Α.Τ.Ε.Ι. Καλαμάτας

Παράρτημα Σπάρτης

Τμήμα Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών

Κρυπτογραφία και το κρυπτοσύστημα Rabin

Παπαδόπουλος Παύλος

Πτυχιακή Εργασία

ΑΜ: 2006026

Κρυπτογραφία και το κρυπτοσύστημα **Rabin**

Επιβλέπων:

Επίκουρος Καθηγητής Καραγιώργος Γρηγόρης
Τμήμα Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών
Α.Τ.Ε.Ι. Καλαμάτας - Παράρτημα Σπάρτης

Ευχαριστίες

Αρχικά, θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα μου και Επίκουρο Καθηγητή του τμήματος κ. Καραγιώργο Γρηγόρη για την καθοδήγηση και τη βοήθεια του καθ΄ όλη τη διάρκεια υλοποίησης της πτυχιακής μου εργασίας. Επίσης, θα ήθελα να ευχαριστήσω τους καθηγητές του τμήματος που μου μετέδωσαν με τον καλύτερο δυνατό τρόπο τις απαραίτητες γνώσεις. Τέλος, ευχαριστώ την οικογένεια μου για τη στήριξη που μου έδωσαν σε όλα τα στάδια της ζωής μου.

Παπαδόπουλος Παύλος
Οκτώβριος 2012

Περίληψη

Η παρούσα Πτυχιακή μελετά την Κρυπτογραφία και ειδικότερα το κρυπτοσύστημα που υλοποιεί τον αλγόριθμο του Rabin. Γίνεται συνοπτική παρουσίαση βασικών σημείων των θεωρητικών βάσεων της Κρυπτογραφίας, ιστορική αναδρομή, παρουσίαση των βασικών ταξινομήσεων των κρυπταλγορίθμων αλλά και επιγραμματική αναφορά των εφαρμογών της.

Ακολουθεί αναλυτική παρουσίαση του αλγορίθμου RSA, καθώς και στη συνέχεια του Rabin που αποτελεί βελτίωση του RSA. Επιχειρείται μια σύγκριση αυτών των δυο αλγορίθμων.

Τέλος, γίνεται υλοποίηση του κρυπτοσυστήματος Rabin για αριθμητική είσοδο, καθώς και της διαδικασίας αποκρυπτογράφησης, γραμμένες σε γλώσσα *C*.

Abstract

The on hand Thesis studies Cryptography, especially the Rabin algorithm Cryptosystem. Basic theoretical foundations of Cryptography are presented. as long as the history of Cryptography, cryptoalgorithm sorting, reference of basic practical applications.

A detailed presentanion of the RSA and Rabin (which is an improvement compared with RSA) algorithms follow. We focus on compairing these two algorithms.

Finally, we implement the Rabin cryptosystem (arithmetic input - plaintext) along with the decryption proccess, all in C programming language.

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Κεφάλαιο 1

Εισαγωγή

Η λέξη κρυπτογραφία προέρχεται από τα συνθετικά «κρυπτός» + «γράφω» και είναι ένας επιστημονικός κλάδος που ασχολείται με τη μελέτη, την ανάπτυξη και τη χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων.

Η κρυπτογραφία είναι ένας κλάδος της επιστήμης της κρυπτολογίας, η οποία ασχολείται με τη μελέτη της ασφαλούς επικοινωνίας. Ο κύριος στόχος της είναι να παρέχει μηχανισμούς για 2 ή περισσότερα μέλη να επικοινωνήσουν χωρίς κάποιος άλλος να είναι ικανός να διαβάζει την πληροφορία εκτός από τα μέλη. Η λέξη κρυπτολογία αποτελείται από την ελληνική λέξη «κρυπτός» και τη λέξη «λόγος» και χωρίζεται σε δύο κλάδους: Την Κρυπτογραφία και την Κρυπτανάλυση με παρεμφερή κλάδο την Στεγανογραφία και αντίστοιχα την Στεγανοανάλυση.

Ιστορικά η κρυπτογραφία χρησιμοποιήθηκε για την κρυπτογράφηση μηνυμάτων δηλαδή μετατροπή της πληροφορίας από μια κανονική κατανοητή μορφή σε έναν γρίφο, που χωρίς τη γνώση του κρυφού μετασχηματισμού θα παρέμενε ακατανόητος. Κύριο χαρακτηριστικό των παλαιότερων μορφών κρυπτογράφησης ήταν ότι η επεξεργασία γινόταν πάνω στη γλωσσική δομή. Στις νεότερες μορφές η κρυπτογραφία κάνει χρήση του αριθμητικού ισοδύναμου, η έμφαση έχει μεταφερθεί σε διάφορα πεδία των μαθηματικών, όπως διακριτά μαθηματικά, θεωρία αριθμών, θεωρία πληροφορίας, υπολογιστική πολυπλοκότητα, στατιστική και συνδυαστική ανάλυση.

Η κρυπτογραφία παρέχει τέσσερις βασικές λειτουργίες (Αντικειμενικοί σκοποί):

- Εμπιστευτικότητα: Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.

- Ακεραιότητα: Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιο-

δοτημένα μέλη και δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης.

- Μη απάρνηση: Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.
- Πιστοποίηση: Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητές τους καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητές τους δεν είναι πλαστές.

1.1 Ορολογία

Κρυπτογράφηση (encryption) ονομάζεται η διαδικασία μετασχηματισμού ενός μηνύματος σε μία ακατανόητη μορφή με τη χρήση κάποιου κρυπτογραφικού αλγορίθμου ούτως ώστε να μην μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη. Η αντίστροφη διαδικασία όπου από το κρυπτογραφημένο κείμενο παράγεται το αρχικό μήνυμα ονομάζεται αποκρυπτογράφηση (decryption).

Κρυπτογραφικός αλγόριθμος (cipher) είναι η μέθοδος μετασχηματισμού δεδομένων σε μία μορφή που να μην επιτρέπει την αποκάλυψη των περιεχομένων τους από μη εξουσιοδοτημένα μέρη. Κατά κανόνα ο κρυπτογραφικός αλγόριθμος είναι μία πολύπλοκη μαθηματική συνάρτηση.

Αρχικό κείμενο (plaintext) είναι το μήνυμα το οποίο αποτελεί την είσοδο σε μία διεργασία κρυπτογράφησης.

Κλειδί (key) είναι ένας αριθμός αρκετών bit που χρησιμοποιείται ως είσοδος στη συνάρτηση κρυπτογράφησης.

Κρυπτογραφημένο κείμενο (ciphertext) είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγόριθμου πάνω στο αρχικό κείμενο.

Κρυπτανάλυση (cryptanalysis) είναι μία επιστήμη που ασχολείται με το «σπάσιμο» κάποιας κρυπτογραφικής τεχνικής ούτως ώστε χωρίς να είναι γνωστό το κλειδί της κρυπτογράφησης, το αρχικό κείμενο να μπορεί να αποκωδικοποιηθεί.

Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγόριθμου κρυπτογράφησης (cipher) και ενός κλειδιού κρυπτογράφησης (key). Συνήθως ο αλγόριθμος κρυπτογράφησης είναι γνωστός, οπότε η εμπιστευτικότητα του κρυπτογραφημένου μηνύματος που μεταδίδεται βασίζεται ως επί το πλείστον στη μυστικότητα του κλειδιού κρυπτογράφησης. Το μέγεθος

του κλειδιού κρυπτογράφησης μετριέται σε αριθμό bits. Γενικά ισχύει ο εξής κανόνας: όσο μεγαλύτερο είναι το κλειδί κρυπτογράφησης, τόσο δυσκολότερα μπορεί να αποκρυπτογραφηθεί το κρυπτογραφημένο μήνυμα από επίδοξους εισβολείς. Διαφορετικοί αλγόριθμοι κρυπτογράφησης απαιτούν διαφορετικά μήκη κλειδιών για να πετύχουν το ίδιο επίπεδο ανθεκτικότητας κρυπτογράφησης.

1.2 Βασικές Έννοιες

Ο αντικειμενικός στόχος της κρυπτογραφίας είναι να δώσει τη δυνατότητα σε δύο πρόσωπα, έστω την Αλίκη και τον Μπόμπ (τηρούμε την παράδοση των Alice και Bob[1]), να επικοινωνήσουν μέσα από ένα μη ασφαλές κανάλι με τέτοιο τρόπο ώστε ένα τρίτο πρόσωπο, μη εξουσιοδοτημένο (ένας αντίπαλος), να μην μπορεί να παρεμβληθεί στην επικοινωνία ή να κατανοήσει το περιεχόμενο των μηνυμάτων.

Ένα κρυπτοσύστημα (σύνολο διαδικασιών κρυπτογράφησης - αποκρυπτογράφησης) αποτελείται από μία πεντάδα (P,C,k,E,D):

- Το P είναι ο χώρος όλων των δυνατών μηνυμάτων ή αλλιώς ανοικτών κειμένων
- Το C είναι ο χώρος όλων των δυνατών κρυπτογραφημένων μηνυμάτων ή αλλιώς κρυπτοκειμένων
- Το k είναι ο χώρος όλων των δυνατών κλειδιών ή αλλιώς κλειδοχώρος
- Η E είναι ο κρυπτογραφικός μετασχηματισμός ή κρυπτογραφική συνάρτηση
- Η D είναι η αντίστροφη συνάρτηση ή μετασχηματισμός αποκρυπτογράφησης

[1]Η Alice και ο Bob είναι συνηθισμένα ψευδώνυμα/χαρακτήρες στην επιστήμη της κρυπτογραφίας και της φυσικής. Τα ονόματα αυτά χρησιμοποιούνται για ευκολία, σε παραδείγματα της μορφής «Το πρόσωπο Α θέλει να στείλει το μήνυμα στο πρόσωπο Β», και ιδιαίτερα σε πολύπλοκα συστήματα τα οποία περιλαμβάνουν πολλά βήματα. Η επιλογή των ονομάτων ακολουθεί την συνέχεια της αγγλικής αλφάβητου (πρώτο γράμμα το Α: ο χαρακτήρας Alice, δεύτερο γράμμα το Β: ο χαρακτήρας Bob). Η επανειλημμένη χρήση αυτών των ονομάτων βοηθάει στην καλύτερη κατανόηση των τεχνικών θεμάτων.

Στην κρυπτογραφία και στην ασφάλεια υπολογιστών, υπάρχουν πολλά ονόματα τα οποία χρησιμοποιούνται για την παρουσίαση των διάφορων πρωτοκόλλων. Τα ονόματα χρησιμοποιούνται για ευκολία, αρκετές φορές είναι ενδεικτικά και χιουμοριστικά για το κάθε παράδειγμα. Σε πολλές από τις υλοποιήσεις των πρωτοκόλλων η αναφορές στην Alice και τον Bob δεν αναφέρονται σε ανθρώπινες ενέργειες αλλά σε διεργασίες του πρωτοκόλλου (π.χ. ένα πρόγραμμα που τρέχει μια ενέργεια).

Η συνάρτηση κρυπτογράφησης E δέχεται δύο παραμέτρους, μέσα από τον χώρο P και τον χώρο k και παράγει μία ακολουθία που ανήκει στον χώρο C. Η συνάρτηση αποκρυπτογράφησης D δέχεται δυο παραμέτρους, τον χώρο C και τον χώρο k και παράγει μια ακολουθία που ανήκει στον χώρο P.

Το Σύστημα του Σχήματος λειτουργεί με τον ακόλουθο τρόπο :

1. Ο αποστολέας επιλέγει ένα κλειδί μήκους ν από τον χώρο κλειδιών με τυχαίο τρόπο, όπου τα ν στοιχεία του k είναι στοιχεία από ένα πεπερασμένο αλφάβητο.

2. Αποστέλλει το κλειδί στον παραλήπτη μέσα από ένα ασφαλές κανάλι.

3. Ο αποστολέας δημιουργεί ένα μήνυμα από τον χώρο μηνυμάτων.

4. Η συνάρτηση κρυπτογράφησης παίρνει τις δυο εισόδους (κλειδί και μήνυμα) και παράγει μια κρυπτοακολουθία συμβόλων (έναν γρίφο) και η ακολουθία αυτή αποστέλλεται διαμέσου ενός μη ασφαλούς καναλιού.

5. Η συνάρτηση αποκρυπτογράφησης παίρνει ως όρισμα τις δύο τιμές (κλειδί και γρίφο) και παράγει την ισοδύναμη ακολουθία μηνύματος.

Ο αντίπαλος παρακολουθεί την επικοινωνία. ενημερώνεται για την κρυπτοακολουθία αλλά δεν έχει γνώση για την κλείδα που χρησιμοποιήθηκε και δεν μπορεί να αναδημιουργήσει το μήνυμα. Αν ο αντίπαλος επιλέξει να παρακολουθεί όλα τα μηνύματα θα προσανατολιστεί στην εξεύρεση του κλειδιού. Αν ο αντίπαλος ενδιαφέρεται μόνο για το υπάρχον μήνυμα θα παράγει μια εκτίμηση για την πληροφορία του μηνύματος.

1.3 Εφαρμογές κρυπτογραφίας

Η εξέλιξη της χρησιμοποίησης της κρυπτογραφίας ολοένα αυξάνεται καθιστώντας πλέον αξιόπιστη τη μεταφορά της πληροφορίας για διάφορους λειτουργικούς σκοπούς:

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 (Hipperlan, bluetooth, 802.11x)
18. Συστήματα ιατρικών δεδομένων και άλλων βάσεων δεδομένων
19. Τηλεσυνδιάσκεψη - Τηλεφωνία μέσω διαδικτύου (VOIP)

Κεφάλαιο 2

Βασική Θεωρία

2.1 Κρυπτογράφηση

Τα κρυπτογραφικά συστήματα ταξινομούνται, γενικά, με βάση τρία ανεξάρτητα κριτήρια

- *Τον τύπο των διαδικασιών που χρησιμοποιούνται για το μετασχηματισμό του αρχικού κειμένου σε ένα κρυπτογράφημα.* Το σύνολο των αλγορίθμων κρυπτογράφησης στηρίζεται σε δύο γενικές αρχές: στην αντικατάσταση (substitution) σύμφωνα με την οποία κάθε στοιχείο του αρχικού κειμένου, είτε είναι δυαδικό ψηφίο, είτε χαρακτήρας, είτε ομάδα δυαδικών ψηφίων ή χαρακτήρων, αντικαθίσταται από άλλο στοιχείο και στη μετάθεση (transposition) στην οποία τα στοιχεία του αρχικού κειμένου αναδιατάσσονται. Βασική προϋπόθεση αποτελεί η μη απώλεια οποιασδήποτε πληροφορίας, ώστε όλες οι διαδικασίες να είναι αντιστρέψιμες. Τα περισσότερα συστήματα, που είναι γνωστά ως συστήματα παραγωγής (product systems), περιλαμβάνουν πληθώρα σταδίων αντικαταστάσεων και μεταθέσεων.

- *Τον αριθμό των κλειδιών που χρησιμοποιούνται.* Εάν ο πομπός και ο δέκτης χρησιμοποιούν το ίδιο κλειδί, τότε το σύστημα αναφέρεται ως συμμετρικό ή μοναδικού κλειδιού ή μυστικού κλειδιού ή συμβατικής κρυπτογραφίας. Εάν, όμως, ο πομπός και ο δέκτης χρησιμοποιούν διαφορετικά κλειδιά, τότε το σύστημα αναφέρεται ως ασύμμετρο, ή σύστημα ζεύγους κλειδιών, ή κρυπτογραφίας δημοσίου κλειδιού.

- *Τον τρόπο με τον οποίο επεξεργάζεται το αρχικό κείμενο.* Ένας κωδικοποιητής τμημάτων (block cipher) επεξεργάζεται την είσοδο ενός τμήματος στοιχείων κάθε φορά, παράγοντας ένα τμήμα εξόδου για κάθε συγκεκριμένο τμήμα εισόδου. Αντίθετα, ένας κωδικοποιητής ροής (stream

cipher) επεξεργάζεται κατά συνεχή τρόπο τα στοιχεία εισόδου και κάθε φορά παράγεται ως έξοδος ένα στοιχείο, με τη σειρά που καταφθάνουν τα δεδομένα.

2.2 Κρυπτανάλυση

Η κρυπτανάλυση είναι η μελέτη για την επινόηση μεθόδων που εξασφαλίζουν την κατανόηση του νοήματος της κρυπτογραφημένης πληροφορίας, έχοντας ως άγνωστες ποσότητες τον κρυφό μετασχηματισμό, το κλειδί, με βάση το οποίο αυτός πραγματοποιήθηκε και το κρυπτογραφημένο μήνυμα. Βασικός στόχος της είναι, ανάλογα με τις απαιτήσεις του αναλυτή κρυπτοσυστημάτων ή αλλιώς κρυπταναλυτή, να βρει το κλειδί, το μήνυμα ή ένα ισοδύναμο αλγόριθμο που θα τον βοηθά να αναγνώσει το (κρυφό) μήνυμα.

Ένας κρυπταλγόριθμος λέγεται ότι έχει «σπάσει», αν βρεθεί μια μέθοδος (πιθανοκρατική ή ντετερμινιστική) που μπορεί να βρει το μήνυμα ή το κλειδί με πολυπλοκότητα μικρότερη από την πολυπλοκότητα της επίθεσης ωμής βίας (brutal force attack).

Στον Πίνακα 2.1 παρουσιάζονται συνοπτικά διάφοροι τύποι επιθέσεων κρυπτανάλυσης, οι οποίοι διαφοροποιούνται, μεταξύ άλλων, με βάση την ποσότητα και το είδος της πληροφορίας που είναι γνωστή στον κρυπταναλυτή. Το πρόβλημα της κρυπτανάλυσης παρουσιάζει σημαντικές δυσκολίες όταν είναι γνωστό στον επιτιθέμενο μόνον το κρυπτογράφημα. Σε μερικές περιπτώσεις δεν είναι γνωστός ούτε ο αλγόριθμος κρυπτογράφησης, αλλά στη γενική περίπτωση μπορεί να υποτεθεί ότι ο αντίπαλος γνωρίζει τον αλγόριθμο που χρησιμοποιείται.

Μια κλασική επίθεση υπό αυτές τις περιστάσεις αποτελεί η προσέγγιση της εξαντλητικής αναζήτησης κλειδιών (brute-force attack), όπου ο επιτιθέμενος δοκιμάζει διαδοχικά όλα τα στοιχεία από το πεδίο όλων των πιθανών κλειδιών. Εάν το μέγεθος του κλειδιού είναι μεγάλο, η επίθεση αυτού του είδους θεωρείται πρακτικά ατελέσφορη. Κατά συνέπεια, ένας επιτιθέμενος για να είναι αποτελεσματικός θα πρέπει να αξιοποιήσει ανάλυση του κρυπτογραφήματος εφαρμόζοντας διάφορες στατιστικές δοκιμές σε αυτό. Ο επιτιθέμενος για να χρησιμοποιήσει αυτή την προσέγγιση θα πρέπει να γνωρίζει τον τύπο του αρχικού κειμένου που χρησιμοποιείται, π.χ. ένα απλό κείμενο σε συγκεκριμένη γλώσσα, ένα εκτελέσιμο αρχείο σε περιβάλλον συγκεκριμένου λειτουργικού συστήματος, ένα αρχείο με πηγαίο κώδικα σε συγκεκριμένη γλώσσα προγραμματισμού κλπ.

Η άμυνα σε επίθεση κρυπτογραφήματος (ciphertext only attack) αποτελεί γενικά εύκολη υπόθεση, επειδή ο αντίπαλος διατηρεί μικρή ποσότητα πληροφοριών με την οποία μπορεί να ασχοληθεί. Παρόλα αυτά, σε πολλές περιπτώσεις ο κρυπταναλυτής μπορεί να διαθέτει και περισσότερες πληροφορίες. Ο κρυπταναλυτής μπορεί να έχει τη δυνατότητα να καταγράψει ένα ή περισσότερα μηνύματα

Τύπος Επίθεσης	Στοιχεία γνωστά στον κρυπταναλυτή
Επίθεση κρυπτογραφήματος (ciphertext - only attack)	Αλγόριθμος κρυπτογράφησης, Κρυπτογράφημα
Επίθεση γνωστού αρχικού κειμένου (known - plaintext attack)	Αλγόριθμος κρυπτογράφησης, Κρυπτογράφημα, Ένα ή περισσότερα ζεύγη (αρχικού κειμένου, κρυπτογραφήματος), παραγόμενα από το μυστικό κλειδί
Επίθεση επιλεγμένου αρχικού κειμένου (chosen - plaintext attack)	Αλγόριθμος κρυπτογράφησης, Κρυπτογράφημα, Αρχικό κείμενο επιλεγμένο από τον κρυπταναλυτή, σε συνδυασμό με το αντίστοιχο κρυπτογράφημα που παράγεται με μυστικό κλειδί
Επίθεση επιλεγμένου κρυπτογραφήματος (chosen - ciphertext attack)	Αλγόριθμος κρυπτογράφησης, Κρυπτογράφημα, Επιλεγμένο απ΄ τον κρυπταναλυτή κρυπτογράφημα, μαζί με το αντίστοιχο αποκρυπτογραφημένο αρχικό κείμενο, που παράχθηκε με το μυστικό κλειδί
Επίθεση επιλεγμένου κειμένου (chosen - text attack)	Αλγόριθμος κρυπτογράφησης, Κρυπτογράφημα, Επιλεγμένο από τον κρυπταναλυτή μήνυμα αρχικού κειμένου, μαζί με το αντίστοιχο κρυπτογράφημα, που παράχθηκε με το μυστικό κλειδί, Επιλεγμένο από τον κρυπταναλυτή κρυπτογράφημα, μαζί με το αντίστοιχο αποκρυπτογραφημένο αρχικό κείμενο, που παράχθηκε με το μυστικό κλειδί

Πίνακας 2.1: Τύποι επιθέσεων σε κρυπτογραφημένα μηνύματα

αρχικού κειμένου, καθώς επίσης και τα αντίστοιχα κρυπτογραφήματα. Σε άλλη περίπτωση, μπορεί να γνωρίζει ότι συγκεκριμένα πρότυπα αρχικού κειμένου θα εμφανιστούν σε ένα μήνυμα. Για παράδειγμα, ένα αρχείο σε μορφή postscript αρχίζει πάντοτε με το ίδιο πρότυπο, ή μπορεί να υπάρξει μία τυποποιημένη επικεφαλίδα ή ένα λογότυπο σε ένα ηλεκτρονικό μήνυμα μεταφοράς κεφαλαίων. Τα προαναφερόμενα παραδείγματα αποτελούν επιθέσεις γνωστών μηνυμάτων. Με αυτή τη γνώση ο αναλυτής μπορεί να είναι σε θέση να συμπεράνει το κλειδί, με βάση τον τρόπο που μετασχηματίστηκε το γνωστό αρχικό κείμενο.

