ΤΕΙ Καλαματας Παραρτημα Σπαρτης

Πτυχιακη Εργασια

Κρυπτογραφία και RSA

Φοιτήτρια:
Μ. Κουρταλη
ΑΜ:2006169

Επιβλέπων Καθηγητής:
Γ. Καραγιωργος

Νοέμβριος 2011
Σπάρτη

Ευχαριστίες

Η παρούσα εργασία εκπονήθηκε κατα το θερινό εξάμηνο του ακαδημαϊκού έτους του 2011. Ευχαριστώ πολύ τον επιβλέποντα καθηγητή Γρηγόρη Καραγιώργο για την υπομονή και το ενδιαφέρον που έδειξε κατά την διάρκεια της συνεργασίας μας, αλλά και για την βοήθεια και τις παρατηρήσεις του για την βελτίωση αυτής της εργασίας.

Περίληψη

Αντικείμενο της παρούσας εργασίας αποτελεί η κρυπτογραφία και το σύστημα κρυπτογράφησης RSA. Στο πρώτο μέρος γίνεται μια σύντομη ιστορική αναδρομή στην εξέλιξη της κρυπτογραφίας από την αρχαιότητα μέχρι σήμερα. Ακολουθεί εισαγωγή στις βασικές της έννοιες, τους στόχους της και μια αναφορά στις εφαρμογές της στη σύγχρονη εποχή. Γίνεται διαχωρισμός των κλασσικών και σύγχρονων κρυπτοσυστημάτων, ενώ περιγράφονται τα συμμετρικά και ασσύμετρα κρυπτοσυστήματα της σύγχρονης κρυπτογραφίας. Ακολουθούν τα διάφορα σχήματα ψηφιακών υπογραφών και οι κύριες τεχνικές αυθεντικοποίησης. Στο πέμπτο κεφάλαιο περιγράφονται κάποια κρυπτογραφικά εργαλεία και τα ποιο σημαντικά αριθμο- θεωρητικά της προβλήματα.

Στο δεύτερο μέρος αναλύεται το ασύμμετρο κρυπτοσύστημαRSA και πιο συγκεκριμένα ο αλγόριθμος RSA και η λειτουργία του. Η μέθοδος της δημιουργίας των κλειδιών, της κρυπτογράφησης και της αποκρυπτογράφησης. Η χρήση της ψηφιακής υπογραφής με RSA καθώς και θέματα που αφορούν στην ασφάλεια του και το πρόβλημα RSA. Τέλος τα συμπεράσματα από την μελέτη αυτή και η σημασία της χρήσης της κρυπτογραφίας στην εποχή μας. Η εργασία γράφτηκε σε γλώσσα Latex.

Περιεχόμενα

Μέρος Ι

Κρυπτογραφία

Κεφάλαιο 1

Εισαγωγή στην Κρυπτογραφία

Η λέξη κρυπτογραφία προέρχεται από τα συνθετικά ¨***κρυπτός***¨ + ¨***γράφω***¨ , είναι ο επιστημονικός κλάδος που ασχολείται με την μελέτη, την ανάπτυξη και την χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης, με σκοπό την απόκρυψη του περιεχομένου μηνυμάτων.Αποτελεί ένα τομέα της επιστήμης της κρυπτολογίας, η οποία ασχολείται με την μελέτη της ασφαλούς επικοινωνίας. Ο κύριος στόχος της είναι να παρέχει μηχανισμούς για δύο ή περισσότερες οντότητες να επικοινωνήσουν χωρίς κάποια μη εξουσιοδοτημένη να είναι ικανή να διαβάζει την πληροφορία. Η λέξη κρυπτολογία αποτελείται από την ελληνική λέξη ¨***κρυπτός***¨ και ¨***λόγος***¨ και χωρίζεται σε δύο κλάδους: Την Κρυπτογραφία και την Κρυπτανάλυση .[14]

«Υπάρχουν δύο είδη κρυπτογράφησης στον κόσμο: αυτή που θα σταματήσει το παιδί της αδελφής σας από την ανάγνωση των αρχείων σας, και η κρυπτογράφηση που θα σταματήσει μεγάλες κυβερνήσεις από την ανάγνωση των αρχείων σας.»

Bruce Schneier, Applied Cryptography

1.1 Ιστορική αναδρομή

Η κρυπτογραφία εμφανίζεται αρχικά με μορφή τέχνης όπου είχε λίγους γνώστες. Η ιστορία της ξεκινά το 4000 πχ στην αρχαία Αίγυπτο όταν σε μια πόλη κοντά στον Νείλο το Menet Khufu, ένας πλοίαρχος έγραψε με ιερογλυφικά σύμβολα την ζωή του άρχοντά του. Οι Φαραώ κρυπτογραφούσαν μηνύματα στα κεφάλια των σκλάβων. Περνά από την αρχαία Ελλάδα περίπου τον 5ο αιώνα π.Χ. οι Σπαρτιάτες χρησιμοποίησαν την ***κρυπτο-***

γραφημένη σκυτάλη για τη μεταφορά στρατιωτικών μηνυμάτων. Ο Πολύβιος (2ος αιώνας πΧ.) επινόησε ένα κρυπτοσύστημα όπου τα γράμματα του απλού κειμένου αντικαθίστανται από ζεύγη συμβόλων (αριθμών). Αναφορά υπάρχει και στην Ιλιάδα από τον Όμηρο, όπου ο Βελερεφόντης πάει στην Λυκία μεταφέροντας ένα κρυπτογραφημένο μήνυμα. Συνεχίζεται με τον Ιούλιο Καίσαρα ο οποίος δημιούργησε έναν αλγόριθμο (μονοαλφαβητικής αντικατάστασης) για να επικοινωνεί με ασφάλεια με τους επιτελείς του.[3]

Ο βραχμάνος λόγιος Βατσιγιάνα έγραψε τον 4ο μΧ. αιώνα το περίφημο Κάμα Σούτρα. Η 45η τέχνη του καταλόγου είναι η μιλεχίτα βικάλπα, δηλ., η τέχνη της μυστικής γραφής. Σημαντική εξέλιξη έγινε τον 9ο αιώνα μ.χ. ο Αλ-Κίντι, γνωστός και ως "ο φιλόσοφος των Αράβων" έγραψε μια πραγματεία με τίτλο "Χειρόγραφο περί αποκρυπτογραφήσεως κρυπτογραφικών μηνυμάτων", και αφορούσε την τεχνική της ανάλυσης συχνοτήτων.[3]

Στη συνέχεια, με έργα των φιλόσοφων Alberti και Tritheimius η τεχνική της πολυαλφαβητικής αντικατάστασης κάνει την εμφάνιση της στην Ευρώπη με το κρυπτοσύστημα **Vigenere**, ή το άθραυστο κρυπτόγραμμα. Ένας άλλος διάσημος κώδικας είναι ο κώδικας Μορς, που αναπτύχθηκε από τον **Samuel Morse** το 1832, και απλώς περιγράφει τον τρόπο κωδικοποίησης του αλφαβήτου σε μακρείς και σύντομους ήχους.[3]

Σημαντική στην εξέλιξη της Θεωρητικής και Εφαρμοσμένης Κρυπτογραφίας ήταν και η ανάπτυξη Πληροφορικής και των Τηλεπικοινωνιών. Το 1920 σημαντικό ήταν το δημοσίευμα του William F. Friedman **The Index of Coincidence and Its Applications in Cryptography** , που έτυχε μεγάλης προσοχής από την επιστημονική κοινότητα. Επίσης ήταν και ο ιδρυτής των Riverbank Laboratories, κρυπτολόγος της Αμερικανικής κυβέρνησης και οδηγός του σπασίματος του κώδικα της Ιαπωνικής Purple Machine κατά τον 2ο Παγκόσμιο Πόλεμο, θεωρείται ο πατέρας της Αμερικάνικης κρυπτανάλυσης. Ενώ την ίδια εποχή έγιναν οι πρώτες αιτήσεις απονομής διπλωμάτων ευρεσιτεχνίας από τον Edward H. Hebern και Arthur Scherbius σχετικά με μια μηχανή κρυπτογράφησης, τον ρότορα. Παρόμοιους μηχανισμούς χρησιμοποιούσαν για περίπου 50 χρόνια στρατιωτικοί οργανισμοί. Μια από τις ποιό γνωστές είναι η συσκευή **ENIGMA**, που την χρησιμοποιούσαν οι Γερμανοί τον Β Παγκόσμιο πόλεμο για την αποστολή μηνυμάτων. Αυτή αποκρυπτογραφήθηκε τελικά από Πολωνούς οι οποίοι αποκάλυψαν μετά τον τρόπο αποκρυπτογράφησης και στους Βρετανούς.[3]

Το 1949 ο Claude Shannon με την εργασία του **The Communication Theory of Secrecy Systems**[2] ξεκινά την εποχή της σύγχρονης κρυπτογραφίας, καθιέρωσε ένα ακριβές μαθηματικό μοντέλο για το τι σημαίνει ασφαλές κρυπτοσύστημα. Ήταν η πρώτη ολοκληρωμένη μαθηματική απόπειρα θεμελίωσης της Θεωρίας της Πληροφορίας, ορίζει

την ποσότητα της πληροφορίας σε ένα μήνυμα ως ελάχιστο αριθμό bit που απαιτούνται για να απεικονιστούν όλα τα δυνατά νοήματα αυτού του μηνύματος. Ορίζει την απόσταση μοναδικότητας (unicity distance) καλούμενη και σημείο μοναδικότητας προσεγγίζοντας την ποσότητα του κρυπτογραφήματος.

Τη δεκαετία του 1970 ο Dr. Horst Feistel στο Watson Research Laboratory της IBM δουλεύοντας στο σύστημα LUCIFER δημιούργησε τον πρόγονο του σημερινού ***Data Encryption Standard (DES)*** . Το 1976 η National Security Agency (NSA) σε συνεργασία με τον Feistel δημιούργησε τον αλγόριθμο FIPS PUB-46, γνωστό σήμερα σαν DES. Το σύστημα DES υιοθετήθηκε ως ομοσπονδιακό πρότυπο των ΗΠΑ για χρήση κατά την επικοινωνία μηνυμάτων μεταξύ κυβερνητικών υπηρεσιών και ως πρότυπο ιδιωτικού τομέα.

Το 1976 οι Diffie και Hellman, συνεργάτες του Feitsel, με το δημοσίευμα **New Directions in Cryptography**[1], έφεραν επανάσταση στο χώρο της Κρυπτογραφίας με την ιδέα της χρήσης του κοινόχρηστου κλειδιού ,όπου χρησιμοποιείτε μέχρι σήμερα .
Από τότε πολλές έρευνες γίνονται για την αναζήτηση και εξέλιξη ασφαλών κρυπτογραφικών συστημάτων, όπως ψηφιακές υπογραφές και κρυπτογραφικά πρωτόκολλα, μηχανισμούς γνησιότητας, ακεραιότητας, ελέγχου πρόσβασης και μη αμφισβήτησης.

1.2 Κρυπτογραφία και Ασφάλεια Πληροφοριών

Η έννοια της πληροφορίας θα πρέπει να λαμβάνεται σαν μια κατανοητή ποσότητα. Απαραίτητο για την εισαγωγή μας στην κρυπτογραφία, είναι να έχουμε κατανοήσει τα θέματα που είναι σχετικά με την ασφάλεια των πληροφοριών. Αυτή μπορεί να εκδηλώνεται διαφορετικά ανάλογα με την κατάσταση και τις απαιτήσεις μας. Ανεξαρτήτως, όλα τα μέλη μιας ανταλλαγής πληροφοριών πρέπει να γνωρίζουν ότι ικανοποιούνται κάποιοι κανονισμοί για την ασφαλή επίτευξη αυτής της επικοινωνίας. Για τον σκοπό αυτό από την αρχαιότητα μέχρι σήμερα , έχει δημιουργηθεί ένα σύνολο πρωτοκόλλων και μηχανισμών σχετικά με την ασφάλεια της μεταφοράς πληροφοριών.

Όταν αναφερόμαστε σε ασφαλή επικοινωνία πληροφοριών, δεν σημαίνει πως είναι αρκετό να εφαρμόζουμε μόνο μαθηματικούς αλγόριθμους και πρωτοκόλλα. Τι γίνεται όταν στέλνουμε φυσικά έγγραφα· Γι' αυτό το σκοπό υπάρχουν διαδικασίες και νόμοι, που πρέπει να τηρούνται μέσα στα πλαίσια της επίτευξης μιας ασφαλούς επικοινωνίας. Για την αποστολή ιδιωτικών επιστολών χρησιμοποιούνται ειδικοί σφραγισμένοι φάκελοι και

η μεταφορά τους γίνεται από τις αρμόδιες υπηρεσίες. Πολλές φορές η ασφάλεια επιτυγχάνεται με μέσω φυσικής εγγραφής στο έγγραφο, όπως για παράδειγμα στην χάραξη των χαρτονομισμάτων. Το ίδιο συμβαίνει και με τα μηνύματα ηλεκτρονικού ταχυδρομείου, όπου ο νόμος έχει και εκεί εφαρμογή και θεωρείται αδίκημα να ανοίγονται τα μηνύματα από μη εξουσιοδοτημένα άτομα.

Εννοιολογικά ο τρόπος που οι πληροφορίες καταγράφονται (σε χαρτί ή μαγνητικά μέσα) δεν έχει αλλάξει δραματικά. Αυτό που έχει αλλάξει πολύ είναι η ικανότητα να του να μπορούν να αντιγράφονται ή να τροποποιούνται , αφού σε ηλεκτρονική μορφή είναι ποιο εύκολο από ότι σε χαρτί. Πολύ σημαντικό εργαλείο σήμερα είναι και η χρήση της ψηφιακής υπογραφής που ενώ αντιστοιχεί μοναδικά σε κάθε άτομο , όπως η χειρόγραφη, είναι ποιο εύκολο να αντιγράφει.Απαραίτητο σε μια κοινωνία όπου βασίζεται στην ασφαλή αποθήκευση και μεταφορά ηλεκτρονικών πληροφοριών, είναι ένα μέσο που θα εξασφαλίζει την ασφάλεια αυτή ανεξάρτητα με το φυσικό μέσο εγγραφής. Η ασφάλεια των επικοινωνιών λοιπόν απαιτεί ένα ευρύ φάσμα νομικών και τεχνικών γνώσεων.[4, σελ.2-4] ***Τα τεχνικά μέσα που χρειάζονται για την ασφάλεια των πληροφοριών παρέχονται μέσω της επιστήμης της κρυπτογραφίας.***

1.3 Στόχοι κρυπτογραφίας

Ο αντικειμενικός σκοπός της κρυπτογραφίας είναι να δώσει την δυνατότητα σε δύο οντότητες, να επικοινωνήσουν μέσα από ένα μη ασφαλές κανάλι με τέτοιο τρόπο ώστε μια τρίτη οντότητα, μη εξουσιοδοτημένη , να μην μπορεί να παρεμβάλει στην επικοινωνία ή να κατανοήσει το περιεχόμενο των μηνυμάτων. Οι βασικοί στόχοι τις είναι τέσσερις και περιγράφονται παρακάτω[4, σελ.4]:

1. ***Εμπιστευτικότητα ή μυστικότητα (confidentiality)*** : το κρυπτογραφημένο μήνυμα που θα στείλει ο αποστολέας μέσω ενός μέσου μετάδοσης στον παραλήπτη, θα είναι αναγνώσιμο από αυτόν και μόνο, δηλαδή η διατήρηση της πληροφορίας κρυφής από όλους, εκτός από εκείνους που είναι εξουσιοδοτημένοι να τη δουν. Η πληροφορία αυτή σε τρίτο άτομο θα είναι ακατανόητη. Η εμπιστευτικότητα αναφέρεται στο περιεχόμενο ηλεκτρονικών αρχείων, την ύπαρξη τους στην ταυτότητα αυτών που επικοινωνούν και στον χρόνο και την ποσότητα ανταλλαγής.

2. ***Ακεραιότητα (integrity)***: είναι ένα άλλο σημαντικό κομμάτι της κρυπτογραφίας. Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη και δεν

μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης. Σημαίνει ότι η διασφάλιση της πληροφορίας έχει παραμείνει αμεταποίητη από την στιγμή που δημιουργήθηκε, μεταδόθηκε και κατά την διάρκεια της αποθήκευσης. Η ακεραιότητα είναι σημαντική για όλους όσους ανταλλάσσουν πληροφορίες, στο e-commerce, που είναι υπεύθυνοι για μυστικά εμπορικών συναλλαγών και για αυτούς που είναι εξαρτώνται από τις επικοινωνίες, όπως στον στρατό.

3. ***Πιστοποίηση (Authentication)***: είναι η τεχνική με την οποία κάποιος πιστοποιεί ότι αυτός με τον οποίο επικοινωνεί είναι αυτός που πρέπει και όχι κάποιος άλλος. Κατά την ίδρυση μιας συνόδου επικοινωνίας απαιτείται η αυθεντικοποίηση των ταυτοτήτων των επικοινωνούντων μελών, δηλαδή το κάθε μέλος αποδεικνύει την ταυτότητα του, προτού αρχίσει η ανταλλαγή πληροφοριών. Συγκεκριμένα στο ηλεκτρονικό εμπόριο είναι αναγκαίο να εξακριβωθεί η ταυτότητα του αποστολέα ενός ηλεκτρονικού εγγράφου. Όμως η εξακρίβωση της ταυτότητας μιας απομακρυσμένης οντότητας είναι αρκετά δύσκολη και απαιτεί σύνθετα πρωτόκολλα βασισμένα στην κρυπτογραφία.

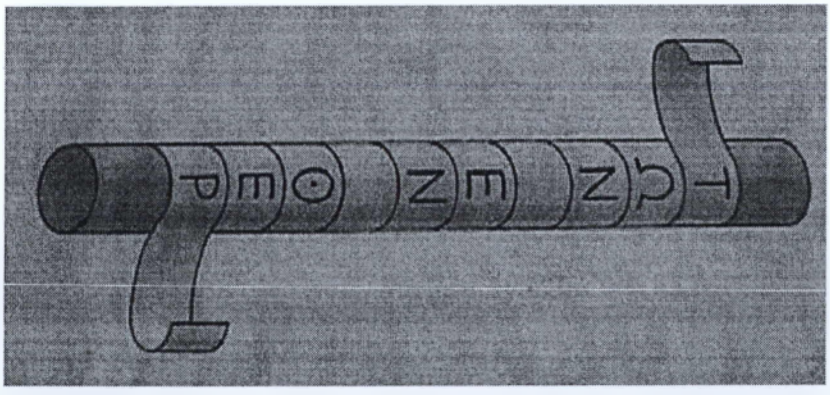
4. ***Μη απάρνηση (Non-repudiation)***: Είναι μια υπηρεσία που εμποδίζει μια οντότητα να αρνηθεί τις προηγούμενες δεσμεύσεις. Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.

1.4 Εφαρμογές Κρυπτογραφίας

Η εξέλιξη της της κρυπτογραφίας στην εποχή μας συνεχίζεται καθώς και των τηλεπικοινωνίων , της Πληροφορικής και άλλων επιστημών . Οι απαιτήσεις για ασφάλεια των πληροφοριών όλο και αυξάνονται και μαζί με αυτές και οι εφαρμογές της κρυπτογραφίας. Ακολουθούν μερικές από αυτές:

1. Ασφάλεια συναλλαγών σε τράπεζες δίκτυα - ATM
2. Κινητή τηλεφωνία (ΤΕΤΡΑ-ΤΕΤΡΑΠΟΛ-GSM)
3. Σταθερή τηλεφωνία (cryptophones)
4. Διασφάλιση Εταιρικών πληροφοριών
5. Στρατιωτικά δίκτυα (Τακτικά συστήματα επικοινωνιών μάχης)

6. Διπλωματικά δίκτυα (Τηλεγραφήματα)
7. Ηλεκτρονικές επιχειρήσεις (πιστωτικές κάρτες, πληρωμές)
8. Ηλεκτρονική ψηφοφορία
9. Ηλεκτρονική δημοπρασία
10. Ηλεκτρονικό γραμματοκιβώτιο
11. Συστήματα συναγερμών
12. Συστήματα βιομετρικής αναγνώρισης
13. Έξυπνες κάρτες
14. Ιδιωτικά δίκτυα (VPN)
15. Word Wide Web
16. Δορυφορικές εφαρμογές (δορυφορική τηλεόραση)
17. Ασύρματα δίκτυα (bluetooth, 802.11x)
18. Συστήματα ιατρικών δεδομένων και άλλων βάσεων δεδομένων
19. Τηλεσυνδιάσκεψη - Τηλεφωνία μέσω διαδικτύου (VOIP)



Κεφάλαιο 2

Κλασσικά Κρυπτοσυστήματα

Τα κλασσικά κρυπτοσυστήματα διακρίνονται στα συστήματα αναδιάταξης και αντικατάστασης. Βασίζονται στην επεξεργασία της γλωσσικής δομής των λέξεων του μηνύματος. Κάθε χαρακτήρας μιας λέξης αντιστοιχεί σε κάποιον του αλφαβήτου. Σκοπός είναι από το αρχικό μήνυμα κατόπιν εφαρμογών μεθόδων κρυπτογράφησης, να παραχθεί μια ακολουθία χαρακτήρων, ώστε να είναι ακατανόητο για οποιοδήποτε μη εξουσιοδοτημένο παραλήπτη να το διαβάσει.

