτογραφική υπόθεση, αλλά μπορεί να σημειωθεί αποτυχία με κάποια μικρή πιθανότητα αυτή η πιθανότητα αποτυχίας είναι ανεξάρτητη από την υπολογιστική δύναμη του πλαστογράφου.

Τα σχήματα υπογραφών αποτυχίας-τερματισμού έχουν το πλεονέκτημα ότι ακόμα κι αν ένας πολύ ισχυρός αντίπαλος μπορεί να πλαστογραφήσει μία μεμονωμένη υπογραφή, η πλαστογραφία μπορεί να ανιχνευθεί και ο μηχανισμός υπογραφής δεν μπορεί να χρησιμοποιηθεί πλέον. Συνεπώς, είναι επίσης κατάλληλος ο όρος αποτυχία -τερματισμός.

Ένα σχήμα υπογραφών αποτυχίας-τερματισμού θα πρέπει να έχει τις ακόλουθες ιδιότητες:

1. Αν ο υπογράφων υπογράψει ένα μήνυμα σύμφωνα με τον μηχανισμό, τότε ο επαληθεύων θα πρέπει κατά τον έλεγχο της υπογραφής να τη δεχθεί.

2. Ο πλαστογράφος δεν μπορεί να κατασκευάσει υπογραφές οι οποίες περνούν στον αλγόριθμο επαλήθευσης χωρίς να δαπανήσει μια εκθετική ποσότητα έργου.

3. Αν ο πλαστογράφος πετύχει την κατασκευή μιας υπογραφής η οποία περνά τον έλεγχο επαλήθευσης τότε, με υψηλή πιθανότητα, ο πραγματικός υπογράφων μπορεί να παραγάγει μια απόδειξη της πλαστογραφίας.

4. Ο υπογράφων δεν μπορεί να κατασκευάσει υπογραφές για τις οποίες να διατυπωθεί ισχυρισμός σε μια μεταγενέστερη χρονική στιγμή ότι είναι πλαστογραφίες. Ο Αλγόριθμος υπογραφών αποτυχίας-τερματισμού (van Heijst-Pedersen) είναι ένα παράδειγμα μηχανισμού αποτυχίας-τερματισμού. Όπως περιγράψαμε, είναι ένα σχήμα υπογραφών μιας χρήσης, αλλά υπάρχουν τρόποι γενίκευσής του ώστε να επιτρέπει πολλαπλές υπογραφές μία δυνατότητα είναι η χρήση δέντρων πιστοποίησης αυθεντικότητας.

**Αλγόριθμος Παραγωγή κλειδιών**

Η παραγωγή κλειδιών μοιράζεται μεταξύ της οντότητας Α και ενός έμπιστου τρίτου μέλους (TTP).
Η οντότητα Α θα πρέπει να κάνει τα εξής:
(α) Να επιλέξει τυχαίους μυστικούς ακεραίους x1, x2, y1, y2 στο διάστημα [0, q - 1].
(β) Να υπολογίσει τα β1 = αx βX2 και β2 = αy βy2 mod p.
(γ) Το δημόσιο κλειδί της Α είναι (β1, β2, p, q, α, β ) το ιδιωτικό κλειδί της Α είναι η τετράδα X = (xb X2, yb y2).

Υποθέτοντας ότι το πρόβλημα του διακριτού λογαρίθμου στην υποομάδα τάξης q της ομάδας Zp είναι δυσεπίλυτο , η μόνη οντότητα που γνωρίζει το a, τον διακριτό λογάριθμο του β ως προς τη βάση α, είναι το TTP.

**Αλγόριθμος Σχήμα υπογραφών αποτυχίας-τερματισμού (van Heijst-Pedersen)**

Αυτό είναι ένα σχήμα ψηφιακών υπογραφών μιας χρήσης του οποίου η ασφάλεια βασίζεται στο πρόβλημα διακριτού λογαρίθμου στην υποομάδα τάξης q της ομάδας Zp .

**1. Παραγωγή υπογραφής**. Για να υπογράψει ένα μήνυμα m e [0, q - 1], η Α θα πρέπει να κάνει τα εξής:
(α) Να υπολογίσει τις τιμές s1m = x1 + my1 mod q και s2 m = x2 + my2 mod q. (β) Η υπογραφή της Α για το m είναι (s1,m, s2,m).