Αντίστοιχη με την επίθεση γνωστών μηνυμάτων (known plaintext attack) είναι η επίθεση πιθανής - λέξης (probable-word attack). Εάν ο επιτιθέμενος ασχολείται με την κρυπτανάλυση κάποιου μηνύματος αγνώστου περιεχομένου μπορεί να μην κατανοεί επακριβώς το περιεχόμενο του μηνύματος. Παρόλα αυτά, εάν ο επιτιθέμενος αναζητά συγκεκριμένες πληροφορίες, τότε κάποια τμήματα του μηνύματος μπορούν να θεωρηθούν γνωστά. Για παράδειγμα, εάν διαβιβάζεται ολόκληρο λογιστικό αρχείο, ο επιτιθέμενος μπορεί να είναι σε θέση να γνωρίζει τη θέση κάποιων λέξεων-κλειδιών στην επικεφαλίδα του αρχείου. Άλλο παράδειγμα αποτελεί ο πηγαίος κώδικας ενός προγράμματος που αναπτύχθηκε από κάποια εταιρία και ο οποίος μπορεί να περιλαμβάνει δήλωση πνευματικών δικαιωμάτων σε κάποια συγκεκριμένη θέση.

Εάν ο κρυπταναλυτής μπορεί με κάποιο τρόπο να παραπλανήσει το πηγαίο σύστημα ώστε να παρεμβάλλει ένα μήνυμα που έχει επιλέξει ο ίδιος, τότε είναι πιθανή μία επίθεση επιλεγμένων μηνυμάτων. Γενικά, εάν ο κρυπταναλυτής είναι σε θέση να επιλέγει τα μηνύματα για κρυπτογράφηση τότε μπορεί σκόπιμα να επιλέγει πρότυπα που αναμένεται να τον υποβοηθήσουν στην αποκάλυψη της δομής του κλειδιού. Στον Πίνακα 2.1 εμφανίζονται και άλλοι δύο τύποι επίθεσης, η επίθεση επιλεγμένου κρυπτογραφήματος (chosen ciphertext attack) και η επίθεση επιλεγμένου κειμένου (chosen text attack), επιθέσεις οι οποίες δεν επιχειρούνται συχνά ως τεχνικές κρυπτανάλυσης, μπορούν όμως να αποτελέσουν δυνητικούς τρόπους επίθεσης.

Τύποι κρυπταναλυτικών επιθέσεων

2.2.1 Κρυπταναλυτικές επιθέσεις σε αλγορίθμους

Υπάρχουν έξι βασικές κρυπταναλυτικές επιθέσεις, κατηγοριοποιημένες ανάλογα με την ικανότητα του αντιπάλου (πόρους - υπολογιστική ισχύ) και το επίπεδο πρόσβασης που έχει ο επιτιθέμενος:

1. **Επίθεση βασισμένη στο κρυπτοκείμενο:** Ο κρυπταναλυτής έχει στην διάθεση του N κρυπτομηνύματα με δεδομένη τη γνώση του αλγορίθμου. Σκοπός είναι να ανακαλύψει τα μηνύματα που περικλείουν τα κρυπτοκείμενα ή να εξαγάγει το κλειδί που χρησιμοποιήθηκε.

2. **Επίθεση βασισμένη στην γνώση μηνυμάτων κρυπτοκειμένων:** Ο κρυπταναλυτής έχει στην διάθεση του μερικά ζευγάρια (μηνυμάτων, κρυπτοκειμένων). Ο στόχος είναι η εξαγωγή του κλειδιού ή ενός αλγορίθμου για την αποκρυπτογράφηση νέων μηνυμάτων (προσεγγιστικός αλγόριθμος) με το ίδιο κλειδί.

3. **Επίθεση βασισμένη στην επιλογή μηνυμάτων:** Ο κρυπταναλυτής έχει καταφέρει να αποκτήσει πρόσβαση στη επιλογή του μηνύματος που θα κρυπτογραφηθεί. Στόχος είναι η εξαγωγή του κλειδιού ή ενός προσεγγιστικού αλγορίθμου.

4. **Προσαρμοσμένη επίθεση, βασισμένη στην επιλογή μηνυμάτων:** Ο κρυπταναλυτής μπορεί να επιλέξει όχι μόνο μία συστάδα μηνυμάτων αλλά μπορεί να επιλέξει ποιο επόμενο μήνυμα θα κρυπτογραφηθεί(Κατάλληλη επιλογή ζευγαριών προσδίδει περισσότερη πιθανότητα για την τιμή του κλειδιού). Στόχος είναι η εξαγωγή του κλειδιού ή ενός προσεγγιστικού αλγορίθμου.

5. **Επίθεση βασισμένη στην επιλογή κρυπτοκειμένων:** Ο κρυπταναλυτής μπορεί να επιλέξει κρυπτοκείμενα για αποκρυπτογράφηση (μελετά πώς συμπεριφέρεται ο αλγόριθμος στην αποκρυπτογράφηση) και έχει πρόσβαση στα αποκρυπτογραφημένα κείμενα.

6. **Προσαρμοσμένη επίθεση βασισμένη στην επιλογή μηνυμάτων - κλειδιών:** Ο κρυπταναλυτής επιλέγει μια σχέση μεταξύ του άγνωστου κλειδιού και του δικό του κλειδιού και βάση των συμπερασμάτων που βγάζει από την ανάλυση (Είσοδος/έξοδος) στο σύστημα - στόχο και στο δικό του αντίγραφο (Κρυπταλγόριθμος) προσεγγίζει, μετά από κάποιες δοκιμές, το σωστό κλειδί.

2.2.2 Επιθέσεις στο κανάλι επικοινωνίας

Υπάρχουν τέσσερεις βασικές απειλές στο κανάλι επικοινωνίας, κατηγοριοποιημένες με κριτήριο την ενεργή ή παθητική συμπεριφορά του αντιπάλου.

1. **Διακοπή γραμμής:** Ο αντίπαλος έχει διακόψει την ροή της πληροφορίας από τον αποστολέα στον παραλήπτη (ενεργή συμπεριφορά)

2. **Υποκλοπή πληροφορίας από το κανάλι:** Ο αντίπαλος αντιγράφει τις πληροφορίες που διαβιβάζονται στο κανάλι επικοινωνίας (παθητική συμπεριφορά - μη ανιχνεύσιμη)

3. **Τροποποίηση πληροφορίας στο κανάλι (Man - in - the - middle επίθεση):** Ο αντίπαλος τροποποιεί τις πληροφορίες που διαβιβάζονται στο κανάλι με τέτοιο τρόπο, ώστε να αλλάξει το περιεχόμενο ή να αναγεννά δική του πληροφορία. (ενεργή συμπεριφορά)

4. **Πλαστογράφηση πηγής:** Ο αντίπαλος προσποιείται ότι είναι ένα από τα μέλη που έχουν πρόσβαση στο κανάλι.

2.3 Ταξινόμηση Μοντέλων αξιολόγησης ασφάλειας

Υπάρχουν 4 βασικά μοντέλα για την αξιολόγηση των αλγορίθμων:

1. Ασφάλεια άνευ όρων
2. Υπολογιστική ασφάλεια
3. Θεωρία πολυπλοκότητας
4. Αποδείξιμη ασφάλεια

Ασφάλεια άνευ όρων (Τέλεια Ασφάλεια)

Αυτή η μέτρηση εστιάζεται στην διάκριση αν ένα κρυπτοσύστημα έχει ασφάλεια άνευ όρων. Η βασική υπόθεση είναι ότι όσο κρυπτοκείμενο και αν κατέχει ο αντίπαλος, δεν υπάρχει αρκετή πληροφορία για να ανακτήσει το ανοικτό κείμενο (μοναδική λύση), όση υπολογιστική ισχύ (άπειρη) και αν έχει στην διάθεση του. Χαρακτηριστικό παράδειγμα το σημειωματάριο μίας χρήσης (one time pad).

Υπολογιστική ασφάλεια (Πρακτική Ασφάλεια)

Αυτή η μέτρηση εστιάζεται στην υπολογιστική προσπάθεια «παράγοντας εργασίας», που χρειάζεται για να διασπαστεί ένα κρυπτοσύστημα. Στόχος των συγχρόνων συστημάτων είναι να εμφανίζουν μεγάλο παράγοντα δυσκολίας ώστε να μην είναι χρονικά δυνατό να διασπαστούν με τα διαθέσιμα (ή και τα μελλοντικά) μέσα.

Ασφάλεια - θεωρία πολυπλοκότητας

Αυτή η μέτρηση εστιάζει στην ταξινόμηση της υπολογιστικής ικανότητας του αντιπάλου υπολογιστικών προβλημάτων ανάλογα με τους πόρους που απαιτούνται για την επίλυση τους. Οι πόροι αναφέρονται σε:

- Το μέγεθος δεδομένων που χρειάζονται σαν είσοδος στην επίθεση
- Τον υπολογιστικό χρόνο που χρειάζεται για να εκτελεστεί η επίθεση
- Το μέγεθος του χώρου αποθήκευσης που χρειάζεται για την επίθεση
- Το πλήθος των επεξεργαστών

Αποδείξιμη ασφάλεια

Αυτή η μέτρηση εστιάζεται στην απόδειξη ισοδυναμίας του μαθηματικού μοντέλου του κρυπτοσυστήματος με κάποιο πολύ γνωστό δύσκολο στην επίλυση του πρόβλημα (θεωρίας αριθμών). Χαρακτηριστικό παράδειγμα η παραγοντοποίηση μεγάλων ακεραίων, που έχει αποδειχθεί εξίσου δύσκολο με το πρόβλημα της κρυπτανάλυσης του αλγορίθμου του **Rabin**, τον οποίο εξετάζει η παρούσα εργασία.

2.4 Βασικά πρωτόκολλα κρυπτογραφίας

2.4.1 Εισαγωγή

Ένα κρυπτογραφικό πρωτόκολλο είναι ένα πρωτόκολλο το οποίο υλοποιείται με κρυπτογραφικούς μηχανισμούς.

Ο χρήστης ενός συστήματος αντιλαμβάνεται την ασφάλεια με τη μορφή των κρυπτογραφικών υπηρεσιών (εμπιστευτικότητα, αυθεντικοποίηση, ακεραιότητα). Οι κρυπτογραφικές υπηρεσίες προσφέρονται με την υλοποίηση των κρυπτογραφικών πράξεων. Οι κρυπτογραφικές πράξεις όμως θα πρέπει να συνδυασθούν και να εκτελεσθούν με συγκεκριμένο τρόπο, προκειμένου να προσφέρουν τις επιθυμητές κρυπτογραφικές υπηρεσίες. Η περιγραφή με την οποία θα δράσουν οι κρυπτογραφικές πράξεις βρίσκεται στο κρυπτογραφικό πρωτόκολλο. Επομένως, ένα κρυπτογραφικό πρωτόκολλο χαρακτηρίζεται από την αυστηρή περιγραφή του τρόπου λειτουργίας και δράσης των κρυπτογραφικών πράξεων, διότι μια μικρή αλλαγή στη λειτουργία μιας κρυπτογραφικής πράξης μπορεί να έχει τεράστιες επιπτώσεις στην ασφάλεια.

Πολλές φορές ένα κρυπτογραφικό πρωτόκολλο παίρνει το όνομα της υπηρεσίας που παρέχει. Έτσι μπορούμε να έχουμε πρωτόκολλα αυθεντικοποίησης, ελέγχου ακεραιότητας, κοκ.

Αποτυχία πρωτοκόλλου (protocol failure) ονομάζεται η κατάσταση όπου ένας αντίπαλος καταφέρνει, με κατάλληλο χειρισμό των μηχανισμών ενός πρωτοκόλλου, να καταστήσει το πρωτόκολλο αδύναμο στο να προσφέρει την κρυπτογραφική υπηρεσία.

Ένα πρωτόκολλο έχει τα ακόλουθα χαρακτηριστικά (Pfleeger, 1989)[6]:

- Είναι καθορισμένο εκ των προτέρων. Δηλαδή ο σχεδιασμός ενός πρωτοκόλλου έχει ολοκληρωθεί προτού χρησιμοποιηθεί το πρωτόκολλο.
- Αμοιβαία συμφωνία. Όλα τα μέλη συμφωνούν να εκτελέσουν τα βήματα του πρωτοκόλλου με τη σειρά που υποδεικνύει το πρωτόκολλο.
- Σαφήνεια. Η εκτέλεση όλων των βημάτων του πρωτοκόλλου θα πρέπει να είναι σαφής, έτσι ώστε κανένα από τα μέλη να μην παρερμηνεύσει τα βήματα που του αναλογούν.
- Πληρότητα. Για οποιαδήποτε κατάσταση που μπορεί να βρεθεί οποιοδήποτε μέλος, θα πρέπει να υπάρχουν προκαθορισμένες ενέργειες.

2.4.2 Ανάλυση των κρυπτογραφικών πρωτοκόλλων

Η ανάλυση των κρυπτογραφικών πρωτοκόλλων έχει στόχο τη διαπίστωση ότι το πρωτόκολλο έχει τη δυνατότητα να προσφέρει την υπηρεσία για την οποία είναι σχεδιασμένο να προσφέρει. Στη βιβλιογραφία υπάρχουν διάφορες τεχνικές ανάλυσης των κρυπτογραφικών πρωτοκόλλων, αλλά φυσικά η ανάλυση δεν περιορίζεται στις τεχνικές αυτές. Γενικά οι τεχνικές ανάλυσης συσχετίζουν το πρωτόκολλο με τους πόρους που απαιτείται να έχει ο αντίπαλος, προκειμένου να καταστήσει το πρωτόκολλο αδύναμο να προσφέρει την επιθυμητή υπηρεσία. Οι κυριότερες τεχνικές ανάλυσης πρωτοκόλλων είναι οι εξής (προσαρμογή από Menezes et al.):

- **ανάλυση με βάση τη θεωρία της πληροφορίας.** Η ανάλυση επικεντρώνεται στην πληροφορία που περιέχουν τα μηνύματα που ανταλλάσσουν τα μέλη που εκτελούν το πρωτόκολλο, τόσο μεταξύ τους, όσο και σε τρίτους. Ο αντίπαλος θεωρείται ότι έχει άπειρη υπολογιστική ισχύ, οπότε ένα πρωτόκολλο το οποίο αποδεικνύεται ασφαλές από πλευράς θεωρίας της πληροφορίας, δεχόμαστε ότι είναι ασφαλές άνευ όρων (unconditionally secure).
- **ανάλυση με βάση τη θεωρία πολυπλοκότητας.** Σύμφωνα με την ανάλυση αυτή, ο αντίπαλος αναλύεται ως προς την υπολογιστική ισχύ και το χρόνο που απαιτείται για να καταρρίψει ένα πρωτόκολλο. Έτσι ένα πρωτόκολλο θεωρείται υπολογιστικά ασφαλές, αν ο αντίπαλος δεν μπορεί να αντεπεξέλθει στους πόρους που απαιτούνται (ισχύς, χρόνος) για να καταρρίψει το πρωτόκολλο.

- **αναγωγή σε «δύσκολα» προβλήματα.** Η ανάλυση αυτή σχετίζεται με την αναγωγή ασφάλειας του πρωτοκόλλου σε ισοδύναμα δύσκολα προβλήματα. Με την τεχνική ανάλυσης με αναγωγή, ένα πρωτόκολλο θεωρείται αποδείξιμα ασφαλές (provably secure).

- **τυπική ανάλυση.** Η τυπική ανάλυση των πρωτοκόλλων περιλαμβάνει εργαλεία ανάλυσης τα οποία είναι κατασκευασμένα ειδικά για τη συγκεκριμένη εργασία. Τα εργαλεία ανάλυσης αποτελούνται από μια γλώσσα ανάλυσης των πρωτοκόλλων και από ένα λογικό μοντέλο. Το πρωτόκολλο μοντελοποιείται και περιγράφεται με τη γλώσσα ανάλυσης και στη συνέχεια εξετάζονται με μια σειρά λογικών κανόνων αν το πρωτόκολλο δύναται να προσφέρει την επιθυμητή υπηρεσία και σε ποιο βαθμό. Ένα από τα πιο επιτυχημένα λογικά μοντέλα ανάλυσης είναι το μοντέλο των Burrows, Abadi και Needham, το οποίο ονομάζεται λογική BAN, από τα αρχικά των δημιουργών του. Η λογική BAN αναλύει το πρωτόκολλο με βάση την πίστη και τη γνώση των μελών για κάποια κατάσταση.

2.4.3 Κατηγορίες πρωτοκόλλων

Τα πρωτόκολλα χωρίζονται σε τρεις κατηγορίες με βάση την ικανότητα προσφοράς της υπηρεσίας, σε σχέση με την απαίτηση συμμετοχής τρίτης οντότητας. Οι κατηγορίες αυτές είναι ονομαστικά:

- Αυτοεπιβαλλόμενα πρωτόκολλα (self enforcing protocols).
- Πρωτόκολλα με δικαστή (adjudicated protocols).
- Πρωτόκολλα με διαιτητή (arbitrated protocols).

Από τις τρεις κατηγορίες πρωτοκόλλων, τα αυτοεπιβαλλόμενα πρωτόκολλα δεν απαιτούν τρίτη οντότητα, σε αντίθεση με τα άλλα δύο τα οποία βασίζονται στη συμμετοχή μιας τρίτης οντότητας.

Τα αυτοεπιβαλλόμενα πρωτόκολλα είναι τα πιο επιθυμητά από τα τρία, καθότι εκτελούνται μεταξύ των επικοινωνούντων μελών και δε βασίζονται στην εμπιστοσύνη τρίτων, χαρακτηρίζονται δε από μεγάλη ταχύτητα εκτέλεσης. Τα αυτοεπιβαλλόμενα πρωτόκολλα έχουν έμφυτους μηχανισμούς οι οποίοι εγγυώνται αμεροληψία, δίνοντας τη δυνατότητα στα επικοινωνούντα μέλη να ανιχνεύσουν αν κάποιο από αυτά επιχειρήσει απάτη.

Σε πολλές περιπτώσεις τα αυτοεπιβαλλόμενα πρωτόκολλα δεν μπορούν να εφαρμοστούν στην πράξη και έτσι απαιτείται τρίτη οντότητα προκειμένου να λυθεί η διαμάχη. Τα πρωτόκολλα με δικαστή έχουν το χαρακτηριστικό να παρέχουν αρκετά στοιχεία ώστε μια τρίτη οντότητα που παίζει το ρόλο του δικαστή να μπορεί να αποφασίσει πιο από τα μέλη διέπραξε την απάτη. Στα πρωτόκολλα

με δικαστή δε συμμετέχει η τρίτη οντότητα κατά την εκτέλεσή τους. Η τρίτη οντότητα καλείται να συμμετάσχει μόνον όταν υπάρξει διαφωνία μεταξύ των επικοινωνούντων μελών. Τα πρωτόκολλα με δικαστή θα πρέπει να έχουν τη δυνατότητα τα στοιχεία τα οποία παρουσιάζονται στο δικαστή να μην μπορούν να τροποποιηθούν χωρίς αυτό να γίνει αντιληπτό. Τα στοιχεία θα πρέπει να δίνουν τη δυνατότητα στο δικαστή να διακρίνει όχι μόνον αν διαπράχθηκε απάτη, αλλά και να αναγνωρίσει το μέλος το οποίο διέπραξε την απάτη.