2.1 Γενικευμένα σχήματα Αντικατάστασης χαρακτήρων

Η τεχνική της αντικατάστασης χαρακτήρων βασίζεται στην αντικατάσταση των χαρακτήρων του μηνύματος με άλλους χαρακτήρες, σύμβολα ή αριθμούς, ώστε να παράγεται ένα εντελώς διαφορετικό μήνυμα από το αρχικό και δυσνόητο. Υπάρχουν οι ακόλουθες τεχνικές αντικατάστασης:

2.1.1 Μονοαλφαβητικής αντικατάστασης

Η αποκρυπτογράφηση γίνεται μέσω της ανάλυσης συχνοτήτων των περισσότερο επιλαμβανόμενων κρυπτοχαρακτήρων ή ομάδων χαρακτήρων του μηνύματος, με αντικατάσταση τους από τους ποιο γνωστούς επαναλαμβανόμενους χαρακτήρες ή ομάδων χαρακτήρων της φυσική γλώσσας. Αυτό συνεχίζεται μέχρι να το μήνυμα που θα προκύψει να βγάζει νόημα. Για να επιτευχθεί αυτό χρησιμοποιούνται και κάποια βοηθητικά εργα-

λεία όπως:
[14]

1. **Η ανάλυση δομής γλώσσας.**

   1. Το πιο κοινό πρώτο γράμμα μέσα σε λέξεις:
   T, O, A, W, B, C, D, S, F, M, R, H, I, Y, E, G, L, N, U, J, K

   2. Το πιο κοινό δεύτερο γράμμα μέσα σε λέξεις:
   H, O, E, I, A, U, N, R, T

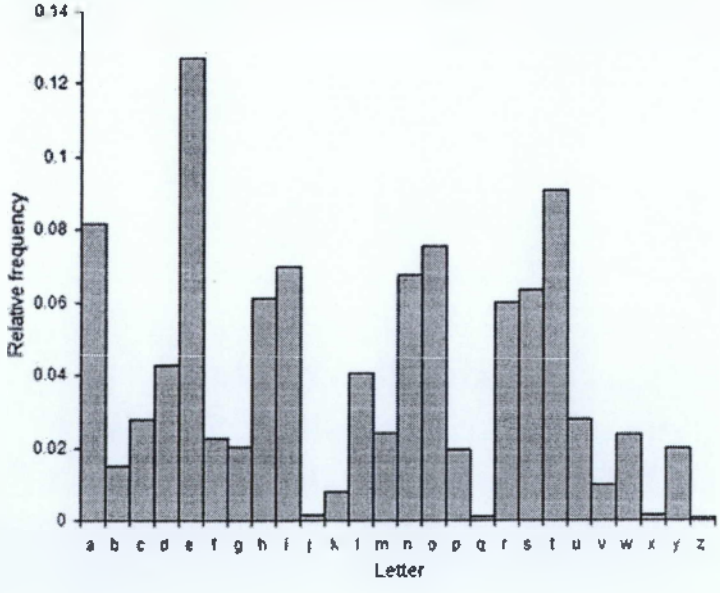
   3. Το πιο κοινό τρίτο γράμμα μέσα σε λέξεις:
   E, S, A, R, N, I

   4. Το πιο κοινό τελευταίο γράμμα μέσα σε λέξεις:
   E, S, T, D, N, R, Y, F, L, O, G, H, A, K, M, P, U, W

   5. Οι περισσότερες λέξεις τελειώνουν με:
   E ,T, D, S

   6. Τα γράμματα που ακολοθούν το: E, R,S,N,D

   7. Τα πιο κοινά διπλά γράμματα:
   SS, EE, TT, FF, LL, MM, OO



2. **Η N- γραμματική πιθανολογική ανάλυση.**

   Η Τριγραμματική ανάλυση σε ένα Αγγλικό κείμενο 763 λέξεων

Λέξεις	Εμφάνιση	Συχνότητα
The	91	11.9%
And	27	3.5%
Had	19	2.5%
Was	15	2%
That	13	1.7%

3. **Ακολουθιακή γραμματική ανάλυση κατά Marcov.**

   Το μήνυμα αναπαριστάται ως μια ακολουθία γραμμάτων. Τα γράμματα που παράγονται από ένα αλφάβητο όμως δεν είναι άσχετα μεταξύ τους αλλά συσχετιζόμενα και αλληλοεξαρτώμενα. Δηλαδή η πιθανότητα εμφάνισης ενός γράμματος εξαρτάται από το ίδιο αλλά και από το προηγούμενο. $P(x_j = b, x_{j-1} = a) = 0.0228302$. Σχηματίζεται ένας πίνακας 26x26 με όλους τους πιθανούς συνδυασμούς.

2.1.2 Ομοφωνικής αντικατάστασης.

[4, σελ.4] Σε κάθε σύμβολο a $\in A$, συσχετίζουμε ένα σύνολο $H(\mathrm{a})$ συμβολοσειρών των t συμβόλων, με τον περιορισμό ότι τα σύνολα $H(\mathrm{a}), \mathrm{a} \in A$, είναι ξένα ανά δύο. Παράδειγμα :Θεωρούμε τα σύνολα A = {a,b},H(a) $= \{00, 10\}$ και H(b) $= \{01, 11\}$. Το τμήμα του μηνύματος απλού κειμένου ab κρυπτογραφείται σε ένα από τα: 0001, 0011, 1001, 1011. Παρατηρούμε ότι το σύνολο τιμών της συνάρτησης κρυπτογράφησης αποτελείται από τα ακόλουθα σύνολα δυαδικών συμβολοσειρών των τεσσάρων στοιχείων:

aa $\leftarrow \{0000, 0010, 1000, 1010\}$

ab $\leftarrow \{0001, 0011, 1001, 1011\}$

ba $\leftarrow \{0100, 0110, 1100, 1110\}$

bb $\leftarrow \{0101, 0111, 1101, 1111\}$

Οποιαδήποτε δυαδική συμβολοσειρά των 4 bit προσδιορίζει μοναδικά ένα στοιχείο του συνόλου τιμών, και ως εκ τούτου, ένα μήνυμα απλού κειμένου.

2.1.3 Πολυαλφαβητικής αντικατάστασης

[4, σελ.4] Στα πολυαλφαβητικά κρυπτοσυστήματα κάθε γράμμα του μηνύματος αντικαθίσταται με ένα σύμβολο κάθε φορά από διαφορετικό αλφάβητο. Είναι από τους ποιο δυνατούς τύπους αντικατάστασης χαρακτήρων. Στην ουσία η κρυπτογράφηση γίνεται με διαφορετικές μονοαλφαβητικές αντικαταστάσεις. Υπάρχουν δύο τύποι:

Κλείδα και ακολουθία
Στην μέθοδο κλείδα και ακολουθία γράφουμε την κλείδα αφαιρώντας τα επαναλαμβανόμενα γράμματα και μετά συμπληρώνουμε τα υπόλοιπα γράμματα του αλφαβήτου.
Κλείδα και αναδιάταξη
Στην μέθοδο κλείδα και αναδιάταξη γράφουμε την κλείδα χωρίς επαναλαμβανόμενα γράμματα και γράφουμε από κάτω τα υπόλοιπα γράμματα σε γραμμές κάτω από τα αρχικά και διαβάζουμε τις στήλες που δημιουργούνται και τις τοποθετούμε στην στήλη κλειδιών.

Τετράγωνο Vigenere [9, σελ. 38]
Γράμματα κλειδιού Γράμματα Μηνύματος.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
E E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O O P Q R S T U V W X Y Z A B C D E F G H I J K L M N

P P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
S S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
W W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
X X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z Z A B C D E F G H I J K L M N O P Q R S T U V W X Y

Για κάθε χαρακτήρα δίνεται ένα γράμμα κλειδί.

Π.χ. ΜΗΝΥΜΑ : SPARTA

ΚΛΕΙΔΙ : AGJOBK

ΚΡΥΠΤΟΚΕΙΜΕΝΟ : SVJGUK

2.2 Σχήμα του Καίσαρα

Αξίζει να τονίσουμε μια από τις ποιο γνωστές μεθόδους μονοαλφαβητικής αντικατάστασης, είναι το «σχήμα του Καίσαρα». Σύμφωνα με αυτό ορίζεται ένας ακέραιος αριθμός κ από το 1 μέχρι όσα είναι τα γράμματα του αλφαβήτου που χρησιμοποιείται. Για το ελληνικό είναι 24-1=23. Τα μεταβαλλόμενα νούμερα κ που χρησιμοποιούνται ονομάζονται κλειδί. Αν το κ=3 τότε η αντιστοίχιση του αλφαβήτου θα είναι η παρακάτω[8, σελ.37-38]:

Κείμενο: α β γ δ ε ζ η θ ι κ λ μ ν ξ ο π ρ ς τ υ φ χ ψ ω

Κρυπτοκείμενο: δ ε ζ η θ ι κ λ μ ν ξ ο π ρ ς τ υ φ χ ψ ω α β γ

Π.χ. το Μ = το μήνυμα είναι κρυπτογραφημένο

Ε(Μ) = χς οκπψδ θμπμ ωυψτχσζυδωκοθπς

Ο παραλήπτης πρέπει να γνωρίζει το κλειδί κ=3 και να κάνει αντίστροφη αντιστοίχιση Α(Ε(Μ),3). Το πρόβλημα είναι ότι η αποκρυπτογράφηση είναι πολύ εύκολη.

2.3 Κρυπτοσυστήματα Αναδιάταξης

Τα κρυπτοσυστήματα αναδιάταξης μεταθέτουν τα σύμβολα του μηνύματος, αλλάζουν την σειρά των συμβόλων χωρίς να τα παραποιούν, δηλαδή κάνουν αναγραμματισμό. Το κείμενο τοποθετείται σε έναν πίνακα και μετά δίπλα σε κάθε γραμμή ξαναγράφουμε τα γράμματα με διαφορετική σειρά. Το καινούργιο κείμενο που παράγεται είναι το κρυπτογράφημα μας. Για να γίνει η αποκρυπτογράφηση ο παραλήπτης πρέπει να γνωρίζει τις στήλες του πίνακα και την σειρά τοποθέτησης τους. Το κλειδί μπορεί να είναι κωδικολέξεις που δείχνουν την πραγματική θέση των γραμμάτων μέσα στο κείμενο.[4, σελ.37-38]

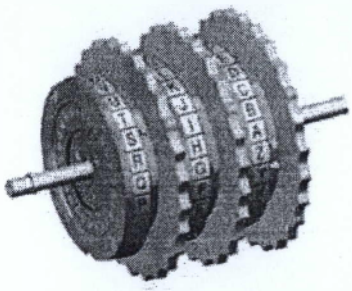
2.4 Σημιωματάριο μιας χρήσης

Σημειωματάριο μιας χρήσης **(one time pad)** είναι ένα κρυπτόγαμμα όπου το κλειδί είναι μια τυχαία ακολουθία bits με μεγάλη περίοδο. Το μήκος του κλειδιού είναι ίσο με το μήκος του μηνύματος. Το κλειδί χρησιμοποιείται μια φορά , ενώ τα στοιχεία του είναι άσχετα μεταξύ τους. Ο Shannon απέδειξε ότι είναι απεριόριστα ασφαλές. Τμήματα μιας ακολουθίας αριθμών γράφονται σε ένα σημειωματάριο. Ο αποστολέας κάθε φορά που χρησιμοποιείται ένα τμήμα για κρυπτογράφηση το διαγράφει αφού μπορεί να χρησιμοποιηθεί μόνο μια φορά . Ο παραλήπτης ο οποίος έχει στην κατοχή του ένα ίδιο σημειωματάριο αποκρυπτογραφεί το κρυπτογράφημα που συνοδεύεται από τον αριθμό της συγκεκριμένης σελίδας κρυπτογράφησης. Γνωστή ήταν η χρήση τους στον 2 Παγκόσμιο Πόλεμο. Το κρυπτοσύστημα που χρησιμοποιήθηκε είναι γνωστό ως κρυπτοσύστημα Vernam:

Το κρυπτοσύστημα Vernam είναι ένα κρυπτοσύστημα, όπου κρυπταλγόριθμος είναι αυτός του Vigenère και το μήκος του κλειδιού είναι ίδιο με το μήκος του κρυπτοκειμένου. Αν το μήνυμα είναι M και το κλειδί K τότε το κρυπτογράφημα C παράγεται από την χρήση μιας exclusive-or XOR μεταξύ του M και του K. $C = M \oplus K$. Η αποκρυπτογράφηση είναι $C \oplus K = M \oplus K \oplus K = M$.[4][σελ.21]

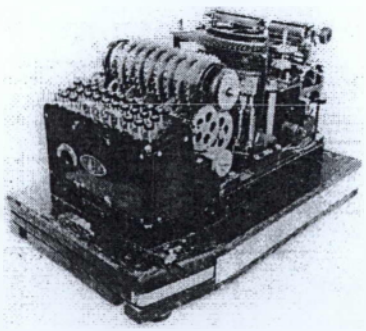
2.5 Ρότορες

Ο ρότορας είναι μια μηχανή που αποτελείται από ένα σύνολο στρεφόμενων κυλίνδρων όπου περνούν ηλεκτρικοί παλμοί. Κάθε ρότορας έχει ένα αλφάβητο και 26 εισόδους και εξόδους, με μια καλωδίωση. Σε κάθε είσοδο του έχει ένα γράμμα του αλφαβήτου που αντιστοιχεί σε ένα άλλο στην έξοδο. Όσο περισσότεροι είναι τόσο ποιο ισχυρή είναι η κρυπτογράφηση.[5, σελ.31]



Enigma

Μια συσκευή κρυπτογράφησης φτιαγμένη από γρανάζια και ρότορες που λειτουργούσε σαν μια ογκώδης γραφομηχανή. Μετέτρεπε το πάτημα του πλήκτρου σε ηλεκτρικό σήμα το οποίο με τη σειρά του περνούσε μέσα από ένα σύστημα τριών γραναζιών που αντιστοιχούσαν σε ένα νέο τυχαίο γράμμα κάθε φορά. Για να αποκρυπτογραφηθεί το μήνυμα έπρεπε όχι μόνο να υπάρχει μια δεύτερη enigma machine, αλλά και να έχει τα εσωτερικά γρανάζια στην ίδια ακριβώς θέση με το αρχικό για να παρακολουθεί το τυχαίο της κρυπτογράφησης. Αυτό φυσικά σημαίνει ότι το σύστημα της κρυπτογράφησης λειτουργούσε μόνο μεταξύ συγχρονισμένων enigma machines από την πρώτη στιγμή της λειτουργίας τους. Αναπτύχθηκε από Γερμανό εφευρέτη Arthur Scherbius.[11, σελ.26]



Κεφάλαιο 3

Σύγχρονα Κρυπτοσυστήματα

Τα σύγχρονα κρυπτοσυστήματα χωρίζονται σε δύο κατηγορίες τα συμμετρικά και τα ασύμμετρα. Στα συμμετρικά χρησιμοποιείται το ίδιο κλειδί και κατά την διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης. Στα ασύμμετρα ή δημοσίου κλειδιού χρησιμοποιείται διαφορετικό κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση.

3.1 Συμμετρικά κρυπτοσυστήματα

Τα συμμετρικά κρυπτοσυστήματα χρησιμοποιούν τεχνικές αντιμετάθεσης και αντικατάστασης. Είναι τα ποιο διαδεδομένα χρονικά, το απλό κείμενο εισάγεται σε ένα αλγόριθμο κρυπτογράφησης μαζί με το κλειδί. Βασική είναι η δημιουργία ενός ασφαλούς καναλιού μεταφοράς του κλειδιού αφού είναι το ίδιο για την κρυπτογράφηση και την αποκρυπτογράφηση. Η ασφάλεια των αλγορίθμων κρυπτογράφησης εξαρτάται από την μυστικότητα του κλειδιού. Τα σχήματα κρυπτογράφησης ονομάζονται συμμετρικού κλειδιού, ενώ το κλειδί τους συμμετρικό κλειδί.
Έστω m ένα μήνυμα που κρυπτογραφείται , e κλειδί κρυπτογράφησης ,d κλειδί αποκρυπτογράφησης και έστω e, d ανήκουν στον κλειδοχώρο k. Οπότε τα σύνολα μετασχηματισμών κρυπτογράφησης και αποκρυπτογράφησης είναι $(E_e : e \in K)$ και $(D_d : d \in K)$. Το κρυπτοκείμενο c που προκύπτει κατα την συμμετρική κρυπτογράφηση θα είναι:

$$E_e(m) = c$$

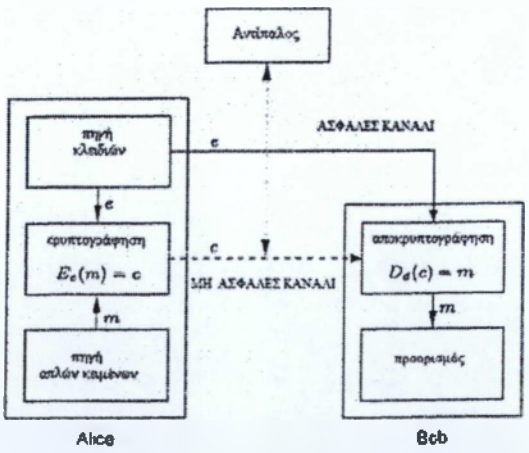
. Για την αποκρυπτογράφηση θα έχω:

$$D_d(c) = m$$

. Σε μια επικοινωνία συμμετρικού κλειδιού βασικό είναι η εύρεση μιας μεθόδου ανταλλαγής με ασφάλεια μέσα από ένα εμπιστευτικό και αυθεντικό κανάλι επικοινωνίας. Αυτό είναι γνωστό ως πρόβλημα συμμετρικού κλειδιού και οφείλεται στο γεγονός ότι $e = d$. Στην παρακάτω εικόνα αναπαρίσταται η επικοινωνία δύο μελών με συμμετρικό κλειδί κρυπτογράφησης.[4, σελ.15-16]

Τα στάδια της επικοινωνίας του σχήματος είναι τα ακόλουθα:

1. Η Alice ή ο Bob αποφασίζουν για ένα συμμετρικό κλειδί κρυπτογράφησης μέσα από την πηγή κλειδιών (κλειδοχώρο).
2. OBob στέλνει το κλειδί μέσα από ένα ασφαλές κανάλι.
3. Η Alice δημιουργεί ένα μήνυμα όπου τα σύμβολα m ανήκουν στον χώρο των μηνυμάτων.
4. Κρυπτογραφεί το μήνυμα με το κλειδί που έλαβε από τον Bob και το στέλνει.
5. OBob λαμβάνει το κρυπτοκείμενο και στην συνέχεια με το ίδιο κλειδί το αποκρυπτογραφεί και αναπαράγει το αρχικό μήνυμα (plaintext).



Η μόνη πληροφορία που πρέπει να μείνει μυστική είναι το κλειδί, αφού από το d μπορεί να παραχθεί το e. Υπάρχουν δύο κλάσεις σχημάτων συμμετρικού κλειδιού: **οι**

κρυπταλγόριθμοι τμήματος και ροής. Στου τμήματος χωρίζεται το μήνυμα απλού κειμένου σε τμήματα σταθερού μήκους και κρυπτογραφείται ένα τμήμα κάθε φορά. Οι κρυπταλγόριθμοι τμήματος χωρίζονται κυρίως σε κρυπταλγόριθμους αναδιάταξης, αντικατάστασης και γινομένου. Οι κρυπταλγόριθμοι ροής είναι στην ουσία απλοί κρυπταλγόριθμοι τμήματος με μήκος τμήματος ένα. Δεν παρουσιάζουν λάθος μετάδοσης και μπορούν να εφαρμόσουν διαφορετικό σχηματισμό κρυπτογράφησης για κάθε σύμβολο του μηνύματος. Γνωστός κρυπταλγοριθμός ροής είναι ο **Vernam**. Οι κρυπταλγόριθμοι τμήματος είναι ποιο ασφαλείς γι' αυτό και χρησιμοποιούνται όταν η ασφάλεια είναι προτεραιότητα , ενώ οι ροής έχουν παρέχουν καλύτερη ταχύτητα .

3.1.1 Κρυπταλγόριθμοι τμήματος (BLOCK CHIPERS)

Τρόποι λειτουργίας των(BLOCK CHIPERS)

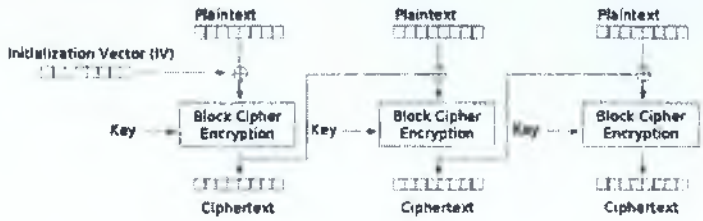
Οι κρυπταλγόριθμοι τμήματος χρησιμοποιούν κάποιους τρόπους λειτουργίας υπεύθυνους για την διασύνδεση τους. Ο σκοπός τους είναι η αύξηση της κρυπτογραφικής τους δύναμης και η αποτελεσματικότερη απόκρυψη πιθανών υπολειμμάτων πληροφορίας του απλού κειμένου που μπορεί να υπάρχει στο κρυπτοκείμενο.

1. **Ηλεκτρονικό κωδικοβιβλίο Electronic Code Book (ECB)**
   Το απλό κείμενο χωρίζεται σε τμήματα blocks , για κάθε ένα από αυτά δημιουργείται και το αντίστοιχο κρυπτογραφημένο. Δημιουργείται ένα βιβλίο με όλα τα ζευγάρια απλού κειμένου και κρυπτοκειμένου για κάθε κλειδί k.[7, σελ.158-163]
   Το κείμενο P χωρίζεται σε τμήματα $[p_1, p_2 \dots p_i]$, κάθε τμήμα αποτελείται από n bits και τροφοδοτείται στον αλγόριθμο.[13]
   Κρυπτογράφηση: $c_i = e_k p_i$,
   Αποκρυπτογράφηση: $p_i = d_k c_i$.

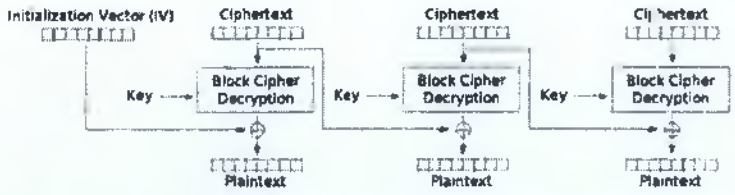
2. **Κρυπταλγόριθμος αλυσιδωτού τμήματος, Chiper Block Changing (CBC)**
   Και εδώ το απλό κείμενο χωρίζεται σε τμήματα blocks, κάθε τμήμα εξαρτάται από το προηγούμενο, αφού η κρυπτογράφηση τους γίνεται μετά από μια XOR του εκάστοτε τμήματος με το προηγούμενο. Οπότε με την αποκρυπτογράφηση του ενός τμήματος καταφέρνουμε την αποκρυπτογράφηση όλου του κειμένου.Το κείμενο P χωρίζεται σε τμήματα $[p_1, p_2 \dots p_i]$[13]
   Κρυπτογράφηση: $c_i = e_k(c_{i-1}) \oplus p_i, c_0 = IV$,
   Αποκρυπτογράφηση: $p_i = e_k(c_{i-1}) \oplus c_i, c_0 = IV$.