**2. Επαλήθευση**. Για να επαληθεύσει την υπογραφή (s1m, s2m) της Α στο m, ο Β θα πρέπει να κάνει τα εξής:
(α) Να προμηθευτεί το αυθεντικό δημόσιο κλειδί (β1, β2, p, q, α, β ) της Α.
Απόδειξη ότι η επαλήθευση υπογραφής λειτουργεί.
U - ββ^ - (αX1 βX2 )(αy1 βy2 )m — αx +my1 βX2 +my2
- αs1,mβs2,m - υ2 (mod p).

Ο αλγόριθμος αυτός είναι ένα σχήμα υπογραφών μιας χρήσης επειδή το ιδιωτικό κλειδί X της Α μπορεί να υπολογιστεί αν υπογραφούν δύο μηνύματα με τη χρήση του X. Πριν περιγράψουμε τον αλγόριθμο για την απόδειξη της πλαστογραφίας είναι απαραίτητος ένας αριθμός από γεγονότα.

Πλήθος από διακεκριμένες τετράδες που αντιπροσωπεύουν ένα δημόσιο κλειδί και μια υπογραφή.

Ας υποθέσουμε ότι το δημόσιο κλειδί της A είναι (β1, β2,p, q, α, β) και το ιδιωτικό κλειδί είναι η τετράδα X = (X1, X2, y1, y2).
(i) Υπάρχουν ακριβώς q2 τετράδες X = (x1, x2, y1, y2) με x1, x2, y1, y2 e Zq οι οποίες δίνουν το ίδιο τμήμα (β1, β2) του δημόσιου κλειδιού.
(ii) Έστω ότι T είναι το σύνολο των q2 τετράδων οι οποίες δίνουν το ίδιο τμήμα του δημόσιου κλειδιού (β1, β2). Για κάθε q e Zq, υπάρχουν ακριβώς q τετράδες στο T οι οποίες δίνουν την ίδια υπογραφή (s1,m, s2,m) για το m. Συνεπώς, οι q2 τετράδες του T δίνουν ακριβώς q διαφορετικές υπογραφές για το m.
(β) Να υπολογίσει τις τιμές υ1 = βφ2* mod p και υ2 = αs1,m βSl,m mod p.
(γ) Να αποδεχτεί την υπογραφή, αν και μόνο αν υ\=υ2.
(iii) Έστω ότι m' e Zq είναι ένα μήνυμα διαφορετικό από το m. Τότε οι q2 τετράδες του T, οι οποίες δίνουν την υπογραφή (s1m, s%m) της A για το m, δίνουν q διαφορετικές υπογραφές για το m'.

Παράδειγμα

Έστω p = 29 και q = 7. Το α = 16 είναι ένας
γεννήτορας της υποομάδας τάξης q της Zp . Παίρνουμε β = α5 mod 29 = 23. Υποθέτουμε ότι το ιδιωτικό κλειδί της A είναι x = (2, 3, 5, 2) το δημόσιο κλειδί της A είναι β1 = α2β3mod29 = 7, β2 = α5 β 2 mod 29 = 16. Ο πίνακας που ακολουθεί παρουσιάζει τις q2 = 49 τετράδες οι οποίες δίνουν το ίδιο δημόσιο κλειδί.

Πίνακας 3.8.3.1

| *τετράδα* | *771* | | | | | | |
|---|---|---|---|---|---|---|---|
| | *0* | *1* | *2* | *3* | *4* | *5* | *6* |
| **166G** | **16** | **05** | **64** | **53** | **42** | **31** | **20** |
| **2352** | **23** | **05** | **50** | **32** | **14** | **66** | **41** |
| **3045** | **30** | **0-J** | **43** | **11** | **56** | **24** | **62** |
| **4431** | **44** | **05** | **36** | **60** | **21** | **52** | **13** |
| **5124** | **51** | **05** | **22** | **46** | **63** | **10** | **34** |
| **6510** | **65** | **05** | **15** | **25** | **35** | **45** | **55** |
| **0203** | **02** | **05** | **01** | **04** | **00** | **03** | **06** |

Αν οι 49 τετράδες αυτού του πίνακα χρησιμοποιηθούν για να υπογραφεί το μήνυμα m = 1, προκύπτουν ακριβώς q = 7 ζεύγη υπογραφής (s1m, s2m). Ο επόμενος πίνακας παρουσιάζει τις δυνατότητες και εκείνες τις τετράδες οι οποίες παράγουν κάθε μια υπογραφή.

