Π Α Ν Ε Π Ι Σ Τ Η Μ Ι Ο Π Α Τ Ρ Ω Ν

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

& ΠΛΗΡΟΦΟΡΙΚΗΣ

Ε Ρ Γ Α Σ Ι Α Ε Ξ Α Μ Η Ν Ο Υ

ΓΙΑ ΤΟ ΜΑΘΗΜΑ

ΔΙΚΤΥΑ ΔΗΜΟΣΙΑΣ ΧΡΗΣΗΣ

ΚΑΙ ΔΙΑΣΥΝΔΕΣΗ ΔΙΚΤΥΩΝ

ΚΡΥΠΤΟΓΡΑΦΙΑ

ΚΥΡΙΑΚΟΥ ΑΝΔΡΟΝΙΚΟΣ

Α.Μ : 235806

ΔΙΔΑΣΚΩΝ: ΧΡΗΣΤΟΣ ΜΠΟΥΡΑΣ

ΠΑΤΡΑ 2017

ΠΕΡΙΕΧΟΜΕΝΑ

ΑΚΡΩΝΥΜΙΑ

AES: Advanced Encryption Standard

CA: Certification Auhority

DES: Data Encryption Standard

DSA: Digital Signature Algorithm

ECES: Elliptic Curve Encryption Scheme

FIPS: Federal Information Processing Standard

IEC: International Electrotechnical Commission

IETF: Internet Engineering Task Force

ISO: International Organization for Standardization

KDC: Key Distribution Center

KTC: Key Translation Center

MD: Message Digest

MIT: Massachusetts Institute of Technology

NESSIE: New European Schemes for Signature, Integrity and Encryption

NIST: National Institute of Standards and Technology

NSA: National Security Agency

PKI: Public Key Infrastructure

RA: Registration Authority

RC4: Rivest Cipher 4

RSA: Rivest, Shamir, Adleman

SHA: Secure Hash Algorithm

TLS: Transport Layer Security

WEP: Wired Equivalent Privacy

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

1.1 Εισαγωγή

Ο όρος Κρυπτογραφία προέρχεται από τις Ελληνικές λέξεις «κρυπτός» (κρυμμένος) και «γράφω». Η ανάγκη για μυστική, αποτελεσματική επικοινωνία ώθησε την ανθρωπότητα από τα αρχαία χρόνια να ανακαλύψει τεχνικές συγκάλυψης μηνυμάτων έτσι ώστε να μπορούν να αναγνωστούν μόνο από τον επιθυμητό παραλήπτη. Στη σημερινή εποχή, που ο κόσμος περιστρέφεται γύρω από την Πληροφορία και ο όγκος των μηνυμάτων (σε οποιαδήποτε μορφή και αν είναι αυτά) που ανταλλάσσονται αγγίζει τα όρια του αναρίθμητου, είναι πιο σημαντικό από ποτέ να μπορούμε να διασφαλίσουμε τόσο την μυστικότητα όσο και την ακεραιότητα της Πληροφορίας. Σε αυτή την εργασία, γίνεται μια προσπάθεια να παρουσιαστούν οι σύγχρονοι μέθοδοι που εφαρμόζονται στην καθημερινότητα των ανθρώπων για την ασφαλή μεταφορά μηνυμάτων πάνω από δικτυακά κανάλια καθώς και οι τρόποι με τους οποίους εξασφαλίζεται η ταυτοποίηση των δυο συμπραττόμενων μερών που προσπαθούν να επικοινωνήσουν.

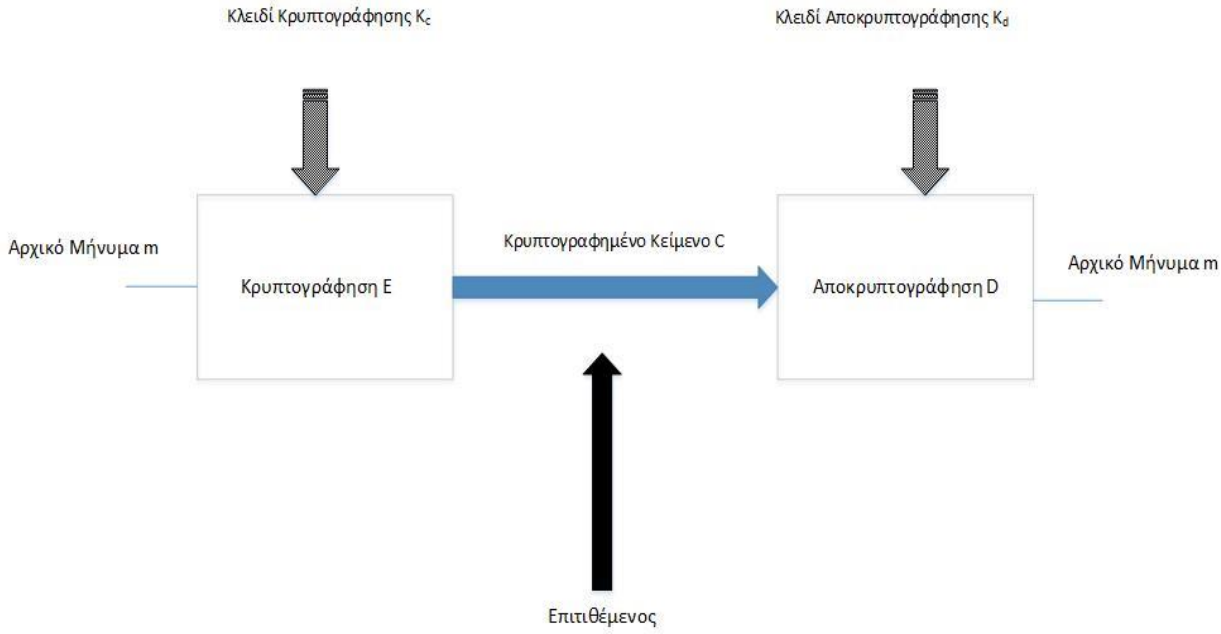
1.2 Ιστορική Αναδρομή

Τα χνάρια της Κρυπτογραφίας εμφανίζονται για πρώτη φορά στην Αρχαία Σπάρτη κατά τον 5ο Αιώνα π.Χ. Εκείνη την περίοδο η μέθοδος που είχε αναπτυχθεί για την ασφαλή κωδικοποίηση των μηνυμάτων ήταν αυτή της *μετάθεσης*. Η μέθοδος αυτή αλλάζει θέση στα γράμματα ενός μηνύματος και έτσι δημιουργεί αναγραμματισμούς. Στην καταγεγραμμένη υλοποίηση, ο αποστολέας ενός μηνύματος τυλίγει γύρω από μια σκυτάλη ένα κομμάτι από δέρμα ή περγαμηνή και γράφει πάνω σε αυτό το μήνυμα του. Ύστερα, η λωρίδα ξετυλίγεται και μπορεί να διαβαστεί μόνο αν εφαρμοστεί σε σκυτάλη ίδιας διαμέτρου με αυτή της αρχικής. Η μέθοδος της μετάθεσης συνέχισε να αναπτύσσεται και στα νεότερα χρόνια μέχρι που για πρώτη φορά εμφανίστηκε βιβλιογραφικά στους Γαλατικούς Πολέμους του Ιουλίου Καίσαρα η μέθοδος της *υποκατάστασης*. Σε αυτή την τεχνική κάθε γράμμα του αλφαβήτου αντικαθίσταται με το κατά 3 θέσεις επόμενο στο αλφάβητο και έτσι το μήνυμα καθίσταται ακατανόητο, ενώ αργότερα, υποστηρίχθηκε και η χρήση διαφορετικού αριθμού θέσεων για την δημιουργία νέων κρυπτογραμμάτων. Τους επόμενους αιώνες, η κρυπτογράφηση των μηνυμάτων βασίστηκε στην χρήση παραπάνω του ενός κρυπτογραφικών αλφαβήτων (π.χ.

κώδικας Vigenère, ο οποίος χρησιμοποιεί 24 αλφάβητα) και αυτό ήταν αρκετό μέχρι τα τέλη του 19ου αιώνα όταν και ο Charles Babbage βρέθηκε σε θέση να το κρυπταναλύσει επιτυχώς. Η μεγάλη επανάσταση έγινε κατά την μηχανοποίηση της Κρυπτογραφίας, γύρω στο 1920, όταν και κατασκευάστηκε η πρώτη μηχανή Enigma. Η λειτουργία αυτής της μηχανής, αλλά και των επόμενων εκδόσεων της, αποτέλεσε τον λόγο τόσο της ανόδου του Αδόλφου Χίτλερ, όσο και της πτώσης του, μιας και η επιτυχία του Bletchley Park (όπου εργαζόταν και ο Alan Turing) στην αποκρυπτογράφηση της έδωσε την ευκαιρία στους Συμμάχους να προετοιμαστούν για τις επιθέσεις των Γερμανών. Κατά το δεύτερο μισό του 20^{ου} αιώνα, η ανάπτυξη των υπολογιστών και του διαδικτύου ώθησε στην δημιουργία ισχυρότερων μορφών και αλγορίθμων κρυπτογράφησης, ικανών να αντέξουν τόσο στις προκλήσεις εκείνης της εποχής αλλά και σχεδιασμένων έτσι ώστε να θεωρούνται στην γενική περίπτωση άθραυστοι ακόμη και σήμερα. [1]

1.3 Βασικές Αρχές Κρυπτογραφίας

Ένα κρυπτογραφικό σύστημα ακολουθεί την ακόλουθη δομή :



Εικόνα 1 : Τυπική δομή κρυπτογραφικού συστήματος

Αρχικά, το μήνυμα m μετασχηματίζεται μέσω της συνάρτησης E η οποία παραμετροποιείται από ένα δεύτερο όρισμα, το κλειδί της κρυπτογράφησης K_c . Με βάση αυτά, δημιουργείται το κρυπτογραφημένο κείμενο C (ciphertext). Το C μπορεί να δεχθεί είτε παθητική επίθεση, στην οποία ο επιτιθέμενος μόνο ακούει, είτε ενεργητική επίθεση, στην

οποία ο επιτιθέμενος μπορεί και να παρέμβει στο μήνυμα. Η αποκρυπτογράφηση γίνεται από την συνάρτηση D η οποία παραμετροποιείται από το κλειδί αποκρυπτογράφησης K_d .