3. **Ανάδραση κρυπταλγόριθμου, Chiper Feed Back (CFB)** Λειτουργεί το ίδιο με τον τον (CBC), η μόνη διαφορά τους είναι ότι στον (CFB), τα δεδομένα κρυπτογραφούνται ανά byte και κάθε byte με τα 7 προηγούμενα του.[7, σελ.158-163]

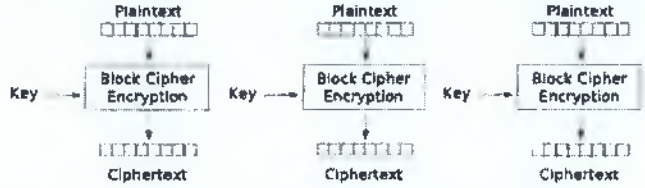
4. **Ανάδραση εξόδου, Output Feed Back (OFB)** Λειτουργεί το ίδιο με τον τον (CFB), μόνο που παρέχει ένα μηχανισμό για την μείωση λαθών.[7, σελ.158-163]



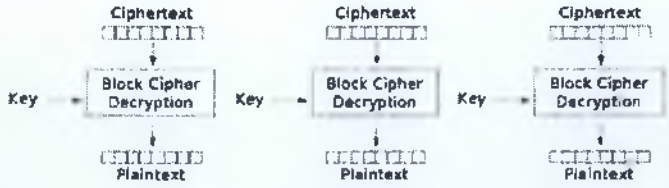
Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption



Electronic Codebook (ECB) mode encryption



Electronic Codebook (ECB) mode decryption

Συμμετρικοί Αλγόριθμοι τμήματος

- **Data Encryption Standard (DES)**
  Το 1972 η NBS (Εθνικό Γραφείο Προτύπων, τώρα NIST, [17]το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας) θέλησε ένα πρότυπο τυποποίησης αλγορίθμου για κρυπτογράφηση, πάνω σε ενα πρόγραμμα για την προστασία των δεδομένων. Το 1974, η IBM πρότεινε ένα σχήμα με βάση τον αλγόριθμο "Lucifer", που εξελίχθηκε στον DES.Ένα ισχυρό αλγόριθμο ευρείας χρήσης με μεγάλη επιρροή στην κρυπτογραφία ο οποίος ανα πέντε χρόνια πιστοποιείται ξανά και ξανά. Η πολυπλοκότητα σε σχέση με το ισχυρό για την εποχή του μήκος κλειδιού τον καθιέρωσε ως παγκόσμιο τραπεζικό πρότυπο. Ο αλγόριθμος DES δέχεται στην είσοδο του κλειδί K μήκους 56 bit και plaintext M= 64 bit και δίνει στην έξοδο 64 bit. Κάνει 16 γύρους γνωστό ως **Feistel network** και για κάθε έναν παράγει 16 δευτερεύοντα κλειδία. Τα κλειδια έχουν μήκος 48 bit. Αρχικά αντιμεταθέτει τα bit του plaintetx, για είσοδο 1 bit έχω έξοδο 58, για 2 έχω 50 και μετά τα αντιστρέφει. Παρακάτω βλέπουμε τον πίνακα της αρχικής αντιμετάθεσης τον αντίστροφο του :[6, κεφ.2, σελ.3-5]

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

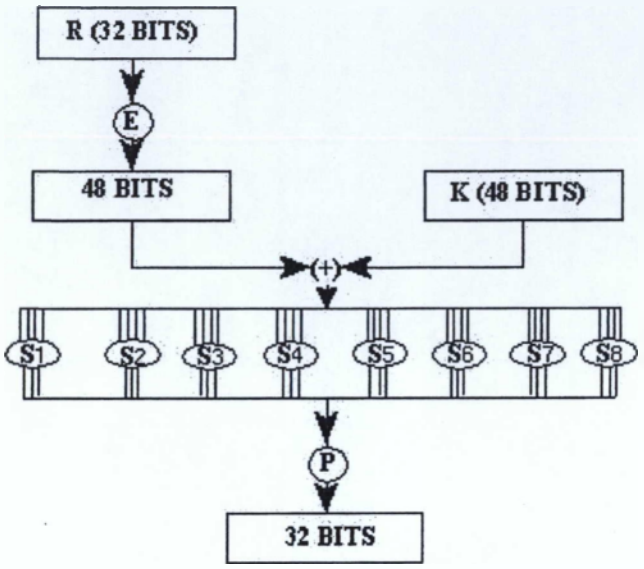
IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Αφού έχει αντιμετατεθεί το M χωρίζεται σε δύο τμήματα 32 αριστερά και 32 δεξιά και εισέρχεται ως είσοδος σε ένα βρόγχο 16 επαναλήψεων ενός μετασχηματισμού f , το R=32 bit με μια αντιμετάθεση γίνεται 48 και υποβάλεται σε μια XOR με τα 48 bit του κλειδιού της τρέχοντος επανάληψης.

Ακολουθεί το σχήμα αναπαράστασης:

Τα 48 bit που προέκυψαν από την **XOR** χωρίζονται σε οκτώ S-Boxes ή πίνακες αντικατάστασης των 6 bits. Ο κάθε πίνακας αντικατάστασης δίνει στην έξοδο 4 bits και μετά απο την εφαρμογή μιας καινουργιας αντιμετάθεσης P, από το αριστερό μέρος της εισόδου παράγονται συνολικά 32 bits, που δίνονται ως καινούργια είσοδος στο δεξί τμήμα την επόμενης επανάληψης. (Αντίστοιχα Λειτουργεί και το δεξί τμήμα της πρώτης επανάληψης δίνοντας είσοδος στο αριστερό τμήμα της επόμενης επανάληψης). Στο τέλος των επαναλήψεων τα 64 bits που προκείπτουν υπόκεινται σε μια τελευταία αντιμετάθεση των δυαδικών τους ψηφίων.[8, σελ.59-61]



- **2DES**

  Το μήκος κλειδιού 56bit στον DES ήταν εύκολο να σπάσει, για λόγους αφάλειας έπρεπε να βρεθεί ένας τρόπος να αντιμετωπιστεί αυτό. Ο 2DES χρησιμοποιεί μήκος κελιδιού 112 bit. Έστω K_1, K_2 56bit κλειδιά με plaintext 64 bit. Το μήνυμα κρυπτογραφείται με το κλειδί K1 και το αποτέλεσμα με το κλειδί K2. Το κρυπτογραφημένο μήνυμα που παράγεται αποκρυπτογραφείται με το κλειδί K_2 και το αποτέλεσμα με το κλειδί K_1.

  $$2DES(K_1||K_2, M) = DES(K_2, DES(K_1, M)$$

  [6, κεφ.2, σελ.9-10]

- **3DES**

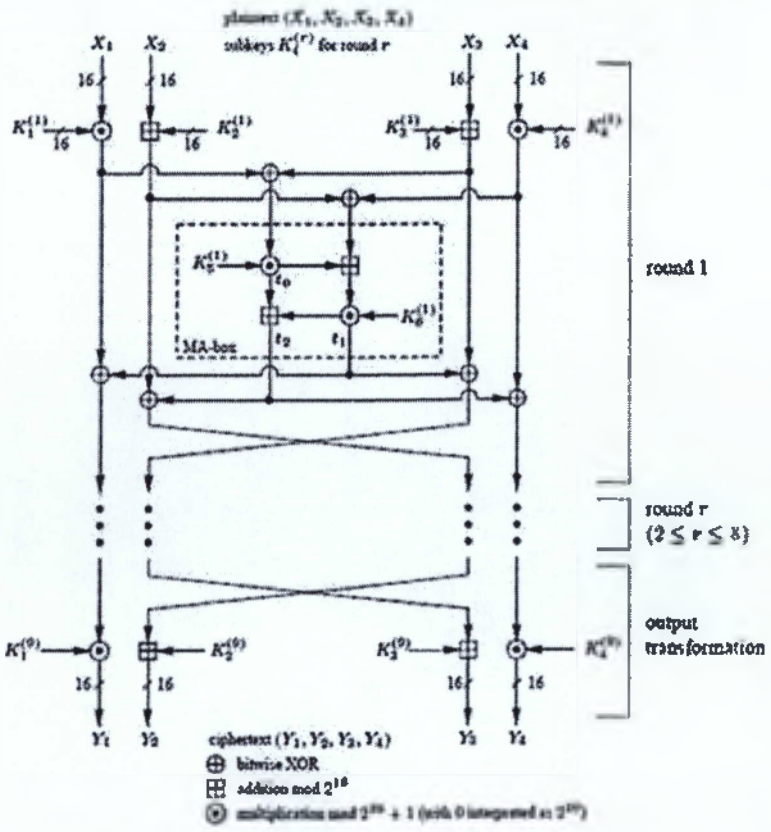
  Ο 3DES χρησιμοποιεί τρεις επαναλήψεις του DES άρα και τρία κλειδιά συνολικού μήκους168 bit. Έστω $K_1, K_2, K_3$56 bit κλειδιά με M plaintext 64 bit. Θεωρείται ποιό ισχυρός από τον DES αλλά μειονεκτεί όσο αναφορά την ταχύτητα. Μπορεί να λέιτουργήσει συμβατά με τον DES ή ανεξάρτητα.[6, κεφ.2, σελ.9-10]

  $$3DES3(K_1||K_2||K_3, M) = DES(K_3, DES^{-1}(K_2, DES(K_1, M)$$

- **IDEA**

  IDEA (International Data Encryption Algorithm)

Κρυπτογραφεί 64 bit plaintext σε 64 bit chipertext με κλειδί εισόδου K 128 bit. Βασισμένος στην δομή του Feitsel, αποτελείται από 8 κύκλους υπολογισμού σε μια έξοδο μετατροπής. Σε κάθε κύκλο r χρησιμοποιούνται υποκλειδιά των 16 bit $K_i^{(r)}, 1 \leq i \leq 6$, για την μετατροπή των 64 bit X εισόδου σε μια έξοδο από 16 bit block τα οποία αποτελούν την είσοδο για τον επόμενο κύκλο. Στον 8 γύρο εξόδου εισάγει την έξοδο μετατροπής με 4 επιπλέον υποκλειδιά και παράγει το τελικό Y κρυπτογράφημα.[5, κεφ. 13.9]



(1) Multiply X1 and the first subkey.
(2) Add X2 and the second subkey.
(3) Add X3 and the third subkey.
(4) Multiply X4 and the fourth subkey.
(5) XOR the results of steps (1) and (3).
(6) XOR the results of steps (2) and (4).
(7) Multiply the results of step (5) with the fifth subkey.
(8) Add the results of steps (6) and (7).
(9) Multiply the results of step (8) with the sixth subkey.

(10) Add the results of steps (7) and (9).
(11) XOR the results of steps (1) and (9).
(12) XOR the results of steps (3) and (9).
(13) XOR the results of steps (2) and (10).
(14) XOR the results of steps (4) and (10). [5][13.9]

3.1.2 Κρυπταλγόριθμοι ροής

Οι κρυπταλγόριθμοι ροής διαφέρουν από τους κρυπταλγόριθμους τμήματος στο ότι κρυπτογραφούν μεμονωμένους χαρακτήρες (συνήθως δυαδικά ψηφία) ενός μηνύματος απλού κειμένου, χρησιμοποιώντας έναν μετασχηματισμό κρυπτογράφησης ο οποίος μεταβάλλεται με τον χρόνο. Επίσης είναι ταχύτεροι από του τμήματος σε επίπεδο υλικού. Προτιμούνται σε περιπτώσεις που έχουμε περιορισμένη προσωρινή μνήμη ή όταν η χαρακτήρες απαιτούν μεμονωμένη επεξεργασία.Ακόμα έχουν περιορισμένο ή και μηδενικό αριθμό σφαλμάτων μεταβίβασης.[4, σελ.191]
Υπάρχουν όμως κάποια κριτήρια που πρέπει να πληρούνται από έναν κρυπταλγόριθμο ροής. Σύμφωνα με τον Kumar αυτά είναι τα ακόλουθα:[7, σελ. 204]
Η περίοδος της κλειδοροής θα πρέπει να είναι όσο το δυνατόν μεγαλύτερη για λόγους αξιοπιστίας. Η ακολουθία έχει πεπερασμένο μέγεθος και σε κάποια στιγμή επαναλαμβάνεται.
Τα bits της ακολουθίας της κλειδοροής θα πρέπει να περνάν με επιτυχία όλους τους γνωστούς ελέγχους περί τυχαιότητας.
Το κλειδί του κρυπταλγόριθμου ροής καθορίζει την αρχική κατάσταση της γεννήτριας της κλειδοροής, που αντιστοιχεί στον προσδιορισμό της αρχικής θέσης στην περιοδική ακολουθία της κλειδοροής.

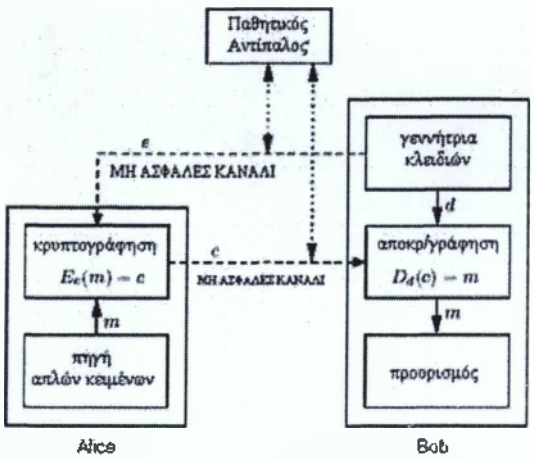
Ο κρυπταλγόριθμος RC4

Ο RC4 είναι από τους πιο διαδεδομένους κρυπταλγόριθμους ροής. Χρησιμοποιείται από πρωτόκολλα ασφαλείας όπως το SSL και για μεγάλο μήκος κλειδιού θεωρείται ασφαλής. Στον RC4 το αλφάβητο του απλού κειμένου αποτελείται από τα γράμματα του συνόλου $\{0,1\}^8$. Οι αποθηκευτικοί χώροι απαρτίζονται από δύο πίνακες $S[0..255]$ και $T[0..255]$, όπου το κάθε στοιχείο του πίνακα αντιστοιχεί σε δυαδική λέξη των 8 bits. Παρόλο που ο RC4 είναι πολύ απλός στην κατασκευή, για μέγεθος κλειδιού ίσο με 128 bits και άνω, παραμένει ασφαλής. Οι σχετικά μικρές απαιτήσεις σε μνήμη και υπολογιστική ισχύ, καθιστούν τον RC4 μια από τις πρώτες επιλογές ως κρυπταλγόριθμο ροής.[7, σελ. 207]

Ο RC4 είναι αρκετά γρήγορος και μπορεί να χρησιμοποιεί κλειδιά μεταβλητού μήκους. Λόγω ταχύτητας μπορεί να χρησιμοποιηθεί σε αρκετές σύγχρονες εφαρμογές. Στη ουσία είναι μια γεννήτρια παραγωγής ψευδοτυχαίων αριθμών με τα αποτελέσματα να προστίθενται αλγεβρικά XOR με την δυαδική ακολουθία δεδομένων. Γι' αυτό και δεν πρέπει να χρησιμοποιεί το ίδιο κλειδί για να κρυπτογραφήσει δύο διαφορετικές ακολουθίες. [12][σελ.133]

3.2 Ασσύμετρη Κρυπτογράφηση(Δημοσίου κλειδιού)

Στην ασσύμετρη κρυπτογράφια ή δημοσίου κλειδιού χρησιμοποιούνται δύο διαφορετικά κλειδιά, ένα για την κρυπτογράφηση (δημόσιο) και έναι για την αποκρυπτογράφηση (ιδιωτικό). Έστω k=κλειδοχώρος και έχουμε $\{E_e : e \in K\}$ για κρυπτογράφηση και $\{D_d : d \in K\}$ για αποκρυπτογράφηση, $\{c \in C\}$ το κρυπτοκείμενο μας και $\{m \in M\}$ το μήνυμα. Χρησιμοποιούμε ένα (E_e, D_d), (και να είναι γνωστό το E_e είναι αδύνατο να υπολογίσουμε το μήνυμα) ώστε $E_e(m) = c$. Έστω ο Bob διαλέγει ένα (e,d) για να επικοινωνήσει με την Alice σύμφωνα με το σχήμα που ακολουθεί:



1. Ο Bob στέλνει το δημόσιο κλειδί e στην Alice χρησιμοποιώντας ένα μη ασφαλές κανάλι και κρατάει αυτός το ιδιωτικό κλειδί k.
2. Η Alice στέλνει ένα μήνυμα mστον Bob κρυπτογραφώντας το με το δημόσιο κλειδί.
3. Ο Bob λαμβάνει το κρυπτογράφημα c το οποίο αποκρυπτογραφεί χρησιμοποιώντας το κρυφό κλειδί d.

Το κλειδί κρυπτογράφησης δεν χρειάζεται να είναι κρυφό για αυτό και χρησιμοποιείται μη ασφαλές κανάλι επικοινωνίας. Εάν το γνωρίζει κάποιος δεν μπορέι να υπολογίσει το ιδιωτικό κλειδί σε αντίθεση με την συμμετρική κρυπτογράφηση που χρησιμοποιείται το ίδιο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση.

3.2.1 Ασύμμετροι αλγόριθμοι Κρυπτογράφησης

El Gamal

[4][σελ.294 -295] Το El Gamal σχήμα κρυπτογράφησης μπορούμε να το δούμε και σαν την συμφωνία κλειδιού του Diffie-Hellman . Σκοπός του αλγορίθμου είναι να καταστήσει εφικτή και ασφαλή μεταξύ δύο χρηστών την ανταλλαγή ενός μυστικού κλειδιού το οποίο ακολούθως θα χρησιμοποιηθεί για κρυπτογράφηση.Η αποτελεσματικότητά του βασίζεται στη δυσκολία υπολογισμού διακριτών λογαρίθμων.

Έστω θέλει να επικοινωνήσει ο Α με τον Β. Κάθε ένας απο τους δύο πρέπει να δημιουργήσει ένα ιδιωτικό και ένα δημόσιο κλειδί.Η δημιουργία των κλειδιών γίνεται με τα ακόλουθα βήματα:

- Πρώτα δημιουργεί έναν τυχαίο μεγάλο πρώτο αριθμό p και μια γεννήτρια α της παλλαπλασιαστικής ομάδας Z_p^* των ακεραίων του modulo p.
- Επιλέγει έναν τυχαίο ακέραιο a, $1 \leq a \leq p-2$ και υπολογίζει το $a^a \ mod \ p$.
- Το δημόσιο κλειδί του είναι το (p, a, a^a) και το ιδιωτικό α.

Ακολουθεί πως ο Β θα κρυπτογραφήσει ένα μήνυμα και ο Α θα το αποκρυπτογραφήσει.

Κρυπτογράφηση

Ο Β κάνει τα ακόλουθα:

- Παίρνει το αυθεντικό δημόσιο κλειδί του Α.
- Αναπαριστά το μήνυμα σαν έναν ακέραιο m στο εύρος $\{0, 1, ..., p-1\}$.
- Επιλέγει έναν τυχαίο ακέραιο k,$1 \leq k \leq p-2$.
- Υπολογίζει γ= $a^k \ mod \ p$ και δ= $m(a)^{a^k} \ mod \ p$.
- Στέλνει το κρυπτογράφημα c=(γ,δ) στον Α.

Αποκρυπτογράφηση

Ο Α για να ανακτήσει το αρχικό μήνυμα από το κρυπτογράφημα κάνει τα ακόλουθα:

- Χρησιμοποιεί το ιδιωτικό κλειδι a για να υπολογίσει το $\gamma^{p-1-a}\ mod\ p$.
- Ανακτά το m υπολογίζοντας το $(\gamma^{-a})\ \delta\ mod\ p$.

Όσο αναφορά στην ασφάλεια του σχήματος κρυπτογράφησης έχει να κάνει με το p το οπόιο πρέπει να έχει 1024 bit το λιγότερο. Γενικά είανι σημαντικό το μέγεθος που πέρνουν οι παραμέτροι του , εξαιτίας της αύξησης του χρόνου υλοποίησης της κρυπτογράφησης και της διαστολής του chipertext. Για το λόγο αυτό συνίσταται μικρότερο μέγεθος modulus.

RSA

Ο RSA πήρε το όνομα του από τους R. Rivest, A. Shamir, και L. Adleman, είναι το ποιο ευρέως διαδεδομένο σχήμα κρυπτογράφησης δημοσίου κλειδιού παρέχει απόρρητο και ψηφιακή υπογραφή και η ασφάλεια του βασίζεται στην παραγοντοποίηση ακεραίου.Αυτό το κρυπτοσύστημα αναλύεται στο δεύτερο μέρος αυτής της εργασίας.

Rabin pubic key

[4][σελ.292] Προτάθηκε το 1979 από τον M.O. Rabin και η ασφάλεια του έγκειται επίσης στη δυσκολία παραγοντοποίησης μεγάλων ακεραίων. Έστω θέλει να επικοινωνήσει ο Α με τον Β. Κάθε ένας απο τους δύο πρέπει να δημιουργήσει ένα ιδιωτικό και ένα δημόσιο κλειδί.Η δημιουργία των κλειδιών γίνεται με τα ακόλουθα βήματα:

- Δημιουργεί δύο τυχαίους μεγάλους πρώτους αριθμούς p,q ιδίου μεγέθους.
- Υπολογίζει $n = pq$.
- Το δημόσιο κλειδί του Α είναι το n και το ιδιωτικό (p,q).

Ακολουθεί πως ο Β θα κρυπτογραφήσει ένα μήνυμα και ο Α θα το αποκρυπτογραφήσει.

Κρυπτογράφηση

Ο Β κάνει τα ακόλουθα:

- Παίρνει το αυθεντικό δημόσιο κλειδί του Α.
- Αναπαριστά το μήνυμα σαν έναν ακέραιο m στο εύρος $\{0, 1, ..., p-1\}$.

- Υπολογίζει το $c = m^2 \ mod \ n$.
- Στέλνει το κρυπτογράφημα c στον Α.

Αποκρυπτογράφηση
Ο Α για να ανακτήσει το αρχικό μήνυμα από το κρυπτογράφημα κάνει τα ακόλουθα:

- Χρησιμοποιεί τον κατάλληλο αλγόριθμό για να βρεί τις τετραγωνικές ρίζες των $m_1, m_2, m_3, m_4, c \ modulo \ n^2$.
- Το μήνυμα που στάλθηκε είναι ένα από τα τέσσερα. Με βάση τον πλεονασμό θα επιλέξει ένα από τα τέσσερα.