Πίνακας 3.8.3.2

| *τετράδα* | *771* | | | | | | |
|---|---|---|---|---|---|---|---|
| | *0* | *1* | *2* | *3* | *4* | *5* | *6* |
| **166G** | **16** | **05** | **64** | **53** | **42** | **31** | **20** |
| **2352** | **23** | **05** | **50** | **32** | **14** | **66** | **41** |
| **3045** | **30** | **0-J** | **43** | **11** | **56** | **24** | **62** |
| **4431** | **44** | **05** | **36** | **60** | **21** | **52** | **13** |
| **5124** | **51** | **05** | **22** | **46** | **63** | **10** | **34** |
| **6510** | **65** | **05** | **15** | **25** | **35** | **45** | **55** |
| **0203** | **02** | **05** | **01** | **04** | **00** | **03** | **06** |

Ο επόμενος πίνακας παρουσιάζει, για κάθε μήνυμα m' e Z7, όλα τα ζεύγη υπογραφών για τις 7 τετράδες που δίνουν την υπογραφή (0, S) της A για m = 1.

*Πίνακας 3.8.3.3*

| *τετράδα* | *771* | | | | | | |
|---|---|---|---|---|---|---|---|
| | *0* | *1* | *2* | *3* | *4* | *5* | *6* |
| **166G** | **16** | **05** | **64** | **53** | **42** | **31** | **20** |
| **2352** | **23** | **05** | **50** | **32** | **14** | **66** | **41** |
| **3045** | **30** | **0-J** | **43** | **11** | **56** | **24** | **62** |
| **4431** | **44** | **05** | **36** | **60** | **21** | **52** | **13** |
| **5124** | **51** | **05** | **22** | **46** | **63** | **10** | **34** |
| **6510** | **65** | **05** | **15** | **25** | **35** | **45** | **55** |
| **0203** | **02** | **05** | **01** | **04** | **00** | **03** | **06** |

***Πιθανότητα επιτυχούς πλαστογραφίας.***

Ας υποθέσουμε ότι ένας αντίπαλος (ο πλαστογράφος) θέλει να παραγάγει την υπογραφή της Α σε κάποιο μήνυμα m'. Υπάρχουν δύο δυνατές περιπτώσεις προς θεώρηση.

(i)Ο πλαστογράφος έχει πρόσβαση μόνο στο δημόσιο κλειδί της υπογράφουσας (δηλ., ο πλαστογράφος δεν κατέχει ένα μήνυμα και μια έγκυρη υπογραφή). Η πιθανότητα ότι η υπογραφή που δημιουργήθηκε από τον αντίπαλο είναι ίδια με την υπογραφή της Α για το m' είναι μόνο q/q2 = 1/q αυτή η πιθανότητα είναι ανεξάρτητη από τους υπολογιστικούς πόρους του αντίπαλου.

(ii) Ο πλαστογράφος έχει πρόσβαση σε ένα μήνυμα m και μια υπογραφή (s1m, s2m) που δημιουργήθηκε από την υπογράφουσα. Η υπογραφή ότι η υπογραφή που δημιουργήθηκε από τον αντίπαλο είναι ίδια με την υπογραφή της Α για το m' είναι μόνο 1/q- πάλι, η πιθανότητα αυτή είναι ανεξάρτητη από τους υπολογιστικούς πόρους του αντίπαλου.
Ας υποθέσουμε τώρα ότι ο αντίπαλος έχει πλαστογραφήσει την υπογραφή της Α σε ένα μήνυμα και ότι η υπογραφή πέρασε το στάδιο της επαλήθευσης. Ο αντικειμενικός στόχος είναι ότι η Α θα πρέπει να είναι σε θέση να αποδείξει ότι η υπογραφή αυτή είναι μια πλαστογραφία. Ο αλγόριθμος που ακολουθεί μας δείχνει πώς μπορεί η Α, με υψηλή πιθανότητα, να χρησιμοποιήσει την πλαστογραφημένη υπογραφή για να παραγάγει το μυστικό α. Αφού το a υποτίθεται ότι είναι γνωστό μόνο στο TTP χρησιμεύει ως απόδειξη της πλαστογραφίας.