Η σχέση η οποία περιγράφει όλα τα παραπάνω είναι η :

$$D_{K_d}\left(E_{K_c}(m)\right) = m$$

Όταν τα K_d και K_c ταυτίζονται πρόκειται για την συμμετρική κρυπτογράφηση στην οποία θα γίνει αναφορά στο Κεφάλαιο 2, ενώ αντίθετα όταν τα κλειδιά είναι διαφορετικά πρόκειται για ασύμμετρη κρυπτογράφηση, για την οποία γίνεται αναφορά στο Κεφάλαιο 3. [2] [3]

Στην Κρυπτογραφία, θεωρείται ότι ο επιτιθέμενος (ή κρυπταναλυτής) γνωρίζει την μέθοδο κρυπτογράφησης και αποκρυπτογράφησης και εδώ εισέρχεται η έννοια του κλειδιού. Το κλειδί αποτελεί μια συμβολοσειρά η οποία διαφοροποιεί κάθε φορά την κρυπτογράφηση. Αυτό είναι και το μοντέλο στο οποίο βασίζεται η σύγχρονη κρυπτογραφία, ότι δηλαδή υπάρχει μια γενική, δημόσια μέθοδος η οποία παραμετροποιείται κάθε φορά από το κλειδί και απορρέει από την *αρχή του Kerckhoff :* η ασφάλεια του αλγορίθμου πρέπει να έγκειται μόνο στην μυστικότητα του κλειδιού και όχι στην μυστικότητα του ίδιου του αλγορίθμου. [2] [3]

1.4 Είδη Κρυπταναλυτικών Επιθέσεων

Οι κρυπταναλυτικές επιθέσεις κατηγοριοποιούνται με βάση των πληροφοριών που κατέχει ο επιτιθέμενος. Πιο αναλυτικά, υπάρχουν τέσσερις βασικές κατηγορίες επιθέσεων :

- επιθέσεις γνωστού κρυπτοκειμένου (ciphertext-only attacks)
- επιθέσεις γνωστού αρχικού μηνύματος (known-plaintext attacks)
- επιθέσεις επιλεγμένου αρχικού μηνύματος (chosen-plaintext attacks)
- επιθέσεις επιλεγμένου κρυπτοκειμένου (chosen-ciphertext attacks)

Στις επιθέσεις γνωστού κρυπτοκειμένου, ο επιτιθέμενος γνωρίζει μόνο ένα κομμάτι του κρυπτοκειμένου (καθώς και τον αλγόριθμο) και προσπαθεί να ανακτήσει το αρχικό μήνυμα ή το κλειδί. Σε αυτή την κατηγορία επιθέσεων εντάσσονται και οι εξαντλητικές επιθέσεις (brute force attacks), οι οποίες και αντιμετωπίζονται με την αύξηση του πλήθους των δυνατών κλειδιών.

Στις επιθέσεις γνωστού αρχικού μηνύματος, ο κρυπταναλυτής μπορεί να έχει και μια επιπλέον γνώση για επιμέρους κομμάτια του μηνύματος και αναζητεί μόνο το κλειδί της

κρυπτογράφησης. Σε πρωτόκολλα επικοινωνίας είναι σύνηθες να εμφανίζονται τυποποιημένα μηνύματα, όπως επικεφαλίδες, και συνεπώς αυτού του είδους οι επιθέσεις παρατηρούνται συχνά.

Κατά τις επιθέσεις επιλεγμένου αρχικού μηνύματος, ο αντίπαλος έχει την δυνατότητα να κρυπτογραφεί μηνύματα της επιλογής του και ύστερα να προσπαθεί να εκμεταλλευτεί το κρυπτοκείμενο που προκύπτει προκειμένου να ανακτήσει το κλειδί.

Τέλος, κατά τις επιθέσεις επιλεγμένου κρυπτοκειμένου, ο επιτιθέμενος έχει πρόσβαση σε συγκεκριμένα κρυπτογράμματα και με την χρήση του αλγορίθμου αποκρυπτογράφησης μπορεί να ανακτήσει το αρχικό μήνυμα και με βάση αυτό να αναζητήσει το κλειδί. Ουσιαστικά, αυτές οι επιθέσεις είναι αντίστροφης λογικής από τις επιθέσεις επιλεγμένου αρχικού μηνύματος. [2]

1.5 Μοντέλα Αξιολόγησης Ασφάλειας

Η αναζήτηση για ένα αντικειμενικό μέτρο το οποίο θα υποδεικνύει κατά πόσο ένα κρυπτογραφικό σύστημα αντιστέκεται σε επιθέσεις οδήγησε στα παρακάτω μαθηματικά μοντέλα.

- Ασφάλεια άνευ όρων (unconditionally secure). Το μοντέλο αυτό αναπτύχθηκε από τον Shannon και απορρέει από την Θεωρία της Πληροφορίας. Βασίζεται στην θεώρηση ότι ακόμα και αν ο αντίπαλος κατέχει άπειρη υπολογιστική ισχύ, το κρυπτοκείμενο δεν δίνει καμία πληροφορία έτσι ώστε να προσδιοριστεί το αρχικό μήνυμα.
- Υπολογιστική ασφάλεια (computationally secure). Σε αυτό το μοντέλο υποτίθεται ότι ο αντίπαλος προκειμένου να ανακτήσει το αρχικό μήνυμα χρειάζεται πολύ μεγαλύτερη υπολογιστική ισχύ από αυτή που διαθέτει. Το μοντέλο αυτό δεν εγγυάται την ασφάλεια ενός κρυπτοσυστήματος, καθώς στο μέλλον μπορεί να ανακαλυφθεί ένα ταχύτερος αλγόριθμος κρυπτανάλυσης ο οποίος να μπορεί να υλοποιηθεί με την δεδομένη υπολογιστική ισχύ.
- Ασφάλεια θεωρητικής πολυπλοκότητας (complexity theoretic). Η ανάλυση αυτή εξετάζει ασυμπτωτικά και όχι πρακτικά το κρυπτοσύστημα καθώς απαιτεί οι παράμετροι ασφαλείας να χρειάζονται πολυωνυμικό τόσο χρόνο όσο και χώρο και άρα η υπολογιστική ισχύς που χρειάζεται να είναι πολυωνυμική.
- Αποδείξιμη ασφάλεια (provable security). Το μοντέλο αυτό κατηγοριοποιεί ένα κρυπτοσύστημα ως ασφαλές όταν μπορεί να αποδειχθεί ότι η ασφάλεια του είναι ισοδύναμη με κάποιο μαθηματικό πρόβλημα το οποίο θεωρείται υπολογιστικά

δύσκολο, όπως η παραγοντοποίηση ενός μεγάλου αριθμού στους πρώτους παράγοντες του και ο υπολογισμός διακριτού λογαρίθμου ενός αριθμού. [4]

ΚΕΦΑΛΑΙΟ 2: ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

2.1 Εισαγωγή

Στην συμμετρική κρυπτογράφηση χρησιμοποιούνται τα ίδια κλειδιά τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση ενός μηνύματος. Οι αλγόριθμοι που αναπτύσσονται, ονομάζονται και αλγόριθμοι ιδιωτικού κλειδιού, καθώς, μόνο τα δύο συν διαλεγόμενα μέλη πρέπει να γνωρίζουν το εκάστοτε κλειδί και για τον λόγο αυτό πρέπει να έχει προηγηθεί μια ασφαλής ανταλλαγή κλειδιού. [2]

2.2 Κρυπταλγόριθμοι Τμήματος

Αρχικά, θα παρουσιαστούν κρυπταλγόριθμοι τμήματος. Οι αλγόριθμοι αυτοί, προτιμώνται από άποψη ασφάλειας από τους αλγορίθμους ροής, αλλά όταν η ταχύτητα έχει πρωταγωνιστικό ρόλο, επιλέγονται οι δεύτεροι. [4] Οι αλγόριθμοι τμήματος, παίρνουν ως είσοδο ένα αρχικό μήνυμα M και αφού το χωρίσουν σε τμήματα των n bits, τα κρυπτογραφούν ξεχωριστά με την χρήση του κλειδιού προκειμένου να δώσουν στην έξοδο ένα τμήμα του κρυπτοκείμενου με μέγεθος n bits. Η λειτουργία αυτών των αλγορίθμων βασίζεται σε μονάδες αντικατάστασης και μονάδες αντιμετάθεσης οι οποίες χρησιμοποιούνται διαδοχικά για την παραγωγή του τελικού αποτελέσματος. [2]

2.2.1 Αλγόριθμος DES – The Data Encryption Standard

Ο αλγόριθμος DES (Data Encryption Standard) υιοθετήθηκε το 1977 από τον NIST (National Institute of Standards and Technology) ως το επίσημο πρότυπο για κρυπτογράφηση μη απορρήτων πληροφοριών. Αναπτύχθηκε από την IBM και βασίστηκε στον προϋπάρχοντα αλγόριθμο, Lucifer.