3.3 Υβριδικά Κρυπτοσυστήματα (ψηφιακού φακέλου)

Τα συμμετρικά κρυπτοσυστήματα είναι πόλύ ταχύτερα από του δημοσίου κλειδιού, ειδικά όταν έχουμε μηνύματα μεγάλου όγκου.Ο συνδυασμός των τεχνικών της συμμετρικής και της ασύμμετρης κρυπτογραφίας ονομάζεται υβριδική κρυπτογραφία ή ψηφιακου φακέλου digital envelope. Η υβριδική κρυπτογραφία μπορεί να χρησιμοποιηθεί για πολλούς παραλήπτες ταυτόχρονα. Για να δημιουργηθεί ένας ψηφιακός φάκελος ακολουθείται η παρακάτω διαδικασία:

1. Δημιουργείται ένα συμμετρικό κλειδί με χρήση ενός αλγορίθμου συμμετρικής κρυπτογραφίας.

2. Η αρχική πληροφορία κρυπτογραφείται με το συμμετρικό κλειδί που έχει δημιουργηθεί.

3. Το συμμετρικό κλειδί κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη.

4. Τα δύο κρυπτογραφημένα κείμενα αποτελούν τον ψηφιακό φάκελο του παραλήπτη.

Ο παραλήπτης ανοίγει τον ψηφιακό του φάκελο αποκρυπτογραφώντας με το ιδιωτικό κλειδί του το κρυπτογραφημένο συμμετρικό κλειδί. Με χρήση του συμμετρικού κλειδιού

- Υπολογίζει το $c = m^2 \ mod \ n$.
- Στέλνει το κρυπτογράφημα c στον Α.

Αποκρυπτογράφηση
Ο Α για να ανακτήσει το αρχικό μήνυμα από το κρυπτογράφημα κάνει τα ακόλουθα:

- Χρησιμοποιεί τον κατάλληλο αλγόριθμό για να βρεί τις τετραγωνικές ρίζες των $m_1, m_2, m_3, m_4, c \ modulo \ n^2$.
- Το μήνυμα που στάλθηκε είναι ένα από τα τέσσερα. Με βάση τον πλεονασμό θα επιλέξει ένα από τα τέσσερα.

3.3 Υβριδικά Κρυπτοσυστήματα (ψηφιακού φακέλου)

Τα συμμετρικά κρυπτοσυστήματα είναι πόλύ ταχύτερα από του δημοσίου κλειδιού, ειδικά όταν έχουμε μηνύματα μεγάλου όγκου.Ο συνδυασμός των τεχνικών της συμμετρικής και της ασύμμετρης κρυπτογραφίας ονομάζεται υβριδική κρυπτογραφία ή ψηφιακου φακέλου digital envelope. Η υβριδική κρυπτογραφία μπορεί να χρησιμοποιηθεί για πολλούς παραλήπτες ταυτόχρονα. Για να δημιουργηθεί ένας ψηφιακός φάκελος ακολουθείται η παρακάτω διαδικασία:

1. Δημιουργείται ένα συμμετρικό κλειδί με χρήση ενός αλγορίθμου συμμετρικής κρυπτογραφίας.

2. Η αρχική πληροφορία κρυπτογραφείται με το συμμετρικό κλειδί που έχει δημιουργηθεί.

3. Το συμμετρικό κλειδί κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη.

4. Τα δύο κρυπτογραφημένα κείμενα αποτελούν τον ψηφιακό φάκελο του παραλήπτη.

Ο παραλήπτης ανοίγει τον ψηφιακό του φάκελο αποκρυπτογραφώντας με το ιδιωτικό κλειδί του το κρυπτογραφημένο συμμετρικό κλειδί. Με χρήση του συμμετρικού κλειδιού

ο παραλήπτης αποκρυπτογραφεί το αρχικό κείμενο. Μετά την επίτευξη μιας ασφαλούς επικοινωνίας μεταξύ αποστολέα και παραλήπτη το συμμετρικό κλειδί καταστρέφεται. Αντί για μηνύματα, τα συστήματα δημοσίου κλειδιού μπορούν να χρησιμοποιηθούν για να κρυπτογραφούν συμμετρικά κλειδιά.Η χρήση της υβριδικής κρυπτογραφίας βοήθα στο να ξεπεραστούν κάποιες σημαντικές αδυναμίες της κρυπτογραφίας δημοσίου κλειδιού. [20]

3.4 Μειονεκτήματα - Πλεονεκτήματα συμμετρικής και ασσύμμετρης κρυπτογράφησης

[4, σελ.31-32]

Πλεονεκτήματα συμμετρικής κρυπτογράφησης

- Οι συμμετρικοί αλγόριθμοι είναι έχουν πολύ υψηλούς ρυθμούς κρυπτογράφησης.
- Έχουν κλειδιά μηκρού μήκους.
- Οι κρυπταλγόριθμοι μπορούν να χρησιμοποιηθούν σαν εργαλεία κρυπτογράφησης. Όπως στην κατασκευή γεννητριών ψευδοτυχαίων αριθμών, σε συναρτήσεις διασποράς και σε σχήματα ψηφιακών υπογραφών.
- Ειναι απλοί κρυπταλγόριθμοι που μπορούν να παράγουν ή να συνθέσουν, την κατασκευή ισχυρών κρυπταλγόριθμων γινομένου.

Μειονεκτήματα συμμετρικής κρυπτογράφησης

- Σε μια επικοινωνία το κλειδί είναι κοινό και πρέπει να μείνει μυστικό και από την πλευρά του παραλήπτη και του αποσιολέα.
- Σε μια επικοινωνία δύο οντοτήτων το κλειδί πρέπει να αλλάζει συχνά για λόγους ασφαλείας.
- Σε μεγάλα δίκτυα είναι απαράιτητη η χρήση έμπιστου τρίτου ατόμου χωρίς όρους , για αποτελεσματικότερη διαχείρηση των κλειδιών.

- Οι μηχανισμοί ψηφιακών υπογραφών απαιτούν ή μεγάλα κλειδιά ή την χρήση έμπιστων τρίτων ατόμων (TTP) για την διαχείρηση τους.

Πλεονεκτήματα ασύμμετρης κρυπτογράφησης

- Μυστικό πρέπει να μένει μόνο το ιδιωτικό κλειδί.
- Για την διαχείρηση των κλειδιών ενός δικτύου είναι αρκετή μόνο η παρουσία ενός TTP ατόμου ενώ στην συμμετρική κρυπτογράφηση η άνευ όρων εμπιστοσύνη.
- Ένα ζευγος ιδιωτικού/ δημοσίου κλειδιού μπορεί να μείνει ίδιο για αρκετές επικοινωνίες μεταξύ δύο οντοτήτων, χωρίς να μεταβληθεί ακόμα και αν δεν χρησιμοποιείται για κάποιο χρονικό διάστημα.
- Διαθέτουν αποδοτικούς μηχανισμούς ψηφιακής υπογραφής με μικρότερο κλειδί για την δημόσια συνάρτηση επαλήθευσης.
- Σε μεγάλα δίκτυα χρησιμοποιούν λιγότερα κλειδια σε αντίθεση με τα συμμετρικά κλειδιά.

Μειονεκτήματα ασύμμετρης κρυπτογράφησης

- Οι ασσύμετροι κρυπταλγόριθμοι είναι ποιό αργοι σε σύκγριση με τους συμμετρικούς.
- Έχουν πολύ μεγαλύτερα μεγέθη κλειδιών από τα συμμετρικά κλειδιά και μέγεθος υπογραφών δημοσίου κλειδιού.
- Κανένα σχήμα δεν έχει αποδειχθεί ότι είναι ασφαλές. Τα πιό ασφαλή βασίζονται στην δυσκολία ενός μικρού συνόλου προβλημάτων της θεωρίας των αριθμών.

Κεφάλαιο 4

Ψηφιακές Υπογραφές-Αυθεντικοποίηση

4.1 Ψηφιακές Υπογραφές

[4, κεφ.11] Η ψηφιακή υπογραφή (Digital signature) είναι ένα μαθηματικό σύστημα που τεχνολογικά ισοδυναμεί με την χειρόγραφη υπογραφή. Είναι μια έννοια της κρυπτογραφίας που έχει πολλές εφαρμογές στην ασφάλεια δεδομένων και συσχετίζει ένα μήνυμα με τον δημιουργό του. Σημαντική είναι η εφαρμογή της στην πιστοποίηση δημοσίων κλειδιών σε μεγάλα δίκτυα. Το πρώτο σχήμα ψηφιακών υπογραφών που ανακαλύφθηκε ήταν το RSA, το οποίο είναι το ποιο διαδεδομένο και χρησιμοποιείται μέχρι σήμερα. Ουσιαστικά ένα σχήμα αποτελείται από των συνδυασμό τριών αλγορίθμων. Έναν για παραγωγή κλειδιών , έναν αλγόριθμο παραγωγή ψηφιακής υπογραφής και έναν επαλήθευσης.

Τα σχήματα ψηφιακών υπογραφών χωρίζονται σε δύο κατηγορίες ανάλογα με το αν απαιτείται η είσοδος του πρωτότυπου μηνύματος στον αλγόριθμο επαλήθευσης ή όχι. Στην πρώτη περίπτωση λέγονται με παράτημα και στην δεύτερη με ανάκτηση μηνύματος. Αν το $|R| > 1$ το σχήμα ονομάζεται τυχαιοκρατικό αλλιώς αιτιοκρατικό.

Συμβολισμός	Σημασία
$\mathcal{M}$	ένα σύνολο στοιχείων που λέγεται *χώρος μηνυμάτων*.
$\mathcal{M}_S$	ένα σύνολο στοιχείων που λέγεται *χώρος υπογραφής* (signing space).
$\mathcal{S}$	ένα σύνολο στοιχείων που λέγεται *χώρος υπογραφών* (signature space).
R	μια 1–1 απεικόνιση από το $\mathcal{M}$ στο $\mathcal{M}_S$ που λέγεται *συνάρτηση περίσσειας*.
$\mathcal{M}_R$	η εικόνα της R (δηλ. $\mathcal{M}_R = \mathrm{Im}(R)$).
R^{-1}	η αντίστροφη της R (δηλ. $R^{-1} : \mathcal{M}_R \to \mathcal{M}$).
$\mathcal{K}$	ένα σύνολο στοιχείων που λέγεται *σύνολο δεικτοδότησης για υπογραφή*.
h	μια μονόδρομη συνάρτηση με πεδίο ορισμού $\mathcal{M}$.
$\mathcal{M}_h$	η εικόνα της h (δηλ. $h : \mathcal{M} \to \mathcal{M}_h$)· το $\mathcal{M}_h \subseteq \mathcal{M}_S$ λέγεται *χώρος τιμών διασποράς*.

4.1.1 Σχήματα ψηφιακών υπογραφών με παράρτημα.

Τα σχήματα με παράρτημα βασίζονται στις συναρτήσεις διασποράς και περίσσειας, ενώ είναι ποιο ασφαλή σε επιθέσεις πλαστογράφησης. Τα ποιο γνωστά είναι τα σχήματα DSA , ElGamal , Schnorr. Ακολουθεί μια γενική περιγραφή της λειτουργίας ενός σχήματος με παράρτημα.

1. **Αλγόριθμος παραγωγής ενός ζεύγους κλειδιών.**

   Απαραίτητο είναι ένα ιδιωτικό κλειδί για την υπογραφή των μηνυμάτων και ένα δημόσιο για την διαδικασία της επαλήθευσης.

   - Ο Α διαλέγει ένα ιδιωτικό κλειδί σε ένα σύνολο $S_A = S_{A,k} : k \in R$. Κάθε μετασχηματισμός υπογραφής $S_{A,k}$ είναι μια 1-1 απεικόνιση από το M_h στο S.
   - Το S_A ορίζει ένα μετασχηματισμό επαλήθευσης (δημόσιο κλειδί)

$$V_A(\tilde{m}, s^*) = \begin{cases} \text{αληθές,} & \text{αν } S_{A,k}(\tilde{m}) = s^* \\ \text{ψευδές,} & \text{διαφορετικά} \end{cases}$$

$$\text{για κάθε } \tilde{m} \in \mathcal{M}_h, s^* \in \mathcal{S} \cdot \text{εδώ, } \tilde{m} = h(m) \text{ για } m \in \mathcal{M}.$$

2. **Παραγωγή ψηφιακής υπογραφής**

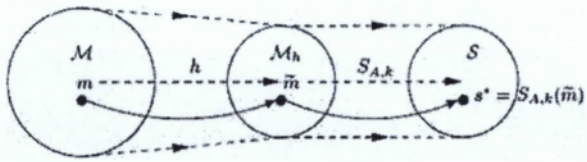
Ο Α παράγει μια υπογραφή $s \in S$ για ένα μήνυμα $m \in M$, που μπορεί να επαληθευτεί από έναν Β.

- Επιλέγει ένα $k \in R$ και υπολογίζει τα $\tilde{m} = h(m)$ και $s^* = S_{A,k}(\tilde{m})$
- Η υπογραφή του Α για το m είναι s^* . Τα m και s^* είναι διαθέσιμα για την επαλήθευση της υπογραφής.

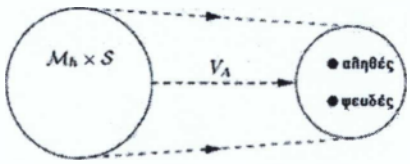
3. **Επαλήθευση ψηφιακής υπογραφής**

Ο Β πρέπει να κάνει τα ακόλουθα για την επαλήθευση:

- Να προμηθευτεί το αυθεντικό δημόσιο κλειδί V_a του Α και να υπολογίσει τα $\tilde{m} = h(m)$ και $u = V_A(\tilde{m}, s^*)$
- Να αποδεχτεί την υπογραφή αν $u =$ αληθές.



(α) Η διεργασία υπογραφής



(β) Η διεργασία επαλήθευσης

4.1.2 Σχήματα ψηφιακών υπογραφών με ανάκτηση μηνύματος.

Στα σχήματα ψηφιακών υπογραφών με ανάκτηση μηνύματος δεν απαιτείται η εισαγωγή του πρωτοτύπου μηνύματος στον μηχανισμό επαλήθευσης. Δεν είναι υποχρεωτική η γνώση του μηνύματος εκ των προτέρων. με ανάκτηση μηνύματος είναι τα σχήματα υπογραφών δημόσιου κλειδιού RSA, Rabin και Nyberg-Rueppel.

1. **Αλγόριθμος παραγωγής ενός ζεύγους κλειδιών.**
   Ο Α πρέπει να κάνει τα ακόλουθα :

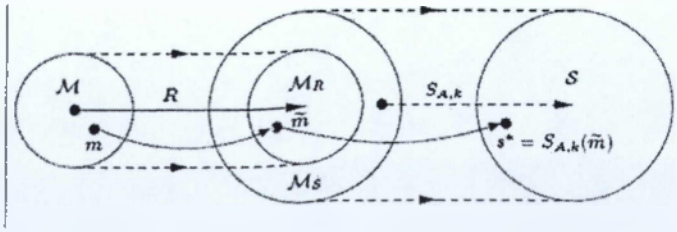
   - Κάνει ένα σύνολο μετασχηματισμών $S_A = \{S_{A,k} : k \in R\}$ Κάθε $S_{A,k}$ είναι μια 1 - 1 απεικόνιση από το M_s στο S και λέγεται μετασχηματισμός υπογραφής.
   - Το S_A ορίζει μια αντίστοιχη απεικόνιση V_A με την ιδιότητα ότι η $V_A \circ S_{A,k}$ είναι η ταυτοτική απεικόνιση στο M_S για κάθε $k \in R$. Η V_A λέγεται μετασχηματισμός επαλήθευσης και κατασκευάζεται έτσι, ώστε να μπορεί να υπολογιστεί χωρίς τη γνώση του ιδιωτικού κλειδιού του υπογράφοντα.

2. **Παραγωγή υπογραφής.**
   Α παράγει μια υπογραφή $s \in S$ για ένα μήνυμα $m \in M$, η οποία μπορεί αργότερα να επαληθευτεί από οποιαδήποτε Β. Το μήνυμα m ανακτάται από το s.

   - Επιλέγει ένα $k \in R$.
   - Να υπολογίσει τα $= R(m)$ και $s^* = S_{A,k}($
   - Η υπογραφή της Α είναι s^* αυτή γίνεται διαθέσιμη σε οντότητες που μπορεί να επιθυμούν να επαληθεύσουν την υπογραφή και να ανακτήσουν το m από αυτή.

3. **Επαλήθευση.**
   Ο Β θα πρέπει να κάνει τα εξής:

   - Να προμηθευτεί το αυθεντικό δημόσιο κλειδί V_A της Α.
   - Να υπολογίσει το $= V_A(s^*)$.
   - Να επαληθεύσει ότι $\in M_R$.
   - Να ανακτήσει το μ από το υπολογίζοντας το $R^{-1}()$.



4.1.3 Τύποι επιθέσεων σε ψηφιακές υπογραφές.

Ο στόχος μιας επίθεσης είναι η πλαστογράφηση της ψηφιακής υπογραφής. Ανάλογα με το είδος της μπορεί να γίνει ολική παραβίαση, δηλ. να υπολογιστεί το ακριβές ιδιωτικό κλειδί του υπογράφων. Επιλεκτική πλαστογράφηση , να πλαστογραφηθεί η υπογραφή για ένα τουλάχιστον συγκεκριμένο μήνυμα. Και υπαρξιακή πλαστογράφηση, να πλαστογραφηθεί τουλάχιστον η υπογραφή για ένα μήνυμα με την συμμετοχή του υπογράφων. Οι δύο κυριότερες κατηγορίες επιθέσεων σε σχήματα ψηφιακών υπογραφών είναι:

1. **Επιθέσεις κλειδιού:** Ο αντίπαλος γνωρίζει το δημόσιο κλειδί.
2. **Επιθέσεις μηνύματος:** Μια επίθεση αυτού του είδους μπορεί να είναι η επίθεση γνωστού μηνύματος, ο αντίπαλος γνωρίζει τις ψηφιακές υπογραφές για ένα σύνολο μηνυμάτων.Άλλη η επίθεση Επιλεγμένου μηνύματος, όπου ο αντίπαλος λαμβάνει υπογραφές για ένα σύνολο μηνυμάτων από μια λίστα πριν την παραβίαση. Και η προσαρμόσιμη επίθεση επιλεγμένου μηνύματος, εδώ ο αντίπαλος ζητάει υπογραφές που εξαρτώνται από το δημόσιο κλειδί ή από άλλες υπογραφές ή μηνύματα του υπογράφων.

4.1.4 Άλλα σχήματα υπογραφών

1. **Επιδιαιτητευόμενες ψηφιακές υπογραφές**
   Το σχήμα αυτό απαιτεί ένα άνευ όρων έμπιστο τρίτο μέλος (TTP) ως μέρος της παραγωγής και επαλήθευσης των υπογραφών. Για να επαληθεύσει μια υπογραφή κάποιος πρέπει να έχει από κοινού με το TTP ένα συμμετρικό κλειδί. Η ασφάλεια του βασίζεται στο επιλεγμένο σχήμα κρυπτογράφησης συμμετρικού κλειδιού.
2. **Το ESIGN Efficient digital SIGNature { αποδοτική ψηφιακή υπογραφή**
   Είναι ένα σχήμα ψηφιακών υπογραφών του οποίου η ασφάλεια βασίζεται στη δυσκολία παραγοντοποίησης ακεραίων. Είναι ένα σχήμα υπογραφών με παράρτημα και απαιτεί μια μονόδρομη συνάρτηση διασποράς.
3. **Σχήματα τυφλών υπογραφών (blind signature schemes).**
   Τα σχήματα αυτά είναι διμερή πρωτόκολλα μεταξύ ενός αποστολέα A και ενός υπογράφοντα B. Από την υπογραφή αυτή, ο A μπορεί να υπολογίσει την υπογραφή του B σε ένα προτεραιότητας μήνυμα m της επιλογής του. Ο B 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.

4. **Σχήματα αδιαμφισβήτητων υπογραφών (undeniable signature schemes).**
   Τα σχήματα αυτά διακρίνονται από τις ψηφιακές υπογραφές ως προς το ότι το πρωτόκολλο επαλήθευσης ο υπογραφών απαιτεί τη συνεργασία του υπογράφοντα.

5. **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 είναι υπογεγραμμένη από την Α, είναι μια πλαστογραφία. Αυτό γίνεται δείχνοντας ότι η υποκείμενη υπόθεση στην οποία βασίζεται ο μηχανισμός υπογραφών έχει παραβιαστεί.

4.2 Αυθεντικοποίηση Ταυτότητας

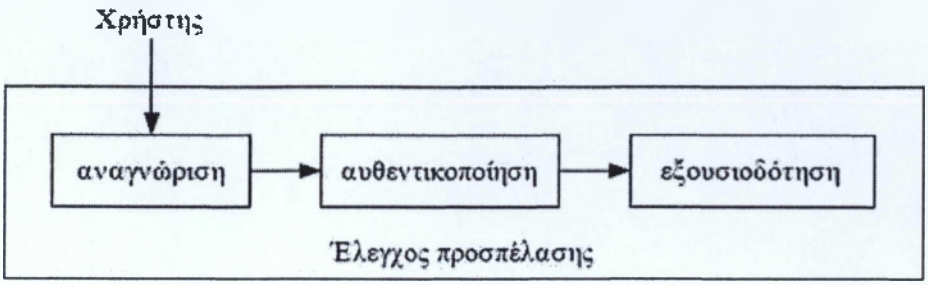
[7, σελ.324-325]

Ορισμοί

Ταυτοποίηση: μιας οντότητας είναι η διδικασία, κατά την οποία η οντότητα εισάγει σε ένα σύστημα τις πληροφορίες που απαιτούνται προκειμένου να συσχετιστεί με ένα από τα αντικείμενα που δικαιούται πρόσβαση στους πόρους του.

Αυθεντικοποίηση:μιας οντότητας είναι η διδικασία, κατά την οποία η οντότητα εισάγει σε ένα σύστημα τις πληροφορίες που απαιτούνται προκειμένου να ελεγχθεί η η συσχέτιση που έγινε κατά την ταυτοποίηση.