***Αλγόριθμος απόδειξης της πλαστογραφίας***

Για να αποδείξουμε ότι μια υπογραφή s'=(s1m,s'2m) σε ένα μήνυμα m είναι μια πλαστογραφία, η υπογράφουσα παράγει τον ακέραιο α = loga β ο οποίος χρησιμεύει ως απόδειξη της πλαστογραφίας.
Η υπογράφουσα (οντότητα Α) θα πρέπει να κάνει τα εξής:
1. Να υπολογίσει ένα ζεύγος υπογραφής s = (slm, ) για το μήνυμα m
χρησιμοποιώντας το ιδιωτικό της κλειδί x
2. Αν s = s να επιστρέψει στο βήμα 1.
3. Να υπολογίσει το α = (s^m - s[mm) (s2mm - s2,m)-1 mod q.
Η πιθανότητα ότι s = s' είναι 1/q.
Από τον αλγόριθμο επαλήθευσης είναι </1,mβ52,,η = a1,m(modp) ή c/1,m-s1,m = αa{s'2,m-s2,m) (modp) ή s1,m - s1,m Ξ a(s2,m - s2,m) (mod q). Συνεπώς a = (s1,m - s1,m) (s2,m - s2,mmod q.

**Αποκήρυξη υπογραφών**

Για να αποκηρύξει μια υπογράφουσα οντότητα μια υπογραφή, απαιτείται μια αποδοτική μέθοδος υπολογισμού λογαρίθμων.

# ΣΥΜΠΕΡΑΣΜΑΤΑ

Σήμερα η κρυπτογραφία είναι αναμφισβήτητα μια καθημερινή πρακτική. Παραδείγματα χρήσης των κρυπτογραφικών αλγορίθμων και τεχνικών περιλαμβάνουν το δίκτυο GSM της κινητής τηλεφωνίας ( η κάρτα SIM των GSM κινητών τηλεφώνων είναι μια «έξυπνη κάρτα». Η συγκεκριμένη τεχνολογία ήταν η πρώτη που έκανε διαθέσιμη στο ευρύ κοινό μια τέτοια κρυπτογραφική υπηρεσία.), τα πρωτόκολλα πιστοποίησης ταυτότητας, τα ψηφιακά πιστοποιητικά, τις ψηφιακές υπογραφές, την ανάληψη χρημάτων από ένα μηχάνημα αυτόματης συναλλαγής (ATM) κτλ. Παρ' όλα αυτά υπάρχουν πολλές περιπτώσεις όπου η χρήση της κρυπτογραφίας από το ευρύ κοινό δεν είναι πάντοτε επιθυμητή.

Παραδοσιακά η κρυπτογραφία χρησιμοποιούνταν από κυβερνητικούς οργανισμούς και στρατιωτικό προσωπικό. Μέσα στα ασαφή όρια της Εθνικής Ασφάλειας , οι κυβερνήσεις θέλουν πάντοτε να μπορούν να αποκρυπτογραφούν οτιδήποτε κρίνουν ότι διακυβεύει ή την υπονομεύει. Οι τρόποι τους είναι η παρακολούθηση τηλεφώνων και η υποκλοπή συνδιαλέξεων που μπορεί να γίνονται και κρυπτογραφικά, καθώς και η παρακολούθηση και υποκλοπή της ηλεκτρονικής αλληλογραφίας ενός πολίτη.

Από την πλευρά των κυβερνητικών υπηρεσιών, είναι λογικό, να μπορούν ( εφόσον εκδοθεί το σχετικό ένταλμα) να αποκρυπτογραφήσουν οτιδήποτε περιέλθει στην κατοχή τους. Γι' αυτό σε διάφορες , υπάρχουν σχετικοί νόμοι που περιορίζουν τη χρήση συγκεκριμένων κρυπτογραφικών τεχνικών. Έτσι, εάν χρησιμοποιηθεί ο αλγόριθμος RSA με μήκος κλειδιού 2048 bits για να κρυπτογραφήσει κάποιο μήνυμα και όχι κλειδιά όπως συνηθίζεται, οι κυβερνητικές υπηρεσίες θα χρειαστούν μερικές δεκάδες αν όχι εκατοντάδες χρόνια ώστε να καταφέρουν να αποκρυπτογραφήσουν κάποιο συγκεκριμένο μήνυμα. Γι' αυτό σε πολλές χώρες απαγορεύεται, δια νόμου, η χρήση ασύμμετρων αλγορίθμων για την κρυπτογράφηση δεδομένων.