Ο DES έχει μήκος τμήματος 64 bits και μήκους κλειδιού 56 bits (στην πραγματικότητα έχει μήκος κλειδιού 64 bits αλλά τα 8 είναι bits ισοτιμίας). Ο αλγόριθμος αρχικά αντιμεταθέτει τα δυο υποτμήματα μήκους 32 bits κάθε τμήματος (Αρχική Αντιμετάθεση) και στην συνέχεια

για 16 γύρους χρησιμοποιεί ένα υποκλειδί από το αρχικό κλειδί μήκους 48 bits για να υλοποιήσει την εξής πράξη :

$$L_i = R_{i-1} \, και \, R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \, με \, i = 1, \dots, 16$$

όπου με L και R συμβολίζουμε το εκάστοτε αριστερά και δεξιά υποτμήματα των 32 bits. Τέλος, ο αλγόριθμος μετά το πέρας των 16 γύρων κάνει την αντίστροφη της Αρχικής Αντιμετάθεσης και αυτό είναι το τελικό αποτέλεσμα. Η αποκρυπτογράφηση ενός τμήματος γίνεται αν ακολουθηθεί η ακριβώς αντίστροφη διαδικασία. [2] [3]

Το 1977 οι Diffie και Hellman χρησιμοποίησαν ένα μήνυμα και την κρυπτογράφηση του και σχεδίασαν ένα μηχάνημα το οποίο μπορούσε να ανακαλύψει το κλειδί κάνοντας εξαντλητική αναζήτηση σε λιγότερο από μια ημέρα. [3]

2.2.2 Αλγόριθμος Triple DES (3DES)

Το 1979, η IBM αποφάσισε ότι το μέγεθος των κλειδιών του DES ήταν πολύ μικρό και έτσι προέβη στην δημιουργία του αλγορίθμου Triple DES.

Ο αλγόριθμος 3DES αποτελεί μια τριπλή κρυπτογράφηση του DES όπου χρησιμοποιούνται 2 κλειδιά (έστω K_1 και K_2) των 56 bit. Η λειτουργία του αλγορίθμου βασίζεται στην κρυπτογράφηση, αποκρυπτογράφηση και ξανά κρυπτογράφηση με χρήση του απλού DES, και ο λόγος που δεν επιλέχθηκε η τριπλή κρυπτογράφηση είναι η προς τα πίσω συμβατότητα (backwards compatibility) με τον απλό αλγόριθμο (στην περίπτωση αυτή $K_1 = K_2$). Πιο συγκεκριμένα η κρυπτογράφηση γίνεται ως εξής :

$$C = E_{K_1}(D_{K_2}\left(E_{K_1}(M)\right))$$

Ο αλγόριθμος 3DES δεν έχει κρυπταναλυθεί επιτυχώς με την χρήση κλειδιού των 112 bits. Παρά το γεγονός ότι κατά την κυκλοφορία του δεν θεωρήθηκε σκόπιμο να χρησιμοποιηθεί και τρίτο κλειδί για λόγους σχέσης ασφάλειας και απόδοσης, στη σύγχρονη εποχή, στην θέση του K_1 στην δεύτερη κρυπτογράφηση, συνήθως υπάρχει ένα K_3, γεγονός που αυξάνει το συνολικό μέγεθος του κλειδιού στα 168 bits. [2] [3]

2.2.3 Αλγόριθμος AES – The Advanced Encryption Standard

Τον Ιανουάριο του 1997, ο NIST προσκάλεσε υποβολή προτάσεων για κρυπτογραφικούς αλγορίθμους προκειμένου να βρεθεί ο διάδοχος του DES και να καθιερωθεί ένα νέο πρότυπο κρυπτογράφησης. Οι απαιτήσεις που έπρεπε να πληρεί ένας υποψήφιος αλγόριθμος ήταν:

- Να είναι συμμετρικός κρυπταλγόριθμος τμήματος
- Να είναι δημόσιες όλες οι λεπτομέρειες του
- Το μήκους του κλειδιού να είναι τουλάχιστον 128 bits, ενώ θα έπρεπε να υποστηρίζονται και κλειδιά των 192 και 256 bits
- Να μπορεί να υλοποιηθεί τόσο σε υλικό όσο και σε λογισμικό
- Να έχει αναδειχθεί η ανθεκτικότητα του σε γνωστές κρυπταναλυτικές επιθέσεις

Μετά από δύο γύρους ψηφοφοριών, ο αλγόριθμος που επικράτησε ήταν ο Rijndael, ο οποίος κατασκευάστηκε από τους Βέλγους Joan Daemen και Vincent Rijmen.

Ο αλγόριθμος που πλέον είναι γνωστός ως AES (Advanced Encryption Standard) χρησιμοποιεί, όπως και ο DES, τόσο μεταθέσεις όσο και υποκαταστάσεις. Η διαφοροποίηση του έγκειται στο γεγονός ότι όλες οι λειτουργίες χρησιμοποιούν bytes προκειμένου να πληρείται η τέταρτη από τις παραπάνω προϋποθέσεις.

Ο αλγόριθμος βασίζεται στην διάσπαση της εισόδου σε τμήματα μεγέθους 1 byte και αντιστοίχιση τους σε στοιχεία ενός πίνακα τεσσάρων γραμμών. Ο αριθμός των στηλών εξαρτάται από το μέγεθος του τμήματος του μηνύματος, ενώ για την περίπτωση των 128 bits, το πλήθος ισούται με τέσσερα. Ο πίνακας που δημιουργείται ονομάζεται κατάσταση (state). Παράλληλα, το κλειδί διασπάται και εκείνο με την σειρά του σε κομμάτια και αποθηκεύεται σε ένα πίνακα ίδιων διαστάσεων με αυτών του state. Το πλήθος των γύρων στον αλγόριθμο εξαρτάται από το μέγεθος της εισόδου και του κλειδιού και αναλυτικότερα είναι 10 για 128 bits κλειδί, 12 για 192 bits κλειδί και 14 για 256 bits κλειδί.

Στον πρώτο γύρο της εκτέλεσης του αλγορίθμου, τα bytes της εισόδου συνδυάζονται με κάποιο byte του κλειδιού με αποκλειστική διάζευξη (XOR) [βήμα AddRoundKey]. Στην συνέχεια και για τους επόμενους N-1 γύρους υλοποιούνται 4 βήματα. Στο πρώτο βήμα, SubBytes, κάθε byte του state αντικαθίσταται μη γραμμικά από ένα byte ενός πίνακα με χρήση μιας μονάδας αντικατάστασης, τις λεπτομέρειες της οποίας δεν θα αναλύσουμε. Ύστερα, στο βήμα ShiftRows, τα bytes στις γραμμές του πίνακα state δέχονται μια αριστερή ολίσθηση κατά ένα διαφορετικό αριθμό θέσεων. Στο βήμα MixColumns, κάθε στήλη του state πολλαπλασιάζεται με ένα δεδομένο πολυώνυμο με συντελεστές τα στοιχεία της στήλης. Τέλος, στο τέταρτο βήμα, εκτελείται ξανά η διαδικασία AddRoundKey. Η διαφοροποίηση στην οποία έγκειται ο τελευταίος γύρος εκτέλεσης είναι ότι δεν υλοποιείται το βήμα MixColumns.

Η αποκρυπτογράφηση ενός μηνύματος γίνεται τρέχοντας τον αλγόριθμο ανάποδα, ενώ υπάρχει και τρόπος με την χρήση του αλγορίθμου ευθέως αλλά με διαφορετικούς πίνακες. [2] [3]

Ο αλγόριθμος AES μέχρι σήμερα δεν έχει καταστεί δυνατόν να κρυπταναλυθεί επιτυχώς, και οι σχεδιαστές του αποδεικνύουν στο [5] την ανθεκτικότητα του σε βασικά είδη επιθέσεων.