Ως αυθεντικοποίηση θεωρείται η διαδικασία πιστοποίησης και επιβεβαίωσης της ταυτότητας των χρηστών, η οποία σε κάθε περίπτωση βασίζεται στα διαπιστευτήρια που κατέχει ο χρήστης. Συγκεκριμένα, κατά τη διαδικασία αυθεντικοποίησης αναγνωρίζεται και επιβεβαιώνεται η ορθότητα της ταυτότητας ενός χρήστη ή κάποιων χαρακτηριστικών της.
Στα πληροφορικά συστήματα η επίτευξη μια επικοινωνίας μεταξύ δύο οντοτήτων δεν γίνεται άμεσα,γι' αυτό και είναι απαραίτητη η αναγνώριση των επικοινωνούντων και η επιβεβαίωση της ταυτότητας τους. Αυτό επιτυγχάνεται με με πρωτόκολλα αυθεντικοποίησης.



4.2.1 Τεχνικές εφαρμογής ελέγχων αυθεντικοποίησης

- **¨Κάτι που γνωρίζει ο χρήστης¨.**

  Είναι πληροφορίες που έχει ο χρήστης και εισάγει στο σύστημα. Μπορεί να είναι κωδικοί πρόσβασης, κλειδιά, PIN. Οι πληροφορίες αυτές δεν κλέβονται εύκολα έχουν εύκολη εφαρμογή και τροποποίηση και δεν αποκαλύπτονται από τον χρήστη. Πολλές φορές όμως είναι εύκολο να τις μαντέψουμε ή να αντιγραφούν με συγκεκριμένες μεθόδους.Υπάρχουν προγράμματα που μπορούν να μαντέψουν τις λέξεις που χρησιμοποιούνται σε συνθηματικά χρησιμοποιώντας συγκεκριμένα λεξικά.

  Είναι πολλοί παράγοντες που πρέπει να ληθφούν υπόψιν κατα την δημιουργία ενός τέτοιου συστήματος αυθεντικοποίησης, όπως η σύνθεση του συνθηματικού, το μήκος του, η διάρκεια ζωής του, η ιδιοκτησία, η αποθήκευση, η μετάδοση, η πηγή και η διανομή του.Η εντροπία είναι μια παράμετρος που αποδίδει το μέτρο δυσκολίας στο να αποκαλυφθεί ένα συνθηματικό και εκφράζεται σε bits.

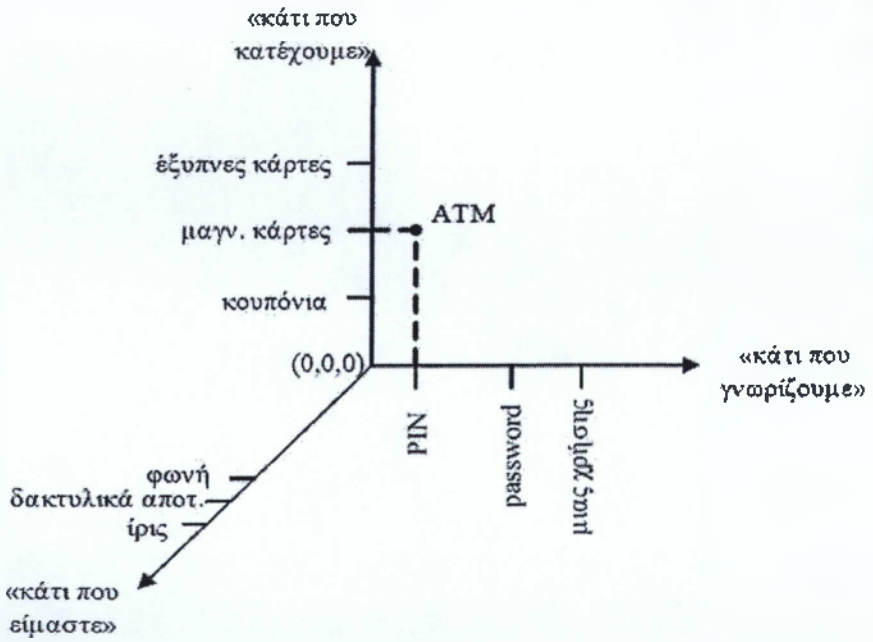
- **¨Κάτι που κατέχει ο χρήστης¨.**

  Πρόκειται για αντικείμενα που έχει στην κατοχή του ο χρήστης όπως μαγνητικές ή έξυπνες κάρτες κ.α.Είναι δύσκολο να αντιγραφούν λόγω της κατασκευής τους, έχουν όμως υψηλό κόστος υλοποίησης και υπάρχει ο κίνδυνος να χαθούν.
  Οι μαγνητικές κάρτες είναι εύκολο να αναγνωσθούν και να τροποποιηθεί η αποθηκευμένη πληροφορία που έχουν. Οι ψηφιακές κάρτες όπως οι τηλεφωνικές κάρτες προπληρωμένου χρόνου, έχουν καλύτερη προστασία αλλά παρακάφηκαν. Οι έξυπνες κάρτες με ενσωματωμένο μικροελεγκτή, αισθητήρες ανίχνευσης επιθέσεων και κρυπτογραφικούς επεξεργαστές παρέχουν την μεγαλύτερη ασφάλεια σε αυτή την κατηγορία.

- **"Κάτι που είναι ο χρήστης".**

  Η χρήση των συστημάτων βιομετρικής τεχνολογίας βασίζεται στα χαρακτηριστικά του ανθρώπινου σώματος. Μπορεί να είναι χαρακτηριστικά του χρήστη όπως δακτυλικά αποτυπώματα, φωνή , αναγνώριση ίριδας ματιού, χαρακτηριστικά προσώπου, γεωμετρία παλάμης, DNA κ.α. Εδώ τίθεται θέμα αξιοπιστίας των τεχνικών αυτών , υψηλό κόστος υλοποίησης, έχουν υψηλές απιτήσεις συντήρησης και υψηλό ποσοστό απόρριψης χρηστών αλλά θεωρούνται τα ποιό ασφαλή. Παρέχουν μοναδικότητα , ταχύτητα και είναι δύσκολη η παραποίηση τους.

Μπορεί η αυθεντικοποίηαη να γίνεται με μια απο τις τεχνικές ή με συνδιασμό τους. Όσες περισσότερες χρησιμοποιούνται τόσο το καλύτερο είναι. Στο σχήμα που ακολουθεί φένεται ο βαθμός αβεβαιότητας, στο σημείο 0 είναι μεγάλος ενώ όσο απομακρύνεται μικραίνει.



Οι μηχανισμοί αυθεντικοποίησης, ανεξάρτητα από τα χαρακτηριστικά που υιοθετούν, αξιοποιούν δύο τύπους κλειδιών:

- Μυστικά κλειδιά: Σε αυτά συμπεριλαμβάνονται τα συνθηματικά, οι κωδικοί και τα συμμετρικά κλειδιά.
- Ασύμμετρα κλειδιά: Σε αυτά συμπεριλαμβάνονται ζεύγη κλειδιών, από τα οποία το

ένα είναι δημόσια γνωστό (δημόσιο κλειδί), ενώ το άλλο παραμένει μυστικό (ιδιωτικό κλειδί).

Συνεπώς τα συστήματα αυθεντικοποίησης μπορούν να χαρακτηριστούν ως μονοδιάστατα ή πολυδιάστατα, ανάλογα με τα διαφορετικά χαρακτηριστικά που αξιοποιούν, ώστε να εξασφαλίσουν το επιθυμητό επίπεδο βεβαιότητας για την ταυτότητα κάποιας ηλεκτρονικής οντότητας.

Εξουσιοδότηση

Αφού τα πρωτόκολλα αυθεντικοποίησης εκτελεστούν ακολουθεί η διαδικασία της εξουσιοδότησης. Οπότε ανάλογα με τα τα δικαιώματα που έχουν εκχωρηθεί στον χρήστη ελέγχει για ποιούς πόρους του συστήματος έχει άδεια προσπέλασης ο σχρήστης. Δηλαδή μόλις γίνει η αυθεντικοποίηση της ταυτότητας του χρήστη του ανατίθεται κάποιος ρόλος σύμφωνα με το μοντέλο εξουσιοδότησης που ακολουθείται.

4.2.2 Σύστημα αυθεντικοποίησης

Ένα σύστημα αυθεντικοποίησης αποτελείται από:

- Το σύνολο A που περιέχει τα δεδομένα που ο χρήστης αποδεικνύει της ταυτότητα του.
- Το σύνολο C περιέχει τα δεδομένα που αποθηκεύει το σύστημα για την επικύρωση της αυθεντικοποίησης.
- Το σύνολο F τις συναρτήσεις που δημιουργούν τις πληροφορίες για την αυθεντικοποίηση. για $f \in F$, τότε $f : A- > C$.
- Το σύνολο L των συναρτήσεων αυθεντικοποίησης, που αναγνωρίζουν τον χρήστη, για $1 \in L$, τότε $AxC- > \{true, false\}$.
- Το σύνολο S συναρτήσεις επιλογής, που δίνουν την δυνατότητα στον χρήστη να δημιουργήσει ή να αλλάξει τις υπάρχουσες πληροφορίες της αυθεντικοποίησης.

Πρωτόκολλο αυθεντικοποίησης Κέρβερος.

[16] Ο Κέρβερος αναπτύχθηκε στο MIT και αποτελεί μέρος του project Athena στα μέσα της δεκαετίας του 80. Οι εκδόσεις 1-3 ήταν για εσωτερική χρήση και οι 4 και5

ανοιχτές σε όλους. Εφαρμόζεται σε περιβάλλον Unix, και επίσης σε Windows 2000 της Microsoft. Είναι πρωτόκολλο τρίτης έμπιστης πηγής .Περιλαμβάνει ένα KDC, το οποίο αποτελεί την έμπιστη οντότητα στην αυθεντικοποίηση των χρηστών και αποτελείται από:

- Authenticaton Server (AS),που έχει τους κωδικούς όλων των χρηστών σε μια βάση δεδομένων και μοιράζεται ενα μοναδικό κλειδί με κάθε εξυπηρετητή. Χρησιμοποιεί τον Data Encryption Standard (DES) για την κρυπτογράφηση των μηνυμάτων.
- Kerberos database η βάση δεδομένων που περιέχει ενα συμμετρικό κλειδί για κάθε χρήστη.
- Ticket Granting Server (TGS) εκδίδει εισητήρια στους clients για την επικοινωνία με τους servers αφού ελένγθει ο client.

Η ανταλλαγή μηνυμάτων γίνεται με τον ακόλουθο τρόπο.

- Επικοινωνεί με την υπηρεσία Authentication Service Exchage για να πάρει ο χρήστης το εισητήριο.
- Επικοινωνεί με την υπηρεσία (Ticket-Granting Service Exchange) για την απόκτηση της service-granting ticket.
- Επικοινωνία (Client/Server Authentication Exchange) για την απόκτηση πρόσβασης στις υπηρεσίες του εξυπηρετητη.[16]

4.2.3 Ψηφιακά πιστοποιητικά

Ένα ψηφιακό πιστοποιητικό συσχετίζει ένα ζεύγος ασύμμετρων κρυπτογραφικών κλειδιών, δημόσιο και ιδιωτικό, με ένα σύνολο πληροφοριών που είναι δυνατό να προσδιορίσει μοναδικά την οντότητα που έχει στην κατοχή της το συγκεκριμένο πιστοποιητικό. Οι διαφορετικές κατηγορίες ψηφιακών πιστοποιητικών, που μπορούν να αξιοποιηθούν από τους χρήστες είναι:[21]

- Ψηφιακό πιστοποιητικό για ψηφιακή υπογραφή ηλεκτρονικών μηνυμάτων και εγγράφων.
- Ψηφιακό πιστοποιητικό για κρυπτογράφηση ηλεκτρονικών μηνυμάτων ή εγγράφων.

Τα ψηφιακά πιστοποιητικά περιλαμβάνουν τα βασικά πεδία που απαιτούνται για αναγνωρισμένα πιστοποιητικά τύπου X509 3.

Πεδίο
Έκδοση (Version)
Αριθμός Σειράς (Serial Number)
Αλγόριθμος Υπογραφής (Signature Algorithm)
Διακριτικό Όνομα Εκδότη (Issuer DN)
Ισχύει Από (Valid From)
Ισχύει Μέχρι (Valid To)
Διακριτικό Όνομα Υποκειμένου (Subject DN)
Δημόσιο Κλειδί Υποκειμένου (Subject Public Key)
Υπογραφή (Signature)

Κεφάλαιο 5

Εργαλεία της κρυπτογραφίας

5.1 Ψευδοτυχαίες Ακολουθίες

Είναι δύσκολο να διευκρινίσουμε τι εννοούμε όταν λέμε ότι επιλέγουμε ή παράγουμε έναν αριθμό τυχαίο. Για παράδειγμα στην λοταρία όπου έχουμε ένα σύνολο αριθμών έστω από το 1 μέχρι το 62, αν μετά από το ανακάτεμα προκύψει ο αριθμός 30 μπορούμε να πούμε ότι παράχθηκε τυχαία. Βέβαια έχει την ίδια πιθανότητα με τους άλλους για να επιλεγεί. Αν το επαναλάβουμε αυτό αρκετές φορές μπορούμε να πούμε ότι έχει παραχθεί μια τυχαία ακολουθία. Ένας από τους μεγαλύτερους μαθηματικούς ο John von Neuman είπε:
«Όποιος προσπαθεί να κατασκευάσει τυχαίους αριθμούς με την χρήση κάποιας αλγοριθμικής μεθόδου είναι αμαρτωλός» .
Στην ουσία δεν υπάρχει καμία μέθοδος παραγωγής τυχαίων αριθμών, αλλά ψευδοτυχαίων. Υπάρχουν πολλές ερευνητικές εργασίες για κρυπτογραφικά ασφαλείς μεθόδους παραγωγής ψευδοτυχαίων αριθμών και ακολουθιών. Οι μέθοδοι αυτοί αποτελούν ένα πολύ σημαντικό κρυπτογραφικό εργαλείο, αφού είναι αναγκαίες για την παραγωγή κλειδιών, η εύρεση καλών μεθόδων όμως είναι δύσκολη. Συνηθίζεται στις κρυπτογραφικές εφαρμογές από ένα πεπερασμένο σύνολο στοιχείων να επιλέγεται ένα, ή από ένα σύνολο συμβολοσειρών σε κάποιο πεπερασμένο αλφάβητο να επιλέγεται τυχαία μια ακολουθία, ή να παράγεται μια ακολουθία συμβόλων από ένα πεπερασμένο σύνολο στοιχείων.[8, σελ.123-125]
Μια ψευδοτυχαία ακολουθία είναι ασφαλής όταν[7, σελ.112-113]:

Κεφάλαιο 5

Εργαλεία της κρυπτογραφίας

5.1 Ψευδοτυχαίες Ακολουθίες

Είναι δύσκολο να διευκρινίσουμε τι εννοούμε όταν λέμε ότι επιλέγουμε ή παράγουμε έναν αριθμό τυχαίο. Για παράδειγμα στην λοταρία όπου έχουμε ένα σύνολο αριθμών έστω από το 1 μέχρι το 62, αν μετά από το ανακάτεμα προκύψει ο αριθμός 30 μπορούμε να πούμε ότι παράχθηκε τυχαία. Βέβαια έχει την ίδια πιθανότητα με τους άλλους για να επιλεγεί. Αν το επαναλάβουμε αυτό αρκετές φορές μπορούμε να πούμε ότι έχει παραχθεί μια τυχαία ακολουθία. Ένας από τους μεγαλύτερους μαθηματικούς ο John von Neuman είπε:
«Όποιος προσπαθεί να κατασκευάσει τυχαίους αριθμούς με την χρήση κάποιας αλγοριθμικής μεθόδου είναι αμαρτωλός» .
Στην ουσία δεν υπάρχει καμία μέθοδος παραγωγής τυχαίων αριθμών, αλλά ψευδοτυχαίων. Υπάρχουν πολλές ερευνητικές εργασίες για κρυπτογραφικά ασφαλείς μεθόδους παραγωγής ψευδοτυχαίων αριθμών και ακολουθιών. Οι μέθοδοι αυτοί αποτελούν ένα πολύ σημαντικό κρυπτογραφικό εργαλείο, αφού είναι αναγκαίες για την παραγωγή κλειδιών, η εύρεση καλών μεθόδων όμως είναι δύσκολη. Συνηθίζεται στις κρυπτογραφικές εφαρμογές από ένα πεπερασμένο σύνολο στοιχείων να επιλέγεται ένα, ή από ένα σύνολο συμβολοσειρών σε κάποιο πεπερασμένο αλφάβητο να επιλέγεται τυχαία μια ακολουθία, ή να παράγεται μια ακολουθία συμβόλων από ένα πεπερασμένο σύνολο στοιχείων.[8, σελ.123-125]
Μια ψευδοτυχαία ακολουθία είναι ασφαλής όταν[7, σελ.112-113]:

- δεν είναι προβλέψιμη, δηλ. και να είναι γνωστό ένα μέρος της να μην μπορεί να προβλεφθεί το επόμενο ή να μην μπορεί να προβλεφθεί εάν είναι γνωστή η μέθοδος παραγωγής της.
- περνά τα στατιστικά τέστ που αναφέρονται παρακάτω:

5.1.1 Στατιστικά τέστ

Στους ελέγχους που παρουσιάζονται θεωρείται ότι οι ακολουθίες είναι δυαδικές. Αν μια ακολουθία περάσει και τα πέντε τεστ που ακολουθούν δεν είναι σίγουρο ότι έχει παραχθεί απο μια γεννήρια τυχαίων ακολουθιών.[4, σελ.181-182]

- **ο έλεγχος της συχνότητας (monobit test)**
  Ελέγχεται ότι οι άσσοι και τα μηδενικά της ακολουθίας έχουν το ίδιο πλήθος. Αν n_o το πλήθος των μηδενικών και n_1 των άσσων η στατιστική, η κατανομή x^2 για βαθμό ελευθερίας 1 είναι:
  $$x^2 = \frac{(n_o - n_1)^2}{n}$$
  Για οποιαδήποτε άλλη τιμή των n_o, n_1 η πηγή θεωρείται πολωμένη.
- **ο σειριακός έλεγχος (two-bit test)**
  Ο σειριακός έλεγχος έλεγχει την εναλλαγή των ψηφίων από 0 σε 1 από 1 σε 0 και την διατήρηση τους. Έστω $n_{00}, n_{01}, n_{10}, n_{11}$ το πλήθος των 00, 01, 10 και 11, η κατανομή x^2 για βαθμό ελευθερίας 2 είναι:
  $$x^2 = n_{00} = n_{01} = n_{10} = n_{11} = \frac{n-1}{4}$$
- **ο έλεγχος του πόκερ (Poker test)**
  Έστω m θετικός ώστε $\left[\frac{n}{m}\right] \geq 5*(2^m)$ και $k = \left[\frac{n}{m}\right]$ και η ακολουθία s. Ο έλεγχος του πόκερ καθορίζει εαν οι ακολουθίες μήκους m εμφανίζονται τον ίδιο αριθμό στην s, όπως θα γινόταν σε μια τυχαία ακολουθία.
- **Ο έλεγχος του Run (Runs test)**
  Ο έλεγχος είναι να καθορίσει αν ο αριθμός των runs, είτε μηδενικά ή άσσοι, με διαφορετικά μήκη s ακολουθιών είναι όπως αναμενόταν για μια τυχαία ακολουθία.
- **Ο έλεγχος της αυτοσυσχέτισης (Autocorrelation test)**
  Ο έλεγχος της αυτοσυσχέτισης δείχνει αν τα δυαδικά ψηφία είναι τυχαία διασπαρμένα μέσα στη δυαδική ακολουθία.

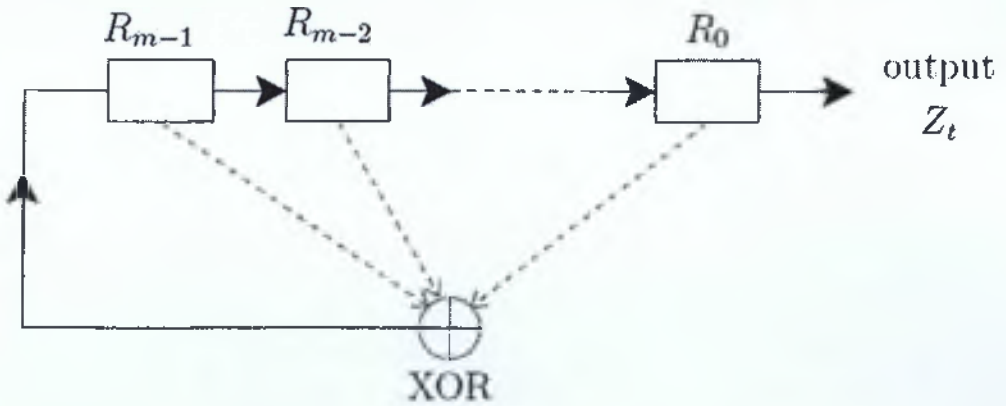
5.1.2 Γεννήτριες παραγωγής ψευδοτυχαίων αριθμών

[10, σελ.106-108] Οι γεννήτριες αυτές είναι κυρίως λογισμικό αλγόριθμοι και βασίζονται σε συμμετρικά και ασσύμετρα κρυπτογραφικά συστήματα. Η ασφάλεια τους εξαρτάται από την ασφάλεια αυτών των κρυπτογραφικών συστημάτων. Μια μικρή ακολουθία τυχαίων αριθμών στην είσοδο της γεννητριας παράγει μια ακολουθία ψευδοτυχαίων αριθμών στην έξοδο της. Υπάρχουν καταχωρητές ολίσθησης γραμμικής ανάδρασης και μη γραμμικοί.

Γραμμικοί καταχωρητές ολίσθησης- Linear shift-register sequences (LSFR)

Ο LSFR είναι απο τις γεννήτριες που χρησιμοποιήθηκαν αρχικά. Προκειται για μια μηχανή από καταχωρητές $R_0,...R_{m-1}$ κατανεμημένους σε σειρά, μαζί με μια πύλη XOR. Ο καταχωρητής R_{m-i} για ci, $1 \leq i \leq m$ πέρνει την τιμή 1 ή 0, ανάλογα με τον αν είναι συνδεδεμένος με την XOR. Μετά την ρύθμιση ενός ρολογιού της μηχανής ξεκινά η λειτουργία του.

Με κάθε χτύπο του ρολογιού ο κάθε καταχωρητής μεταφέρει το περιεχόμενο bit που έχει στον επόμενο δεξιά μέχρι την έξοδο Z_t, κάθε έξοδος της XOR αποτελεί καινούργια είσοδο για τον αριστερότερο καταχωρητή R_{m-1}.
Ακολουθεί το ανάλογο σχήμα.