Τέλος, τα πρωτόκολλα με διαιτητή είναι αυτά στα οποία η τρίτη οντότητα συμμετέχει κατά τη διάρκεια εκτέλεσης του πρωτοκόλλου. Η συμμετοχή τρίτου κατά τη διάρκεια εκτέλεσης του πρωτοκόλλου έχει σαν αποτέλεσμα τη χαμηλή ταχύτητα εκτέλεσης του πρωτοκόλλου, που είναι και το βασικό μειονέκτημα της κατηγορίας αυτής. Σε δίκτυα υπολογιστών όπου χρησιμοποιείται κάποιος server ως διαιτητής, μπορεί να υπάρξει αισθητή μείωση στην απόδοση, αν η υπηρεσία του διαιτητή χρησιμοποιείται με μεγάλη συχνότητα.

2.5 Είδη Κρυπτοσυστημάτων

Τα κρυπτοσυστήματα χωρίζονται σε 2 μεγάλες κατηγορίες τα Κλασσικά Κρυπτοσυστήματα και τα Μοντέρνα Κρυπτοσυστήματα (Συμμετρικά κρυπτοσυστήματα και Ασύμμετρα κρυπτοσυστήματα).

2.5.1 Συμμετρικά Κρυπτοσυστήματα

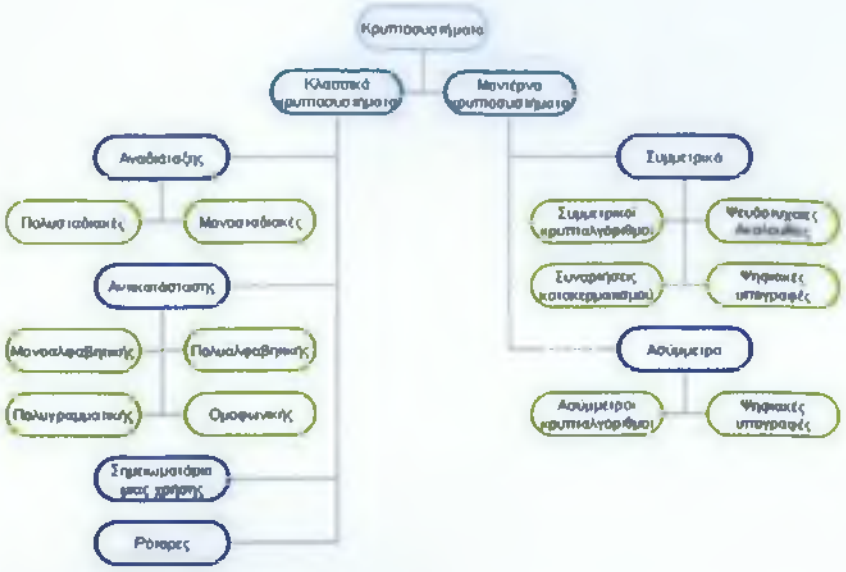
Συμμετρικό κρυπτοσύστημα είναι το σύστημα εκείνο το οποίο χρησιμοποιεί κατά τη διαδικασία της κρυπτογράφησης - αποκρυπτογράφησης ένα κοινό κλειδί. Η ασφάλεια αυτών των αλγορίθμων βασίζεται στη μυστικότητα του κλειδιού. Τα συμμετρικά κρυπτοσυστήματα προϋποθέτουν την ανταλλαγή του κλειδιού μέσα από ένα ασφαλές κανάλι επικοινωνίας ή μέσα από την φυσική παρουσία των προσώπων. Αυτό το χαρακτηριστικό καθιστά δύσκολη την επικοινωνία μεταξύ απομακρυσμένων ατόμων.

Τα στάδια της επικοινωνίας είναι τα ακόλουθα:

1. Ο Κώστας ή η Βασιλική αποφασίζει για ένα κλειδί το οποίο το επιλέγει τυχαία μέσα από τον κλειδοχώρο.

2. Η Βασιλική αποστέλλει το κλειδί στον Κώστα μέσα από ένα ασφαλές κανάλι.

3. Ο Κώστας δημιουργεί ένα μήνυμα όπου τα σύμβολα m ανήκουν στον χώρο των μηνυμάτων.



Σχήμα 2.1: Δενδρική Αναπαράσταση των βασικών κατηγοριών Κρυπτοσυστημάτων

4. Κρυπτογραφεί το μήνυμα με το κλειδί που έλαβε από τη Βασιλική και η παραγόμενη κρυπτοσυμβολοσειρά αποστέλεται.

5. Η Βασιλική λαμβάνει την κρυπτοσυμβολοσειρά και στη συνέχεια με το ίδιο κλειδί την αποκρυπτογραφεί και η έξοδος που παράγεται είναι το μήνυμα.

Λίστα Συμμετρικών Κρυπταλγορίθμων

Οι συμμετρικοί κρυπτογραφικοί αλγόριθμοι μπορούν να χωριστούν σε δύο διαφορετικές κατηγορίες με βάση τον τρόπο κρυπτογράφησης των μηνυμάτων:

- Δέσμης (Block Ciphers), οι οποίοι χωρίζουν το μήνυμα σε κομμάτια και κρυπτογραφούν κάθε ένα από τα κομμάτια αυτά χωριστά.

- Ροής (Stream Ciphers), οι οποίοι κρυπτογραφούν μία ροή μηνύματος (stream) χωρίς να τη διαχωρίζουν σε τμήματα.

Παραθέτουμε ορισμένα παραδείγματα κρυπταλγορίθμων:
Συμμετρικοί Κρυπταλγόριθμοι Τμήματος (Block Ciphers): Data Encryption Standard, 3-Way, Blowfish, CAST, CMEA, Triple-DES, DEAL FEAL, GOST, IDEA, LOKI, Lucifer. MacGuffin, Twofish MARS,

MISTY, MMB, NewDES, RC2, RC5, RC6, REDOC, Rijndael, Safer, Serpent, SQUARE, Skipjack, Tiny Encryption Algorithm

Συμμετρικοί Κρυπταλγόριθμοι ροής (Stream Ciphers): ORYX, RC4, SEAL

Συμμετρικοί Κρυπταλγόριθμοι Κατακερματισμού: MD2, MD4, MD5, RIPEMD, SHA1, Snefru, Tiger

2.5.2 Ασύμμετρα Κρυπτοσυστήματα

Το ασύμμετρο κρυπτοσύστημα ή κρυπτοσύστημα δημοσίου κλειδιού (Κρυπτογράφηση Δημόσιου Κλειδιού) δημιουργήθηκε για να καλύψει την αδυναμία μεταφοράς κλειδιών που παρουσίαζαν τα συμμετρικά συστήματα. Χαρακτηριστικό του είναι ότι έχει δυο είδη κλειδιών ένα ιδιωτικό και ένα δημόσιο. Το δημόσιο είναι διαθέσιμο σε όλους ενώ το ιδιωτικό είναι μυστικό. Η βασική σχέση μεταξύ τους είναι: ό,τι κρυπτογραφεί το ένα, μπορεί να το αποκρυπτογραφήσει μόνο το άλλο. Οι δυνατότητες της ασύμμετρης κρυπτογραφίας οδήγησαν στη δημιουργία των ψηφιακών υπογραφών και ακολούθως στην ανάπτυξη της Υποδομής Δημόσιου Κλειδιού (Public Key Infrastructure) και στα Ψηφιακά πιστοποιητικά.

Τα στάδια της επικοινωνίας είναι τα ακόλουθα:

1. Η γεννήτρια κλειδιών του Μένιου παράγει 2 ζεύγη κλειδιών
2. Η γεννήτρια κλειδιών της Ελένης παράγει 2 ζεύγη κλειδιών
3. Η Ελένη και ο Μένιος ανταλλάσσουν τα δημόσια ζεύγη
4. Ο Μένιος δημιουργεί ένα μήνυμα όπου τα σύμβολα m ανήκουν στον χώρο των μηνυμάτων.
5. Κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί της Ελένης και η παραγόμενη κρυπτοσυμβολοσειρά αποστέλλεται.
6. Η Ελένη λαμβάνει την κρυπτοσυμβολοσειρά και στη συνέχεια με το ιδιωτικό της κλειδί την αποκρυπτογραφεί και η έξοδος που παράγεται είναι το μήνυμα.

Λίστα Ασύμμετρων Κρυπταλγορίθμων

- RSA
- Ανταλλαγή κλειδιού Diffie-Hellman
- DSA

- Paillier
- El Gamal
- Κρυπτογραφία ελλειπτικών καμπυλών (ECC)

2.6 Κρυπτογραφία Συμμετρικού Κλειδιού

Η κρυπτογράφηση συμμετρικού κλειδιού (Symmetric Cryptography) βασίζεται στην ύπαρξη ενός και μόνο κλειδιού, το οποίο χρησιμοποιείται τόσο στην κρυπτογράφηση όσο και στην αποκρυπτογράφηση του μηνύματος. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα συναλλασσόμενα μέρη.

Ένα πρόβλημα το οποίο υφίσταται στους αλγόριθμους κρυπτογράφησης είναι η αδυναμία ανταλλαγής του κλειδιού με κάποιο ασφαλή τρόπο. Στην σύγχρονη ψηφιακή εποχή ο αποστολέας και ο παραλήπτης του μηνύματος πολλές φορές δεν γνωρίζονται, οπότε για την μετάδοση του κλειδιού από τον έναν στον άλλο θα πρέπει να υπάρχει κάποιο ασφαλές κανάλι επικοινωνίας. Φυσικά το διαδίκτυο δεν μπορεί να αποτελέσει κανάλι ασφαλούς επικοινωνίας, οπότε η χρήση της συμμετρικής κρυπτογράφησης σε εφαρμογές ηλεκτρονικού εμπορίου, ανταλλαγής ηλεκτρονικών μηνυμάτων κοκ ουσιαστικά δεν υφίσταται.

Το βασικό πλεονέκτημα των αλγορίθμων συμμετρικού κλειδιού είναι ότι η διαδικασία της κρυπτογράφησης και αποκρυπτογράφησης είναι πολύ γρήγορη και δεν καταναλώνει σημαντική υπολογιστική ισχύ.

Οι πιο γνωστοί αλγόριθμοι αυτού του είδους είναι οι DES, Triple DES, IDEA, RC2, RC4, AES.

Παράδειγμα

Θα παρουσιάσουμε ένα αναλογικό παράδειγμα από την καθημερινή ζωή το οποίο περιγράφει την κρυπτογράφηση συμμετρικού κλειδιού. Έστω η Alice και ο Bob, θέλουν να επικοινωνήσουν με ασφάλεια χρησιμοποιώντας το δημόσιο ταχυδρομείο. Η Alice θέλει να στείλει ένα καμουφλαρισμένο-κρυφό μήνυμα στον Bob και περιμένει μια καμουφλαρισμένη-κρυφή απάντηση από αυτόν.

Σύμφωνα με την κρυπτογράφηση συμμετρικού κλειδιού η Alice θα βάλει το μήνυμά της μέσα σε ένα κουτί με λουκέτο για το οποίο έχει το κλειδί. Στέλνει το κλειδαμπαρωμένο κουτί με το δημόσιο ταχυδρομείο στον Bob. Ο Bob έχει ένα ίδιο κλειδί (το οποίο έχει πάρει από την Alice στο παρελθόν, σε διαπροσωπική συνάντηση που είχαν) και μόλις λαμβάνει το κουτί, ανοίγει το λουκέτο και διαβάζει το μήνυμα. Ο Bob βάζει το μήνυμά του στο κουτί, το κλειδώνει και το στέλνει με δημόσιο ταχυδρομείο στην Alice.

Το πρόβλημα εδώ είναι ότι το κλειδί για το λουκέτο είναι κοινό και για την Alice και για τον Bob και για να δώσει αντίγραφο του κλειδιού ο ένας με τον άλλον θα πρέπει να συναντηθούν γιατί δεν είναι ασφαλές να το στείλουν με το δημόσιο ταχυδρομείο (ίσως τότε κάποια διεφθαρμένη υπάλληλος του ταχυδρομείου, π.χ. η Mallory θα μπορούσε να υποκλέψει το κλειδί και να δημιουργήσει ένα αντίγραφο ώστε στο μέλλον να υποκλέπτει ή να παραποιεί τα μηνύματα που ανταλλάσσονται στο κουτί).

2.6.1 Data Encryption Standard

Περιγραφή του DES

Η Data Encryption Standard (DES), είναι το όνομα της Federal Information Processing Standard (FIPS) 46-3, το οποίο περιγράφει τον αλγόριθμο κρυπτογράφησης δεδομένων (DEA). Ο DEA επίσης ορίζεται με το πρότυπο ANSI X3.92. Επίσης είναι μια βελτίωση του αλγορίθμου Lucifer που αναπτύχθηκε από την IBM στις αρχές του 1970. Η IBM, η Υπηρεσία Εθνικής Ασφάλειας (NSA) και το Εθνικό Γραφείο Προτύπων (NBS, σήμερα Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας NIST) ήταν οι υπηρεσίες που ανέπτυξαν τον αλγόριθμο.

Το DES έχει μελετηθεί εκτενώς από τη δημοσίευσή του και είναι ο πιο ευρέως χρησιμοποιούμενος συμμετρικός αλγόριθμος στον κόσμο. Το DES είναι 64-bit και χρησιμοποιεί ένα 56-bit κλειδί κατά τη διάρκεια της εκτέλεσης (έχει 8 bits ισοτιμίας από το πλήρες κλειδί 64-bit).Ο DES είναι ένα συμμετρικό κρυπτογραφικό σύστημα, και συγκεκριμένα ένα 16-γύρο cipher Feistel. Όταν χρησιμοποιείται για την επικοινωνία, τόσο αποστολέας και ο παραλήπτης πρέπει να γνωρίζει το ίδιο μυστικό κλειδί, το οποίο μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση και την αποκρυπτογράφηση του μηνύματος, ή για τη δημιουργία και την επαλήθευση ενός κώδικα ταυτότητας μηνυμάτων (MAC). Ο DES μπορεί επίσης να χρησιμοποιηθεί για μεμονωμένους χρήστες κρυπτογράφησης, όπως για την αποθήκευση αρχείων σε έναν σκληρό δίσκο σε κρυπτογραφημένη μορφή.

Ο DES είναι αρχετυπικός block cipher, δηλαδή, ένας πρωτότυπος κρυπταλγόριθμος συμμετρικού κλειδιού, που λαμβάνει μια σειρά από bits απλού κειμένου (plaintext bits) σταθερού μήκους και την μετατρέπει, μέσω μιας σειράς πολύπλοκων ενεργειών, σε μια άλλη σειρά bits, το κρυπτοκείμενο (chiphertext) με το ίδιο μήκος. Στην περίπτωση του DES το μέγεθος μπλοκ (block size: Η σειρά των bits σταθερού μήκους) είναι 64 bits.

Ο DES χρησιμοποιεί, επίσης, ένα κλειδί για να προσαρμόσει την μετατροπή, ώστε η αποκρυπτογράφηση να μπορεί, υποθετικά, να πραγματοποιηθεί μόνο από εκείνους που γνωρίζουν το συγκεκριμένο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση. Το κλειδί φαινομενικά αποτελείται από 64 bits. Ωστόσο, στην

πραγματικότητα μόνο 56 από αυτά χρησιμοποιήθηκαν από τον αλγόριθμο. Τα υπόλοιπα 8 bits χρησιμοποιούνται αποκλειστικά για τον έλεγχο της ισοτιμίας (parity) και στη συνέχεια απορρίπτονται (αυτά καλούνται parity bits), εξ ου και αναφέρεται συνήθως ως κλειδί μήκους 56 bits.

Όπως οι άλλοι block αλγόριθμοι κρυπτογράφησης, έτσι και ο DES από μόνος του δεν είναι ασφαλής τρόπος κρυπτογράφησης αλλά, αντίθετα, πρέπει να χρησιμοποιηθεί με ειδικό τρόπο λειτουργίας (mode of operation). Ο FIPS-81 ορίζει πολλούς τρόπους χρήσης του DES. Περαιτέρω παρατηρήσεις σχετικά με τη χρήση του DES περιέχονται στο FIPS-74.

Γενική δομή

ECB (Electronic Book Code) Αυτή είναι η τακτική του αλγορίθμου DES. Τα δεδομένα είναι χωρισμένα σε 64-bit μπλοκ και κάθε μπλοκ είναι κρυπτογραφημένο, ένα κάθε φορά. Ξεχωριστή κρυπτογράφηση με διαφορετικά μπλοκ είναι εντελώς ανεξάρτητα μεταξύ τους. Αυτό σημαίνει ότι εάν τα δεδομένα μεταδίδονται μέσω δικτύου ή τηλεφωνικής γραμμής, σφάλματα μετάδοσης θα επηρεάσουν μόνο το μπλοκ που περιέχει το σφάλμα. Αυτό σημαίνει επίσης, ωστόσο, ότι το μπλοκ μπορεί να τροποποιηθεί, και η δράση αυτή θα περνάει απαρατήρητη.

Ο ECB είναι ο πιο αδύναμος των διαφόρων μέσων, επειδή δεν απαιτούνται πρόσθετα μέτρα ασφαλείας που εφαρμόζονται, εκτός από το βασικό αλγόριθμο DES. Ωστόσο, ο ECB είναι ο γρηγορότερος και ευκολότερος για την εφαρμογή, καθιστώντας την πιο κοινή λειτουργία του DES.

CBC (Cipher Block Chaining) Σε αυτόν τον τρόπο λειτουργίας του, κάθε μπλοκ της ECB κρυπτογραφημένη ciphertext είναι XORed με το επόμενο μπλοκ plaintext είναι κρυπτογραφημένη, έτσι ώστε όλα τα μπλοκ εξαρτώνται από όλα τα προηγούμενα μπλοκ. Αυτό σημαίνει ότι για να βρει το plaintext ενός συγκεκριμένου μπλοκ, θα πρέπει να γνωρίζει το ciphertext, το κλειδί, και το κρυπτογράφημα του προηγούμενου μπλοκ.

Το πρώτο μπλοκ για να είναι κρυπτογραφημένο δεν έχει προηγούμενο ciphertext, έτσι ώστε το plaintext είναι XORed με έναν αριθμό 64-bit που ονομάζεται Initialization Vector ή IV για συντομία. Έτσι, αν τα δεδομένα μεταδίδονται μια γραμμή δικτύου ή τηλεφώνου και υπάρχει ένα σφάλμα μετάδοσης, το σφάλμα θα μεταφερθεί σε όλα τα επόμενα μπλοκ από το κάθε μπλοκ εξαρτάται από το τελευταίο. Αυτός ο τρόπος λειτουργίας είναι πιο ασφαλής από ECB, διότι το επιπλέον βήμα XOR προσθέτει ένα ακόμη στρώμα στη διαδικασία κρυπτογράφησης.

CFB (Cipher Feedback) Σε αυτή τη λειτουργία, μπλοκ plaintext που είναι λιγότερο από 64 bits μήκος μπορεί να είναι κρυπτογραφημένα. Κανονικά,

ειδική επεξεργασία, πρέπει να χρησιμοποιηθεί για να χειριστεί τα αρχεία των οποίων το μέγεθος δεν είναι ένα τέλειο πολλαπλάσιο των 8 bytes, αλλά αυτή η λειτουργία αφαιρεί ότι η αναγκαιότητα (Stealth χειρίζεται αυτή την περίπτωση, με την προσθήκη πολλών bytes ομοίωμα στο τέλος ενός αρχείου πριν την κρυπτογράφηση αυτού).

Η plaintext από μόνη της δεν είναι στην πραγματικότητα αλλά πέρασε μέσω του αλγορίθμου DES, απλώς XORed με ένα μπλοκ εξόδου από αυτήν, με τον ακόλουθο τρόπο: Ένας 64-bit μπλοκ που ονομάζεται Μητρώο Shift χρησιμοποιείται ως plaintext συμβολή DES. Αυτό έχει αρχικά οριστεί σε κάποια αυθαίρετη τιμή, και κρυπτογραφημένη με τον αλγόριθμο DES. Η ciphertext στη συνέχεια διέρχεται από ένα επιπλέον στοιχείο που ονομάζεται M-box, το οποίο απλά επιλέγει την άκρως αριστερή M bits του ciphertext, όπου M είναι ο αριθμός των bits στο μπλοκ που θέλουμε για την κρυπτογράφηση. Η τιμή αυτή είναι XORed με το πραγματικό απλό, και η έξοδος του ότι είναι ο τελικός ciphertext. Τέλος, το ciphertext επανατροφοδοτεί το Μητρώο Shift, και χρησιμοποιείται ως σπόρος plaintext για το επόμενο μπλοκ ώστε να είναι κρυπτογραφημένα.

Όπως και με τρόπο CBC, ένα λάθος σε ένα μπλοκ επηρεάζει όλες τις επόμενες μπλοκ κατά τη διάρκεια της μετάδοσης δεδομένων. Αυτός ο τρόπος λειτουργίας είναι παρόμοια με τη διασυνοριακή συνεργασία και είναι πολύ ασφαλής, αλλά είναι πιο αργή από ό,τι ο ECB χάρη στην επιπλέον πολυπλοκότητα.