2.3 Κρυπταλγόριθμοι Ροής

Οι κρυπταλγόριθμοι ροής εμφανίζονται τόσο σε συμμετρική, όσο και σε ασύμμετρη μορφή. Στην παρούσα ενότητα θα γίνει αναφορά μόνο στην πρώτη κατηγορία, καθώς η δεύτερη ξεφεύγει από τους στόχους της παρούσας εργασίας. Η λειτουργία των κρυπταλγορίθμων ροής διαφοροποιείται από τους κρυπταλγορίθμους τμήματος στο γεγονός ότι η κρυπτογράφηση γίνεται κάθε χρονική στιγμή και όχι σε επίπεδο τμήματος αλλά σε επίπεδο συμβόλου. Σε αυτή την κατηγορία αλγορίθμων, χρησιμοποιείται μια ψευδοτυχαία ακολουθία συμβόλων η οποία ονομάζεται κλειδοροή και η οποία συνδυάζεται με το αρχικό κείμενο προκειμένου να παραχθεί το κρυπτογραφημένο μήνυμα. Όπως αναφέρθηκε και παραπάνω, οι κρυπταλγόριθμοι ροής είναι ιδανικοί για τηλεπικοινωνιακές εφαρμογές καθώς χαρακτηρίζονται από χαμηλές απαιτήσεις μνήμης αλλά και μικρή διάδοση σφαλμάτων. [2]

2.3.1 Αλγόριθμος RC4

Ο RC4 είναι ένας από τους πιο δημοφιλείς κρυπταλγορίθμους ροής. Σχεδιάστηκε από τον Ron Rivest και κυκλοφόρησε πρώτη φορά το 1994. [4]

Ο αλγόριθμος χρησιμοποιεί κλειδιά μήκους 40 εώς 2048 bits και η λειτουργία του βασίζεται σε μεταθέσεις και πράξεις αποκλειστικής διάζευξης (XOR). Η απλή δομή του καθώς και οι μικρές απαιτήσεις σε μνήμη, τον έκαναν ευρέως διαδεδομένο και έτσι χρησιμοποιήθηκε σε πρωτόκολλα όπως το WEP και το TLS. [4]

Σύμφωνα με το [6], η χρήση του δεν είναι πλέον ασφαλής και έτσι πλέον δεν προτιμάται.

ΚΕΦΑΛΑΙΟ 3: ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

3.1 Εισαγωγή

Η ασύμμετρη ή κρυπτογραφία δημοσίου κλειδιού είναι η νεότερη μορφή κρυπτογραφίας. Εμφανίστηκε για πρώτη φορά το 1976 από τους Diffie και Hellman και βασίζεται στην μαθηματική σχέση των κλειδιών κρυπτογράφησης και αποκρυπτογράφησης, τα οποία πλέον δεν ταυτίζονται. [3] Κάθε χρήστης που θέλει να χρησιμοποιήσει αυτή την μέθοδο κρυπτογράφησης κατέχει δύο κλειδιά, ένα ιδιωτικό και ένα δημόσιο. Το δημόσιο κλειδί μπορεί να διανεμηθεί δημόσια και οποιοσδήποτε θελήσει να στείλει ένα μήνυμα σε αυτόν τον χρήστη, έχει την δυνατότητα να το χρησιμοποιήσει. Η αποκρυπτογράφηση του μηνύματος μπορεί να γίνει μόνο από τον χρήστη που κατέχει το ιδιωτικό κλειδί, ενώ παρά το γεγονός ότι τα κλειδιά σχετίζονται μαθηματικά, δεν υπάρχει τρόπος να υπολογιστεί το ιδιωτικό με βάση το δημόσιο. [2]

3.2 Κρυπτοσύστημα RSA

Ο αλγόριθμος RSA είναι το πρώτο αλλά και πιο διαδεδομένο κρυπτοσύστημα δημοσίου κλειδιού. Αναπτύχθηκε το 1977 από τους Rivest, Shamir και Adleman. Η ασφάλεια του εγγυείται από την δυσκολία της παραγοντοποίησης ενός σύνθετου ακεραίου σε γινόμενο πρώτων παραγόντων. [4]

Ένας χρήστης για να δημιουργήσει τα δυο κλειδιά του, επιλέγει δυο μεγάλους τυχαίους αριθμούς, έστω p και q, για τους οποίους πρέπει η διαφορά p-q να είναι επίσης μεγάλη. Στη συνέχεια, υπολογίζει το γινόμενο $n = p * q$, καθώς και την τιμή $\varphi(n) = (p-1)(q-1)$. Ύστερα, επιλέγει ένα αριθμό e, ο οποίος πρέπει να είναι σχετικά πρώτος με το φ(n) και μεγαλύτερος του 1. Τέλος, υπολογίζει d τέτοιο ώστε $d * e \equiv 1 \, mod \, \varphi(n)$.

Από τα παραπάνω, το ιδιωτικό του κλειδί είναι το d και το δημόσιο του, το ζευγάρι n,e.

Προκειμένου να κρυπτογραφήσει κάποιος ένα μήνυμα m, υπολογίζει το $c = m^e mod\ n$, ενώ η αποκρυπτογράφηση γίνεται υπολογίζοντας την ποσότητα $m = c^d mod\ n$. [2]

Μέχρι την ημερομηνία συγγραφής της εργασίας, το μεγαλύτερο μήκος κλειδιού που έχει κρυπταναλυθεί επιτυχώς είναι 768 bit, [7] , ενώ το συνιστώμενο μήκος είναι 2048 bits.

3.3 **Κρυπτοσύστημα ElGamal**

Το κρυπτοσύστημα ElGamal παρουσιάστηκε από τον Taher ElGamal το 1984. Βασίζεται στο πρόβλημα του διακριτού λογαρίθμου το οποίο ορίζεται ως η εύρεση ενός ακεραίου k τέτοιου ώστε $g^k \equiv y\ mod\ p, με\ 0 \leq k \leq p-2$.

Για τη δημιουργία κλειδιών, ένας χρήστης δημιουργεί ένα μεγάλο πρώτο αριθμό p και ένα γεννήτορα g, διαλέγει ένα τυχαίο αριθμό α και υπολογίζει το $g^a\ mod\ p$. Το ιδιωτικό κλειδί του χρήστη είναι το α και το δημόσιο κλειδί του είναι η τριάδα p, g, g^a.

Η κρυπτογράφηση ενός μηνύματος m γίνεται με την επιλογή ενός ακεραίου k με $1 \leq k \leq p-2$ και τον υπολογισμό δυο τιμών, των $\gamma = g^k\ mod\ p$, $\delta = m * (g^b)^k mod\ p$, τα οποία και αποστέλλονται. Η αποκρυπτογράφηση, αντίστοιχα, γίνεται με τον υπολογισμό του $\tilde{m} = \gamma^{p-1-b}\ mod\ p$. [2]

3.4 Κρυπτοσυστήματα Ελλειπτικών Καμπυλών

Τα κρυπτοσυστήματα των ελλειπτικών καμπυλών προτάθηκαν το 1986 και το 1987 ανεξάρτητα. Το μαθηματικό πρόβλημα στο οποίο βασίζονται είναι αυτό του διακριτού λογαρίθμου πάνω στις ελλειπτικές καμπύλες, το οποίο αναζητεί ένα ακέραιο k, προκειμένου να ικανοποιείται η σχέση $Q = k * P$ όπου Q και P, δύο σημεία της καμπύλης.

Λόγω της ομοιότητας με το μαθηματικό πρόβλημα που ορίζει το κρυπτοσύστημα ElGamal, έχουν δημιουργηθεί πρωτόκολλα όπως το ECES (Elliptic Curve Encryption Scheme) τα οποία βασίζονται στον παραπάνω αλγόριθμο και χρησιμοποιούνται σε συστήματα ελλειπτικών καμπυλών.

Κάθε χρήστης για να δημιουργήσει τα δύο κλειδιά του, αρχικά, πρέπει να συμφωνήσει με τους υπόλοιπους χρήστες για την επιλογή του ίδιου πεπερασμένου σώματος F_p αλλά και της ίδιας καμπύλης E. Στη συνέχεια, υπολογίζει το σημείο P, το οποίο πρέπει να έχει μεγάλη τάξη και επιλέγει το k για να ικανοποιείται η σχέση $Q = k * P$. Το δημόσιο κλειδί του χρήση είναι το ζευγάρι Q και P, και το ιδιωτικό είναι ο ακέραιος k.