5.2 Συναρτήσεις Κατακερματισμού - (hash functions)

[4, κεφ.9]Οι συναρτήσεις κατακερματισμού αποτελούν ένα πολύ σημαντικό εργαλείο στην κρυπτογραφία, με μεγάλη εφαρμογή στις ψηφιακές υπογραφές, τα πρωτόκολλα ταυτοποίησης και την ακαεραιότητα των δεδομένων. Πρόκειται για συναρτήσεις που απεικονίζουν δυαδικές συμβολοσειρές εισόδου αυθαίρετου μήκους σε σταθερού μήκους. Μια συνάρτηση κατακερματισμού h(x) ορίζεται εαν ισχύουν τα ακολουθα:

1. Για κάθε είσοδο x η έξοδος y=h(x) είναι μικρότερη.
2. Να έχει αποδοτικότητα, δηλ. για κάθε x είσοδο να μπορεί υπολογιστεί η h(x) έξοδος.
3. Να είναι μονόδρομη, δεν μπορούμε να βρούμε μια τιμή x ώστε h(x)=y.
4. δοθέντων x, h(x), είναι υπολογιστικά αδύνατο να βρεθεί x΄ τέτοιο ώστε h(x΄) = h(x).
5. Ασθενής αντίσταση σε συγκρούσεις (weak collision resistance): Δοθέντος x,h(x) δεν γίνεται να βρεθεί ένα k, με $k \neq x$ ώστε h(k)=h(x).
6. Ισχυρή αντίσταση σε συγκρούσεις (strong collision resistance): Είναι ανέφικτο υπολογιστικά να βρεθεί k και x, με $k \neq x$, ώστε h(x)=h(k).

Όταν πάνω από ένα στοιχεία του πεδίου ορισμού της συνάρτησης αντιστοχεί στο ίδιο στοιχείο του συνόλου τιμών λέμε ότι έχουμε σύγκρουση. Μια hash συνάρτηση είναι ανθεκτική σε συγκρούσεις όταν δεν υπάρχει τρόπος να ανακαλύπτονται στοιχεία που να καταλήγουν στην ίδια σύνοψη. Υπάρχουν δύο είδη συναρτήσεων αυτές που κάνουν χρήση κλειδιού και αυτές που δεν χρησιμοποιούν κλειδί.

- **Συναρτήσεις κατακερματισμού MDC (Modification Detection Codes - Κώδικας ανίχνευσης τροποποίησης)**
  Η κρυπτογραφική συνάρτηση εδώ δεν χρησιμοποιεί μυστικό κλειδί και έχει ασθενή αντίσταση σε συγκρούσεις. Χρησιμοποιείται για την επικοινωνία ενός με πολλούς, δηλ. έχουμε έναν αποστολέα και πολλούς παραλήπτες. Σε αυτή την περίπτωση δεν υπάρχει κλειδί η συνάρτηση εφαρμόζεται στο μήνυμα , κρυπτογραφείται και μεταδίδεται.Η ταυτοποίηση μπορεί να γίνει από οποιονδήποτε.
- **Συναρτήσεις κατακερματισμού MAC (Message Authentication Codes - Κώδικας αυθεντικοποίησης μηνύματος)**

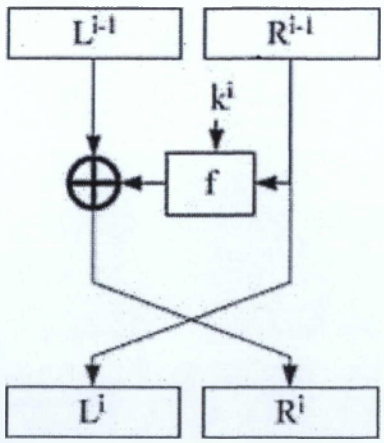
Η κρυπτογραφική συνάρτηση εδώ χρησιμοποιεί μυστικό κλειδί και έχει ασθενή αντίσταση σε συγκρούσεις. Πιστοποιεί την αυθεντικότητα του μηνύματος και της πηγής του. Χρησιμοποιείται συνήθως για την επικοινωνία δύο πλευρών, όταν η επικοινωνία είναι αμφίδρομη. Σ' αυτές τις συναρτήσεις η εμπιστευτικότητα δεν είναι υψηλή όσο η ακεραιότητα. Η ασφάλεια του εξαρτάται από το μέγεθος και την μυστικότητα του κλειδιού.

5.3 Δύκτια Feitsel

Η κρυπτογραφική πράξη τύπου Feitsel είναι της μορφής του Σχήματος που ακολουθεί, η οποία αποτελεί και έναν γύρο σε κρυπτοσύστημα γινομένου. Το βασικό χαρακτηριστικό ενός δικτύου Feitselείναι η πλήρης ελευθερία στην επιλογή της συνάρτησης γύρου f.

Σε κάθε γύρο η είσοδος χωρίζεται στο αριστερό και στο δεξιό τμήμα. Τα δύο τμήματα της εισόδου του i-στού γύρου συμβολίζονται με L^{i-1} και R^{i-1}, ενώ οι έξοδοι συμβολίζονται με L^i και R^i. Στον πρώτο γύρο τα τμήματα L^0 και R^0, αντιστοιχούν στο απλό κείμενο, ενώ στον τελικό γύρο, τα τμήματα L^r και R^r.

Κατά τον γύροi, η συνάρτηση γύρου f δέχεται ως είσοδο το δεξιό τμήμα της εισόδου και το κλειδί k^i το οποίο προέρχεται από το πρόγραμμα κλειδιού. Η έξοδος της συνάρτησης συνδυάζεται με το αριστερό τμήμα της εισόδου με αποκλειστική διάζευξη και το αποτέλεσμα της πράξης αντισιοιχίζεται στο δεξιό τμήμα της εξόδου, ενώ το δεξιό τμήμα της εισόδου αντιστοιχίζεται στο αριστερό τμήμα της εξόδου.



5.4 Πρώτοι αριθμοί στην κρυπτογραφία

Στην κρυπτογραφία δημοσίου κλειδιού είναι απαραίτητη η χρήση μεγάλων πρώτων αριθμών. Πριν χρησιμοποιοηθούν όμως πρέπει να ελέγχεται άν είναι όντως πρώτοι.Γι' αυτό το λόγο υπάρχουν πολλά τέστ τρόποι για να επιβεβαιώσουμε ότι ενας αριθμός είναι πρώτος. Δύο από αυτά είναι:[5][11.5]

5.4.1 Fermat Primality-Test

Το θεώρημα αυτό ισχύει για όλους τους πρώτους αριθμούς. Ένας αριθμός p είναι πρώτος και $1 \leq a \leq p$ αν :
$a^{p-1} \equiv 1 \pmod{p}$

5.4.2 Lehmann Primality-Test

Για να ελένξουμε ότι ένας αριθμός p είναι πρώτος :
Διαλέγουμε έναν αριθμό $a < p$ και υπολογίζουμε το $a^{(p-1)/2} mod p$
Άν $a^{(p-1)/2} mod p \neq 1$ ή $-1 \pmod{p}$, δεν είναι πρώτος.
Άν $a^{(p-1)/2} mod p \equiv 1$ ή $-1 \pmod{p}$, κατα 50% δεν είναι πρώτος.
Επαναλαμβάνεται το τέστ t φορές και αν το απότέλεσμα είναι 1 ή -1 αλλα όχι παντα ίσο με 1, τότε είναι πιθανόν πρώτος με ρυθμό λάθους 1 στη 2^t.

5.5 Αριθμο-θεωρητικά προβλήματα

5.5.1 Το πρόβλημα του διακριτού λογαρίθμου

Η ασφάλεια πολλών κρυπτογραφικών τεχνικών οφείλεται στη δυσεπιλυσιμότητα του προβλήματος διακριτού λογαρίθμου.Μια μερική λίστα αυτών περιλαμβάνει τη συμφωνία κλειδιών Diffie-Hellman και των παράγωγών της , την κρυπτογράφηση ElGamal
Έστω G μια πεπερασμένη κυκλική ομάδα τάξης n. Έστω a ένας γεννήτορας της G και έστω $b \in G$. Ο διακριτός λογάριθμος του b ως προς τη βάση a, συμβολικά $log_a b$, είναι ο μοναδικός ακέραιος $x, 0 \leq x \leq n-1$, τέτοιος ώστε$b = a^x$. Το πρόβλημα διακριτού

λογαρίθμου είναι δοθέντος ενός πρώτουp, ενός γεννήτορα a και ενός στοιχείου b να βρεθεί ο ακέραιος $x, 0 \leq x \leq p-2$, τέτοιος ώστε $a^x \equiv b(mod p)$.[4][κεφ.3]

5.5.2 Το πρόβλημα παραγοντοποίησης ακεραίων

Η ασφάλεια πολλών κρυπτογραφικών τεχνικών εξαρτάται από τη δυσκολία επίλυσης του προβλήματος παραγοντοποίησης ακεραίων. Μια μερική λίστα τέτοιων πρωτοκόλλων συμπεριλαμβάνει το σχήμα κρυπτογράφησης δημόσιου κλειδιού RSA, το σχήμα ψηφιακών υπογραφών RSA και το σχήμα κρυπτογράφησης δημόσιου κλειδιού Rabin.
Το πρόβλημα παραγοντοποίησης ακεραίων (FACTORING) είναι το εξής: δοθέντος ενός θετικού ακεραίου n, να βρεθεί η ανάλυσή του σε γινόμενο πρώτων παραγόντων δηλαδή, να γραφεί , $poup_i$ είναι ανά δύο διαφορετικοί πρώτοι και κάθε$e_i \geq 1$.
Μια μη τετριμμένη παραγοντοποίηση του n είναι η παραγοντοποίηση της μορφής $n = pq$, όπου $1 < p < n$ και $1 < q < n$, οι p και q λέγονται μη τετριμμένοι παράγοντες του n. Εδώ οι p και q δεν είναι απαραιτήτως πρώτοι. Για να λύσουμε το πρόβλημα της παραγοντοποίησης ενός ακεραίου αρκεί να μελετήσουμε αλγορίθμους που διασπούν το ν, δηλαδή να βρούμε μια μη τετριμμένη παραγοντοποίηση $n = pq$. Άπαξ και βρεθούν, οι παράγοντες p και q μπορούν να ελεγχθούν για να πιστοποιηθεί αν είναι πρώτοι. Ο αλγόριθμος για τη διάσπαση ακεραίων μπορεί τότε να εφαρμοστεί αναδρομικά στον p και/ή στον q , αν βρεθεί κάποιος ότι είναι σύνθετος. Με αυτόν τον τρόπο μπορεί να πραγματοποιηθεί η παραγοντοποίηση του ν σε πρώτους.[4][κεφ.3]

Μέρος ΙΙ

Κρυπτογράφηση Δημοσίου κλειδιού RSA

Κεφάλαιο 6

Εισαγωγή στο RSA

Ο RSA ανακαλύφθηκε από τους Rivest, Shamir, Adleman απ' όπου πήρε και το όνομά του είναι ένα από τα πιο παλιά και διαδεδομένα κρυπτοσυστήματα ασύμμετρης κρυπτογράφησης. Την ιδέα βέβαια για την δημιουργία ενός κρυπτοσυστήματος δημοσίου κλειδιού προτάθηκε από τους Diffie και Hellman το 1976. Αλλά το πρώτο κρυπτοσύστημα υλοποιήθηκε από τους Rivest, Shamir, Adleman το 1978 .

Αποτελεί χρυσή σταθερά στην κρυπτογράφηση δημοσίου κλειδιού. Βασίζεται στις αρχές της θεωρίας των αριθμών και η ασφάλεια του, στη δυσκολία της πραγματοποίησης ενός σύνθετου ακεραίου, εφόσον δεν έχει ανακαλυφθεί ακόμα ένας αλγόριθμος που να μπορεί να παραγοντοποιεί σε πολυωνυμικό χρόνο έναν ακέραιο. Έχει πολλές εφαρμογές και χρησιμοποιείται σε πολλές συναλλαγές που απαιτούν ασφάλεια στο Internet. Είναι ικανός για ασφαλή κρυπτογράφηση , δημιουργία ψηφιακών υπογραφών και μεταβίβαση σύντομων κλειδιών.

Στην ουσία η χρήση του βασίζεται στο ότι δεν υπάρχει αλγόριθμος που να υπολογίζει τους παράγοντες ενός σύνθετου ακεραίου και στο ότι ο υπολογισμός μιας μεγάλης δύναμης ενός αριθμού σε modular μπορεί να γίνει σε επιτρεπτό γραμμικό χρόνο.Οι πρώτοι αριθμοί p και q θα πρέπει να είναι αρκετά μεγάλοι, ώστε ο καλύτερος γνωστός αλγόριθμος παραγοντοποίησης να απαιτεί χρόνο μεγαλύτερο από αυτόν με τον οποίο πρέπει να προστατευθούν τα δεδομένα.Στον παρακάτω πίνακα ακολουθεί το μέγεθος των p, q (bits) κατα περίπτωση :
[7, σελ.220,223]

p, q (bits)	n(bits)	χρόνος προστασίας	τύπος δεδομένων
256	512	μερικές εβδομάδες	πληροφορίες που επηρεάζουν το χρηματιστήριο
512	1024	50 - 100 χρόνια	προσωπικά μυστικά
1024	2048	' 100 χρόνια	εμπορικά μυστικά, προσωπικά μυστικά
2048	4096	ηλικία του σύμπαντος	στρατιωτικά μυστικά

[7, σελ.220,223]

6.1 Ο αλγόριθμος RSA

[4, σελ.285-286] Ακολουθεί μια γενική συνοπτική περιγραφή του αλγόριθμου:
p, q: πρώτοι αριθμοί κρατούνται μυστικοί.
n : υπόλοιπο modulus πρέπει να αποτελείται από τουλάχιστον 200 ψηφία και είναι γνωστό σε όλους .
m :μήνυμα
c : κρυπτογράφημα.
e :δημόσιο κλειδί.
d :ιδιωτικό κλειδί.
h :ψηφιακή υπογραφή.
H :συνάρτηση κατακερματισμού.

6.1.1 Παραγωγή ζεύγους κλειδιών με RSA

Ο RSA χρησιμοποιεί ένα ιδιωτικό και ένα δημόσιο ζεύγος κλειδιών. Το ζεύγος κλειδιών (n,e) , είναι ένα ζεύγος ακεραίων και το n ονομάζεται modulus RSA, αυτό προκύπτει από το γινόμενο δύο τυχαίων, κρυφών, πρώτων αριθμών p, q ιδίου μεγέθους bit.Η ασφάλεια της απόκρυψης βασίζεται στο γεγονός της μη ύπαρξης γρήγορων αλγορίθμων για την παραγοντοποίηση αριθμών.
Αν οι p, q είναι αρκετά μεγάλοι, το γινόμενό τους ν δεν μπορεί να παραγοντοποιηθεί μέσα σε λογικό χρόνο . Το δημόσιο κλειδί e που λέγεται και εκθέτης κρυπτογράφησης είναι ακέραιος και ισχύει $1 < e < \phi$ και $gcd(e, \phi) = 1$ με $\phi = (p-1)(q-1)$. Το ιδιωτικό κλειδί d, είναι ένας ακέραιος και ισχύει $1 < d < \phi$ και $ed \equiv (mod\phi)$.

Παραγωγή κλειδιών

- Επιλέγουμε δύο μεγάλους πρώτους αριθμούς p, q .
- Υπολογίζεται το $n = pq$.
- Υπολογίζεται η συνάρτηση Euler $\phi(n) = \phi(p)\phi(q) = (p-1)(q-1)$.
- Επιλέγεται ένας πρώτος αριθμός $1 < e < \phi(n)$ και $gcd(e, \phi) = 1$ όπου δημοσιοποιείται.
- Υπολογίζεται το $d, 1 < d < \phi(n)$ έτσι ώστε $ed - 1(mod\phi(n))$.
- Το ζευγάρι (e, n) αποτελεί το δημόσιο κλειδί και το (d, n) το ιδιωτικό κλειδί.

6.1.2 Κρυπτογράφηση RSA

Κατά την κρυπτογράφηση του το μήνυμα m χωρίζεται σε ομάδες - block $m_1, m_2, ...$ bits τέτες ώστε κάθε block να αναπαρίσταται από έναν ακέραιο μεταξύ 0 και n. Ο αποστολέας μηνύματος m κάνει χρήση του ζεύγους (e, n) του παραλήπτη και μετασχηματίζει το μήνυμα m σε c .
Το κρυπτογραφημένο κέιμενο υπολογίζεται από το

$$c = m^e mod n$$

6.1.3 Αποκρυπτογράφηση RSA

Η παραγόμενη ακολουθία αριθμών ή χαρακτήρων διαβιβάζεται στον παραλήπτη. Ο παραλήπτης επανασυνθέτει το μήνυμα m από το c με εφαρμογή του τύπου

$$m = c^d mod n$$

Αφού $ed \equiv 1(mod\phi(n))$ Υπάρχει ένας ακέραιος k τέτοιος ώστε $ed = 1+k\phi(n)$ Α $gcd(m, p) = 1$ τότε σύμφωνα με το θεώρημα του fermat

$$m^{p-1} \equiv 1(mod p)$$

Υψώνω και τις δύο πλευρές στην δύναμη $k(q-1)$ και πολλαπλασιάζω με m.

$$m^{1+k(p-1)(q-1)} \equiv m(modp)$$

Αν $gcd(m,p) = p$

$$m^{ed} \equiv m(modp)$$

$$m^{ed} \equiv m(modq)$$

$$m^{ed} \equiv m(modn)$$

$$c^d \equiv (m^e)^d \equiv m(modn)$$

6.1.4 Ψηφιακή υπογραφή RSA

Για την αποστολή ενός υπογεγραμμένου μηνύματος αφού ο RSA επιτρέπει την ψηφιακή υπογραφή κάνουμε τον εξής υπολογισμό:

$$S_{(m)} = m^d \pmod{n}$$

Και η επαλήθευση της από :

$$V = s^e \pmod{n}$$

Όπου ισχύει η σχέση:

$$_{(s)}e \cdot d \equiv 1 \pmod{\phi_{(n)}}$$

Ο παραλήπτης υπολογίζει την s^e.

6.1.5 Παράδειγμα

Έστω ο Bob θέλει να στείλει ένα μήνυμα στην Alice " CALL ME".

Παραγωγή ζεύγους κλειδιών

Για την παραγωγή δημοσίου και ιδιωτικού κλειδιού:

- Η Alice επιλέγει δύο πρώτους αριθμούς $p = 43$, $q = 31$ και υπολογίζει το γινόμενο τους

$$n = p \cdot q = 43 \cdot 31 = 1333$$

- Υπολογίζει την συνάρτηση Euler

$$\phi(n) = \phi(p)\phi(q) = (p-1)(q-1) = (43-1)(31-1) = 1260$$

- Επιλέγει έναν τυχαίο πρώτο αριθμό $e, 1 < e < \phi(n)$, που να μην έχει κοινούς διαιρέτες με τους p και q
  π.χ $e = 97$ και να ικανοποιεί την σχέση $gcd(e, \phi(n)) = 1$

- Η Alice πρέπει να βρει ένα αριθμό d που να ικανοποιεί την ακόλουθη σχέση:

$$97 \equiv d \equiv 1 \pmod{1260}$$

- Χρησιμοποιεί το επεκταμένο αλγόριθμο του Ευκλείδη για να βρεί το d. Σύμφωνα με τον αλγόριθμο εάν θέλουμε να βρούμε τον μέγιστο κοινό διαιρέτη g για δύο αριθμούς a,b και x,y ώστε να επαληθεύεται η σχέση $ax + by = g$. Διαιρούμε τον a με τον b και πέρουμε την $a = kb + r$.
  Στο παράδειγμα μας έχουμε:
  $g = 1$
  $a = a\phi(n) = 1260$
  $b = e = 97$
  $d = y$
  Οπότε η σχέση γίνεται : $\phi(n)x + ey = g$
  δηλ. $1260x + 97y = 1$

  Για να βρώ το x, y από την σχέση $a = kb + r$ έχω:

$$1260 = 12 \cdot 97 + 96 \tag{6.1}$$

$$97 = 1 \cdot 96 + 1 \tag{6.2}$$

$$96 = 96 \cdot 1 + 0 \tag{6.3}$$

Από την (5.2)

$$
\begin{aligned}
1 &= 97 - 1 \cdot 96 \\
&= 97 - 1 \cdot (1260 - 12 \cdot 97) \\
&= 97 - 1 \cdot 1260 + 12 \cdot 97 \\
&= -1 \cdot 1260 + 13 \cdot 97
\end{aligned}
\tag{6.4}
$$

(5.1)

(6.5)

Προκύπτει $x = -1$ και $y = 13 = d$
Οπότε από τα παραπάνω το ζεύγος του δημοσίου κλειδιού είναι $(e, n) = (97, 1333)$ όπου η alice το δημοσιοποιεί και το ιδιωτικό είναι $(d, n) = (13, 1333)$ το οποίο διατηρεί μυστικό.

Κρυπτογράφηση

Ο Bob θέλει να στείλει το μήνυμα "CALL ME" στην Alice

- Μετατρέπει το κάθε γράμμα ανάλογα με την θέση του στο αλφάβητο. C = 03
  A = 01
  L = 12
  L = 12
  M = 13
  E = 05

- Χωρίζει το μήνυμα σε blocks ίσου μεγέθους bits με $0 < mi < n$. $m_1 = 0301$
  $m_2 = 1212$
  $m_3 = 1305$

- Για να το κρυπτογραφήσει υπολογίζει την:

$$c_i = m_i^e \pmod{n}$$

Οπότε πρέπει να βρει τα:
$c_i = m_i^e \pmod{n} = 301^{97} \pmod{1333}$

$c_i = m_i^e \pmod n = 1212^{97} \pmod{1333}$
$c_i = m_i^e \pmod n = 1305^{97} \pmod{1333}$

Παρατηρούμε ότι στο RSA προκύπτει η ανάγκη για τον υπολογισμό μεγάλων δυνάμεων αριθμών. Αυτό αντιμετωπίζεται με την μέθοδο Square and Multiply. Συνοπτικά με τη μέθοδο αυτή αναλύουμε τον αριθμό που θέλουμε να υψώσουμε στην δυαδική του αναπαράσταση. Ανάλογα με το τι είναι το κάθε ψηφίο υψώνουμε στο τετράγωνο το τρέχον αποτέλεσμα και πολλαπλασιάζουμε με τον αρχικό αριθμό μας αν είναι 1 ή δεν κάνουμε τίποτα αν είναι 0. Στο δικό μας παράδειγμα έχουμε: $e = 97$ $n = 1333$ Μετατρέπουμε το 97 στην δυαδική του αναπαράσταση 97=(1100001) και θέτουμε αρχικά $c_i = 1$.