OFB (Output Feedback) Αυτό είναι παρόμοιο σε λειτουργία CFB, εκτός από το ότι η παραγωγή του ciphertext DES είναι για να επανατροφοδοτεί το Μητρώο Shift, και όχι η πραγματική τελική ciphertext. Το μητρώο Shift έχει οριστεί σε μια αυθαίρετη αρχική τιμή, και πέρασε μέσα από τον αλγόριθμο DES. Η έξοδος από την DES διέρχεται μέσα από το M-box και στη συνέχεια να επανατροφοδοτεί το Shift για να προετοιμαστεί για το επόμενο μπλοκ. Η τιμή αυτή είναι συνέχεια XORed με το πραγματικό απλό (το οποίο μπορεί να είναι μικρότερο των 64 bits σε μήκος, όπως η λειτουργία CFB), και το αποτέλεσμα είναι το τελικό ciphertext.

Σημειώστε ότι σε αντίθεση με CFB και CBC, ένα σφάλμα μετάδοσης σε ένα μπλοκ δεν θα επηρεάσει τα επόμενα μπλοκ γιατί από τη στιγμή που ο παραλήπτης έχει την αρχική τιμή Εγγραφή Shift, θα συνεχίσει να παράγει νέα Shift Εγγραφή, απλό κείμενο χωρίς καμία περαιτέρω εισαγωγή δεδομένων. Αυτός ο τρόπος λειτουργίας είναι λιγότερο ασφαλής από ό,τι η CFB λειτουργία, επειδή μόνο το πραγματικό προϊόν ciphertext και DES ciphertext είναι απαραίτητο για να βρείτε το απλό κείμενο του πιο πρόσφατου μπλοκ. Η γνώση του κλειδιού δεν είναι απαραίτητη.

Ασφάλεια και κρυπτανάλυση

Αν και οι περισσότερες πληροφορίες που έχουν δημοσιευθεί αφορούν στην κρυπτανάλυση του DES απ' ότι οποιουδήποτε άλλου block cipher, η πρακτικότερη επίθεση μέχρι και σήμερα είναι ακόμα η προσέγγιση brute force (ωμής βίας). Είναι γνωστές διάφορες δευτερεύουσες κρυπταναλυτικές ιδιότητες και τρεις θεωρητικές επιθέσεις είναι δυνατές, που ακόμα κι αν έχουν μια θεωρητική πολυπλοκότητα μικρότερη από την επίθεση brute force, απαιτείται να φέρουν ιλιγγιώδες μέγεθος γνωστών ή προεπιλεγμένων plaintext και δεν αποτελούν, στην πράξη, πηγή ανησυχίας.

Επίθεση brute-force (ωμής βίας) Για οποιοδήποτε κρυπταλγόριθμο, η πιο βασική μέθοδος επίθεσης είναι η brute force - δοκιμάζοντας συνεχόμενα κάθε πιθανό κλειδί. Το μήκος του κλειδιού καθορίζει το πλήθος των πιθανών κλειδιών και ως εκ τούτου την δυνατότητα πραγματοποίησης αυτής της προσέγγισης. Τέθηκαν από νωρίς ερωτήσεις για την επάρκεια του μήκους κλειδιού του DES, πριν ακόμα υιοθετηθεί ως πρότυπο. Το μικρό μήκος κλειδιού ήταν αυτό που, στην ουσία, υπαγόρευσε την ανάγκη για την αντικατάσταση του αλγόριθμου, παρά η θεωρητική κρυπτανάλυση. Είναι γνωστό ότι η NSA ενθάρρυνε, αν δεν έπεισε, την IBM για να μειώσει το μήκος του κλειδιού από τα 128 στα 64 bits και από εκεί σε 56 bits. Αυτό λαμβάνεται συχνά ως ένδειξη ότι η NSA σκέφτηκε ότι θα ήταν σε θέση να «σπάσει» κλειδιά αυτού του μήκους ακόμη και στα μέσα της δεκαετίας του '70.

Στον ακαδημαϊκό κόσμο έγιναν διάφορες προηγμένες προτάσεις για μια μηχανή που θα αποσκοπούσε στο να «σπάει» τον DES. Το 1977, οι Diffie και Hellman πρότειναν μια μηχανή που θα στοίχιζε, κατ' εκτίμηση, 20 εκατομμύρια δολάρια, η οποία θα μπορούσε να βρει ένα κλειδί DES σε μία και μόνο ημέρα. Μέχρι το 1993, ο Wiener είχε προτείνει μια μηχανή αναζήτησης κλειδιού με κοστολόγηση 1 εκατομμύριο δολάρια, που θα έβρισκε ένα κλειδί μέσα σε 7 ώρες. Εντούτοις, καμία από αυτές τις πρόωρες προτάσεις δεν εφαρμόστηκε, τουλάχιστον καμία εφαρμογή δεν αναγνωρίστηκε δημόσια. Η ευπάθεια του DES επιδείχθηκε πρακτικά προς το τέλος της δεκαετίας του '90.

Το 1997, η εταιρεία RSA Security υποστήριξε μια σειρά διαγωνισμών με βραβείο 10.000 δολλάρια στην πρώτη ομάδα που θα «έσπαζε» ένα μήνυμα, το οποίο είχε κρυπτογραφηθεί με τον DES. Τον διαγωνισμό κέρδισε το πρόγραμμα DESCHALL, που δημιουργήθηκε από τους Rocke Verser, Matt Curtin, και Justin Dolske, χρησιμοποιώντας ιδανικούς κύκλους χιλιάδων υπολογιστών σε ολόκληρο το Διαδίκτυο. Η δυνατότητα πραγματοποίησης του «σπασίματος» του DES καταδείχθηκε γρήγορα το 1998 όταν φτιάχτηκε μια ρουτίνα «σπασίματος» του DES από την EFF (Electronic Frontier Foundation), μια ομάδα αστικών δικαιωμάτων του Κυβερνοχώρου, με κόστος περίπου 250,000 δολλάρια. Το

κίνητρό τους ήταν να δείξουν ότι ο DES ήταν το ίδιο εύθραυστος στην πράξη όπως και στην θεωρία:

Υπάρχουν πολλοί άνθρωποι που δεν θα πιστέψουν μια αλήθεια έως ότου μπορούν να τη δουν με τα μάτια τους. Δείχνοντάς τους μία φυσική μηχανή που μπορεί να «σπάσει» τον DES σε μερικές ημέρες είναι ο μόνος τρόπος να πειστούν μερικοί άνθρωποι ότι δεν μπορούν να εμπιστευθούν την ασφάλειά τους στον DES.

Η μηχανή εμφάνισε ένα κλειδί με χρήση brute force σε κάτι περισσότερο από 2 ημέρες. Περίπου στον ίδιο χρόνο ένας πληρεξούσιος του αμερικανικού Υπουργείου Δικαιοσύνης ανήγγελλε ότι ο DES δεν ήταν δυνατό να παραβιαστεί.

Η μόνη άλλη επιβεβαιωμένη μηχανή που «έσπαζε» τον DES ήταν η μηχανή COPACOBANA (σύντμηση του βέλτιστου κόστους και παράλληλα ενός code breaker) που δημιουργήθηκε πιο πρόσφατα από τις ομάδες των πανεπιστημίων του Μπόχουμ και του Κίελου της Γερμανίας. Αντίθετα από τη μηχανή της EFF, η COPACOBANA αποτελείται από εμπορικά διαθέσιμα, ανασχηματισμένα ολοκληρωμένα κυκλώματα. 120 αυτών των FPGAs του τύπου XILINX Spartan3-1000 τρέχουν σε παράλληλη σύνδεση. Ομαδοποιούνται σε 20 DIMM ενότητες, που κάθε μια περιέχει 6 FPGAs. Η χρήση των ανασχηματισμένων υλικών κάνει την μηχανή να βρίσκει εφαρμογή και σε άλλες λειτουργίες για «σπάσιμο» κωδικών.

Μια από τις πιο ενδιαφέρουσες πτυχές του COPACOBANA είναι ο παράγοντας του κόστους της. Μια μηχανή μπορεί να κατασκευαστεί με κόστος περίπου 10.000 δολλάρια. Η μείωση κόστους από έναν, κατά προσέγγιση, παράγοντα της τάξης του 25% από αυτή της μηχανής της EFF είναι ένα εντυπωσιακό παράδειγμα για τη συνεχή βελτίωση του ψηφιακού υλικού. Κατά ενδιαφέροντα τρόπο, ο νόμος του Moore προβλέπει μια βελτίωση της τάξης περίπου 32%, δεδομένου ότι περίπου οκτώ έτη έχουν μεσολαβήσει μεταξύ του σχεδιασμού των δύο μηχανών, πράγμα το οποίο επιτρέπει περίπου πέντε διπλασιασμούς της ισχύος των υπολογιστών (ή 5 μειώσεις τις τάξεως του 50% του κόστους για τον ίδιο υπολογισμό).

2.7 Κρυπτογραφία Δημοσίου Κλειδιού

Η κρυπτογράφηση δημοσίου κλειδιού (Public Key Cryptography) ή ασύμμετρου κλειδιού (Asymmetric Cryptography) επινοήθηκε στο τέλος της δεκαετίας του 1970 από τους Whitfield Diffie και Martin Hellman και παρέχει έναν εντελώς διαφορετικό μοντέλο διαχείρισης των κλειδιών κρυπτογράφησης. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό μυστικό κλειδί όπως στην περίπτωση της κρυπτογράφησης συμμετρικού κλειδιού, αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες.

Συγκεκριμένα κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης: το ένα ονομάζεται ιδιωτικό κλειδί (private key) και το άλλο δημόσιο κλειδί (public key). Το ιδιωτικό κλειδί θα πρέπει ο κάθε χρήστης να το προφυλάσσει και να το κρατάει κρυφό, ενώ αντιθέτως το δημόσιο κλειδί μπορεί να το ανακοινώνει σε όλη τη διαδικτυακή κοινότητα ή σε συγκεκριμένους παραλήπτες. Υπάρχουν δε και ειδικοί εξυπηρετητές δημοσίων κλειδιών (public key servers) στους οποίους μπορεί κανείς να απευθυνθεί για να βρει το δημόσιο κλειδί του χρήστη που τον ενδιαφέρει ή να ανεβάσει το δικό του δημόσιο κλειδί για να είναι διαθέσιμο στο κοινό.

Τα δύο αυτά κλειδιά (ιδιωτικό και δημόσιο) έχουν μαθηματική σχέση μεταξύ τους. Εάν το ένα χρησιμοποιηθεί για την κρυπτογράφηση κάποιου μηνύματος, τότε το άλλο χρησιμοποιείται για την αποκρυπτογράφηση αυτού. Η επιτυχία αυτού του είδους κρυπτογραφικών αλγορίθμων βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης.

Η κρυπτογράφηση δημοσίου κλειδιού λύνει ένα σημαντικότατο πρόβλημα που υπήρχε στους κρυπτογραφικούς αλγόριθμους συμμετρικού κλειδιού. Συγκεκριμένα, οι κρυπτογραφικοί αλγόριθμοι συμμετρικού κλειδιού χρησιμοποιούν ένα κοινό μυστικό κλειδί, το οποίο το γνωρίζουν τόσο ο αποστολέας του κρυπτογραφημένου μηνύματος όσο και ο παραλήπτης. Αυτό το κοινό μυστικό κλειδί χρησιμοποιείται κατά τη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης του μηνύματος. Προκύπτει όμως το εξής πρόβλημα: Εάν υποθέσουμε ότι το κανάλι επικοινωνίας δεν είναι ασφαλές, τότε πως γίνεται ο αποστολέας να στείλει το κλειδί κρυπτογράφησης στον παραλήπτη για να μπορέσει αυτός με τη σειρά του να αποκρυπτογραφήσει το μήνυμα· Αυτό το πρόβλημα είναι ιδιαίτερα έντονο στις σύγχρονες ψηφιακές επικοινωνίες όπου σε πολλές περιπτώσεις ο αποστολέας δεν γνωρίζει καν τον παραλήπτη και απέχει από αυτόν αρκετές χιλιάδες χιλιόμετρα. Οι κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού λύνουν αυτό το πρόβλημα και ανοίγουν νέους δρόμους για εφαρμογές της κρυπτογράφησης (ηλεκτρονικά μηνύματα, διαδικτυακές αγορές κοκ).

2.7.1 Τρόπος Λειτουργίας

Δημιουργία κλειδιών: Η δημιουργία του δημόσιου και του ιδιωτικού κλειδιού γίνεται από ειδικές συναρτήσεις οι οποίες δέχονται ως είσοδο έναν μεγάλο τυχαίο αριθμό και στην έξοδο παράγουν το ζεύγος των κλειδιών. Είναι προφανές ότι όσο πιο τυχαίος είναι ο αριθμός που παρέχεται ως είσοδος στη γεννήτρια κλειδιών τόσο πιο ασφαλή είναι τα κλειδιά που παράγονται. Σε σύγχρονα προγράμματα κρυπτογράφησης ο τυχαίος αριθμός παράγεται ως εξής: Κατά τη διαδικασία κατασκευής των κλειδιών, το πρόγραμμα σταματάει για 5 λεπτά και καλεί τον χρήστη να συνεχίσει να εργάζεται με τον υπολογιστή. Στη

συνέχεια για να παράξει τον τυχαίο αριθμό συλλέγει στα 5 αυτά λεπτά τυχαία δεδομένα που εξαρτώνται από τη συμπεριφορά του χρήστη (κινήσεις ποντικιού, πλήκτρα του πληκτρολογίου που πατήθηκαν, κύκλοι μηχανής που καταναλώθηκαν κοκ). Με βάση αυτά τα πραγματικά τυχαία δεδομένα υπολογίζεται ο τυχαίος αριθμός και εισάγεται στη γεννήτρια κλειδιών για να κατασκευαστεί το δημόσιο και το ιδιωτικό κλειδί του χρήστη.

Εμπιστευτικότητα

Οι κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού μπορούν να εγγυηθούν εμπιστευτικότητα (confidentiality), δηλαδή ότι το κρυπτογραφημενο μήνυμα που θα στείλει ο αποστολέας μέσω του διαδικτύου στον παραλήπτη θα είναι αναγνώσιμο από αυτόν και μόνο. Για να επιτευχθεί η εμπιστευτικότητα, ο αποστολέας θα πρέπει να χρησιμοποιήσει το δημόσιο κλειδί του παραλήπτη για να κρυπτογραφήσει το μήνυμα. Στη συνέχεια στέλνει το κρυπτογραφημένο μήνυμα στον παραλήπτη και ο τελευταίος μπορεί να το αποκρυπτογραφήσει με το ιδιωτικό κλειδί του. Δεδομένου ότι το ιδιωτικό κλειδί του παραλήπτη είναι γνωστό μονάχα στον ίδιο και σε κανέναν άλλον, μονάχα ο παραλήπτης μπορεί να αποκρυπτογραφήσει το μήνυμα και να το διαβάσει. Άρα λοιπόν με αυτόν τον τρόπο ο αποστολέας γνωρίζει ότι το κρυπτογραφημένο μήνυμα μπορεί να αποκρυπτογραφηθεί μονάχα από τον παραλήπτη και έτσι διασφαλίζεται η εμπιστευτικότητα του μηνύματος.

Πιστοποίηση

Χρησιμοποιώντας κατάλληλα τους κρυπτογραφικούς αλγορίθμους δημοσίου κλειδιού μπορεί να επιτευχθεί πιστοποίηση (authentication), δηλαδή ο παραλήπτης να γνωρίζει με ασφάλεια την ταυτότητα του αποστολέα. Για να επιτευχθεί αυτό θα πρέπει ο αποστολέας να χρησιμοποιήσει το ιδιωτικό του κλειδί για την κρυπτογράφηση του μηνύματος. Στη συνέχεια στέλνει το μήνυμα στον παραλήπτη και ο τελευταίος χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για την αποκρυπτογράφησή του. Δεδομένου ότι το ιδιωτικό κλειδί του αποστολέα είναι γνωστό μονάχα στον ίδιο, ο παραλήπτης μπορεί να είναι σίγουρος για την ταυτότητα του αποστολέα.

Εμπιστευτικότητα και Πιστοποίηση

Συνδυάζοντας τις δύο τεχνικές που παρουσιάστηκαν παραπάνω είναι εφικτό να επιτύχουμε εμπιστευτικότητα του μηνύματος και πιστοποίηση του αποστολέα. Δηλαδή αφενός το μήνυμα παραμένει γνωστό μονάχα στον αποστολέα και τον παραλήπτη και αφετέρου ο παραλήπτης γνωρίζει με ασφάλεια ποιος του έστειλε το μήνυμα. Για να επιτευχθεί αυτό ο αποστολέας μπορεί να κρυπτογραφήσει το

μήνυμα πρώτα με το δικό του ιδιωτικό κλειδί και στη συνέχεια με το δημόσιο κλειδί του παραλήπτη. Όταν ο παραλήπτης λάβει το μήνυμα θα πρέπει να χρησιμοποιήσει το ιδιωτικό του κλειδί για να το αποκρυπτογραφήσει (εμπιστευτικότητα) και στη συνέχεια να αποκρυπτογραφήσει το αποτέλεσμα χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα (πιστοποίηση).

Παράδειγμα

Θα παρουσιάσουμε ένα αναλογικό παράδειγμα από την καθημερινή ζωή το οποίο περιγράφει την κρυπτογράφηση δημόσιου κλειδιού ή ασυμμετρική κρυπτογράφηση. Έστω η Alice και ο Bob, θέλουν να επικοινωνήσουν με ασφάλεια χρησιμοποιώντας το δημόσιο ταχυδρομείο. Η Alice θέλει να στείλει ένα καμουφλαρισμένο-κρυφό μήνυμα στον Bob και περιμένει μια καμουφλαρισμένη-κρυφή απάντηση από αυτόν.

Σύμφωνα με την κρυπτογράφηση συμμετρικού κλειδιού η Alice θα βάλει το μήνυμά της μέσα σε ένα κουτί με λουκέτο για το οποίο έχει το κλειδί. Στέλνει το κλειδαμπαρωμένο κουτί με το δημόσιο ταχυδρομείο στον Bob. Ο Bob έχει ένα ίδιο κλειδί (το οποίο έχει πάρει από την Alice στο παρελθόν, σε διαπροσωπική συνάντηση που είχαν) και μόλις λαμβάνει το κουτί, ανοίγει το λουκέτο και διαβάζει το μήνυμα. Ο Bob βάζει το μήνυμά του στο κουτί, το κλειδώνει και το στέλνει με δημόσιο ταχυδρομείο στην Alice.

Το πρόβλημα εδώ είναι ότι το κλειδί για το λουκέτο είναι κοινό και για την Alice και για τον Bob και για να δώσει αντίγραφο του κλειδιού ο ένας με τον άλλον θα πρέπει να συναντηθούν γιατί δεν είναι ασφαλές να το στείλουν με το δημόσιο ταχυδρομείο (ίσως τότε κάποια διεφθαρμένη υπάλληλος του ταχυδρομείου, π.χ. η Mallory θα μπορούσε να υποκλέψει το κλειδί και να δημιουργήσει ένα αντίγραφο ώστε στο μέλλον να υποκλέπτει ή να παραποιεί τα μηνύματα που ανταλλάσσονται στο κουτί).

Στην πράξη της ασυμμετρικής κρυπτογραφίας, ο Bob και η Alice έχουν ξεχωριστές κλειδαριές. Πρώτα η Alice βάζει το μυστικό μήνυμα στο κουτί, το κλειδώνει με το λουκέτο που έχει μόνο αυτή κλειδί. Το στέλνει το κουτί στον Bob με απλό δημόσιο ταχυδρομείο. Όταν ο Bob λαμβάνει το κουτί, προσθέτει το δικό του λουκέτο στο κουτί και στο στέλνει πίσω στην Alice. Η Alice λαμβάνει το κουτί με δύο λουκέτα, αφαιρεί το δικό της λουκέτο και το στέλνει πίσω στον Bob. Όταν ο Bob λαμβάνει το κουτί έχει πάνω μόνο το δικό του λουκέτο, το οποίο μπορεί να ξεκλειδώσει και να δει το μήνυμα της Alice. Σε αυτό το παράδειγμα η διαδικασία της αποκρυπτογραφίας είναι ίδια με τη διαδικασία της κρυπτογραφίας.