Η διαδικασία της κρυπτογράφησης ενός μηνύματος γίνεται με την ακόλουθη διαδικασία. Ο αποστολές επιλέγει ένα αριθμό k και υπολογίζει το $R = k * P$, όπου P είναι το σημείο βάσης του παραλήπτη. Ύστερα, ο αποστολέας υπολογίζει το $Q = k * Q_{παραλήπτη}$ καθώς και το $c = z * x \ (mod\ p)$, όπου με z αναπαρίσταται το μήνυμα σε ακέραια μορφή, x είναι το σημείο Q και p η τάξη του σώματος που ορίζεται η καμπύλη. Τελικά, η κρυπτογράφηση αποτελείται από το ζευγάρι (R,c). Για την διαδικασία της αποκρυπτογράφησης, ο παραλήπτης υπολογίζει το $Q = k_{παραλήπτη} * R$ και το $z = \frac{c}{x} \ (mod\ p)$ όπου οι συμβολισμοί έχουν αντιστοιχία με τα παραπάνω, και το αποτέλεσμα που προκύπτει είναι το μήνυμα σε ακέραια μορφή. [2]

ΚΕΦΑΛΑΙΟ 4: ΚΡΥΠΤΟΓΡΑΦΙΚΕΣ ΣΥΝΑΡΤΗΣΕΙΣ ΚΑΤΑΚΕΡΜΑΤΙΣΜΟΥ

4.1 Εισαγωγή

Ένα από τα θέματα με τα οποία έρχεται αντιμέτωπη η κρυπτογραφία είναι αυτό της ακεραιότητας ενός μηνύματος. Τόσο η αλλοίωση λόγω της μεταφοράς μέσα από κανάλια επικοινωνίας, όσο και κακόβουλοι χρήστες, πολλές φορές μπορούν να διαφοροποιήσουν σε μικρό ή μεγάλο βαθμό ένα μήνυμα. Οι κρυπτογραφικές συναρτήσεις κατακερματισμού, έρχονται να δώσουν λύση σε αυτό, μεταξύ άλλων προβλημάτων, αντιστοιχώντας το μήνυμα σε μια συμβολοσειρά προκαθορισμένου μεγέθους (message digests). Ο τελικός χρήστης που παραλαμβάνει ένα μήνυμα, μπορεί να το δώσει σαν όρισμα στην ίδια συνάρτηση και αν οι συμβολοσειρές (message digests) ταυτίζονται να ξέρει ότι δεν υπήρξε αλλοίωση.

Προκειμένου να θεωρηθεί μια συνάρτηση κατακερματισμού αποδεκτή για χρήση στην κρυπτογραφία πρέπει να πληροί συγκεκριμένες προϋποθέσεις :

- Το κείμενο εισόδου να μπορεί να έχει οσοδήποτε μήκος.
- Η συνάρτηση να μπορεί να υπολογιστεί γρήγορα (σε πολυωνυμικό χρόνο) συναρτήσει του μήκους της εισόδου.
- Η συμβολοσειρά εξόδου πρέπει να έχει σταθερό μήκος, με ελάχιστο τα 128 bits και συνηθισμένο τα 160 bits.
- Να μην μπορεί να βρεθεί $x \neq y$ με $H(x) = H(y)$ σε πολυωνυμικό χρόνο.
- Να είναι αδύνατο δεδομένης της τιμής H(x) να μπορεί να ανακτηθεί το x.

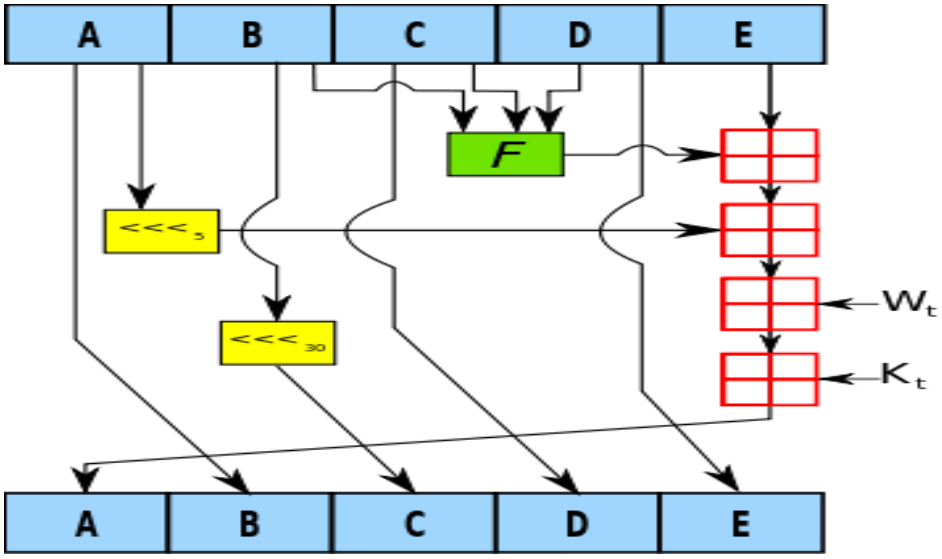
Παρακάτω, παρουσιάζονται οι πιο διαδεδομένες συναρτήσεις κατακερματισμού καθώς περιγράφεται συνοπτικά η λειτουργία τους. [2]

4.2 Οικογένεια Συναρτήσεων SHA

4.2.1 Συνάρτηση SHA-1

Η συνάρτηση κατακερματισμού SHA-1 δημιουργήθηκε από την NSA (National Security Agency) και υιοθετήθηκε από τον NIST ως στάνταρ για μη απόρρητες πληροφορίες (FIPS). [8]

Το μέγιστο μέγεθος κειμένου που δέχεται η συνάρτηση είναι 2^{64} και παράγει έξοδο των 160 bits. Η επεξεργασία γίνεται σε block των 512 bits, το οποίο χωρίζεται σε λέξεις των 32 bits και στις οποίες εφαρμόζονται προσαυξήσεις, ολισθήσεις και προσθέσεις σε τέσσερις γύρους των είκοσι βημάτων. Σχηματικά, ένα γύρος εμφανίζεται στο Σχήμα 2 όπου με A,B,C,D,E αναπαρίστανται λέξεις των 32 bits, F είναι μια συνάρτηση η οποία διαφοροποιείται ανά γύρο, W_t είναι η προσαυξημένη λέξη στον γύρο t, ενώ K_t είναι μια σταθερά που και αυτή αλλάζει ανά γύρο. Τέλος, τα ⊞ προσομοιώνουν πρόσθεση mod 2^{32}.



Εικόνα 2 : Αναπαράσταση γύρου της SHA-1

(Πηγή : Wikipedia, https://commons.wikimedia.org/wiki/File:SHA-1.svg , άδεια CC Attribution-Share Alike 2.5 Generic)

Δεν έχει πραγματοποιηθεί επιτυχώς επίθεση στην συνάρτηση SHA-1, αλλά έχουν αναπτυχθεί θεωρητικές μέθοδοι οι οποίες υπονομεύουν την ασφάλεια της και συνεπώς, η χρήση της έχει αρχίσει να εγκαταλείπεται. [9]

4.2.2 Συνάρτηση SHA-2

Η συνάρτηση κατακερματισμού SHA-2 αποτελεί την επόμενη έκδοση της SHA-1. Παρουσιάστηκε για πρώτη φορά από τον NIST το 2001 και διαφοροποιείται από τον

προκάτοχο της τόσο σε μέγεθος εξόδου, όπου δημιουργούνται συμβολοσειρές μήκους 224,256,384 και 512 bits στις αντίστοιχες SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256. Παράλληλα, υποστηρίζονται τμήματα εισόδου εώς 2^{1024} καθώς και τμήματα υπολογισμού των 64 bits. [8]

Παρά την σχέση της με την SHA-1, οι θεωρητικές επιθέσεις που αναφέρθηκαν παραπάνω, δεν έχουν εφαρμογή στην SHA-2, αλλά έχουν αναπτυχθεί επιθέσεις που θεωρούνται πρακτικές σύμφωνα με το [10].

4.2.3 Συνάρτηση SHA-3

Η συνάρτηση SHA-3 είναι προϊόν διαγωνισμού που διενέργησέ ο NIST από το 2008 μέχρι και το 2015, όποτε και προτυποποιήθηκε. [11] Η συνάρτηση αυτή δεν έχει σχέση με τις προηγούμενες δύο και αποτελεί ένα μέρος του αλγορίθμου Keccak που κατασκευάστηκε από τους Joan Daemen, Guido Bertoni, Michael Peeters, και Gilles Van Assche.

Σε αντιστοιχία με την SHA-2 υποστηρίζονται διαφορετικά μεγέθη εξόδου μήκους 224, 256, 384, και 512 bits στις αντίστοιχες εκδόσεις SHA3-224, SHA3-256, SHA3-384 και SHA3-512 καθώς και μεγέθη εξόδου που καθορίζονται από την είσοδο στις εκδόσεις SHAKE128 και SHAKE256. Τα τμήματα που χρησιμοποιούνται για τον υπολογισμό έχουν μέγεθος 1600 bits (σε επιμέρους μέρη λέξεων των 64 bits) και το μέγεθος της εισόδου δεν περιορίζεται από κάποιο μέγεθος. [11]

4.3 Message Digest 5 – Message Digest 6

4.3.1 Message Digest 5 (MD5)

Η συνάρτηση κατακερματισμού MD5 κατασκευάστηκε από τον Ron Rivest το 1991.

Η είσοδος στην συνάρτηση αυτή δεν περιορίζεται από κάποια ποσότητα και η παραγόμενη έξοδος έχει μήκος 128 bits. Η επεξεργασία γίνεται σε blocks των 512 bits και βασίζεται σε λογικές πράξεις OR,NOT και XOR.

Χρησιμοποιείται, πλέον, μόνο για checksums καθώς έχει γίνει πληθώρα επιθέσεων, τόσο brute force αλλά και δημιουργίας ίδιων εξόδων από διαφορετικά μηνύματα, οι οποίες την κατέστησαν ανασφαλή. [2]

4.3.2 Message Digest 6 (MD6)

Η συνάρτηση MD6 παρουσιάστηκε για πρώτη φορά το 2008, όταν και ήταν υποψήφια για το διαγωνισμό ανάδειξης του SHA-3.