- Για $m_1 = 0301$
  $b_6 = 1 \rightarrow c_1 = c_1^2 m_1 \pmod n = 1^2 \cdot 301 \pmod{1333} = 301$
  $b_5 = 0 \rightarrow c_1 = c_1^2 m_1 \pmod n = 301^2 \cdot 301 \pmod{1333} = 27270901 \pmod{1333} = 387$
  $b_4 = 0 \rightarrow c_1 = c_1^2 \pmod n = 387^2 \pmod{1333} = 149769 \pmod{1333} = 473$
  $b_3 = 0 \rightarrow c_1 = c_1^2 \pmod n = 473^2 \pmod{1333} = 223729 \pmod{1333} = 1118$
  $b_2 = 0 \rightarrow c_1 = c_1^2 \pmod n = 1118^2 \pmod{1333} = 1249924 \pmod{1333} = 903$
  $b_1 = 0 \rightarrow c_1 = c_1^2 \pmod n = 903^2 \pmod{1333} = 815409 \pmod{1333} = 946$
  $b_0 = 1 \rightarrow c_1 = c_1^2 m_1 \pmod n = 946^2 \cdot 301 \pmod{1333} = 269369716 \pmod{1333} = 1102$
  $c_1 = 1075$

- Για $m_2 = 1212$
  $b_6 = 1 \rightarrow c_2 = c_2^2 m_2 \pmod n = 1^2 \cdot 1212 \pmod{1333} = 1212$
  $b_5 = 0 \rightarrow c_2 = c_2^2 m_2 \pmod n = 1212^2 \cdot 1212 \pmod{1333} = 1780360128 \pmod{1333} = 1329$
  $b_4 = 0 \rightarrow c_2 = c_2^2 \pmod n = 1329^2 \pmod{1333} = 1766241 \pmod{1333} = 16$
  $b_3 = 0 \rightarrow c_2 = c_2^2 \pmod n = 16^2 \pmod{1333} = 256 \pmod{1333} = 256$
  $b_2 = 0 \rightarrow c_2 = c_2^2 \pmod n = 256^2 \pmod{1333} = 65536 \pmod{1333} = 219$
  $b_1 = 0 \rightarrow c_2 = c_2^2 \pmod n = 219^2 \pmod{1333} = 47961 \pmod{1333} = 1306$
  $b_0 = 1 \rightarrow c_2 = c_2^2 m_2 \pmod n = 1306^2 \cdot 1212 \pmod{1333} = 2067230832 \pmod{1333} = 1102$
  $c_2 = 1102$

- Για $m_3 = 1305$
  $b_6 = 1 \rightarrow c_3 = c_3^2 m_3 \pmod{n} = 1^2 \cdot 1305 \pmod{1333} = 1305$
  $b_5 = 0 \rightarrow c_3 = c_3^2 m_3 \pmod{n} = 1305^2 \cdot 1305 \pmod{1333} = 2222447625 \pmod{1333} = 709$
  $b_4 = 0 \rightarrow c_3 = c_3^2 \pmod{n} = 709^2 \pmod{1333} = 502681 \pmod{1333} = 140$
  $b_3 = 0 \rightarrow c_3 = c_3^2 \pmod{n} = 140^2 \pmod{1333} = 19600 \pmod{1333} = 938$
  $b_2 = 0 \rightarrow c_3 = c_3^2 \pmod{n} = 938^2 \pmod{1333} = 879844 \pmod{1333} = 64$
  $b_1 = 0 \rightarrow c_3 = c_3^2 \pmod{n} = 64^2 \pmod{1333} = 4096 \pmod{1333} = 97$
  $b_0 = 1 \rightarrow c_3 = c_3^2 m_3 \pmod{n} = 97^2 \cdot 1305 \pmod{1333} = 12278745 \pmod{1333} = 482$
  $c_3 = 0482$

- Ο Bob στέλνει στην Alice την ακολουθία : 1075 1102 0482

Αποκρυπτογράφηση

- Η Alice για αν αποκρυπτογραφήσει το μήνυμα χρησιμοποιεί το μυστικό ιδιωτικό της κλειδί $d = 13$ υπολογίζοντας την:

$$m_i = c_i^d \pmod{n}$$

$m_1 = 1075^{13} \pmod{1333}$
$m_2 = 1102^{13} \pmod{1333}$
$m_3 = 482^{13} \pmod{1333}$
Μετατρέπει το $d = 13$ στην δυαδική του αναπαράσταση $d = 1101$ και θέτει αρχικά $m_i = 1$

- Για $c_1 = 1075$

$b_3 = 1 \rightarrow m_1^2 c_1 \pmod{n} = 1^2 \cdot 1075 \pmod{1333} = 1075$
$b_2 = 1 \rightarrow m_1^2 c_1 \pmod{n} = 1075^2 \cdot 1075 \pmod{1333} = 1242296875 \pmod{1333} = 860$
$b_1 = 0 \rightarrow m_1^2 \pmod{n} == 860^2 \pmod{1333} = 739600 \pmod{1333} = 1118$
$b_0 = 1 \rightarrow m_1^2 c_1 \pmod{n} = 1118^2 \cdot 1075 \pmod{1333} = 1343668300 \pmod{1333} = 301$

$m_1 = 301$ που ισχύει.

- Για $c_2 = 1102$
  $b_3 = 1 \rightarrow m_2^2 c_2 \pmod{n} = 1^2 \cdot 1102 \pmod{1333} = 1102$
  $b_2 = 1 \rightarrow m_2^2 c_2 \pmod{n} = 1102^2 \cdot 1102 \pmod{1333} = 1338273208 \pmod{1333} = 1193$
  $b_1 = 0 \rightarrow m_2^2 \pmod{n} = 1193^2 \pmod{1333} = 1423249 \pmod{1333} = 938$
  $b_0 = 1 \rightarrow m_2^2 c_2 \pmod{n} = 938^2 \cdot 1102 \pmod{1333} = 969588088 \pmod{1333} = 1212$

  $m_2 = 1212$ που ισχύει.

- Για $c_3 = 482$

  $b_3 = 1 \rightarrow m_3^2 c_3 \pmod{n} = 1^2 \cdot 482 \pmod{1333} = 482$
  $b_2 = 1 \rightarrow m_3^2 c_3 \pmod{n} = 482^2 \cdot 482 \pmod{1333} = 111980168 \pmod{1333} = 170$
  $b_1 = 0 \rightarrow m_3^2 \pmod{n} == 170^2 \pmod{1333} = 28900 \pmod{1333} = 907$
  $b_0 = 1 \rightarrow m_3^2 c_3 \pmod{n} = 907^2 \cdot 482 \pmod{1333} = 396516818 \pmod{1333} = 1305$

  $m_3 = 1305$ που ισχύει.

6.2 Ψηφιακή υπογραφή RSA

Κατά την κρυπτογράφηση και αποκρυπτογράφηση δημοσίου κλειδιού RSA ο χώρος των μηνυμάτων και κρυπτομηνυμάτων είναι ο ίδιος. Λόγω του ότι η συνάρτηση κρυπτογράφησης είναι 1-1, μπορούμε να δημιουργήσουμε ψηφιακές υπογραφές με την αντιστροφή κρυπτογράφησης και αποκρυπτογράφησης. Η ψηφιακή υπογραφή RSA είναι αιτιοκρατικό σχήμα ψηφιακών υπογραφών με ανάκτηση μηνύματος. Ο χώρος υπογραφών είναι πάλι ο ίδιος με των μηνυμάτων και των κρυπτοκειμένων. Το σχήμα αυτό ψηφιακών υπογραφών προϋποθέτει ότι τα ζεύγη του ιδιωτικού και δημοσίου κλειδιού είναι γνωστά και στις ονότητες επικοινωνίας.

Επειδή η ψηφιακή υπογραφή αποτελείται από το μήνυμα αποκρυπτογραφημένο με το ιδιωτικό κλειδί του αποστολέα, το σύστημα ψηφιακών υπογραφών RSA μπορεί να λειτουργήσει ως σύστημα ψηφιακής υπογραφής με αυτοανάκτηση, αν σταλεί μόνον η ψηφιακή υπογραφή χωρίς το μήνυμα. [4, σελ.433-434]

Ορισμός: Έστω από το γινόμενο δύο πρώτων αριθμών p, q $n = pq$ με $m = s = z_n$. Μια ψηφιακή υπογραφή RSA ορίζεται από την ακόλουθη σχέση:

$$S_{(m)} = m^d \pmod{n}$$

Και η επαλήθευση της από :

$$V = s^e \pmod{n}$$

Όπου ισχύει η σχέση:

$$e \cdot d \equiv 1 \pmod{\phi_{(n)}}$$

[4, σελ.433-434]

6.2.1 Παράδειγμα

Έστω θέλουμε να υπογράψουμε ψηφιακά ένα μήνυμα. Για την κρυπτογράφηση της υπογραφής του μηνύματος χρησιμοποιείται το μυστικό ιδιωτικό κλειδί , ενώ για την επαλήθευση από τον παραλήπτη του μηνύματος το δημόσιο.

Θα χρησιμοποιήσουμε τα ίδια p και q με το προηγούμενο παράδειγμα, γνωρίζουμε το $\phi(n) = 1333$, $e = 97 = [1100001]$, $d = 13 = [1101]$ και έχουμε : $m_1 = 0301$
$m_2 = 1212$
$m_3 = 1305$
Πρέπει να βρούμε τις τιμές που ικανοποιούν τις παρακάτω σχέσεις :

$s_1 = 301^{13} \pmod{1333}$
$s_2 = 1212^{13} \pmod{1333}$
$s_3 = 1305^{13} \pmod{1333}$

- Για $m_1 = 0301$

$b_3 = 1 \rightarrow s_1^2 m_1 \pmod n = 1^2 \cdot 301 \pmod{1333} = 301$
$b_2 = 1 \rightarrow s_1^2 m_1 \pmod n = 301^2 \cdot 301 \pmod{1333} = 387$
$b_1 = 0 \rightarrow s_1^2 \pmod n == 387^2 \pmod{1333} = 473$
$b_0 = 1 \rightarrow s_1^2 m_1 \pmod n = 473^2 \cdot 301 \pmod{1333} = 602$

$s_1 = 602$

- Για $m_1 = 1212$

$b_3 = 1 \rightarrow s_2^2 m_2 \pmod n = 1^2 \cdot 1212 \pmod{1333} = 1212$
$b_2 = 1 \rightarrow s_2^2 m_2 \pmod n = 1212^2 \cdot 1212 \pmod{1333} = 1329$
$b_1 = 0 \rightarrow s_2^2 \pmod n == 1329^2 \pmod{1333} = 16$
$b_0 = 1 \rightarrow s_2^2 m_2 \pmod n = 16^2 \cdot 1212 \pmod{1333} = 1016$

$s_2 = 1016$

- Για $m_3 = 1305$

$b_3 = 1 \rightarrow s_3^2 m_3 \pmod n = 1^2 \cdot 1305 \pmod{1333} = 1305$
$b_2 = 1 \rightarrow s_3^2 m_3 \pmod n = 1305^2 \cdot 1305 \pmod{1333} = 709$
$b_1 = 0 \rightarrow s_3^2 \pmod n == 709^2 \pmod{1333} = 140$
$b_0 = 1 \rightarrow s_3^2 m_3 \pmod n = 140^2 \cdot 1305 \pmod{1333} = 396$

$s_1 = 396$

Άρα προκύπτει το [0602 1016 396]. Για να γίνει όμως η επαλήθευση από τον παραλήπτη χρησιμοποιείται το δημόσιο κλειδί και πρέπει να υπολογιστούν οι παρακάτω σχέσεις:

$V_1 = 602^{97} \pmod{1333}$
$V_2 = 1016^{97} \pmod{1333}$
$V_3 = 396^{97} \pmod{1333}$

- Για $s_1 = 602$

$b_6 = 1 \rightarrow v_1 = v_1^2 s_1 \pmod{n} = 1^2 \cdot 602 \pmod{1333} = 602$
$b_5 = 0 \rightarrow v_1 = v_1^2 s_1 \pmod{n} = 602^2 \cdot 602 \pmod{1333} = 430$
$b_4 = 0 \rightarrow v_1 = v_1^2 \pmod{n} = 430^2 \pmod{1333} = 946$
$b_3 = 0 \rightarrow v_1 = v_1^2 \pmod{n} = 946^2 \pmod{1333} = 473$
$b_2 = 0 \rightarrow v_1 = v_1^2 \pmod{n} = 473^2 \pmod{1333} = 1118$
$b_1 = 0 \rightarrow v_1 = v_1^2 \pmod{n} = 1118^2 \pmod{1333} = 903$
$b_0 = 1 \rightarrow v_1 = v_1^2 s_1 \pmod{n} = 903^2 \cdot 602 \pmod{1333} = 301$

$v_1 = 301$ που ισχύει.

- Για $s_2 = 1016$

$b_6 = 1 \rightarrow v_2 = v_2^2 s_2 \pmod{n} = 1^2 \cdot 1016 \pmod{1333} = 1016$
$b_5 = 0 \rightarrow v_1 = v_2^2 s_2 \pmod{n} = 1016^2 \cdot 1016 \pmod{1333} = 1021$
$b_4 = 0 \rightarrow v_1 = v_2^2 \pmod{n} = 1021^2 \pmod{1333} = 35$
$b_3 = 0 \rightarrow v_1 = v_2^2 \pmod{n} = 35^2 \pmod{1333} = 1225$
$b_2 = 0 \rightarrow v_1 = v_2^2 \pmod{n} = 1225^2 \pmod{1333} = 1000$
$b_1 = 0 \rightarrow v_1 = v_2^2 \pmod{n} = 1000^2 \pmod{1333} = 250$
$b_0 = 1 \rightarrow v_1 = v_2^2 s_2 \pmod{n} = 250^2 \cdot 1016 \pmod{1333} = 1212$

$v_1 = 1212$ που ισχύει.

- Για $s_3 = 396$

$b_6 = 1 \rightarrow v_3 = v_3^2 s_3 \pmod{n} = 1^2 \cdot 396 \pmod{1333} = 396$
$b_5 = 0 \rightarrow v_3 = v_3^2 s_3 \pmod{n} = 396^2 \cdot 396 \pmod{1333} = 1331$
$b_4 = 0 \rightarrow v_3 = v_3^2 \pmod{n} = 1331^2 \pmod{1333} = 4$
$b_3 = 0 \rightarrow v_3 = v_3^2 \pmod{n} = 4^2 \pmod{1333} = 16$
$b_2 = 0 \rightarrow v_3 = v_3^2 \pmod{n} = 16^2 \pmod{1333} = 256$
$b_1 = 0 \rightarrow v_3 = v_3^2 \pmod{n} = 256^2 \pmod{1333} = 219$
$b_0 = 1 \rightarrow v_3 = v_3^2 s_3 \pmod{n} = 219^2 \cdot 396 \pmod{1333} = 11305$

$v_1 = 1305$ που ισχύει.

6.2.2 Επιθέσεις και ασφάλεια ψηφιακών υπογραφών RSA

[4, σελ.435-437]

Παραγοντοποίηση ακεραίων

Είναι πολύ σημαντική η τιμή και το μέγεθος των p και q από τον αποστολέα ώστε η παραγοντοποίηση n να είναι αδύνατο να υπολογιστεί. Αυτό γιατί εάν ένα μη εξουσιοδοτημένο άτομο καταφέρει να παραγοντοποιήσει το modulus n, τότε με την χρήση του επεκταμένου αλγόριθμου του Ευκλείδη από τον δημόσιο κλειδί και το Φ(n) μπορεί να βρεί το ιδιωτικό κλειδί d, λύνοντας την σχέση $ed \equiv 1 \pmod{\phi(n)}$.
Έτσι μπορεί να παραβιάσει όλο το σύστημα και να υποκλέψει τα δεδομένα του αποστολέα και του παραλήπτη.

Πολλαπλασιαστική ιδιότητα του RSA

Έστω ότι έχουμε ένα modulus n με ιδιωτικό κλειδί d. Εάν θέσουμε $k = [lgn]$ και αντιπροσωπεύσει το μήκος της δυαδικής αναπαράστασης n και t θετικός , $t < t/2$. Έστω $w = 2^t$ κσι $[1-, n2^{-1}]$. Η συνάρτηση $R(m) = m2^t$ είναι η συνάρτηση περίσσειας.
Στο RSA το σχήμα έχει την πολλαπλασιατική ή ομοιομορφική ιδιότητα. Αν $s_1 = m_1^d \pmod{n}$ και $s_2 = m_2^d \pmod{n}$, οι υπογραφές μηνυμάτων με περίσσεια, τότε για το $s = s_1 s_2 \pmod{n}$ ισχύει η ιδιότητα $s = (m_1 m_2)^d \pmod{n}$.
Αν το $m = m_1 m_2$ έχει περίσσεια , τότε έχουμε μια έγκυρη υπογραφή. οπότε είναι σημαντικό η συνάρτηση R περισσείας να μην είναι πολλαπλασιατική.

Πρόβλημα ανατμηματοποίησης

Μια συνήθης χρήση του RSA είναι η υπογραφή ενός μηνύματος και η κρυπτογράφηση της. Βασικός παράγοντας όμως είναι τα μεγέθη των modulus. Έστω ότι η Alice θέλει να στείλει ένα μήνυμα στο Bob, εάν το $n_a > n_b$ τότε μπορεί να ο Bob να μην μπορεί να κάνει ανάκτηση του μηνύματος. Η πιθανότητα να εμφανισιεί αυτό το πρόβλημα είναι $(n_a - n_b/n_a)$

Το πρόβλημα της ανατμηματοποίησης μπορεί να λυθεί με τους παρακάτω τρόπους.

Με αναδιάταξη.

Δεν ενδείκνυται για λόγους ασφάλειας αλλά θα μπορούσε να αποτελεί μια λύση στο πρόβλημα. Αυτό γίνεται με το να γίνει πρώτη η πράξη με το μικρότερο modulus. Δηλαδή στην περίπτωση που το $n_a > n_b$, τότε θα πρέπει πρώτα η Alice να κρυπτογραφήσει το μήνυμα που θέλει να στείλει με το δημόσιο κλειδί του Bob και μετά να το υπογράψει ψηφιακά, κάνοντας με το μυστικό ιδιωτικό της κλειδί. Συνήθως όμως δεν αλλάζει η σειρά των πράξεων για λόγους ασφαλείας. Αυτό γιατί είναι εύκολο από ένα μη εξουσιοδοτημένο άτομο να καταφέρει να αλλάξει τη υπογραφή με μια άλλη. Επίσης το γεγονός ότι ο αντίπαλος δεν γνωρίζει τι είναι υπογεγραμμένο μπορεί να λειτουργήσει υπέρ του.

Δύο moduli ανα χρήστη.

Πρέπει κάθε χρήστης να έχει από δύο moduli, ένα για την κρυπτογράφηση και ένα για την ψηφιακή υπογραφή. Ακόμα το κάθε moduli της ψηφιακής υπογραφής να είναι μικρότερο από αυτό της κρυπτογράφησης, έτσι δεν θα υπάρξει λάθος στην αποκρυπτογράφηση και θα εξαλειθφεί το πρόβλημα της αναδιάταξης. Αν το moduli της υπογραφής είναι k bits τότε της κρυπτογράφησης θα πρέπει να είναι τουλάχιστον (k + 1) bits μεγαλύτερο.

Μορφή του modulus

Δεν λύνεται εντελώς το πρόβλημα με αυτή την μέθοδο αλλά μπορούμε να ελλατώσουμε σημαντικά την εμφάνιση λαθών κατά την αποκρυπτογράφηση. Για να επιτευχθεί αυτό πρέπει η επιλογή των πρώτων αριθμών που συνθέτουν το modulus να είναι τέτοια, ώστε σε ένα modulus n , t bits τα υψηλότερης αξίας bits να είναι 1 και τα υπόλοιπα 0. Για να γίνει αυτό επιλέγεται ένας πρώτος αριθμός p = t/2 bits και αναζητείται ένας q μεταξύ των διαστημάτων $[2^{t-1}/p]$ και $[(2^{t-1} + 2^{t-k-1})/p]$. Ενώ για το modulus n πρέπει να ισχύει $2^{t-1} \leq n \leq 2^{t-1} + 2^{t-k-1}$.

Άλλα χαρακτηριστικά για την δημιουργία ψηφιακών υπογραφών

1. Για την δημιουργία του modulus συνίσταται το ελάχιστο 768 bits ενώ για μεγάλου χρόνου ζωής υπογραφές 1024 bits.

2. Επίσης η αποδοτικότητα του εύρους ζώνης ορίζεται από την συνάρτηση περίσσειας, η οποία καθορίζεται από το ISO/IEC 9796, δέχεται μηνύματα k bits και τα κωδικοποιεί σε 2k.

3. Η ψηφιακή υπογραφή RSA ταιριάζει σε περιπτώσεις όπου ή επαλήθευση υπογραφής είναι η κύρια πράξη. Αν για παράδειγμα ένα έμπιστο τρίτο μέλος δημιουργεί ένα πιστοποιητικό δημοσίου κλειδιού απαιτείται μια παραγωγή δημοσίου κλειδιού. Ενώ η υπογραφή αυτή επαληθεύεται πόλλες φορές από πολλές οντότητες.

4. Ένα σχήμα ψηφιακών υπογραφών με ανάκτηση μηνύματος μπορεί να τροποποιηθεί με τον κατάλληλο αλγόριθμο σε ψηφιακή υπογραφή με παράρτημα.