Η κρίσιμη διαφορά στο κλειδί ασυμμετρικής κρυπτογράφησης είναι ότι η Alice και ο Bob ποτέ δεν χρειάζεται να στείλουν αντίγραφο του κλειδιού ο ένας στον άλλον. Σε αυτή την περίπτωση αποφεύγουμε την περίπτωση της

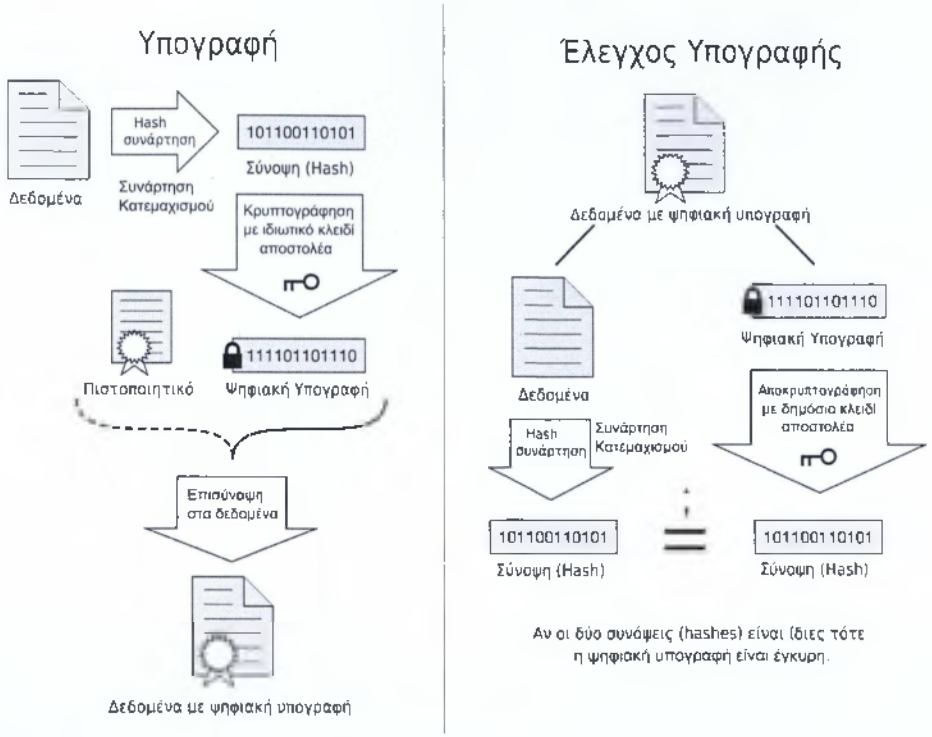
διεφθαρμένης υπάλληλου στο ταχυδρομείο, την Mallory η οποία ενδέχεται να υποκλέψει το κλειδί κατά τη μεταφορά. Σε αυτή την περίπτωση η Alice και ο Bob δεν χρειάζεται να εμπιστευτούν το δημόσιο ταχυδρομείο. Επιπρόσθετα ο Bob επιτρέπει σε όποιον επιθυμεί να αντιγράψει το κλειδί του και τα μηνύματα της Alice προς τον Bob θα είναι εκτεθειμένα σε κίνδυνο υποκλοπής. Όμως όλα τα μηνύματα της Alice προς άλλους θα είναι μυστικά, αφού οι υπόλοιποι θα παρέχουν διαφορετικά λουκέτα για να κλειδώσει η Alice το μήνυμα στο κουτί πριν το στείλει σε αυτούς.

Ψηφιακές Υπογραφές

Η κρυπτογράφηση δημόσιου κλειδιού μαζί με την συνάρτηση κατακερματισμού (hash function) βρίσκει εφαρμογή στις ψηφιακές υπογραφές. Υπολογίζεται με την συνάρτηση κατακερματισμού, η σύνοψη (digest) του μηνύματος/εγγράφου. Στη συνέχεια η σύνοψη κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα (ο οποίος με αυτήν την ενέργεια υπογράφει ψηφιακά το μήνυμα έγγραφο). Η κρυπτογραφημένη σύνοψη είναι η ψηφιακή υπογραφή η οποία επισυνάπτεται στο μήνυμα/έγγραφο. Μαζί με την ψηφιακή υπογραφή μπορεί να επισυναφθεί και ένα πιστοποιητικό του δημόσιου κλειδιού (το οποίο έχει εκδοθεί από κάποιο αξιόπιστο πάροχο/οργανισμό υπηρεσιών πιστοποίησης: το πιστοποιητικό ταυτοποιεί ένα δημόσιο κλειδί με τον δικαιούχο του). Στη διαδικασία ελέγχου της ψηφιακής υπογραφής, ξεχωρίζεται η ψηφιακή υπογραφή από το μήνυμα/έγγραφο. Η ψηφιακή υπογραφή αποκρυπτογραφείται με το δημόσιο κλειδί του αποστολέα και εξάγεται η σύνοψη. Παράλληλα υπολογίζεται η σύνοψη του ληφθέντος μηνύματος/εγγράφου. Αν οι δύο συνόψεις είναι ίδιες σημαίνει ότι το μήνυμα/έγγραφο έχει την υπογραφή του αποστολέα (που ανήκει το δημόσιο κλειδί) και ότι το μήνυμα/έγγραφο δεν έχει παραποιηθεί κατά τη μεταφορά.

2.8 Ψηφιακές Υπογραφές

Η Ψηφιακή Υπογραφή είναι ένα μαθηματικό σύστημα που χρησιμοποιείται για την απόδειξη της γνησιότητας ενός ψηφιακού μηνύματος ή εγγράφου. Μια έγκυρη ψηφιακή υπογραφή δίνει στον παραλήπτη την πιστοποίηση ότι το μήνυμα που δημιουργήθηκε ανήκει στον αποστολέα που το υπέγραψε ψηφιακά και ότι δεν αλλοιώθηκε-παραποιήθηκε κατά την μεταφορά. Οι ψηφιακές υπογραφές χρησιμοποιούν συνδυασμό μιας κρυπτογραφικής συνάρτησης κατατεμαχισμού (hash function) για δημιουργία της σύνοψης (hash) σε συνδυασμό με ασυμμετρική κρυπτογραφία για κρυπτογράφηση/αποκρυπτογράφηση σύνοψης (ο συνδυασμός σύνοψης και κρυπτογράφησης με ασυμμετρική κρυπτογραφία αποδεικνύει την ακεραιότητας του εγγράφου αλλά και την απόδειξη ταυτότητας του



Σχήμα 2.2: Σχηματική αναπαράσταση του διαγράμματος Ψηφιακής Υπογραφής

αποστολέα).

Σε μερικές χώρες όπως τις ΗΠΑ και κάποιες χώρες της Ευρωπαϊκής ένωσης, οι ψηφιακές υπογραφές έχουν και νομική υπόσταση. Οι ψηφιακές υπογραφές σε ψηφιακά έγγραφα είναι παρόμοιες με τις αντίστοιχες χειρόγραφες υπογραφές σε έντυπα έγγραφα. Όταν οι ψηφιακές υπογραφές υλοποιούνται - εφαρμόζονται σωστά (με χρήση ασφαλών κρυπτογραφικών αλγορίθμων), είναι πολύ δυσκολότερο να πλαστογραφηθούν σε σχέση με τις αντίστοιχες χειρόγραφες. Επίσης το φυσικό πρόσωπο που ψηφιακά υπογράφει το ψηφιακό έγγραφο δεν μπορεί να ισχυριστεί ότι δεν το υπόγραψε (όσο το ιδιωτικό κλειδί που χρησιμοποίησε δεν υποκλάπηκε). Κάποιες υλοποιήσεις των ψηφιακών υπογραφών προσθέτουν και την ημερομηνία υπογραφής του εγγράφου, ώστε και το ιδιωτικό κλειδί να υποκλαπεί, η ψηφιακή υπογραφή να είναι έγκυρη.

Η ψηφιακή υπογραφή μπορεί να προστεθεί σε οποιαδήποτε σειρά από bits (δηλαδή δεδομένα): παραδείγματα χρήσης είναι τα μηνύματα ηλεκτρονικού ταχυδρομείου, έγγραφα, μηνύματα που στέλνονται στο διαδίκτυο κλπ. Πολλοί οργανισμοί υιοθετούν την χρήση των ψηφιακών υπογραφών ώστε να αποφεύ-

γεται η αποστολή τυπωμένων εγγράφων (επικυρωμένα με χρήση σφραγίδων και υπογραφών).

2.8.1 Ορισμός

Η ψηφιακή υπογραφή αποτελείται από τρεις αλγόριθμους:

- Ο αλγόριθμος δημιουργίας δημόσιου και ιδιωτικού κλειδιού: Ο αλγόριθμος αυτός χρησιμοποιεί μια γεννήτρια τυχαίων αριθμών και με βάση αυτόν τον τυχαίο αριθμό δημιουργεί το δημόσιο και ιδιωτικό κλειδί (με το ιδιωτικό κλειδί δημιουργείται η ψηφιακή υπογραφή και με το δημόσιο κλειδί ελέγχεται η ψηφιακή υπογραφή).

- Ο αλγόριθμος προσθήκης ψηφιακής υπογραφής σε μηνύματα ή έγγραφα: Χρησιμοποιώντας το μήνυμα/έγγραφο και το ιδιωτικό κλειδί (το οποίο ανήκει μόνο σε αυτόν που υπογράφει το έγγραφο), δημιουργεί την ψηφιακή υπογραφή.

- Ο αλγόριθμος έλεγχου ψηφιακής υπογραφής μηνύματος ή εγγράφου: Χρησιμοποιώντας το μήνυμα/έγγραφο και το δημόσιο κλειδί (το δημόσιο κλειδί είναι διαθέσιμο σε όλους, και συσχετίζεται με το ιδιωτικό κλειδί και ανήκει σ΄ αυτόν που υπέγραψε ψηφιακά το μήνυμα/έγγραφο), ελέγχει την αυθεντικότητα (ποιος το υπέγραψε) αλλά και την ακεραιότητα (ότι το μήνυμα δεν παραποιήθηκε) του μηνύματος/εγγράφου.

Σύμφωνα με την ασυμμετρική κρυπτογράφηση κάποιος που γνωρίζει το δημόσιο κλειδί δεν μπορεί να δημιουργήσει (είναι υπολογιστικά ανέφικτο) το αντίστοιχο ιδιωτικό κλειδί. Επίσης κάποιος ο οποίος έχει το δημόσιο κλειδί μπορεί να ελέγξει την αυθεντικότητα και ακεραιότητα ενός μηνύματος/εγγράφου το οποίο είναι ψηφιακά υπογεγραμμένο.

Ένα πρόβλημα με τις ψηφιακές υπογραφές είναι ότι δεν γνωρίζουμε αν το δημόσιο κλειδί (κατά την διάρκεια ελέγχου της υπογραφής) που έχουμε ανήκει σε αυτόν που ισχυρίζεται ότι είναι. Για αυτό ακριβώς τον λόγο υπάρχει ο Πάροχος Υπηρεσιών Πιστοποίησης ο οποίος είναι ένας οργανισμός - οντότητα ο οποίος πιστοποιεί την σχέση ενός ανθρώπου με το δημόσιο κλειδί του. Ο Πάροχος Υπηρεσιών Πιστοποίησης θα πρέπει να εμπνέει εμπιστοσύνη γιατί είναι η αρχή η οποία εκδίδει **ψηφιακά πιστοποιητικά**[1]. Τα ψηφιακά πιστοποιητικά ταυτοποιούν ένα δημόσιο κλειδί με τον δικαιούχο του. Πολλές φορές

[1]Το Ψηφιακό πιστοποιητικό είναι ένα ηλεκτρονικό έγγραφο που χρησιμοποιείται για την αναγνώριση μίας οντότητας (φυσικό πρόσωπο, εξυπηρετητής, οργανισμός κοκ) και την ανάκτηση του δημοσίου κλειδιού αυτής. Η έκδοση ενός ψηφιακού πιστοποιητικού γίνεται μετά από αίτηση του ενδιαφερομένου σε μία Αρχή Πιστοποίησης. Η Αρχή Πιστοποίησης επιβεβαιώνει την ταυτότητα του αιτούντος και εκδίδει το πιστοποιητικό, το οποίο συνοπτικά

αυτός που υπογράφει ψηφιακά ένα ηλεκτρονικό έγγραφο, ενδέχεται να επισυνάψει στο έγγραφο μαζί με την ψηφιακή υπογραφή και το ψηφιακό πιστοποιητικό του δημόσιου κλειδιού.

2.8.2 Παράδειγμα

Έστω ότι η Alice και ο Bob θέλουν να επικοινωνήσουν μεταξύ τους και συγκεκριμένα η Alice θέλει να στείλει στον Bob ένα υπογεγραμμένο μήνυμα.

- Αρχικά η Alice και ο Bob θα πρέπει να συμφωνήσουν ποιον αλγόριθμο δημόσιου κλειδιού (ασυμμετρικής κρυπτογράφησης: π.χ. PGP, Digital Signature Standard) και ποιον αλγόριθμο κατατεμαχισμού (π.χ. MD5) θα χρησιμοποιήσουν.

- Η Alice και ο Bob έχουν ζευγάρια δημοσίων και ιδιωτικών κλειδιών σύμφωνα με τον αλγόριθμο που επέλεξαν στο προηγούμενο βήμα. Θα πρέπει να ανταλλάξουν μεταξύ τους τα δημόσια κλειδιά τους.

- Η Alice θέλει να στείλει ένα υπογεγραμμένο μήνυμα στον Bob. Αρχικά θα περάσει το μήνυμα από τον αλγόριθμο κατατεμαχισμού που επέλεξαν στο πρώτο βήμα και θα παράγει την σύνοψη (digest) του μηνύματος.

- Η Alice θα κρυπτογραφήσει την σύνοψη με το ιδιωτικό κλειδί της και θα προσθέσει την κρυπτογραφημένη εκδοχή της στο τέλος του εγγράφου. Αν θέλει, μπορεί επίσης να προσθέσει και ένα πιστοποιητικό που πιστοποιεί ότι το δημόσιο κλειδί που θα χρησιμοποιηθεί από τον Bob αργότερα για την αποκρυπτογράφηση της υπογραφής ανήκει στην Alice (το πιστοποιητικό θα πρέπει να έχει εκδοθεί από ένα έμπιστο πάροχο υπηρεσιών πιστοποίησης). Θα αποστείλει στον Bob το τελικό έγγραφο (έγγραφο το οποίο έχει ψηφιακά υπογραφεί από την Alice - και ίσως περιέχει και ένα ψηφιακό πιστοποιητικό δημόσιου κλειδιού).

- Ο Bob θα ξεχωρίσει την κρυπτογραφημένη σύνοψη από το τέλος του εγγράφου και θα το αποκρυπτογραφήσει χρησιμοποιώντας το δημόσιο κλειδί της Alice (το έχει λάβει στο δεύτερο βήμα). Εφόσον η αποκρυπτογράφηση γίνει με επιτυχία γνωρίζει ότι η σύνοψη δεν έχει αλλοιωθεί και ότι ανήκει στην Alice. Κατόπιν θα πάρει το μήνυμα και θα το περάσει από

περιλαμβάνει τα εξής στοιχεία: Το ονοματεπώνυμο και διάφορες άλλες πληροφορίες σχετικά με τον κάτοχο του πιστοποιητικού, το δημόσιο κλειδί του κατόχου του πιστοποιητικού, την ημερομηνία λήξης του πιστοποιητικού, το όνομα και την ψηφιακή υπογραφή της Αρχής Πιστοποίησης που το εξέδωσε. Το πιο διαδεδομένο πρότυπο ψηφιακών πιστοποιητικών είναι το X.509. Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται ευρέως για διάφορες κρυπτογραφημένες ηλεκτρονικές συναλλαγές μέσω του διαδικτύου.

τον αλγόριθμο κατατεμαχισμού που έχει συμφωνήσει στο πρώτο βήμα και θα συγκρίνει την σύνοψη που υπολόγισε ο ίδιος με την σύνοψη που αποκρυπτογράφησε από την ψηφιακή υπογραφή. Αν οι συνόψεις είναι ίδιες, ο Bob γνωρίζει ότι το αρχικό μήνυμα δεν έχει αλλοιωθεί. Αν θέλει να βεβαιωθεί ότι το δημόσιο κλειδί που χρησιμοποίησε ανήκει πραγματικά στην Alice θα διαβάσει το ψηφιακό πιστοποιητικό της Alice.

Η κρυπτογράφηση με το ασύμμετρο κρυπτοσύστημα μπορεί να αξιοποιηθεί και με άλλον τρόπο. Υποθέτουμε ότι ο Β επιθυμεί να αποστείλει ένα μήνυμα στον Α. Στις καταγραφείσες απαιτήσεις δεν περιλαμβάνεται πλέον η εμπιστευτικότητα του κειμένου, αλλά ο Α επιθυμεί να είναι σίγουρος για την προέλευση του κειμένου, δηλαδή απαιτείται αυθεντικοποίηση (authenticity) του αποστολέα του μηνύματος. Σε αυτή την περίπτωση, ο Β κρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί. Όταν ο Α παραλάβει το κρυπτογραφημένο μήνυμα, το αποκρυπτογραφεί με το δημόσιο κλειδί του Β, εξασφαλίζοντας έτσι ότι το αρχικό μήνυμα έχει κρυπτογραφηθεί από τον Β. Κανένας άλλος δεν κατέχει και δε γνωρίζει το ιδιωτικό κλειδί του Β, συνεπώς, κανένας δεν μπορεί να δημιουργήσει κρυπτογραφημένο κείμενο το οποίο να αποκρυπτογραφείται με το δημόσιο κλειδί του Β.

Έτσι, όλο το κρυπτογραφημένο κείμενο αποτελεί μία ψηφιακή υπογραφή (digital signature). Επιπλέον, είναι αδύνατον να αλλοιωθεί το μήνυμα χωρίς γνώση του ιδιωτικού κλειδιού του Β, οπότε εξασφαλίζεται αυθεντικοποίηση του αποστολέα, αλλά και ακεραιότητα των δεδομένων.

Ένα πρόβλημα που δημιουργείται σε αυτή την περίπτωση αφορά το χώρο αποθήκευσης: κάθε μήνυμα πρέπει να είναι αποθηκευμένο σε μη κρυπτογραφημένη μορφή για πρακτικούς λόγους. Πρέπει, επίσης, να φυλάσσεται ένα αντίγραφο σε κρυπτογραφημένη μορφή, ώστε η προέλευση και τα περιεχόμενα να μπορούν να προσδιοριστούν εύκολα σε περίπτωση αμφισβήτησης και διαφωνίας. Ένας εύκολος τρόπος για να επιτευχθούν τα ίδια αποτελέσματα, θα ήταν να κρυπτογραφηθεί μικρό τμήμα από bits, το οποίο θα αποτελεί συνάρτηση του κειμένου. Ένα τέτοιο τμήμα ονομάζεται αυθεντικοποιητής (authenticator) και θα πρέπει να είναι αδύνατο να τροποποιηθεί το μήνυμα, χωρίς να αλλάξει ο αυθεντικοποιητής. Αν ο αυθεντικοποιητής κρυπτογραφηθεί με το ιδιωτικό κλειδί του αποστολέα, τότε χαρακτηρίζεται ως ψηφιακή υπογραφή (digital signature).

Για τη δημιουργία μιας ψηφιακής υπογραφής ενός κειμένου από μία οντότητα, συνήθως κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα η σύνοψη του μηνύματος.

Θα πρέπει να τονιστεί ότι η ψηφιακή υπογραφή δεν προσφέρει εμπιστευτικότητα για το μήνυμα, αλλά αποτελεί υπηρεσία που ικανοποιεί απαιτήσεις ακεραιότητας μηνύματος, αυθεντικοποίησης αποστολέα και μη αποποίησης αποστολής μηνύματος.

2.9 Συναρτήσεις Κατακερματισμού και Ακεραιότητα Δεδομένων

Η συνάρτηση κατακερματισμού, γνωστή και ως συνάρτηση κατατεμαχισμού, είναι μια μαθηματική συνάρτηση που έχοντας ως είσοδο μια αυθαίρετου μεγέθους ομάδα δεδομένων δίνει έξοδο μια καθορισμένου μεγέθους στοιχειοσειρά (string) (συνήθως ένα ακέραιο αριθμό), πολύ μικρότερη από την είσοδο. Η έξοδος της συνάρτησης μπορεί να χρησιμοποιηθεί ως δείκτης σε κάποιο πίνακα. Οι τιμές που επιστρέφει η συνάρτηση κατακερματισμού ονομάζονται τιμές κατακερματισμού (hash values), κώδικες κατακερματισμού (hash codes), αθροίσματα κατακερματισμού (hash sums) ή απλά τιμές κατακερματισμού (hashes).

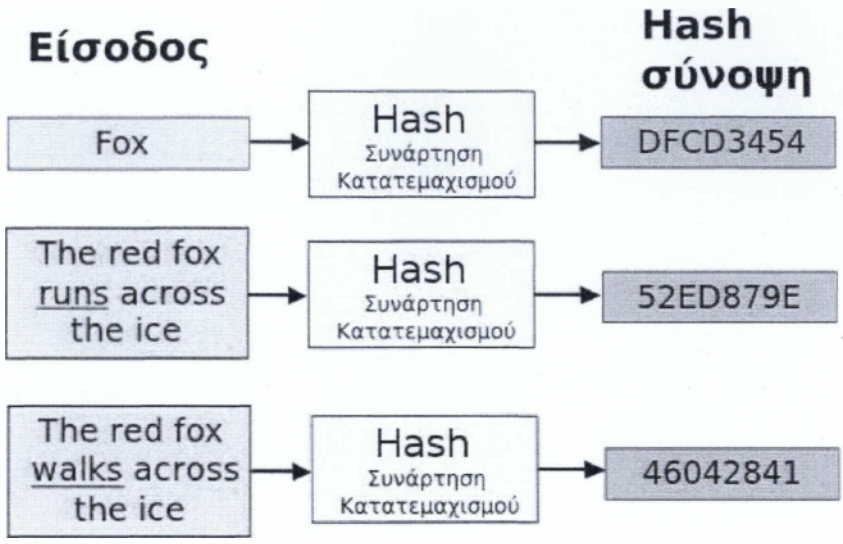
Οι συναρτήσεις κατακερματισμού χρησιμοποιούνται συνήθως για να επιταχυνθεί η αναζήτηση σε κάποιο πίνακα ή σε εργασίες σύγκρισης δεδομένων (π.χ. εύρεση στοιχείων σε μια βάση δεδομένων, εύρεση παρόμοιων εγγραφών σε ένα μεγάλο αρχείο βάσης κλπ).