Κατά τον σχεδιασμό της, δόθηκε μεγάλη βάση στην ταχύτητα και παρά την επιλογή για σειριακή εκτέλεση, ο αλγόριθμος αποδίδει ιδιαίτερα όταν χρησιμοποιεί δομές δέντρων Merkle. Η είσοδος περιορίζεται στα 512 bytes και οι πράξεις γίνονται σε λέξεις των 64 bits. Η έξοδος είναι μεταβλητού μήκους από 160 εώς 512 bits και το πλήθος των επαναλήψεων εξαρτάται από το μέγεθος της εξόδου. Οι λογικές πράξεις που χρησιμοποιούνται είναι η XOR και η AND, ενώ ταυτόχρονα χρησιμοποιείται αριστερή και δεξιά ολίσθηση. [2]

4.4 Συνάρτηση Whirlpool

Η συνάρτηση Whirlpool είναι η πλέιον διαδεδομένη συνάρτηση κατακερματισμού. Έχει υιοθετηθεί από τον NESSIE (New European Schemes for Signatures, Integrity and Encryption) καθώς και από τους ISO (International Organization for Standardization) και IEC (International Electrotechnical Commission).

Η είσοδος της συνάρτησης είναι μέχρι 2^{512} bits και η έξοδος είναι των 512 bits. Οι πράξεις που εκτελούνται είναι σε τμήματα των 512 bits και οι επαναλήψεις που εκτελούνται είναι δέκα. Βασίζεται στο μοντέλο Merkle-Damgard.που αναφέρθηκε παραπάνω. [2]

Οι δημιουργοί της συνάρτησης έχουν δώσει άδεια χρήσης τύπου public domain. [12]

ΚΕΦΑΛΑΙΟ 5: ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

5.1 Εισαγωγή

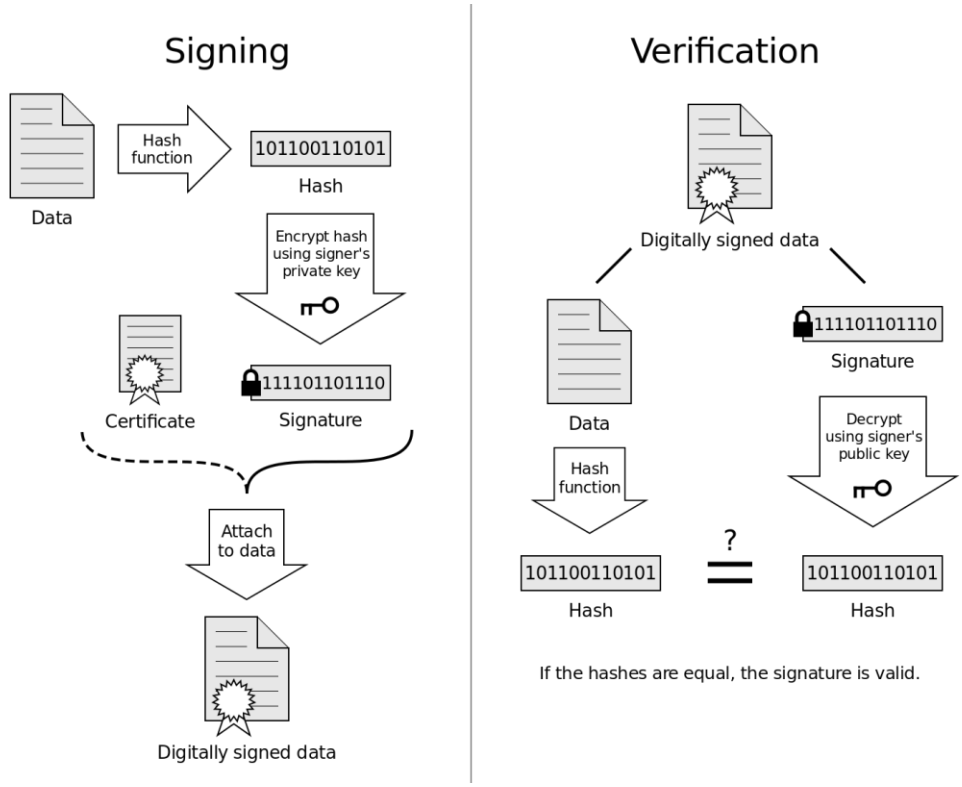
Οι ψηφιακές υπογραφές αποτελούν εκτενείς συμβολοσειρές οι οποίες αντιστοιχίζουν μονόδρομα οντότητες με μηνύματα ή αρχεία. Η λειτουργία τους είναι αντίστοιχη με αυτή της καθημερινής ζωής και εξασφαλίζουν την απόδειξη της ταυτότητας ενός μέλους με την επίδειξη μια χαρακτηριστικής πληροφορίας.

Ένα σχήμα ψηφιακών υπογραφών πρέπει να πληροί τις ακόλουθες ιδιότητες για να είναι αξιόπιστο :

- Ο παραλήπτης θα πρέπει να μπορεί να πιστοποιήσει την ταυτότητα του αποστολέα.
- Ο αποστολές δεν πρέπει να μπορεί να τροποποιήσει το περιεχόμενο ενός μηνύματος.
- Ο παραλήπτης δεν πρέπει να μπορεί να αναπαράγει το μήνυμα του αποστολέα.

Οι παραπάνω σχεδιαστικές προϋποθέσεις είναι εφάμιλλες αυτών που ικανοποιεί η κρυπτογραφία δημοσίου κλειδιού και άρα στην πράξη χρησιμοποιούνται παρόμοιες τεχνικές που θα αναλυθούν παρακάτω.

Παράλληλα, είναι σημαντικό να αναφερθεί ότι υπάρχουν δύο είδη ψηφιακών υπογραφών, οι υπογραφές με προσθήκη οι οποίες δίνουν σαν είσοδο το αρχικό μήνυμα στον αλγόριθμο επιβεβαίωσης και οι υπογραφές με ανάκτηση μηνύματος οι οποίες αναδημιουργούν το αρχικό μήνυμα από την υπογραφή. Στην πράξη χρησιμοποιούνται οι υπογραφές με προσθήκη καθώς είναι πιο αποδοτικές. [2] [3] [4]



Εικόνα 3 : Μοντέλο χρήσης ψηφιακών υπογραφών

(Πηγή : Wikipedia, https://commons.wikimedia.org/wiki/File:Digital_Signature_diagram.svg, άδεια CC Attribution-Share Alike 3.0 Unported)

Όπως παρουσιάζεται στην Εικόνα 3, οι υπογραφές με προσθήκη λειτουργούν ως ακολούθως. Το μήνυμα προς αποστολή, αρχικά, δίνεται ως είσοδος σε μια συνάρτηση κατακερματισμού η οποία υπολογίζει την υπογραφή με βάση το ιδιωτικό κλειδί του αποστολέα και στέλνει το αποτέλεσμα μαζί με το μήνυμα στον παραλήπτη. Ο παραλήπτης από πλευράς του, εφαρμόζει το δημόσιο κλειδί του αποστολέα στην υπογραφή και ταυτόχρονα δίνει ως είσοδο στην συνάρτηση κατακερματισμού το μήνυμα. Αν τα δυο αποτελέσματα ταυτιστούν τότε ξέρει ότι μπορεί να εμπιστευθεί την εγκυρότητα της υπογραφής. [4]

5.2 Ψηφιακές Υπογραφές RSA

Η χρήση των ψηφιακών υπογραφών είναι παρόμοια με την κρυπτογράφηση ενός μηνύματος με τον συγκεκριμένο αλγόριθμο. Υπενθυμίζεται ότι το δημόσιο κλειδί μιας οντότητας είναι ένα ζευγάρι (n,e) και το ιδιωτικό ένας ακέραιος d.

Για την δημιουργία της υπογραφής, ο αποστολέας, αφού πρώτα συνοψίσει το μήνυμα με χρήση μιας hash συνάρτησης (H), χρησιμοποιεί το ιδιωτικό του κλειδί για να υπολογίσει την υπογραφή του, ως εξής : $S_A = H^d \ mod \ n$.

Ο παραλήπτης επιβεβαιώνει την υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα και υπολογίζοντας το $S_A{}^e \ mod\ n = H$, το οποίο στην συνέχεια συγκρίνει με το αποτέλεσμα της συνάρτησης κατακερματισμού $H' = h(m)$. Αν οι δυο τιμές είναι ίσες τις αποδέχεται αλλιώς τις απορρίπτει. [2]

5.3 Ψηφιακές Υπογραφές ElGamal

Στην κρυπτογράφηση με την μέθοδο ElGamal, το δημόσιο κλειδί του αποστολέα είναι η τριάδα (p,g,y) και το ιδιωτικό του ο αριθμός x.

Η δημιουργία της υπογραφής με χρήση ElGamal, αρχικά, χρειάζεται την επιλογή ενός αριθμού k του οποίου ο μέγιστος κοινός διαιρέτης με το p-1 είναι το 1. Στη συνέχεια, γίνεται υπολογισμός του $r = g^k mod\ p$ και του $k^{-1} mod(p-1)$. Τέλος, υπολογίζεται το $s = k^{-1}(h(m) - x * r) mod\ (p-1)$, το οποίο σε συνδυασμό με το r αποτελούν την υπογραφή.