Πριν μερικά χρόνια, η δημιουργία ενός προγράμματος κρυπτογράφησης, του PGP( Pretty Good Privacy) και η ελεύθερη διανομή του μέσα από το διαδίκτυο δημιούργησε προβλήματα στις μυστικές υπηρεσίες της κυβέρνησης και συγκεκριμένα στην NSA (National security Agency). Ο δημιουργός του, Phil Zimmerman, κατηγορήθηκε υπονόμευση της εθνικής ασφάλειας της χώρας του, αφού διανέμοντας το δωρεάν, μπορούσαν να το προμηθευτούν τρομοκράτες, κακοποιοί, παιδεραστές κτλ. Μετά από αλλεπάλληλες δίκες, τα δύο μέρη ήρθαν σε συμβιβασμό. Το PGP μπορούσε να χρησιμοποιηθεί ελεύθερα μέσα στο έδαφος των Ηνωμένων Πολιτειών αλλά όχι σε διεθνές επίπεδο. Για περιπτώσεις που απαιτούνταν κρυπτογραφημένη επικοινωνία από ή προς το εξωτερικό, το μέγιστο μήκος κλειδιού που μπορούσε να χρησιμοποιηθεί ορίστηκε στα 40 bits, ενώ λίγα χρόνια αργότερα αυξήθηκε στα 56, που ισχύει και σήμερα. Η επιλογή αυτή δεν έγινε τυχαία, αφού το συγκεκριμένο μήκος μπορεί να κρυπταναλυθεί, μέσα σε ένα εύλογο χρονικό διάστημα, από τις συγκεκριμένες κυβερνητικές υπηρεσίες. Σήμερα, διανέμονται δωρεάν δύο εκδόσεις του προγράμματος, μια για τους πολίτες των Η.Π.Α και μια για τους πολίτες του υπόλοιπου κόσμου.

Στον πραγματικό κόσμο ο τρόπος διασφάλισης της εμπιστευτικότητας διασφαλίζεται με τη χρήση της υπογραφής. Στον ηλεκτρονικό κόσμο χρησιμοποιούμε τις ψηφιακές υπογραφές. Η χρήση των ψηφιακών υπογραφών σε εφαρμογές που απαιτούν πιστοποίηση ταυτότητας (authentication) προϋποθέτουν πως ο κάθε χρήστης ενός ιδιωτικού κλειδιού είναι άμεσα συνδεδεμένος με αυτό.

Στη καθημερινή μας ζωή, υπάρχουν πολλές περιπτώσεις που ο κάτοχος ενός δημόσιου κλειδιού δεν είναι και ο ιδιοκτήτης ή ο δημιουργός του. Αυτό συμβαίνει, κυρίως, γιατί η δημιουργία κρυπτογραφικού κλειδιού απαιτεί κάποιες ελάχιστες μαθηματικές γνώσεις ή/και υπολογιστικούς πόρους, τόσο σε υλικό όσο και σε λογισμικό, το οποίο δεν είναι πάντοτε διαθέσιμο στο χρήστη. Η χρήση της κρυπτογραφίας στόχο έχει να αυξήσει την ασφάλεια των ήδη υπαρχουσών εφαρμογών χωρίς επιπρόσθετα προβλήματα στη λειτουργικότητα τους. Ο χρήστης ενδιαφέρεται περισσότερο για τη αποτελεσματική χρήση της εφαρμογής και όχι για την ασφάλεια της.

Αυτός είναι και ο λόγος που, αρκετοί χρήστες αναθέτουν σε κάποιο έμπιστο τρίτο μέρος τη δημιουργία κλειδιών(στις περισσότερες περιπτώσεις ο χρήστης ίσως δεν ενημερώνεται καθόλου γι' αυτή τη διαδικασία). Το περίεργο είναι πως σχεδόν κανείς χρήστης δε θέλει να υπογράφει αντ' αυτού το τρίτο μέρος, παρ' όλο που αυτό το δημιούργησε και γνωρίζει τα κλειδιά του, με αποτέλεσμα να δημιουργείται η άποψη κατά πόσο οι οντότητες που δημιουργούν κλειδιά εκ μέρους των χρηστών θα πρέπει να γνωρίζουν την τιμή των κλειδιών αυτών ή να κρατούν ένα εφεδρικό αντίγραφο (backup key). Η πιθανότητα απώλειας των κλειδιών από το χρήστη εντείνει αυτή τη σκέψη. Η απώλεια ενός κλειδιού, μπορεί να έχει καταστροφικές συνέπειες, κρίνοντας απαραίτητο το εφεδρικό κλειδί. Όμως, μειώνεται η ασφάλεια και η προστασία, αφού ένας επιτιθέμενος θα μπορεί να χρησιμοποιήσει τα κλειδιά.