Μια συνάρτηση κατακερματισμού μπορεί να αντιστοιχίζει δύο ή περισσότερους εισόδους στην ίδια τιμή κατακερματισμού. Στις περισσότερες εφαρμογές είναι επιθυμητή η ελαχιστοποίηση αυτών συγκρούσεων. Αυτό σημαίνει ότι η συνάρτηση κατακερματισμού θα πρέπει να αντιστοιχίζει κάθε είσοδο σε διαφορετική τιμή κατακερματισμού. Ανάλογα με την εφαρμογή χρήσης, η συνάρτηση κατακερματισμού σχεδιάζεται με διαφορετικές προδιαγραφές. Η ιδέα αυτών των συναρτήσεων εμφανίστηκε το 1950 αλλά ακόμη και σήμερα ο σχεδιασμός μιας καλής συνάρτησης κατακερματισμού είναι αντικείμενο έρευνας.

Οι συναρτήσεις κατακερματισμού συσχετίζονται (αν και πολλές φορές μπερδεύονται ως έννοιες) με τις συναρτήσεις αθροίσματος ελέγχου (π.χ. ο Κυκλικός Έλεγχος Πλεονασμού), τον υπολογισμό ψηφίου ελέγχου (check digit), δακτυλικά αποτυπώματα (fingerprints), κώδικες ελέγχου λαθών (error correcting codes) και την κρυπτογραφική συνάρτηση κατακερματισμού.

2.9.1 Κρυπτογραφική Συνάρτηση Κατακερματισμού

Η κρυπτογραφική συνάρτηση κατακερματισμού (cryptographic hash function) είναι μια συνάρτηση κατακερματισμού (hash function) η οποία είναι σχεδιασμένη για να χρησιμοποιείται στην κρυπτογραφία. Γενικά η συνάρτηση κατακερματισμού είναι μια μαθηματική συνάρτηση που έχοντας ως είσοδο μια αυθαίρετου μεγέθους ομάδα δεδομένων δίνει έξοδο μια καθορισμένου μεγέθους στοιχειοσειρά (string) (η συμβολοσειρά είναι συνήθως μικρότερη σε μέγεθος από την



Σχήμα 2.3: Παράδειγμα συνάρτησης κατακερματισμού

αρχική είσοδο). Η έξοδος δεν μπορεί με αντιστροφή (με κανένα τρόπο) να μας παράγει την αρχική είσοδο. Η έξοδος αποκαλείται συνήθως «σύνοψη» (digest).

Μια ιδεατή κρυπτογραφική συνάρτηση κατακερματισμού έχει τις παρακάτω ιδιότητες:

- Είναι εύκολο να υπολογιστεί η σύνοψη για οποιαδήποτε είσοδο.
- Δεν είναι εφικτό να βρεις την είσοδο από την σύνοψη.
- Δεν είναι εφικτό να τροποποιήσεις την είσοδο χωρίς να τροποποιηθεί η σύνοψη.
- Δεν είναι εφικτό να βρεθούν δύο διαφορετικές είσοδοι που δίνουν την ίδια σύνοψη.

Οι συναρτήσεις κατακερματισμού βρίσκουν εφαρμογή στις εφαρμογές ασφάλειας πληροφοριών, ενδεικτικά στις ψηφιακές υπογραφές, Message authentication codes (MACs) και άλλες μορφές πιστοποίησης αυθεντικότητας των δεδομένων.

Διάσημες συναρτήσεις κατακερματισμού είναι η MD5 και η SHA-1. Το 2008 βρέθηκαν προβλήματα ασφάλειας στην συνάρτηση MD5 σε επίθεση στο πρωτόκολλο Secure Socket Layer (SSL). Η συνάρτηση SHA-0 και η SHA-1 αναπτύχθηκαν από την Υπηρεσία Εθνικής Ασφάλειας (National Security Agency: NSA) των ΗΠΑ. Τον Φεβρουάριο 2005, μια επιτυχημένη επίθεση

στην συνάρτηση SHA-1 δημοσιεύθηκε. Η θεωρητική αδυναμία της συνάρτησης SHA-1 είναι γνωστή και έτσι αναπτύχθηκε η συνάρτηση SHA-2.

Σύνοψη μηνύματος

Η σύνοψη ενός μηνύματος είναι το αποτέλεσμα (έξοδος) της συνάρτησης κατακερματισμού. Η σύνοψη είναι συνήθως μικρότερη από το αρχικό μήνυμα και δεν μπορούμε να ξαναγυρίσουμε στο αρχικό μήνυμα από αυτή. Οι κρυπτογραφικοί αλγόριθμοι κατακερματισμού είναι φτιαγμένοι με τέτοιο τρόπο ώστε μια μικρή μεταβολή στα δεδομένα εισόδου (π.χ. Ένα μόνο γράμμα ή ακόμα και ένα μόνο bit) να προκαλεί ολοκληρωτική αλλαγή στην έξοδο (πλήρης αλλαγή της σύνοψης).

Χρήσεις συνάρτησης

- **Ψηφιακές υπογραφές:** η συνάρτηση κατακερματισμού χρησιμοποιείται κατά την διάρκεια δημιουργίας της ψηφιακής υπογραφής. Χρησιμοποιώντας την συνάρτηση κατακερματισμού, από το μήνυμα/έγγραφο παράγεται η σύνοψη. Η σύνοψη κρυπτογραφείται με το ιδιωτικό κλειδί (ασυμμετρική κρυπτογράφηση) του ιδιοκτήτη/αποστολέα του μηνύματος/εγγράφου. Η κρυπτογραφημένη σύνοψη είναι η ψηφιακή υπογραφή του μηνύματος/εγγράφου. Ο έλεγχος της ψηφιακής υπογραφής γίνεται με την ανάποδη διαδικασία: υπολογίζεται η σύνοψη του μηνύματος/εγγράφου, αποκρυπτογραφείται η ψηφιακή υπογραφή με το δημόσιο κλειδί του ιδιοκτήτη/αποστολέα και συγκρίνονται οι δυο συνόψεις. Αν είναι ίδιες το έγγραφο ανήκει στον ιδιοκτήτη/αποστολέα που το έχει υπογράψει και δεν έχει παραποιηθεί.
- **Κωδικοί πρόσβασης:** Για λόγους ασφάλειας σε συστήματα όπως το UNIX, οι κωδικοί πρόσβασης δεν αποθηκεύονται ως κείμενο αλλά στην θέση τους αποθηκεύονται οι συνόψεις (υπολογίζεται η σύνοψη του κωδικού με μια δυνατή κρυπτογραφική συνάρτηση κατακερματισμού όπως η MD5). Στον έλεγχο του κωδικού πρόσβασης ο κωδικός εισάγεται στην συνάρτηση κατακερματισμού και υπολογίζεται η σύνοψη. Αν η σύνοψη είναι ίδια με αυτή που είναι αποθηκευμένη ο κωδικό πρόσβασης είναι έγκυρος.

2.9.2 Ασφάλεια χρήσης της Συνάρτησης Κατακερματισμού

Η συνάρτηση κατακερματισμού αναφέρεται σε έναν αλγόριθμο, ο οποίος είναι σε θέση να υπολογίζει μία τιμή βασισμένη σε ένα ηλεκτρονικό αντικείμενο, όπως

ένα μήνυμα ή ένα αρχείο, χαρτογραφώντας το ηλεκτρονικό αυτό αντικείμενο σε ένα άλλο παρόμοιο (ηλεκτρονικό αντικείμενο). Το νέο ηλεκτρονικό αντικείμενο το οποίο εξάγεται ονομάζεται «σύνοψη του αρχικού μηνύματος». Ωστόσο, οι πρόσφατες εξελίξεις στον τομέα της «κρυπτανάλυσης» μετά τις επιθέσεις αντοχής ειδικά σε συναρτήσεις κατακερματισμού τύπου MD5 και SHA-1 (όπως αναφέρθηκε και παραπάνω), είχαν ως αποτέλεσμα τον κλονισμό της εμπιστοσύνης του βαθμού ασφαλείας ο οποίος διέπει τις λειτουργίες των συναρτήσεων κατακερματισμού. Επιπλέον, αμφιβολίες δημιουργήθηκαν για την ικανότητα σχεδιασμού ασφαλών σε επιθέσεις συναρτήσεων κατακερματισμού.

Αυτού του είδους οι επιθέσεις επιβεβαιώνουν ότι η «ασφάλεια των συναρτήσεων κατατεμαχισμού» των οποίων η κατασκευή βασίζεται στις αποκτηθείσες εμπειρίες, μπορεί να κινδυνεύσει απροσδόκητα. Το γεγονός αυτό επισημαίνει την ανάγκη ανανέωσης των μηχανισμών σχεδιασμού, κατά τους οποίους κρίνεται αναγκαία η αποφυγή χρησιμοποίησης των βασικών κρυπτογραφικών δομών. Συνεπώς, διαπιστώνεται ότι οι μελλοντικές κινήσεις θα πρέπει να βασίζονται όσο το δυνατόν λιγότερο σε διαδικασίες οι οποίες παρουσιάζουν ανοχή στις επιθέσεις.

Χαρακτηριστικό παράδειγμα συστημάτων των οποίων η ασφάλεια συχνά διακυβεύεται, δηλαδή συστήματα τα οποία παρουσιάζουν ανοχή στις επιθέσεις είναι τα «ψηφιακά πιστοποιητικά». Σε αυτού του είδους τα συστήματα οι επιθέσεις στις συναρτήσεις κατακερματισμού, μεταφράζονται σε «πλαστογραφία».

2.9.3 Πίνακες Κατακερματισμού

Οι συναρτήσεις κατακερματισμού κυρίως χρησιμοποιούνται σε πίνακες κατακερματισμού (hash tables), για γρήγορη εύρεση εγγραφών σε βάσεις δεδομένων. Για παράδειγμα σε ένα λεξικό έχουμε τις λέξεις - κλειδιά και τους αντίστοιχους ορισμούς - περιγραφές. Η συνάρτηση κατακερματισμού που μπορεί να εξυπηρετήσει αντιστοιχώντας τις λέξεις - κλειδιά με τις αντίστοιχες τιμές κατακερματισμού (ονομάζεται πίνακας κατακερματισμού - hash table).

Σε γενικές γραμμές μια συνάρτηση κατακερματισμού μπορεί να αντιστοιχίζει διαφορετικά κλειδιά στην ίδια τιμή κατακερματισμού. Τότε η τιμή κατακερματισμού αντιστοιχίζει σε ένα σύνολο από εγγραφές, αντί για μια μόνο εγγραφή. Για αυτόν ακριβώς η/οι εγγραφή/ές που αντιστοιχίζει μια τιμή κατακερματισμού ονομάζεται bucket (μεταφράζεται ως κουβάς ή κάδος και σημαίνει μονάδα αποθήκευσης). Ο πίνακας κατακερματισμού τότε ονομάζεται ευρετήριο κατακερματισμού (hash indices ή bucket indices).

Γενικότερα στην τεχνική του ευρετηρίου κατακερματισμού, η συνάρτηση κατακερματισμού μας δείχνει σε ποιο σημείο μέσα στην βάση βρίσκεται η εγγραφή. Στην πράξη μας δείχνει σε ποιο σημείο θα πρέπει να ξεκινήσουμε για την αναζήτηση.

Κεφάλαιο 3

Κλασική Κρυπτογραφία

3.1 Στεγανογραφία

Η στεγανογραφία είναι ουσιαστικά η απόκρυψη της ύπαρξης του ίδιου του μηνύματος. Παρ' όλο που η διάκρισή της, ως έννοιας, από την Κρυπτογραφία είναι πολύ λεπτή, υπάρχουν σημαντικές τεχνικές διαφοροποιήσεις ανάμεσά τους. Κατά καιρούς έχουν αναφερθεί διάφορες στεγανογραφικές μέθοδοι. Από την εποχή της αρχαιότητας αναφέρεται και η ακόλουθη -για την εποχή μας τόσο απίθανη!- μέθοδος. Εάν κάποιος ήθελε να στείλει ένα μήνυμα, έπαιρνε έναν αγγελιοφόρο, ξύριζε το κεφάλι του, έγραφε το μήνυμα που ήθελε στο ξυρισμένο κεφάλι του, περίμενε μέχρι να μεγαλώσουν τα μαλλιά του και τον έστελνε εκεί που ήθελε. Ο παραλήπτης, από την άλλη, μόλις έφτανε ο αγγελιοφόρος, του ξύριζε και πάλι το κεφάλι και διάβαζε το μήνυμα!

Μια άλλη μέθοδος χρησιμοποιεί εικόνες για τη μεταφορά κρυμμένων μηνυμάτων.

3.2 Τεχνικές Αντικατάστασης

3.2.1 Μονοαλφαβητική Αντικατάσταση

Η **μέθοδος του Καίσαρα** μπορεί να γενικευτεί εάν στη θέση του κλειδιού χρησιμοποιήσουμε έναν οποιονδήποτε αριθμό k μικρότερο του 24 και μεγαλύτερο του μηδενός. Ωστόσο, και η γενικευμένη μέθοδος του Καίσαρα δεν είναι ασφαλής, αφού υπάρχουν μόνο 23 δυνατά κλειδιά. Έτσι, η εξέταση όλων αυτών οδηγεί με βεβαιότητα στην παραβίαση (κρυπτανάλυση) του κώδικα, αν και είναι δυνατό να υποτεθεί η τιμή του k από την εξέταση της συχνότητας εμφάνισης των γραμμάτων στον κώδικα.

Ακόμα, εάν χρησιμοποιήσουμε για την κρυπτογράφηση τη σχέση $C =$

$(aM + k)mod26$ (αγγλικό αλφάβητο), όπου a μεγαλύτερος ή ίσος του 1 και σχετικά πρώτος του 26, έχουμε τον επονομαζόμενο Affine Κωδικοποιητή. Η αποκρυπτογράφηση επιτυγχάνεται με τη σχέση $M = b(C - k)mod26$, όπου b είναι ο αντίστροφος του $amod26$, δηλαδή $ab = m26 + 1$ (m οποιοσδήποτε ακέραιος). Εάν η μέθοδος αυτή, καθώς και άλλες, συνδυαστούν με τεχνικές συμπίεσης, το έργο του κρυπταναλυτή γίνεται πιο δύσκολο.

3.2.2 Πολυαλφαβητική Αντικατάσταση

Επιτρέποντας το κλειδί να έχει περισσότερες της μιας τιμής, δηλαδή κρυπτογραφώντας το πρώτο γράμμα του μηνύματος με την πρώτη τιμή του κλειδιού, το δεύτερο γράμμα του μηνύματος με τη δεύτερη τιμή του κλειδιού κ.ο.κ., επιτυγχάνουμε κάποια βελτίωση της ασφάλειας της τεχνικής της αντικατάστασης. Στην περίπτωση κλειδιού με δύο τιμές (π.χ. το κλειδί = ς ε) μπορούμε, αφού πάρουμε ανά δύο τα γράμματα του μηνύματος, το πρώτο γράμμα να το κρυπτογραφούμε, όπως προηγουμένως, με κλειδί τον αντίστοιχο αριθμό του «ς», k = 17, και το δεύτερο γράμμα του ζεύγους με κλειδί τον αντίστοιχο αριθμό του «ε», k = 5.

Ένας κωδικοποιητής (cipher) που χρησιμοποιεί πολυαλφαβητική αντικατάσταση είναι και ο Vigenere, ο οποίος έχει πάρει το όνομά του από το δημιουργό του.

3.2.3 Κωδικοποιητής του Vernam

Αν το πλήθος των γραμμάτων της λέξης - κλειδιού είναι 10, τότε κάθε δέκατο γράμμα του μηνύματος κρυπτογραφείται με το ίδιο γράμμα του κλειδιού. Το μήκος ή πλήθος των γραμμάτων του κλειδιού ονομάζεται περίοδος του κωδικοποιητή. Οι κωδικοποιητές με μεγαλύτερες περιόδους είναι σαφώς ισχυρότεροι από εκείνους με μικρότερες περιόδους. Με τη βοήθεια των υπολογιστών όμως μπορεί εύκολα να παραβιαστούν και κωδικοποιητές αντικατάστασης με πολύ μεγάλες περιόδους.

Ωστόσο, αν το μήκος του κλειδιού είναι ίσο με αυτό του μηνύματος και τα γράμματα ή σύμβολα που απαρτίζουν το κλειδί δημιουργούνται κατά τυχαίο τρόπο, τότε επιτυγχάνεται απόλυτη ασφάλεια. Η μέθοδος αυτή κρυπτογράφησης λέγεται μπλοκ μιας χρήσης (one - time pad). Η δυσκολία εφαρμογής αυτής της μεθόδου έγκειται όχι στη δημιουργία αλλά στη διανομή και αποθήκευση των κλειδιών, δηλαδή των τυχαίων ακολουθιών γραμμάτων ή συμβόλων ή αριθμών ή δυαδικών ψηφίων, από τους αποστολείς και παραλήπτες, και την απαίτηση για συγχρονισμό μεταξύ αυτών.

3.3 Δημιουργία (ψευδο-) τυχαίων ακολουθιών

Μια γεννήτρια ψευδοτυχαίων ακεραίων (Pseudo Random Number Generator - PRNG) για κρυπτογραφικές εφαρμογές ονομάζεται Κρυπτογραφικά Ασφαλής Γεννήτρια Ψευδοτυχαίων Ακεραίων - ΚΑΓΨΑ (cryptographically secure PRNG - CSPRNG).

Μια απαίτηση για μια Κρυπτογραφικά Ασφαλή Γεννήτρια Ψευδοτυχαίων Ακεραίων είναι ότι αν ο αντίπαλος δεν γνωρίζει τον «σπόρο» δεν έχει παρά ελάχιστο πλεονέκτημα για να ξεχωρίσει την έξοδο από την Γεννήτρια σε σχέση με μια τυχαία ακολουθία. Με άλλα λόγια, μια ΚΑΓΨΑ πρέπει να περνάει όλους τους στατιστικούς ελέγχους που είναι περιορισμένα σε πολυωνυμικό χρόνο σε σχέση με το μέγεθος του σπόρου. Αυτή η ιδιότητα δεν μπορεί να αποδειχθεί, αλλά μπορούν να παρουσιαστούν ισχυρά επιχειρήματα με την αναγωγή του προβλήματος ΚΑΓΨΑ σε ένα πρόβλημα που θεωρείται «δύσκολο», όπως η παραγοντοποίηση ακεραίων. Γενικά, απαιτούνται χρόνια μελέτης και έρευνας για να επιβεβαιωθεί ότι ένας αλγόριθμος δημιουργεί μια βεβαιωμένη ΚΑΓΨΑ.

Παραθέτουμε ορισμένες περιπτώσεις ΚΑΓΨΑ:

- Αλγόριθμοι κρυπτογράφησης ροών (Stream ciphers)
- Αλγόριθμοι κρυπτογράφησης που τρέχουν με λειτουργία ανάδρασης εισόδου (output feedback mode).
- Γεννήτριες Ψευδοτυχαίων Αριθμών που σχεδιάστηκαν ειδικά ώστε να είναι κρυπτογραφικά ασφαλείς, όπως η Microsoft's Cryptographic Application Programming Interface συνάρτηση CryptGenRandom, ο αλγόριθμος Yarrow (που χρησιμοποιείται στο Mac OS X και στο FreeBSD) καθώς και ο Fortuna.
- Συνδυαστικές Γεννήτριες Ψευδοτυχαίων Αριθμών που προσπαθούν να συνδυάσουν διάφορους αλγορίθμους υλοποίησης ΓΨΑ με τον στόχο να απαλείψουν όλες τις μη - τυχαιότητες.
- Διάφορες κατασκευές, βασισμένες σε υποθέσεις μαθηματικής δυσκολίας. Ορισμένα παραδείγματα: οι αλγόριθμοι Micali - Schnorr και Blum Blum Shub, που παρέχουν μια ισχυρή απόδειξη ασφάλειας. Τέτοιοι αλγόριθμοι είναι σχετικά αργοί σε σύγκριση με τις παραδοσιακές κατασκευές καθώς και μη πρακτικοί για τις περισσότερες εφαρμογές.

Κεφάλαιο 4

Ο αλγόριθμος Rabin

4.1 Αναλυτική παρουσίαση του αλγόριθμου RSA

Παραθέτουμε μια σύντομη παρουσίαση του αλγορίθμου RSA, που αποτελεί τη βάση πάνω στην οποία υλοποιήθηκε ο αλγόριθμος και το κρυπτοσύστημα Rabin.

Ο RSA είναι αλγόριθμος για κρυπτογράφηση δημοσίου κλειδιού. Βασίζεται στην υποτιθέμενη δυσκολία παραγοντοποίησης μεγάλων ακεραίων, το πρόβλημα της παραγοντοποίησης. Το ακρωνύμιο RSA σημαίνει Ron Rivest, Adi Shamir και Leonard Adleman, δηλαδή τους εισηγητές του το 1978.