Η επιβεβαίωση της υπογραφής γίνεται με έλεγχο του αν $1 \leq r \leq p-1$. Ύστερα, υπολογίζεται το $u_1 = y^r * r^s mod\ p$ και το h(m). Τέλος, υπολογίζεται η τιμή $u_2 = g^{h(m)} mod p$ το οποίο και συγκρίνεται με το u_1 και αν είναι ίσες γίνεται αποδοχή της υπογραφής.

5.4 Το Πρότυπο Ψηφιακής Υπογραφής

Ο αλγόριθμος Digital Signature Algorithm (DSA) αποτελεί το πρότυπο που προτάθηκε από τον NIST το 1991. Βασίζεται, όπως και ο El Gamal, στο πρόβλημα του υπολογισμού του διακριτού λογαρίθμου. Η αρχική του έκδοση απαιτούσε την χρήση της SHA-1 ως συνάρτησης κατακερματισμού, αλλά θέματα που συζητήθηκαν παραπάνω, οδήγησαν στην υιοθέτηση της SHA-2. [13] Σε αντίθεση με τα παραπάνω, ο συγκεκριμένος αλγόριθμος δεν θεωρείται κρυπτοσύστημα αλλά χρησιμοποιείται αποκλειστικά σε ψηφιακές υπογραφές. [4]

Η δημιουργία ενός κλειδιού για μια ψηφιακή υπογραφή DSA βασίζεται στην επιλογή ενός πρώτου αριθμού q τέτοιο ώστε να είναι μεγαλύτερος από το 2^{N-1} και μικρότερος από το 2^N καθώς και ενός πρώτου αριθμού p με μήκος L bits τέτοιο ώστε q|p-1 όπου οι παράμετροι N και L προσδιορίζονται στην τυποποίηση. Ύστερα, πρέπει να επιλεγεί ένα στοιχείο h τέτοιο ώστε η έκφραση $g = h^{\frac{p-1}{q}} mod\ p$ να είναι διάφορη του 1 και ένας ακέραιος x στο [1,q-1]. Τέλος, υπολογίζεται το $y = g^x mod p$. Το δημόσιο κλειδί είναι το σύνολο (p,q,g,y) και το ιδιωτικό είναι το x.

Για την δημιουργία μιας δημόσιας υπογραφής, ένας χρήστης πρέπει να επιλέξει ένα ακέραιο x στο διάστημα [1,q-1], να υπολογίσει τις ποσότητες $r = (g^k mod\ p) mod\ q$, $k^{-1}\ mod\ q$ και $s = k^{-1}\big(H(m)\big) + xr)\ mod\ q$, ενώ στην περίπτωση που s = 0, πρέπει να επαναληφθούν τα βήματα από την αρχή. Η υπογραφή αποτελείται από το ζευγάρι (r,s).

Η επιβεβαίωση της υπογραφής γίνεται, αρχικά, με τον έλεγχο ότι r και s ανήκουν στο [1,q-1]. Αν δεν ισχύει αυτός ο περιορισμός, η υπογραφή απορρίπτεται. Σε αντίθετη περίπτωση υπολογίζονται τα : $w = s^{-1} mod\ q$, $u_1 = H(m)w$ και $u_2 = rw\ mod\ q$. Η υπογραφή γίνεται αποδεκτή αν και μόνο αν $r = (g^{u_1} y^{u_2} mod\ p)\ mod\ q$.

Χαρακτηριστικά, για να επιτευχθεί 80 bits ασφάλεια, ένα δημόσιο κλειδί έχει μέγεθος 1024 bits, ένα ιδιωτικό 160 bits και το μέγεθος της υπογραφής είναι 320 bits. [2]

ΚΕΦΑΛΑΙΟ 6 : ΔΙΑΧΕΙΡΙΣΗ ΚΛΕΙΔΙΩΝ

6.1 Εισαγωγή

Όπως αναφέρθηκε και παραπάνω, τα κλειδιά αποτελούν το σημαντικότερο μέρος ενός κρυπτογραφικού συστήματος, είτε αυτό πρόκειται για συμμετρικό, είτε για ασύμμετρο. Η δημιουργία, διανομή, εγκατάσταση, χρήση, ανανέωση, ανάκληση φύλαξη και καταστροφή των κλειδιών έχουν αποτελέσει σημαντικά μεγάλη περιοχή έρευνας και έχουν αναπτυχθεί τεχνικές για την επιτυχή διεκπεραίωση τους. [4]

Ανάλογα με την χρήση τους τα κλειδιά διακρίνονται σε τρεις κατηγορίες :

- Τα κλειδιά συνόδου (session keys) χρησιμοποιούνται για την κρυπτογράφηση μόνο μιας περιόδου επικοινωνίας και ύστερα καταστρέφονται.
- Τα κλειδιά τερματικού (terminal keys) είναι κλειδιά συνόδου τα οποία κατέχονται από ένα χρήστη και κρυπτογραφούν παρά πάνω από μια περιόδους επικοινωνίας του χωρίς να καταστραφούν.
- Τα κύρια κλειδιά (master keys) χρησιμοποιούνται για την ασφαλή αποθήκευση τερματικών και κλειδιών συνόδου προκειμένου να απλοποιήσουν τον όγκο των δεδομένων που πρέπει να διαχειριστεί ένας χρήστης. [4]

Τα κλειδιά, επίσης, για να θεωρηθούν ασφαλή πρέπει να διέπονται από κάποιες ιδιότητες. Αρχικά, κάθε χρήστης θα πρέπει, με βάση το κλειδί, να μπορεί να καθορίσει την ταυτότητα του μέρους με το οποίο επιθυμεί να ανταλλάξει μηνύματα αλλά και να μπορεί να επιβεβαιώσει ότι είναι ενεργός. Παράλληλα, κάθε χρήστης θα πρέπει να μπορεί να γνωρίζει το ποιος έχει πρόσβαση σε ένα κλειδί που έχει εδραιωθεί αλλά και να υπάρχει κάποιο εχέγγυο ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να αποκτήσουν πρόσβαση σε ένα κλειδί συνόδου. Ύστερα, ένα κλειδί θα πρέπει να χαρακτηρίζεται ως φρέσκο, δηλαδή να μην έχει εδραιωθεί η χρησιμοποιηθεί στο παρελθόν από κάποιον άλλο χρήστη. Τέλος, είναι πολύ σημαντικό τα κλειδιά να είναι ανθεκτικά σε επιθέσεις γνωστού κλειδιού, δηλαδή να μην μπορεί μια ευπάθεια σε ένα κλειδί να αποκαλύψει όλα τα υπόλοιπα κλειδιά της συνόδου. Αυτή η έννοια

κατηγοριοποιείται στην μυστικότητα προς τα εμπρός (forward secrecy) όπου η ανακάλυψη ενός μακροπρόθεσμου κλειδιού δεν συνεπάγεται την ανακάλυψη των κλειδιών της συνόδου, και μυστικότητα προς τα πίσω (backward secrecy) όπου ισχύει το ανάποδο, δηλαδή η ανακάλυψη ενός κλειδιού συνόδου δεν συνεπάγεται την ανακάλυψη μακροπρόθεσμων κλειδιών. [2] [4]

6.2 Εδραίωση Κλειδιού

Ως εδραίωση κλειδιού θεωρούμε όλες εκείνες τις διαδικασίες που χρειάζονται να επιτελεστούν προκειμένου δύο χρήστες να είναι σε θέση να επικοινωνήσουν ασφαλώς. Τα πρωτόκολλα της κατηγορίας αυτής περιλαμβάνουν την δημιουργία, μεταφορά και εγκατάσταση κλειδιών τα οποία συνήθως είναι κλειδιά συνόδου. [2] [4]

6.2.1 Εδραίωση Κλειδιού σε Συμμετρικά Κρυπτοσυστήματα

Το πρόβλημα που υπεισέρχεται στα συμμετρικά κρυπτοσυστήματα είναι αυτό του μεγάλου όγκου κλειδιών, ο οποίος είναι ανάλογος του τετραγώνου του πλήθους των συμπραττόμενων μερών. Η λύση στο πρόβλημα δίνεται από τη δημιουργία ενός Κέντρου Διανομής Κλειδιών (Key Distribution Centre, KDC) και ενός Κέντρου Μετάφρασης Κλειδιών (Key Translation Centre, KTC) . [4]

Στην περίπτωση των Κέντρων Διανομής Κλειδιών, ένας χρήστης Α πρέπει να έχει μοιραστεί εκ των προτέρων ένα κλειδί με το κέντρο και όταν θελήσει να επικοινωνήσει με ένα χρήστη Β, το Κέντρο δημιουργεί ένα κλειδί το οποίο κρυπτογραφεί με το κλειδιά του Α και του Β και τους τα στέλνει αντίστοιχα.

Στην περίπτωση των Κέντρων Διαχείρισης Κλειδιών, ο χρήστης Α δημιουργεί ένα κλειδί το οποίο το στέλνει στο Κέντρο, το οποίο αναλαμβάνει να το αποκρυπτογραφήσει με χρήση του κλειδιού μακράς διαρκείας του Α, και στην συνέχεια να το κρυπτογραφήσει με χρήση του κλειδιού του Β και να το στείλει στον Β.