Ένας επιτιθέμενος, μπορεί να αποκτήσει με κάποιο τρόπο το ιδιωτικό κλειδί του χρήστη, είτε να αντικαταστήσει το δημόσιο κλειδί του χρήστη με το αντίστοιχο δικό του. Οι τρόποι απόκτησης ενός ιδιωτικού κλειδιού, πέρα από τα φυσικά μέσα, είναι οι μαθηματικές επιθέσεις ( εύρεση παραγόντων p,q σε ένα ιδιωτικό RSA κλειδί) και η κλοπή μιας κρυπτοσυσκευής. Σε αυτή την περίπτωση απλουστεύουν τα πράγματα αφού δε χρειάζεται να γνωρίζουμε την τιμή του κλειδιού, αρκεί μόνο η κατοχή του.

Η διαδικασία της ταυτοποίησης και αυθεντικοποίησης αποτελούν μέρος της ασφάλειας των υπολογιστικών και πληροφοριακών συστημάτων. Η αναγνώριση και η επαλήθευση της ταυτότητας ενός λογικού υποκειμένου που ζητά προσπέλαση σε ένα αυτοματοποιημένο Πληροφοριακό Σύστημα αποτελεί το βασικό στοιχείο της διαδικασίας ελέγχου της προσπέλασης.

Τα συστήματα αυθεντικοποίησης και διανομής κλειδιών χρησιμοποιούνται σε δίκτυα και κατανεμημένα συστήματα προκειμένου να παράσχουν υπηρεσίες ασφάλειας στο επίπεδο εφαρμογής. Τα ψηφιακά πιστοποιητικά έχουν τη μορφή δυαδικών αρχείων και η λειτουργία τους στηρίζεται στην κρυπτογραφία δημόσιου κλειδιού.

Μια εταιρία ή ένας οργανισμός που διαθέτει στους χρήστες την Αρχή Πιστοποίησης (Certification Authority-CA), χρειάζεται να πληροί συγκεκριμένα κριτήρια ώστε να εμπνέει εμπιστοσύνη για την εγκυρότητα της.

Τέλος, τα ψηφιακά πιστοποιητικά δεν έχουν απεριόριστη διάρκεια ζωής. Μια Αρχή Πιστοποίησης (CA) πρέπει να μπορεί να γνωρίζει ανά πάσα στιγμή τα πιστοποιητικά που έχει εκδώσει αλλά και αυτά που βρίσκονται εκτός λειτουργίας (έχουν λήξει). Συνήθως αυτό γίνεται με μια λίστα ανακληθέντων πιστοποιητικών ( certificate revocation list – CRL) η οποία περιλαμβάνει τα πιστοποιητικά που έχουν ανακληθεί. Μια CA κρατά μια ξεχωριστή λίστα για τα πιστοποιητικά που έχουν λήξει και μια για αυτά που έχουν ανακληθεί.

# Βιβλιογραφία


[1]Γκρίτζαλης Δ. & Γκρίτζαλης Σ. & Κατσίκας Σ., *Ασφάλεια Πληροφοριακών Συστημάτων.* Αθήνα (2004)

[2]Γρηγοριάδης Ν. & Πάτσος Δ. & Σουρής Α. , *Ασφάλεια της Πληροφορίας.* Αθήνα (2004)

[3]Coppersmith, D., *The Data Encryption Standard (DES) and Its Strength Against Attacks.* IBM Journal of Research and Development, May (1994)

[4]Denning, D., *Cryptography and Data Security.* Addison-Wesley, Reading(1982)

Diffie W. & Hellman M., *Privacy and Authentication : An Introduction to Cryptography.* Proceedings *of the IEEE, March (1979)*

[5]ΕΕΤΤ: Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείου http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html

[6]Fiestel, H., *Cryptography and Computer Privacy.* Prentice Hall (1997)

[7]Menezes J. Alfred & Van Oorschot Paul & Vanstone A. Scott, *Handbook of Applied Cryptography*.(March 2010)

[7]Σημειώσεις διαλέξεων από τους Pehlivanoglou S. &Todd J. & Zhon S. H.

[8]Stallings W., *Βασικές αρχές ασφάλειας δικτύων. Εφαρμογές και Πρότυπα.* (2008)

[9]www.wikipedia.gr