Ο χρήστης του RSA πολλαπλασιάζει δυο μεγάλους πρώτους αριθμούς και δημοσιεύει το γινόμενό τους, μαζί με μια βοηθητική τιμή, σαν το δημόσιο κλειδί. Οι πρώτοι παράγοντες πρέπει να παραμείνουν μυστικοί. Ο καθένας μπορεί να χρησιμοποιήσει το δημόσιο κλειδί για να κρυπτογραφήσει ένα μήνυμα, αλλά με τις μέχρι σήμερα δημοσιευμένες μεθόδους, αν το δημόσιο κλειδί είναι αρκετά μεγάλο, μόνο όσοι ξέρουν τους πρώτους παράγοντες ρεαλιστικά μπορούν να αποκωδικοποιήσουν το μήνυμα.

Παραμένει ανοιχτό ερώτημα, γνωστό και ως το «πρόβλημα RSA», αν το σπάσιμο της κωδικοποίησης RSA είναι εξίσου δύσκολο με το πρόβλημα της παραγοντοποίησης. Αυτό το γεγονός παραμένει το βασικό μειονέκτημα του συγκεκριμένου αλγορίθμου σε σχέση με τον αλγόριθμο Rabin, του οποίου το σπάσιμο έχει αποδειχθεί ότι είναι εξίσου δύσκολο με το πρόβλημα της παραγοντοποίησης.

4.1.1 Λειτουργία

Ο RSA βασίζεται στη δυσκολία παραγοντοποίησης μεγάλων αριθμών (σήμερα, συνήθως της τάξης των 1024 με 2048 bits). Χρησιμοποιούνται δυο κλειδιά, ένα

δημόσιο κατά τη διάρκεια της κρυπτογράφησης και ένα κρυφό για την αποκρυπτογράφηση.

Δημιουργία των κλειδιών

1. Επιλογή δυο τυχαίων (μεγάλων) πρώτων αριθμών p και q έτσι ώστε $p \neq q$
2. Υπολογίζουμε $n = pq$
3. Υπολογίζουμε την συνάρτηση του Όιλερ, $\phi(n) = (p-1)(q-1)$
4. Επιλογή ενός αριθμού $e > 1$, έτσι ώστε $e \wedge \phi(n) = 1$
5. Υπολογίζουμε τον αριθμό d έτσι ώστε $de \equiv 1 mod \phi(n)$

Για την εύρεση πρώτων αριθμών χρησιμοποιούνται πιθανολογικοί αλγόριθμοι. Συνηθισμένες επιλογές είναι το 3, 7 και $2^{16}+1$. Μικροί αριθμοί οδηγούν σε ταχύτερους υπολογισμούς αλλά και σε πιο αδύνατη ασφάλεια.

Τα κλειδιά είναι τα εξής:

- δημόσιο: (n, e)
- κρυφό: (n, d)

Μπορούμε τώρα να δημοσιεύσουμε το πρώτο κλειδί, δίνοντας έτσι τη δυνατότητα σε οποιονδήποτε να μας στείλει κρυπτογραφημένα μηνύματα που μόνο εμείς (χάρη στο κρυφό κλειδί) μπορούμε να αποκρυπτογραφήσουμε.

Κρυπτογράφηση

Το μήνυμα μπορεί να αντιπροσωπευθεί από έναν αριθμό m (π.χ. «RSA» $\rightarrow$ $0x525341$, όπου $0x52$ είναι ο δεκαεξαδικός κωδικός ASCII του χαρακτήρα R. $0x53$ του S και τέλος $0x41$ του A). Το κρυπτογραφημένο μήνυμα c υπολογίζεται με τον εξής τρόπο: $c = m^e mod n$.

Αποκρυπτογράφηση

Αφού ληφθεί ένα κρυπτογραφημένο μήνυμα c, για να διαβάσουμε το αρχικό μήνυμα προβαίνουμε στον ακόλουθο υπολογισμό:

$$m = c^d mod n \equiv (m^e)^d mod n \equiv m^{ed} mod n$$

Ξέρουμε πως $ed \equiv 1(mod p-1)$ και $ed \equiv 1(mod q-1)$, οπότε με το μικρό θεώρημα του Φερμά, έχουμε:

$$m^{ed} \equiv m1 \equiv mmodp - 1 \text{ και}$$
$$m^{ed} \equiv m1 \equiv mmodq - 1$$

Οι αριθμοί p και q είναι πρώτοι μεταξύ τους, χρησιμοποιώντας λοιπόν το Κινέζικο Θεώρημα Υπολοίπων, έχουμε:

$$m^{ed} \equiv mmodn$$

Ψηφιακή υπογραφή

Ο RSA επιτρέπει την ψηφιακή υπογραφή μηνυμάτων. Αν θέλουμε να αποστείλουμε ένα υπογεγραμμένο μήνυμα, μπορούμε να το κάνουμε με τον εξής τρόπο (χρησιμοποιώντας το κρυφό κλειδί (n, d)):

$$s = m^d modn$$

Ο παραλήπτης του μηνύματος m και της υπογραφής s, υπολογίζει την τιμή s^e χάρη στο δημόσιο κλειδί (n, e) και τη συγκρίνει με το m. Αυτή η λύση, αν και λειτουργεί, δεν χρησιμοιποιείται ποτέ, για λόγους ασφαλείας. Αντί να υπογραφεί το μήνυμα ως έχει, προτιμάται η χρήση μιας συνάρτησης κατακερματοποίησης (hash function) H:

$$s = H(m)^d modn$$

Ο παραλήπτης προβαίνει στη ίδια μέθοδο, αρκεί να γνωρίζει και ποία συνάρτηση κατακερματοποίησης χρησιμοποιήθηκε.

4.1.2 Ασφάλεια και πρακτικοί προβληματισμοί

Αν και ο αλγόριθμος θεωρείται ασφαλής όταν χρησιμοποιούνται πολύ μεγάλες παράμετροι, η κακή του χρήση μπορεί να οδηγήσει σε μεγάλες αδυναμίες ασφάλειας. Εκτός από αυτό, μέχρι σήμερα κανένας δεν έχει αποδείξει ότι η ασφάλεια του εξαρτάται αποκλειστικά από την παραγοντοποίηση των ακεραίων. Επίσης, υπάρχει πάντα η πιθανότητα να ανακαλύψει κάποιος έναν αλγόριθμο (ή να έχει ήδη ανακαλύψει) ο οποίος μπορεί να παραγοντοποιεί αριθμούς σε πολυωνυμικό χρόνο.

Επίθεση επαναληπτικής κρυπτογράφησης

Αφού ο αλγόριθμος χρησιμοποιεί επαναληπτική συνάρτηση είναι δυνατός ένας τρόπος επίθεσης με τη χρήση επαναλαμβανόμενων κρυπτογραφήσεων. Αν έχουμε στην κατοχή μας το κρυπτογραφημένο μήνυμα και το δημόσιο κλειδί με

KeyGen(k): Υποθέτουμε ότι το k είναι άρτιος. Διάλεξε δυο διαφορετικούς πρώτους p και q, τυχαία, από τα διαστήματα $2^{\frac{k}{2}-1} < p,\ q < 2^{\frac{k}{2}}$. Έστω $N = p \cdot q$ έτσι ώστε $2^{k-2} < N < 2^k$ το N ν' αναπαριστάται με κ bits. Επίλεξε έναν τυχαίο ακέραιο με κ-bits e, πρώτο με τους $(p-1)$ και $(q-1)$ (ή επίλεξε $e = 2^16 + 1 = 65537$ και επέμεινε $p, q \not\equiv 1 \mod e$. Καθόρισε $d = e^{-1}(\mod \lambda(N))$, όπου το $\lambda(N) = lcm(p-1, q-1)$ είναι η **συνάρτηση λάμδα Carmichael**. Πάραξε το δημόσιο κλειδί $pk = (N, e)$ και το ιδιωτικό κλειδί $sk = (N, d)$. Μετονόμασε τα p και q, αν χρειάζεται, ώστε $p < q$. Τότε $p < q < 2 \cdot p$ και κατά συνέπεια $\sqrt{N/2} < p < \sqrt{N}$. Ορίζουμε τον χώρο μηνυμάτων εισόδου (message space) ως $M_k = \{0,1\}^{k-1}$ ή $M_k = \{0,1\}^{k-2}$ και ως χώρο κρυπτοκειμένων (ciphertext space) ως $C_k = \{0,1\}^k$.

Encrypt$(m, (N, e))$: Υποθέτουμε ότι $m \in M_k$.

- Υπολόγισε το $c = m^e (\mod N)$ (ενδεχομένως με προσθήκη «παραγεμίσματος»).
- Επίστρεψε το κρυπτοκείμενο c.

Decrypt$(c, (N, d))$: Υπολόγισε το $m = c^d (\mod N)$ και εκτύπωσε είτε το m είτε $\perp$ αν $m \notin M_k$.

Sign$(m, (N, d))$: Υπολόγισε το $s = m^d (\mod N)$.

Verify$(m, s, (N, e))$: Έλεγξε αν $m \equiv s^e (\mod N)$.

Πίνακας 4.1: Παρουσίαση του αλγορίθμου RSA και των σχημάτων ψηφιακής υπογραφής[4]

το οποίο κρυπτογραφήθηκε τότε μπορούμε να ακολουθήσουμε την εξής διαδικασία:

Κρυπτογραφούμε το ήδη κρυπτογραφημένο μήνυμα με το δημόσιο κλειδί. Επαναλαμβάνουμε τη διαδικασία κρυπτογράφησης του αποτελέσματος μέχρι να πάρουμε κείμενο ίδιο με το πρώτο κρυπτογραφημένο μήνυμα. Η αμέσως προηγούμενη κρυπτογράφηση περιέχει το αποκρυπτογραφημένο κείμενο.

Προβλήματα που οφείλονται στην κακή χρήση ή υλοποίηση

Κοινό n Αν υποθέσουμε πως έχουμε στην κατοχή μας δυο κλειδιά του τύπου (n, e_1) και (n, e_2) (δηλαδή το ίδιο n), και δυο κρυπτογραφήσεις (c_1, c_2) του ιδίου μηνύματος m με τα κλειδιά αυτά (π.χ. αν «κρυφακούμε» σε ένα δίκτυο):

$$c_1 = m^{e_1} \mod n \text{ και}$$
$$c_2 = m^{e_2} \mod n$$

μπορούμε να βρούμε το αρχικό μήνυμα m χωρίς να έχουμε πρόσβαση στα κρυφά κλειδιά. Είναι πολύ πιθανόν να έχουμε:

$$e_1 \wedge e_2 = 1$$

οπότε και με το θεώρημα του Bezout:

$$\exists (u, v), e_1 \cdot u + e_2 \cdot v = 1$$

Για να βρούμε το αρχικό μήνυμα m, υπολογίζουμε λοιπόν:

$$(c_1)^u \cdot (c_2)^v \equiv (m^{e_1})^u \cdot (m^{e_2})^v \equiv m^{e_1 \cdot u + e_2 \cdot v} \equiv m^1 \equiv m \mod n$$

Μικρό e (π.χ. e = 3) Ένα μήνυμα m κρυπτογραφείται κι αποστέλλεται από τρεις διαφορετικούς χρήστες με χρήση των δημοσίων κλειδιών $(n_1, 3)$, $(n_2, 3)$ και $(n_3, 3)$. Ο κακόβουλος χρήστης έχει λοιπόν στην κατοχή του:

- $m^3 \mod n_1$
- $m^3 \mod n_2$
- $m^3 \mod n_3$

Χάρη στο Κινεζικό Θεώρημα Υπολοίπων, μπορεί να υπολογίσει:

$$m^3 \mod n_1 \cdot n_2 \cdot n_3$$

και να βρει πια εύκολα[1] το αρχικό μήνυμα m.

[1] $m^3 < n_1 \cdot n_2 \cdot n_3$ που σημαίνει πως η κυβική ρίζα μπορεί να υπολογιστεί στο $\mathbf{N}$

Τυφλή υπογραφή Αν ένας κακόβουλος χρήστης έχει ένα κρυπτογραφημένο μύνημα c με τελικό παραλήπτη, μπορεί να μπερδέψει τον τελευταίο έτσι ώστε να του το αποκρυπτογραφήσει ο ίδιος ο παραλήπτης.

Για να αποφύγει το πρόβλημα αυτό, ο παραλήπτης δεν πρέπει να χρησιμοποιεί το ίδιο κλειδί για την υπογραφή και για την αποκρυπτογράφηση μηνυμάτων, ούτε όμως και να υπογράφει ό,τι του ζητούν «στα τυφλά».

Το κρυπτοσύστημα Rabin αποτελεί μια ασύμμετρη κρυπτογραφική τεχνική, που, όπως και ο RSA, σχετίζεται με τη δυσκολία της παραγοντοποίησης. Παρ' όλα αυτά, ο αλγόριθμος Rabin έχει το πλεονέκτημα ότι το πρόβλημα πάνω στο οποίο βασίζεται έχει αποδειχθεί εξίσου δύσκολο με την **παραγοντοποίηση ακεραίων**, πράγμα που δεν έχει αποδειχθεί ακόμα για τον αλγόριθμο RSA. Έχει το μειονέκτημα ότι κάθε έξοδος της συνάρτησης Rabin μπορεί να παραχθεί από οποιαδήποτε από τις τέσσερις πιθανές εισόδους. Αν κάθε έξοδος είναι κρυπτογραφημένη, απαιτείται επιπλέον πολυπλοκότητα για την αποκρυπτογράφηση ώστε να εντοπίσει ποια από τις τέσσερις πιθανές εισόδους είναι το πραγματικό κείμενο.

Ο αλγόριθμος Rabin είναι βασικά ο RSA με την βέλτιστη επιλογή για το e, συγκεκριμένα $e = 2$. Η ασφάλεια του Rabin σχετίζεται περισσότερο με την παραγοντοποίηση σε σχέση με τον RSA.

4.2 Ιστορία

Ο αλγόριθμος δημοσιεύτηκε τον Ιανουάριο του 1979 από τον Michael O. Rabin. Το κρυπτοσύστημα Rabin ήταν το πρώτο μη-συμμετρικό κρυπτοσύστημα όπου η ανάκτηση ολόκληρου του κειμένου εισόδου από το κρυπτογραφημένο κείμενο αποδείχθηκε εξίσου δύσκολο με την παραγοντοποίηση ακεραίων.

Στον εισηγητή του αλγορίθμου έχει απονεμηθεί το βραβείο Turing, δηλαδή το Νόμπελ της Επιστήμης των Υπολογιστών (για άλλη εργασία του).

4.3 Δημιουργία κλειδιού

Όπως όλα τα κρυπτοσυστήματα ασύμμετρου κλειδιού, το κρυπτοσύστημα Rabin χρησιμοποιεί δυο κλειδιά, ένα δημόσιο και ένα ιδιωτικό. Το δημόσιο κλειδί είναι απαραίτητο για κωδικοποίηση και μπορεί να δημοσιευτεί, όμως το ιδιωτικό κλειδί πρέπει να επεξεργαστεί μόνο από τον παραλήπτη του μηνύματος.

Η ακριβής διαδικασία δημιουργίας κλειδιού ακολουθεί:

- Επίλεξε δυο διαφορετικούς μεγάλους πρώτους p και q. Μια συχνή επιλογή είναι $p = q = 3(mod4)$, για την απλοποίηση του υπολογισμού των

KeyGen(k): Δημιούργησε δυο τυχαίους $k/2$-bits ακεραίους p και q, έτσι ώστε $p \equiv q \equiv 3 (\mod 4)$ και θέσε $N = p \cdot q$. Πάραξε το δημόσιο κλειδί $pk = N$ καθώς και το ιδιωτικό κλειδί $sk = (p, q)$. Υποθέτουμε ότι ο χώρος κειμένων εισόδου και κρυπτοκειμένων είναι $C_k = M_k = (Z/NZ)^*$.
Encrypt$(m, (N, e))$: Υποθέτουμε ότι $m \in M_k$.
Decrypt$(c, (N, d))$: Υπολόγισε το $m = c^d (\mod N)$ και εκτύπωσε είτε το m είτε $\perp$ αν $m \notin M_k$.
Sign$(m, (N, d))$: Υπολόγισε το $s = m^d (\mod N)$.
Verify$(m, s, (N, e))$: Έλεγξε αν $m \equiv s^e (\mod N)$.

Πίνακας 4.2: Παρουσίαση του αλγορίθμου Rabin[4]

τετραγωνικών ριζών *modulop* και q. Ο αλγόριθμος δουλεύει με οποιουσδήποτε πρώτους.

- Έστω $n = p \cdot q$. Το n αποτελεί το δημόσιο κλειδί. Οι πρώτοι p και q αποτελούν το ιδιωτικό κλειδί.

Για την κρυπτογράφηση ενός μηνύματος, απαιτείται μόνο το δημόσιο κλειδί n. Για να αποκωδικοποιηθεί το κρυπτογραφημένο κείμενο, είναι απαραίτητοι οι δυο παράγοντες p και q του δημοσίου κλειδιού n.

Ας δούμε ένα παράδειγμα (ακατάλληλο για πραγματικό πρόβλημα): αν $p = 5$, $q = 13$ τότε $n = p \cdot q = 65$. Το δημόσιο κλειδί (δηλ. το 65) θα δημοσιευτεί, καθώς και το κρυπτογραφημένο κείμενο θα αποσταλεί. Επίσης, για να αποκρυπτογραφηθεί το μήνυμα, τα ιδιωτικά κλειδιά 5 και 13, θα πρέπει να είναι γνωστά στον παραλήπτη. (Φυσικά, η επιλογή των κλειδιών είναι ανεπιτυχής, καθώς η παραγοντοποίηση του 65 είναι προφανής, στην πραγματικότητα θα είχαν απαιτηθεί πολύ μεγαλύτεροι πρώτοι).

4.4 Κρυπτογράφηση

Για την κωδικοποίηση, χρησιμοποιείται μόνο το δημόσιο κλειδί n, παράγοντας το κρυπτογραφημένο κείμενο από το κείμενο εισόδου. Η διαδικασία ακολουθεί:

Έστω $P = \{0, 1, ..., n-1\}$ ο χώρος κειμένων εισόδου (αποτελούμενος από αριθμούς) και $m \in P$ είναι το κείμενο εισόδου. Το κρυπτογραφημένο κείμενο c υπολογίζεται ως εξής:

$$c = m^2 \mod n$$

Ας δούμε ένα απλό παράδειγμα: έστω $P = \{0, 1, ..., 75\}$ ο χώρος κειμένων εισόδου. Επιλέγουμε $m = 27$ ως κείμενο εισόδου. Το κρυπτοκείμενο είναι κατά συνέπεια $c = m^2 \mod n = 27^2 \mod 65 = 14$. Το συγκεκριμένο αποτέλεσμα 14 μπορεί να επιτευχθεί από ακριβώς τέσσερις εισόδους, τις: $\{12, 27, 38, 53\}$. Αυτό είναι αληθές για τα περισσότερα κρυπτογραφημένα κείμενα που προκύπτουν από τον αλγόριθμο Rabin, δηλαδή είναι μια συνάρτηση 4-1.

4.4.1 Απλό παράδειγμα υλοποίησης του αλγορίθμου Rabin

Ακολουθεί ένα απλό παράδειγμα υλοποίησης του υπό εξέταση αλγορίθμου, γραμμένο σε γλώσσα προγραμματισμού C.

```
#include <stdio.h>

#define LEN 76
#define P 5
#define Q 13

int main(void)
{
int i, plain[LEN], cipher[LEN], N = P*Q;

for (i=0; i<LEN; i++) {
plain[i] = i;
cipher[i] = ((plain[i])*(plain[i])) % N;
}

for (i=0; i<LEN; i++) {
printf("%d\t%d\n", plain[i], cipher[i]);
}

return 0;
}
```

4.5 Αποκρυπτογράφηση

Για την αποκρυπτογράφηση, τα ιδιωτικά κλειδιά είναι απαραίτητα. Η διαδικασία ακολουθεί:

Αν τα c και r είναι γνωστά, τότε το κείμενο εισόδου είναι $m \in \{0, 1, ..., n-1\}$ και $m^2 \equiv c(\mod r)$. Για τον σύνθετο r (όπως και αυτός που προκύπτει από τον αλγόριθμο του Rabin: $n = pq$) δεν υπάρχει γνωστή αποδοτική μέθοδος για την εύρεση του m. Αν ο r είναι πρώτος, (όπως είναι οι p και q από τον αλγόριθμο του Rabin), μπορούμε να εφαρμόσουμε το **Κινέζικο Θεώρημα Υπολοίπων**[2] για την εύρεση του m.