5. Δεν είναι ασφαλές να χρησιμοποιούνται modulus καθολικής εφαρμογής

6.3 Ασφάλεια και Επιθέσεις στο σχήμα RSA

Ο RSA θεωρείται ασφαλής αλγόριθμος με την χρήση όμως μεγάλων παραμέτρων κατα την υλοποίηση του. μερικές απειλές βασίζονται στην μη προσεκτική σχεδίαση και εκτέλση της κρυπτογράφησης. Υπάρχουν όμως και απειλές που δεν έχουν καμμία σχέση με το πρόβλημα της δυσκολίας της παραγοντοποίησης ακεραίου. Δεν είναι λοιπόν υποχρεωτική η γνώση του modulus για παραβιαστεί ένα σύστημα RSA. Ακολουθούν οι επιθέσεις που μπορεί να δεχθεί συνήθως ένα σχήμα κρυπτογράφησης RSA και θέματα σχετικά με την ασφάλεια του:

1. **Επίθεση μικρού εκθέτη κρυπτογράφησης - αποκρυπτογράφησης.**

   Εάν χρησιμοποιηθεί μικρός εκθέτης e κατά την κρυπτογράφηση ή την ψηφιακή υπογραφή μειώνεται ο χρόνος κρυπτιογράφησης , αλλά δεν είναι ασφαλές. Αν κρυπτογραφούμε μηνύματα γραμμικώς εξαρτημένα με διαφορετικά κλειδιά αλλά ίδιο e υπάρχει πρόβλημα αδυναμίας του σχήματος και είναι ευάλωτο σε επίθεση. Θα πρέπει στην περίπτωση αυτή τα μηνύματα να είναι γραμμικός ανεξάρτητα. Ενώ αν τα μηνύματα είναι ίδια απαιτούνται e μηνύματα για επίθεση.
   Για να αντιμετωπιστούν τέτοιου είδους επιθέσεις πρέπει να διασφαλίζεται ότι $m^e \pmod{n} \neq m^e$ με επικόλληση των μηνυμάτων τυχαία. Αυτό επιτυγχάνεται με διάφορες εφαρμογές όπως η PGP. Υπάρχει όμως και η περίπτωση επίθεσης όταν έχουμε μικρό εκθέτη αποκρυπτογράφησης αν και δεν συμβαίνει συχνά όταν οι

εκθέτες επιλέγονται τυχαία. Η μικρότερη δυνατή τιμή για το e είναι 3 για θέματα ασφαλείας όμως συνίσταται τουλάχιστον $e = 216 + 1 = 65537$. Στην περίπτωση που το d είναι μικρότερο από το $\frac{1}{4}$ του n μπορεί να γίνει επίθεση και να ανακτηθεί το n.[4, σελ.288]

2. **Επίθεση σε κοινό modulus**

Το σχήμα RSA μπορεί να υλοποιηθεί και με την χρήση του ίδιου modulus χωρίς όμως αυτό να σημαίνει ότι είναι και ασφαλές. Ένα τέτοιο σχήμα θα ήταν πολύ αδύναμο σε επιθέσεις. Αυτό γιατί αν ένα μήνυμα κρυπτογραφηθεί με διαφορετικά κλειδιά e και d με κοινό moduluseίναι εύκολο να ανακτηθεί, αν οι e και d είναι πρώτοι μεταξύ τους χωρίς να είναι απαραίτητο να είναι γνωστοί.
Τέτοιες επιθέσεις γίνονται σε ομάδες χρηστών όταν η χρησιμοποιούν τον ίδιο μηχανισμό για την παραγωγή των κλειδιών τους, αλλά και όταν ένας χρήστης στέλνει ένα μήνυμα σε πολλούς αποδέκτες. Δηλ. σε μοντέλα επικοινωνίας «ένα προς πολλά».[4, σελ.289]

3. **Επίθεση επαναληπτικής κρυπτογράφησης**
Η επίθεση αυτή βασίζεται στην περιοδικότητα του της συνάρτησης του σχήματος. Έστω δημόσιο κλειδί (e,n) και θέλω να κρυπτογραφήσω ένα μήνυμα m. Η κρυπτογράφηση θα είναι:

$$c = m^e \pmod{n}$$

Εάν $c^{(0)}$ το κρυπτογράφημα του μηνύματος , ένα τρίτο άτομο έχοντας το $c^{(0)}$ μπορεί να εκτελέσει τις πράξεις: $c^i \equiv (c^{(i-1)})^e \pmod{n}$,για $i = 1, 2, 3, \ldots$ Για κάποιο $i = k$ θα είναι σε θέση να βρει το $c^{(k)}$ που αποτελεί το μήνυμα. Αυτό όμως θα το επιβεβαιώσει στο επόμενο βήμα για $i = k + 1$. Η τιμή του k που μας οδηγεί στο αρχικό μήνυμα λέγεται εκθέτης ανάκτησης. Για περισσότερη ασφάλεια θα πρέπει ο εκθέτης ανάκτησης να είναι όσο το δυνατό μεγαλύτερος αν και λόγω της περιοδικότητας του έχει κάποιο ανώτατο όριο. Μπορούμε να υπολογίσουμε το ανώτατο όριο εκθέτη ανάκτησης με το θεώρημα Carmichael.[7, σελ.227]

Όταν $i = 0$ μπορώ να βρω το m . Αυτό ισχύει όταν $k = i = \psi(\psi(n))$. Άρα το $\psi(\psi(n))$ πρέπει να είναι όσο το δυνατό μεγαλύτερο από την:

$$\psi(n) = \psi(p \cdot q) = 2lcm(p - 1/2, q - 1/2)$$

Αυτό γίνεται με το να έχουν μεγάλους παράγοντες τα $(p-1)/2, (q-1)/2$ και ο μέγιστος κοινός διαιρέτης να είναι μικρός. Οι βέλτιστες τιμές επιτυγχάνονται όταν οι p και q είναι μεταξύ τους ασφαλής πρώτοι.

4. **Forward search attack**

   Εάν ο χώρος μηνυμάτων είναι μικρός ή εύκολα προβλέψιμος, ένας αντίπαλος μπορεί να αποκρυπτογραφήσει το κρυπτοκείμενο. Αυτό γίνεται με το να δοκιμάσει όλα τα πιθανά μηνύματα μέχρι να καταλήξει στο σωστό ώστε να αποκρυπτογραφείται το κρυπτόγραμμα. Μια τέτοια επίθεση προλαμβάνεται με την μέθοδο salting message. Στην μέθοδο αυτή παράγονται ψευδοτυχαία bitstring κατάλληλου μήκους, που επισυνάπτονται στο μήνυμα πριν από την κρυπτογράφηση. Είναι ανεξάρτητα και είναι διαφορετικά για κάθε κρυπτογράφηση. [4, σελ.288]

5. **Απόκρυψη μηνύματος**

   Ένα μήνυμα $m, 0 \leq m \leq n-1$ είναι φανερό εάν κρυπτογραφεί τον εαυτό του. $m^e \equiv m \pmod{n}$. Τέτοια μηνύματα έχω συνήθως για $m = 0, m = 1$ και $m = n-1$. Ο πραγματικός αριθμός αυτών των μηνυμάτων ορίζεται από την παρακάτω σχέση:

   $$[1 + gcd(e-1, p-1)] \cdot [1 + gcd(e-1, q-1)]$$

   [4, σελ.290]

6.4 Το πρόβλημα RSA.

Γνωστό και ώς RSAP το πρόβλημα RSA είναι το εξής: Γνωρίζοντας το n όπου ξέρουμε ότι $n = p \cdot q$, ένα επίσης θετικό e όπου να ισχύει $gcd(e, (p-1)(q-1)) = 1$ και έναν ακέραιο c, να βρούμε έναν ακέραιο m που να ικανοποιεί την παρακάτω σχέση

$$m^e \equiv c \pmod{n}$$

Η δυσκολία δηλαδη είναι η εύρεση της e-οστής ρίζας που ικανοποιεί την παραπάνω σχέση. βασική προυπόθεση όμως είναι οι n και e να μας διασφαλίζουν ότι για κάθε $c \in \{0, 1, ..., n-1\}$ υπάρχει ένας $m \in \{0, 1, ..., n-1\}$ ώστε $m^e \equiv c \pmod{n}$.[4, σελ.98]

Συμπεράσματα

Η κρυπτογραφία από την αρχαιότητα μέχρι σήμερα έχει εξελιχθεί σε μεγάλο βαθμό.«Η κρυπτογραφία έγινε αόρατο κομμάτι της καθημερινής μας ζωής με την έλευση των Μηχανών Αυτόματων Συναλλαγών (ATM)», λέει ο Steven Levy συγγραφέας του βιβλίου «Crypto: When the Code Rebels beat the Government» .Θα ήταν δύσκολο να φανταστούμε την ζωή μας χωρίς τις εφαρμογές της, αφού σε νομικό και κοινωνικό επίπεδο, τίθεται ζήτημα προστασίας του απορρήτου σε όλες τις εκδοχές δικτυακής συναλλαγής (email, εμπορικές συναλλαγές, τραπεζικό και ιατρικό απόρρητο) και γενικότερα ζήτημα προστασίας προσωπικών δεδομένων του κάθε χρήστη του Internet. (τα προσωπικά στοιχεία, όπως ο αριθμός της πιστωτικής μας κάρτας, που στέλνουμε σε διάφορα ηλεκτρονικά μαγαζιά, ακόμα και τα κινητά τηλέφωνα έχουν ενσωματωμένα κρυπτογραφικά συστήματα.)
Η κρυπτογράφηση παίζει σημαντικό ρόλο στην προστασία δεδομένων εξασφαλίζοντας το απόρρητο των προσωπικών πληροφοριών. Οι μέθοδοι κρυπτογράφησης διασφαλίζουν την ασφάλεια των δεδομένων, αλλά και την διατήρηση της εμπιστευτικότητας των πληροφοριών, την προστασία τους από αλλοίωση, καταστροφή ή φθορά. Σημαντικό είναι επίσης ότι επιτρέπουν την επαλήθευση της πηγής των πληροφοριών, όπως για παράδειγμα συμβαίνει με τα συστήματα ηλεκτρονικής υπογραφής, όπου το κλειδί αποκρυπτογράφησης είναι διαθέσιμο , ενώ το μυστικό κλειδί κρυπτογράφησης εγγυάται την αυθεντικότητα και την ακεραιότητα ενός αρχείου.
Οι τεχνολογίες κρυπτογράφησης είναι ανεξάρτητες από τις ιδιότητες των μέσων στα οποία εφαρμόζονται ενώ εκτελούνται με μεγάλη ταχύτητα . Δηλαδή τα δεδομένα τροποποιούνται τόσο ώστε καμία χρήσιμη πληροφορία δεν μπορεί να εξαχθεί από αυτά, ενώ τα μέσα παραμένουν ανεπηρέαστα. Η εμπιστευτικότητα διασφαλίζεται μέσω της μυστικότητας του μοναδικού κλειδιού που χρησιμοποιείται για την αποκρυπτογράφηση.Η χρήση των διαφορετικών αλγορίθμων, πρωτοκόλλων και μεθόδων κρυπτογράφησης που χρησιμοποιούνται ανεβάζουν την ασφάλεια σε υψηλό επίπεδο. Ακόμα και να είναι μια επίθεση επιτυχής ο αντίπαλος θα πρέπει να διαθέτει μεγάλη υπολογιστική ισχύ ή πολύ χρόνο, κάτι το οποίο θα καθιστούσε την πληροφορία μη επίκαιρη.
Το γεγονός ότι η ασφάλεια των αλγορίθμων κρυπτογράφησης βαζίζεται σε κάποια αριθμοθεωριτηκά προβλήματα, (όπως το πρόβλημα της παραγοντοποίησης μεγάλων ακεραίων ή του διακριτού λογάριθμου), καθιστά την παραβίαση τους σχεδόν αδύνατη , χωρίς να έχει όμως αποδειχθεί αδύνατη. Κλείνοντας μπορούμε να πούμε με βεβαιότητα πως όντως η κρυπτογραφία είναι η τέχνη που εξελίχθηκε σε επιστήμη.

Παράρτημα Α΄

Α΄.1 Ορολογία Κρυπτογραφίας

- ***Algorithm*** - Αλγόριθμος ορίζεται μια πεπερασμένη σειρά ενεργειών, αυστηρά καθορισμένων και εκτελέσιμων σε πεπερασμένο χρόνο, που στοχεύουν στην επίλυση ενός προβλήματος.
- ***Authorization*** - Εξουσιοδότηση επιτρέπει σ' έναν χρήστη την πρόσβαση σε περιοχές ή στο σύνολο ενός δικτύου βάσει της ταυτότητάς του.
- ***Cipher*** - Όρος που αναφέρεται στην κρυπτογράφηση μηνυμάτων. Είναι συνώνυμος με τους όρους Encryption και Encode.
- ***CipherText*** { Κρυπτογράφημα και είναι το κρυπτογραφημένο (κωδικοποιημένο) αρχείο, κείμενο ή μήνυμα που στέλνει ο αποστολέας στον παραλήπτη. Το αρχικό (αυθεντικό), δηλ. το μη κρυπτογραφημένο μήνυμα, αποκαλείται PlainText.
- ***Code*** - Αποδίδεται στα ελληνικά με τον όρο Κώδικας και αναφέρεται στη χρήση χαρακτήρων ή λέξεων για την αναπαράσταση άλλων λέξεων ή προτάσεων.
- ***Cracker*** - Χρήστης ο οποίος εισβάλει σε σύστημα στο οποίο δεν έχει νόμιμη πρόσβαση με σκοπό να παραποιήσει ή ακόμη και να καταστρέψει δεδομένα και πληροφορίες ή και να δημιουργήσει παράνομα αντίγραφα νόμιμων προγραμμάτων.
- ***Cryptoanalysis*** { Κρυπτανάλυση και αναφέρεται στην τέχνη της της αποκρυπτογράφησης, των κρυπτοσυστημάτων. Μπορεί να αναφέρεται επίσης και στην εύρεση λαθών ή και ελλείψεων κατά την εφαρμογή ενός αλγορίθμου κρυπτογράφησης.
- ***Cryptology*** - Κρυπτολογία και αναφέρεται στη μελέτη της κρυπτογραφίας και της κρυπτανάλυσης.

- ***Cryptosystem*** - Κρύπτοσύστημα οι μεθόδοι κρυπτογράφησης και αποκρυπτογράφησης καθώς και διαπίστωσης της ταυτότητας του αποστολέα ενός μηνύματος.
- ***Data Enrcyption***- Κρυπτογράφηση Δεδομένων με τη χρήση μαθηματικών εργαλείων για την καθιέρωση της εμπιστοσύνης ανάμεσα στον αποστολέα και τον παραλήπτη (αποδέκτη) ενός μηνύματος.
- ***Decryption*** - Αποκρυπτογράφηση και είναι η μέθοδος επαναφοράς ενός μηνύματος, που έχει κρυπτογραφηθεί σε μη αναγνώσιμη μορφή (cipher text), στην κανονική ή αρχική του του μορφή (plain text).
- ***Digital Signature*** - Ψηφιακή Υπογραφή και πρόκειται για ειδικό αρχείο το οποίο δημιουργείται από κείμενο που το υπογράφει και το κρυπτογραφεί ο κάτοχός του.
- ***Encryption*** - Κρυπτογράφηση και είναι η μέθοδος μετατροπής κάποιων πληροφοριών σε απόρρητο κώδικα, που είναι γνωστό και ως κρυπτογράφημα (cipher text).
- ***Hacker*** - Χρήστης ο οποίος εισβάλει σε σύστημα στο οποίο δεν έχει νόμιμη πρόσβαση, αλλά μόνο για πειραματισμό και ευχάριστη απασχόληση καθώς και για να εντοπίσει και να υποδείξει κενά στα συστήματα ασφαλείας των υπολογιστικών συστημάτων.
- ***Key*** - Κλειδί μια συλλογή από δυαδικά ψηφία που είναι αποθηκευμένα σ' ένα αρχείο που χρησιμοποιείται για την κρυπτογράφηφη ή αποκρυπτογράφηση ενός μηνύματος.
- ***Passphrase*** - Κωδική Φράση και είναι ουσιαστικά το ίδιο πράγμα με το Πασσωορδ με τη διαφορά ότι είναι πιο περίπλοκο και συνεπώς πιο δύσκολο να εντοπισθεί.
- ***Password*** - Κωδικός Πρόσβασης και είναι μια μοναδική και απόρρητη λέξη κλειδί με την οποία σε συνδυασμό με το (username) μπορούμε να αποδείξουμε την ταυτότητά μας όταν εισερχόμαστε σε περιορισμένης πρόσβασης σελίδες ή εφαρμογές ή και αλλού.
- ***PlainText*** - Είναι το αυθεντικό αρχείο, κείμενο ή μήνυμα, το οποίο πρέπει να λάβει κανονικά ο παραλήπτης.
- ***Private Key*** - Ιδιωτικό Κλειδί ενός κρυπτογραφικού συστήματος. Μπορεί να το χρησιμοποιεί ο κάτοχός του για να υπογράφει ηλεκτρονικά τα εξερχόμενα μηνύματά του καθώς και για να αποκρυπτογραφεί τα εισερχόμενα μηνύματά του.

- ***Public Key*** - Δημόσιο Κλειδί και είναι το κοινό κλειδί ενός κρυπτογραφικού συστήματος. Μπορεί να το χρησιμοποιεί ένας οποιοσδήποτε τρίτος για να κρυπτογραφεί τα εξερχόμενα μηνύματά του προς τον κάτοχο του αντίστοιχου ιδιωτικού κλειδιού καθώς και για να αποκρυπτογραφεί τα εισερχόμενα μηνύματα που έχουν κωδικοποιηθεί με το ιδιωτικό κλειδί του αποστολέα.

- ***User Identification*** - Αναφέρεται στην πιστοποίηση, δηλ. στον έλεγχο της ταυτότητας ή του δικαιώματος πρόσβασης σ' έναν δικτυακό τόπο, που γίνεται με το όνομα χρήστη και τον κωδικό πρόσβασης.

- ***Username*** - Αποδίδεται στα ελληνικά με τον όρο Όνομα Χρήστη ή και Αναγνωριστικό και χρησιμοποιείται συνήθως σε συνδυασμό μ' έναν Κωδικό Πρόσβασης για την εισαγωγή σ' ένα σύστημα ή δίκτυο πολλαπλών χρηστών.

Α΄.2 Το παράδοξο της ημερομηνίας γέννησης

Σύμφωνα με το παράδοξο της ημερομηνίας γέννησης αν σε μια αίθουσα βρίσκονται 23 άτομα η πιθανότητα δύο από αυτά να έχουν ίδια ημέρα γέννησης είναι 50%. Αν n τα άτομα και p_n η πιθανότητα να έχουν δύο άτομα γενέθλια την ίδια μέρα. Η πιθανότητα να μην έχει κάνεις γενέθλια την ίδια μέρα είναι $p'_n = 1 - p_n$. Για το πρώτο άτομο που θα εισέλθει στην αίθουσα η πιθανότητα θα είναι 365/365 δηλ. 1 κ.ο.κ. Έτσι προκύπτει ότι:

$$p'_n = 1 - \frac{365!}{(365-n)!365^n}$$

, για $n = 23$ τότε $p'_n = 0.507$ δηλ. 50%.

Το παράδοξο των γενεθλίων αναφέρεται συχνά στη Θεωρία των Πιθανοτήτων για να μας δείξει ότι τα αποτελέσματα της μπορεί να διαφέρουν αρκετά από την διαίσθηση μας.

Α΄.3 Εκτεταμένος Αλγόριθμος του Ευκλείδη.

Ο αλγόριθμος αυτός χρησιμοποιείται για να βρεθεί ο μέγιστος κοινός διαιρέτης d δύο ακέραιων αριθμών a και b , αλλά και οι ακέραιοι x και y που ικανοποιούν την σχέση $ax + by = d$. Είσοδος : Ακέραιοι θετικοί a και b με $a \geq b$. Έξοδος : $d = gcd(a, b)$ και x , y ώστε $ax + by = d$.

1. If $b = 0$ then set$d \leftarrow a, x \leftarrow 1, y \leftarrow 0$, and return$(d, x, y)$.
2. Set $x2 \leftarrow 1, x1 \leftarrow 0, y \leftarrow 0, y1 \leftarrow 1$.
3. While $b > 0$ do the following:
   $q \leftarrow [a/b], r \leftarrow a - qb, x \leftarrow x2 - qx1, y \leftarrow y2 - qy1.\ a \leftarrow b, b \leftarrow r, x2 \leftarrow x1, x1 \leftarrow x, y2 \leftarrow y1, andy1 \leftarrow y$.
4. Set $d \leftarrow a, x \leftarrow x2, y \leftarrow y2$, and return$(d, x, y)$.

Α΄.4 Αλγόριθμος Square and Multiply.

Ο square and multiply algorithm χρησιμοποιείται για τον υπολογισμό των μεγάλων δυνάμεων.

$c = 1$
for $i = k - 1$ to 0 do
$c = c2modn$
if $bi = 1$ then $c = c \cdot m \cdot modn$
end for
output $c = m \cdot modn$

Βιβλιογραφία

[1] "New Direction in Cryptography" by Whitfield Diffie and Martin Hellman Invited paper, 1976
http://securespeech.cs.cmu.edu/reports/DiffieHellman.pdff

[2] "A Mathematical Theory of Communication" by Shannon.C.E Bell System Technical Journal, 1948
http://cm.bell-labs.com/cm/ms/what/shannonday/shannon1948.pdf

[3] "The Codebreakers: The story of secret writing" byD. Kahn, Macmillan Publishing Company, 1967

[4] "Handbook of Applied Cryptography" by A. Menezes, P. van Oorschot, and S. Vanstone, CRC Press, 1996,
http://www.cacr.math.uwaterloo.ca/hac

[5] "Applied Cryptography: Protocols, Algorithms, and Source Code in C " by B. Schneier, Wiley, 1996

[6] "Introduction to Modern Cryptography" by Mihir Bellare and Phillip Rogaway,california , 2005

[7] "Technical Cryptography and cryptanalysis" by katos V. and Stefanidis G. ,ZYGOS, 2003

[8] "Modern Cryptography - An enjoyable journey through the paths of" by Nastou P., Spirakis P. and Stamatiou K. ,Ellinika Grammata, 2003

[9] "Safety and security of computer systems" by Dr.Zorkadis V. ,Aigian University

[10] "Complexity and Cryptography - An Introduction " by John Tablot and Dominic , University Press Cambridge Press, 2006,
http://www. Cambridge.org/978052185239

[11] "Applied Cryptanalysis:Breaking chipers in the real world " by Mark Stamp, Richard M. Iow, John Wiley and sons Inc publications, 2007

[12] "Information Security " by A.Souris, D. Patsos, N. Grigoriadis . New Teqhnology, 2004

[13] http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

[14] http://www.wikipedia.gr

[15] http://www.itl.nist.gov/fipspubs/fip46-2.htm

[16] http://www.contrib.andrew.cmu.edu/ shadow/kerberos.html general

[17] http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[18] http://dspace.lib.uom.gr

[19] http://users.uom.gr/ steph/material/crypto/

[20] http://www.rsa.com/rsalabs/node.asp?id=2184

[21] http://www.ermis.gov.gr/portal/page/portal/ermis /items/pdfs/pkiguidesw.pdf