Κατά συνέπεια, πρέπει να υπολογιστούν οι τετραγωνικές ρίζες[3]:

$$m_p = \sqrt{c} \mod p \text{ και}$$
$$m_q = \sqrt{c} \mod q.$$

Εφαρμόζοντας τον Επεκταμένο Αλγόριθμο του Ευκλείδη[4], θέλουμε να βρούμε τα y_p και y_q ώστε:

$$y_p \cdot p + y_q \cdot q = 1$$

Τώρα, με τη χρήση του Κινέζικου Θεωρήματος Υπολοίπων, βρίσκουμε τις τέσσερις τετραγωνικές ρίζες $+r, -r, +s, -s$, οι οποίες βρίσκονται στο σύνολο $\{0, 1, ..., n-1\}$.

$$r = (y_p \cdot p \cdot m_q + y_q \cdot q \cdot m_p) \mod n$$
$$-r = n - r$$
$$s = (y_p \cdot p \cdot m_q - y_q \cdot q \cdot m_p) \mod n$$
$$-s = n - s$$

Μια απ' αυτές τις τετραγωνικές ρίζες $\mod n$ είναι το αρχικό κείμενο. Ο Rabin υπέδειξε στη δημοσίευσή του ότι αν κάποιος μπορεί να υπολογίσει τα r και s, τότε μπορεί να βρει την παραγοντοποίηση του n διότι είτε $\gcd(|r-s|, n) = p$ είτε $\gcd(|r-s|, n) = q$ όπου gcd σημαίνει Μέγιστος Κοινός Διαιρέτης. Από

[2]Το Κινέζικο θεώρημα υπολοίπων μας παρέχει μια μέθοδο επίλυσης συστημάτων γραμμικών ισοτιμιών. Οι λύσεις μπορούν να βρεθούν χρησιμοποιώντας έναν εύκολο και αποδοτικό αλγόριθμο. Στη βασική του μορφή, το Κινέζικο Θεώρημα Υπολοίπων θα βρει έναν αριθμό n, που όταν διαιρεθεί με ορισμένους διαιρέτες δίνει ορισμένα υπόλοιπα.

[3]Ορισμός: Τετραγωνική ρίζα ενός μη αρνητικού αριθμού a (συμβολικά: $\sqrt{a}$), ονομάζουμε ένα μη αρνητικό αριθμό x με την ιδιότητα : $x^2 = a$ δηλ. $\sqrt{a} = x \Leftrightarrow x^2 = a$.

[4]Αποτελεί επέκταση του αλγορίθμου του Ευκλείδη. Πέρα από την εύρεση του μέγιστου κοινού διαιρέτη δυο ακεραίων a και b, όπως κάνει ο απλός αλγόριθμος του Ευκλείδη, επίσης υπολογίζει δυο ακεραίους x και y (από τους οποίους ο ένας συνήθως είναι αρνητικός), που ικανοποιούν την ταυτότητα του *Bézout*: $a \ x + b \ y = \gcd(a, b)$. Ο Επεκταμένος Αλγόρθμος του Ευκλείδη είναι ιδιαιτέρως χρήσιμος όταν οι αριθμοί a και b είναι πρώτοι μεταξύ τους.

τη στιγμή που ο Μέγιστος Κοινός Διαιρέτης μπορεί να υπολογιστεί αποτελεσματικά, μπορεί να βρεθεί η παραγοντοποίηση του n αποδοτικά, αρκεί να ξέρεις τα r και s.

4.6 Υπολογισμός τετραγωνικών ριζών

Η αποκρυπτογράφηση απαιτεί τον υπολογισμό των τετραγωνικών ριζών του κρυπτογραφημένου κειμένου c modulo τους ακεραίους p και q. Επιλέγοντας $p \equiv q \equiv 3 \mod 4$ μπορούμε να υπολογίσουμε τις τετραγωνικές ρίζες m_p και m_q ως εξής:

$$m_p = c^{\frac{p+1}{4}} \mod p \text{ και}$$
$$m_q = c^{\frac{q+1}{4}} \mod q$$

4.6.1 Παράδειγμα

Η υπόθεση ότι $p \equiv 3(\mod 4)$, υποννοεί ότι ο αριθμός $\frac{(p+1)}{4}$ είναι ακέραιος. Η υπόθεση είναι τετριμμένη για $c \equiv 0(\mod p)$. Άρα, μπορούμε να υποθέσουμε ότι ότι ο p δεν διαιρεί τον c. Τότε,

$$m_p^2 \equiv c^{\frac{p+1}{2}} \equiv c \cdot c^{\frac{p-1}{2}}$$

Αν $c \equiv m^2(\mod pq)$ προκύπτει ότι $c \equiv m^2(\mod p)$. Άρα ο c είναι **τετραγωνικό υπόλοιπο** modulo p, γεγονός που συνεπάγεται ότι $m_p^2 \equiv c(\mod p)$.

Η σχέση $p \equiv 3(\mod 4)$ δεν είναι προαπαιτούμενη, γιατί οι τετραγωνικές ρίζες modulo με άλλους ακεραίους μπορούν επίσης να υπολογιστούν. Για παράδειγμα, ο Rabin προτείνει οι τετραγωνικές ρίζες modulo με άλλους ακεραίους να βρεθούν με τη χρήση μιας ειδικής περίπτωσης του αλγορίθμου του Berlekamp[5].

4.7 Εφαρμογές του αλγορίθμου

Είναι ευρέως γνωστό ότι η κρυπτογραφία δημοσίου κλειδιού εμφανίστηκε για να ρυθμίσει τα δυο βασικά ελαττώματα της κρυπτογραφίας συμμετρικού κλειδιού:

- **Το πρόβλημα του διαμοιρασμού κλειδιού** - Πριν την εξασφάλιση ασφαλούς επικοινωνίας σε επισφαλή κανάλια (με τη χρησιμοποίηση

[5] Ο αλγορίθμος του Berlekamp είναι μια γνωστή μέθοδος παραγοντοποίησης πολυωνύμων σε πεπερασμένα πεδία (επίσης γνωστά και ως πεδία Galois).

κρυπτογράφησης δεδομένων), οι συμμετέχοντες ήταν υποχρεωμένοι να βασίζονται στην ανταλλαγή των κλειδιών κωδικοποίησης - αποκωδικοποίησης με τη χρήση ασφαλών καναλιών, διαφορετικών από αυτών που χρησιμοποιούνται για την ίδια την επικοινωνία.

- **Το πρόβλημα της αυθεντικοποίησης** - Η κρυπτογραφία συμμετρικού κλειδιού δεν παρείχε κανένα μέσο αυθεντικοποίησης στα μέρη που εμπλέκονται στην επικοινωνία, όπως και κανένα στοιχείο για την ακεραιότητα δεδομένων του μεταδιδόμενου μηνύματος.

Παρ' όλα αυτά, αφού τα κρυπτοσυστήματα δημοσιού κλειδιού είναι αρκετές τάξεις μεγέθους (εκατοντάδες φορές για να είμαστε υπολογιστικά ακριβείς) αργότερα από τα κρυπτοσυστήματα συμμετρικού κλειδιού, τα πρώτα δεν μπορούν να υπερισχύσουν στα δεύτερα. Με αυτά ως δεδομένα, ο ρόλος των κρυπτοσυστημάτων δημοσίου κλειδιού είναι περιορισμένος στο να παρέχει βοηθητική υποστήριξη στα ήδη υπάρχοντα κρυπτοσυστήματα ιδιωτικού κλειδιού. Κατά συνέπεια, οι πραγματικές εφαρμογές των κρυπτοσυστημάτων δημοσίου κλειδιού, ειδικά του κρυπτοσυστήματος Rabin, μπορούν να συνοψιστούν ως εξής:

1. **Κρυπτογράφηση μικρών ποσοτήτων δεδομένων** - Η μεγάλη απόκλιση όσον αφορά το χρόνο για τα δυο είδη κρυπτοσυστημάτων, γίνεται λιγότερο σημαντική όταν πρέπει να κρυπτογραφηθούν και ν' αποκρυπτογραφηθούν μικρές ποσότητες δεδομένων. Αν τέτοια δεδομένα πρόκειται να μεταφερθούν μέσω μη ασφαλούς σύνδεσης, τότε η κρυπτογραφία δημόσιου κλειδιού γίνεται η μοναδική λογική επιλογή. Τέτοιες πρακτικές εφαρμογές είναι οι *τραπεζικές συναλλαγές μέσω Ίντερνετ*, όταν ο χρήστης παρέχει τα στοιχεία του τραπεζικού του λογαριασμού (ή πιστωτικής κάρτας κλπ.) μέσω γραφικής διεπαφής (ιστοσελίδα).[20]

2. **Ανταλλαγή κλειδιών συμμετρικών κρυπτοσυστημάτων** - Ο διαχειριστής ενός δικτύου υπολογιστών, είτε αυτό είναι LAN είτε εικονικό (virtual private network), μπορεί να διακινήσει ένα κοινό συμμετρικό κλειδί (όπως το κλειδί AES) σε όλους. Αυτό το κλειδί μπορεί να χρησιμοποιηθεί για να ασφαλίσει (μέσω κρυπτογράφησης) οποιαδήποτε μελλοντική επικοινωνία μεταξύ των συμμετεχόντων στο δίκτυο.

3. **Ψηφιακές υπογραφές** - Έχουν αναλυθεί εκτενώς σε άλλα υποκεφάλαια.

4.8 Αξιολόγηση του αλγορίθμου

4.8.1 Αποτελεσματικότητα του αλγορίθμου

Η αποκωδικοποίηση παράγει τρία λανθασμένα αποτελέσματα μαζί με το σωστό, έτσι ώστε το σωστό κείμενο εισόδου πρέπει να μαντευτεί. Αυτό αποτελεί το μέγιστο μειονέκτημα του κρυπτοσυστήματος Rabin και αποτελεί έναν από τους παράγοντες που έχουν αποτρέψει ευρεία πρακτική χρήση αυτού του αλγορίθμου.

Αν το κείμενο εισόδου πρόκειται να αναπαραστήσει ένα μήνυμα κειμένων, η μαντεψιά δεν είναι δύσκολη. Αν, παρ' όλα αυτά, το κείμενο πρόκειται να αναπαραστήσει μια αριθμητική τιμή, αυτό το θέμα δημιουργεί πρόβλημα που πρέπει να επιλυθεί με τη χρήση κάποιου είδους αποσαφήνισης. Είναι πιθανό να επιλεχθούν κείμενα εισόδου με ειδικές δομές, ή να εισαχθεί περισσότερη πληροφορία για να αντιμετωπιστεί αυτό το πρόβλημα. Μια μέθοδος απάλειψης της αμφιβολίας αντιστροφής προτάθηκε από τους Blum και Williams: οι δυο πρώτοι που χρησιμοποιούνται ως ιδιωτικά κλειδιά

4.8.2 Αποδοτικότητα

Για την κρυπτογράφηση, πρέπει να υπολογιστεί ένα τετράγωνο modulo n. Αυτό είναι πιο αποτελεσματικό από τον αλγόριθμο RSA, που απαιτεί τον υπολογισμό τουλάχιστον ενός κύβου.

Για την αποκρυπτογράφηση, εφαρμόζεται το Κινέζικο Θεώρημα Υπολοίπων, μαζί με δυο υψώσεις υπολοίπων σε κάποια δύναμη. Εδώ η αποδοτικότητα είναι παρόμοια με τον RSA.

Η αποσαφήνιση εισάγει επιπλέον υπολογιστικά κόστη, και αυτή είναι η βασική αιτία που έχει εμποδίσει την πλατιά πρακτική διάδοση του κρυπτοσυστήματος Rabin.

4.8.3 Ασφάλεια

Το βασικό πλεονέκτημα του κρυπτοσυστήματος Rabin είναι ότι η τυχαία είσοδος μπορεί να εξαχθεί από το κρυπτογραφημένο κείμενο μόνο αν ο αποκωδικοποιητής είναι ικανός να παραγοντοποιήσει αποτελεσματικά το δημόσιο κλειδί n. Αξίζει να σημειωθεί ότι αυτό είναι αρκετά χαμηλό επίπεδο ασφαλείας. Διάφορες επεκτάσεις του αλγορίθμου Rabin μπορούν να πετύχουν αρκετά υψηλότερα επίπεδα ασφάλειας.

Έχει αποδειχθεί ότι η αποκωδικοποίηση του κρυπτοσυστήματος Rabin είναι εξίσου «δύσκολη» με το πρόβλημα της παραγοντοποίησης ακεραίων, αρκετά διαφορετικό από τον RSA. Κατά συνέπεια τα συστήματα Rabin είναι «πιο ασφαλή» κατ' αυτή την έννοια από τα RSA, και θα παραμείνει έτσι μέχρι την

ανακάλυψη μιας γενικής λύσης του προβλήματος της παραγοντοποίησης ακεραίων ή να αποδειχθεί ότι η αποκωδικοποίηση του RSA είναι εξίσου «δύσκολη» με το πρόβλημα της παραγοντοποίησης ακεραίων.

4.9 Το σχήμα ψηφιακών υπογραφών Rabin

Το Σχήμα Ψηφιακής Υπογραφής Rabin στην Κρυπτογραφία, είναι μια μέθοδος ψηφιακής υπογραφής που προτάθηκε από τον Micahel O. Rabin το 1979. Πρόκειται για ένα από τα πρώτα σχήματα ψηφιακής υπογραφής που είχαν προταθεί, καθώς και το πρώτο που συνέδεε τη δυσκολία πλαστογραφίας με το πρόβλημα της παραγοντοποίησης ακεραίων. Λόγω της απλότητάς του και του κυρίαρχου ρόλου που έπαιζε στην πρώιμη κρυπτογραφία δημοσίου κλειδιού, το Σχήμα Ψηφιακής Υπογραφής Rabin καλύπτεται σχεδόν σε όλα τα πανεπιστημιακά συγγράμματα για την κρυπτογραφία. Θεωρείται μη - πλαστογραφήσιμο στον βαθμό που το πρόβλημα της παραγοντοποίησης ακεραίων παραμένει δυσεπίλυτο. Το Σχήμα Ψηφιακής Υπογραφής Rabin, φυσικά, είναι στενά συνδεδεμένο με το κρυπτοσύστημα Rabin.

4.9.1 Παρουσίαση του αλγορίθμου

Ο αλγόριθμος βασίζεται σε μια ανθεκτική στις συγκρούσεις συνάρτηση κατακερματισμού: $H : \{0,1\} \to \{0,1\}^k$.

Δημιουργία κλειδιού

- Ο υπογράφων S διαλέγει πρώτους ακεραίους p, q μεγέθους $k/2$ bits ο καθένας και υπολογίζει το γινόμενο $n = p \cdot q$.
- Ο S διαλέγει ένα τυχαίο b στο διάστημα $\{0, 1, \ldots, n\}$.
- Το δημόσιο κλειδί είναι το (n, b).
- Το ιδιωτκό κλειδί είναι το (p, q).

Υπογραφή

- Για να υπογράψει ένα μήνυμα m, ο αποστολέας S διαλέγει τυχαίο «παραγέμισμα» (padding) U και υπολογίζει το $H(mU)$.
- Ο S επιλύει το $x \cdot (x + b) = H(mU) \mod n$.

- Αν δεν υπάρχει λύση, τότε ο S διαλέγει καινούριο «παραγέμισμα» και ξαναδοκιμάζει. Αν η H είναι πραγματικά τυχαία, τότε ο αναμενόμενος αριθμός προσπαθειών είναι τέσσερις.
- Η υπογραφή στο m είναι το ζεύγος (U, x).

Πιστοποίηση

- Δοθέντος ενός μηνύματος m και της υπογραφής (U, x) ο πιστοποιητής V υπολογίζει το $x \cdot (x + n)$ και το $H(mU)$ και βεβαιώνει ότι είναι ίσα.

4.10 Υλοποίηση σε C

Παραθέτουμε μια απλή υλοποίηση του κρυπτοσυστήματος Rabin και των βασικών συναρτήσεών του.

4.10.1 rabin.c

```
#include <stdio.h>
#include <math.h>

/* to par'adeigma 'eqei epilege'i ap'o:
http://en.wikipedia.org/wiki/Rabin_cryptosystem */

#define LEN 76
/* epilog'h idiwtiko'u kleidio'u */
#define P 7
#define Q 11

int rabin_key_generation(void);
int rabin_encryption(int);
int rabin_decryption(int);
void extended_euclid(int, int, int *, int *, int *);

int main(void)
{
int i, plain[LEN], cipher[LEN];

for (i=0; i<LEN; i++) {
plain[i] = i;
cipher[i] = rabin_encryption(plain[i]);
```

```
printf("%d\t%d\n", plain[i], cipher[i]);
}

rabin_decryption(15);

return 0;
}

/* sun'arthsh dhmiourg'ias dhmos'iou kleidio'u */
int rabin_key_generation(void)
{
return P*Q;
}

/* sun'arthsh pou epistr'efei thn kruptogr'afhsh Rabin en'os arijmo'u */
int rabin_encryption(int m)
{
return ((m*m) % rabin_key_generation());
}

/* sun'arthsh pou epistr'efei thn apokruptogr'afhsh Rabin
en'os kruptokeim'enou (arijmo'u) */
int rabin_decryption(int c)
{
/* r1, r2, s1, s2 e'inai oi 4 pijan'es apokruptograf'hseis */
int m_p, m_q, y_p, y_q, d=1, r1, r2, s1, s2;
m_p = c^((P+1)/4) % P;
m_q = c^((Q+1)/4) % Q;

extended_euclid(P, Q, &y_p, &y_q, &d);
//printf("%d, %d", y_p, y_q);

r1 = (y_p * P * m_q + y_q * Q * m_p) % (P*Q);
r2 = (P*Q) - r1;
s1 = (y_p * P * m_q - y_q * Q * m_p) % (P*Q);
s2 = (P*Q) - r1;

printf("\n\n%d, %d, %d, %d\n", r1%(P*Q), r2%(P*Q), s1%(P*Q), s2%(P*Q));

return 0;
}
```

```
void extended_euclid(int a, int b, int *x, int *y, int *d)
/* upolog'izei a * (*x) + b * (*y) = gcd(a, b) = (*d) */
{
  int q, r, x1, x2, y1, y2;

  if (b == 0) {
    *d = a, *x = 1, *y = 0;
    return;
  }
  x2 = 1, x1 = 0, y2 = 0, y1 = 1;
  while (b > 0) {
    q = a / b, r = a - q * b;
    *x = x2 - q * x1, *y = y2 - q * y1;
    a = b, b = r;
    x2 = x1, x1 = *x, y2 = y1, y1 = *y;
  }
  *d = a, *x = x2, *y = y2;
}
```

4.10.2 Αξιολόγηση

Η παραπάνω υλοποίηση σε C είναι απλή «μεταγραφή» των ψευδοκωδίκων που υπάρχουν στη βιβλιογραφία. Έγινε δοκιμή για μικρές τιμές πρώτων ακεραίων (7 και 11), μπορεί εύκολα να δοκιμαστεί για μεγαλύτερους.

Κεφάλαιο 5

Επίλογος

Η παρούσα Πτυχιακή μελέτησε το θέμα της Κρυπτογραφίας και ειδικότερα το κρυπτοσύστημα που υλοποιεί τον αλγόριθμο του Rabin. Προηγήθηκε σύντομη παρουσίαση βασικών σημείων των θεωρητικών βάσεων της Κρυπτογραφίας, ιστορική αναδρομή, παρουσίαση των βασικών ταξινομήσεων των κρυπταλγορίθμων αλλά και επιγραμματική αναφορά των εφαρμογών της.

Ακολούθησε αναλυτική παρουσίαση του αλγορίθμου RSA, καθώς και στη συνέχεια του Rabin που αποτελεί βελτίωση του RSA. Επιχειρήθηκε μια σύγκριση αυτών των δυο αλγορίθμων. Η παρουσίαση περιλάμβανε επιγραμματική ιστορική αναδρομή, παρουσίαση του αλγορίθμου (δηλαδή τα βασικά σημεία), των βασικών χρήσεων, κριτική της ασφάλειας και της αποδοτικότητας καθώς και το σχήμα των ψηφιακών υπογραφών.

Τέλος, έγινε υλοποίηση του κρυπτοσυστήματος Rabin για αριθμητική είσοδο, καθώς και της διαδικασίας αποκρυπτογράφησης, γραμμένες σε γλώσσα C.

Βιβλιογραφία

[1] http://el.wikipedia.org/wiki/Κρυπτογραφία

[2] Hans Delfs. Helmut Knebl: Introduction to Cryptography, Principles and Applications. 2nd Edition

[3] Tilborg, Encyclopedia of Cryptography and Security

[4] Steven Galbraith, Mathematics of Public Key Cryptography

[5] Alfred J. Menezes et al, Handbook of Applied Cryptography

[6] Βασίλειος Ζορκάδης, Κρυπτογραφία. Εκδόσεις Ελληνικού Ανοιχτού Πανεπιστημίου

[7] http://el.wikipedia.org/wiki/RSA

[8] http://en.wikipedia.org/wiki/Rabin_cryptosystem

[9] Rabin. Michael. Digitalized Signatures and Public-Key Functions as Intractable as Factorization. MIT Laboratory for Computer Science, January 1979.

[10] John Talbot, Dominic Welsh, Complexity and Cryptography, An Introduction

[11] Bruce Schneier. Applied Cryptography

[12] Wenbo Mao, Modern Cryptography Theory and Practice

[13] Mihir Bellare. Phillip Rogaway, The Exact Security of Digital Signatures - How to Sign with RSA and Rabin

[14] Mark Stamp, Richard M. Low, Applied Cryptanalysis

[15] Nick Galbreath, Cryptogrphy for Internet and Database Applications

[16] Oded Goldreich, Foundations of Cryptography Basic Techniques

[17] Henk van Tilborg, Fundamentals of Cryptology

[18] Jeffrey Hoffstein, Jill Pipher, Joseph Silverman, An Introduction to Mathematical Cryptography

[19] Rolf Oppliger, Contemporary Cryptography

[20] Mihnea Radulescu, Public - Key Cryptography: The RSA and the Rabin Cryptosystems