Η διαφορά ανάμεσα στα δύο κέντρα έγκειται, ουσιαστικά, ότι στην πρώτη περίπτωση η δημιουργία των κλειδιών γίνεται κεντρικοποιημένα, ενώ στην δεύτερη με κατανεμημένο τρόπο. [2]

Η εξάρτηση από το εκάστοτε κέντρο επιφυλάσσει και αυτή με τη σειρά της νέους κινδύνους. Αν κάποιος επιτιθέμενος βρεθεί σε θέση να προσβάλλει ένα χρήστη τότε δεν θα υπάρξει πρόβλημα στην λειτουργία του συστήματος αλλά αν εκτεθεί το κέντρο τότε όλο το σύστημα θα καταρρεύσει. Πιο συγκεκριμένα, η λειτουργία που έχει περιγραφεί δεν έχει τρόπο

να εντοπίσει ενεργές επιθέσεις επανάληψης παλαιών μηνυμάτων. Έτσι είναι επιτακτική η ανάγκη αυθεντικοποίησης τόσο στην περίπτωση της πρώτης επικοινωνίας ενός χρήστη για την απόκτηση ενός κλειδιού, όσο και στην περίπτωση της μεταφοράς ενός κλειδιού όταν θέλουν δύο χρήστες να επικοινωνήσουν. [4]

Μερικές τεχνικές οι οποίες εφαρμόζονται για να αντιμετωπιστεί το παραπάνω πρόβλημα είναι η επισύναψη επιπλέον πληροφορίας στα πρωτόκολλα. Η πρώτη προσέγγιση είναι αυτή της χρονοσφραγίδας (timestamp) όπου καταγράφεται η ημερομηνία, η ώρα, τα λεπτά και τα δευτερόλεπτα και η οποία διασταυρώνεται κατά την διαβίβαση ενός μηνύματος. Η δεύτερη προσέγγιση είναι αυτή της προσθήκης ενός μοναδικού αριθμού (nonce) ο οποίος δεν είναι προβλέψιμος και καθορίζει μονοσήμαντα ένα μήνυμα που ανταλλάσσεται. [4]

6.2.2 Το πρωτόκολλο Κέρβερος

Το πρωτόκολλο αυθεντικοποίησης Κέρβερος χρησιμοποιείται για την αυθεντικοποίηση μελών δικτύου τα οποία μπορεί να είναι χρήστες ή δικτυακές υπηρεσίες. Αναπτύχθηκε από το Massachusetts Institute of Technology (MIT) και το 2005 ανανεώθηκε από το Internet Engineering Task Force (IETF) προκειμένου να αυξηθεί η ασφάλεια του και να καλυφθούν αδυναμίες σε προηγούμενες εκδόσεις όπως η αποκλειστική χρήση του DES και η λήξη της διάρκειας ζωής των εισιτηρίων. [14]

Η λειτουργία του Κέρβερος βασίζεται σε ένα Κέντρο Διανομής Κλειδιών και για την περαιτέρω αύξηση της ασφάλειας της λειτουργίας του χρησιμοποιεί ένα εισιτήριο το οποίο ζητάει ο εκάστοτε χρήστης και το οποίο διέπεται από ένα χρόνο ζωής καθώς και από δεδομένα αυθεντικοποίησης του χρήστη Α στον χρήστη Β.

Ο χρήστης Α, όταν θέλει να επικοινωνήσει με τον χρήστη Β, δημιουργεί ένα μοναδικό αριθμό n_A τον οποίο στέλνει στο κέντρο μαζί με τις δυο ταυτότητες, την δική του και του χρήστη Β. Το κέντρο δημιουργεί το εισιτήριο του χρήστη Β για το οποίο επιλέγει χρόνο ζωής και στο οποίο κρυπτογραφεί το κλειδί συνόδου. Έπειτα το κέντρο στέλνει στον χρήστη Α το εισιτήριο του χρήστη Β καθώς και κρυπτογραφημένες με το κλειδί του χρήστη Α την διάρκεια ζωής και το κλειδί της συνόδου. Στη συνέχεια, ο χρήστης Α δημιουργεί τα δεδομένα αυθεντικοποίησης τα οποία αποτελούνται από το κλειδί συνόδου, μια νέα χρονοσφραγίδα και την ταυτότητα του Α , και τα στέλνει στον χρήστη Β σε συνδυασμό με την ταυτότητα του τελευταίου. Ο χρήστης Β παραλαμβάνει το εισιτήριο και ανακτά το κλειδί της συνόδου και το χρόνο ζωής. Στο σημείο αυτό ελέγχει αν είναι εντός χρονικών ορίων και αφού αποκρυπτογραφήσει το κείμενο αυθεντικοποίησης συγκρίνει την ταυτότητα με αυτή του

εισιτηρίου και ελέγχει την χρονοσφραγίδα. Τέλος, ο χρήστης Β κρυπτογραφεί την χρονοσσφραγίδα του χρήστη Α με το κλειδί της συνόδου και το αποστέλλει προκειμένου να αποδείξει ότι γνωρίζει το σωστό κλειδί. [4]

6.2.3 Εδραίωση Κλειδιού σε Ασύμμετρα Κρυπτοσυστήματα

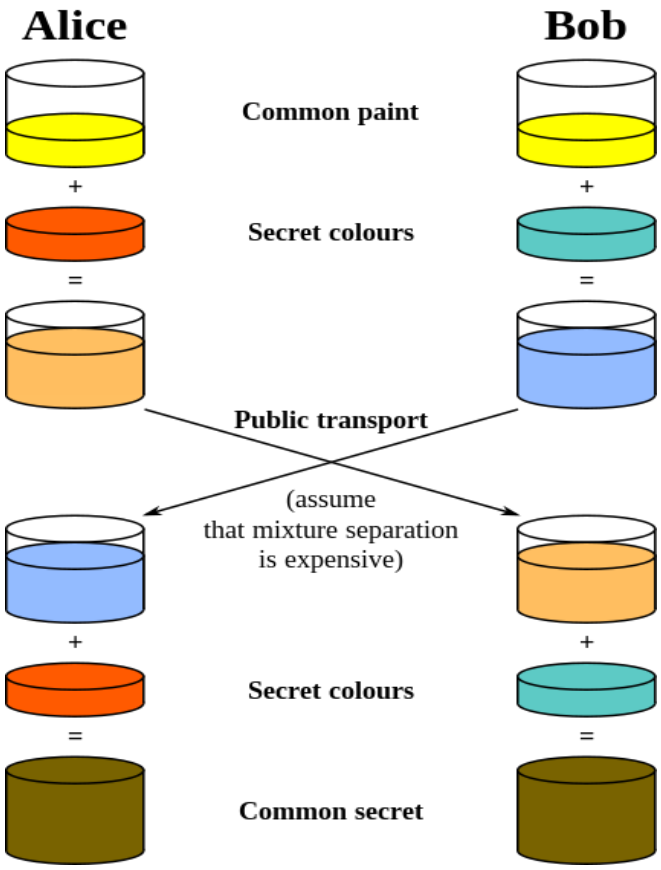
Η ασύμμετρη κρυπτογραφία διαφοροποιείται σε μεγάλο βαθμό από την συμμετρική στο γεγονός ότι πλέον δεν χρειάζεται κάποιο κέντρο προκειμένου να επικοινωνήσουν δύο μέρη. Από τη στιγμή που δεν είναι αναγκαίο ασφαλές κανάλι για την μεταφορά των κλειδιών, ο ρόλος πλέον των κέντρων περιορίζεται στην αποτροπή επιθέσεων προσποίησης ταυτότητας. [4]

6.2.4 Το πρωτόκολλο συμφωνίας των Diffie – Hellman

Το πρωτόκολλο των Diffie και Hellman είναι από τα πρώτα πρωτόκολλα ασύμμετρης εδραίωσης κλειδιών και βασίζεται στο πρόβλημα του διακριτού λογαρίθμου.

Για την λειτουργία του, τα δύο μέρη που θέλουν να επικοινωνήσουν αρκεί να επιλέξουν δημόσια έναν πρώτο αριθμό p και ένα γεννήτορα α του συνόλου Z_p^*. Στη συνέχεια, το κάθε μέρος αρκεί να επιλέξει ένα τυχαίο ακέραιο x και y και ο μεν χρήστης Α στέλνει την ποσότητα $\alpha^x \ mod \ p$, ενώ ο χρήστης Β την ποσότητα $\alpha^y \ mod \ p$. Το κλειδί της συνόδου είναι το $\alpha^{xy} \ mod \ p$. Τέλος, κάθε μέρος για να αποκρυπτογραφήσει το κλειδί, το υψώνει στον μυστικό εκθέτη που έχει επιλέξει.

Η εικόνα 4, σκιαγραφεί την παραπάνω ιδέα αντικαθιστώντας τους μαθηματικούς όρους με χρώματα.



Εικόνα 4 : Ιδέα Diffie-Hellman

(Πηγή : Wikipedia, https://commons.wikimedia.org/wiki/File:Diffie-Hellman_Key_Exchange.svg, άδεια Not eligible for copyright protection)

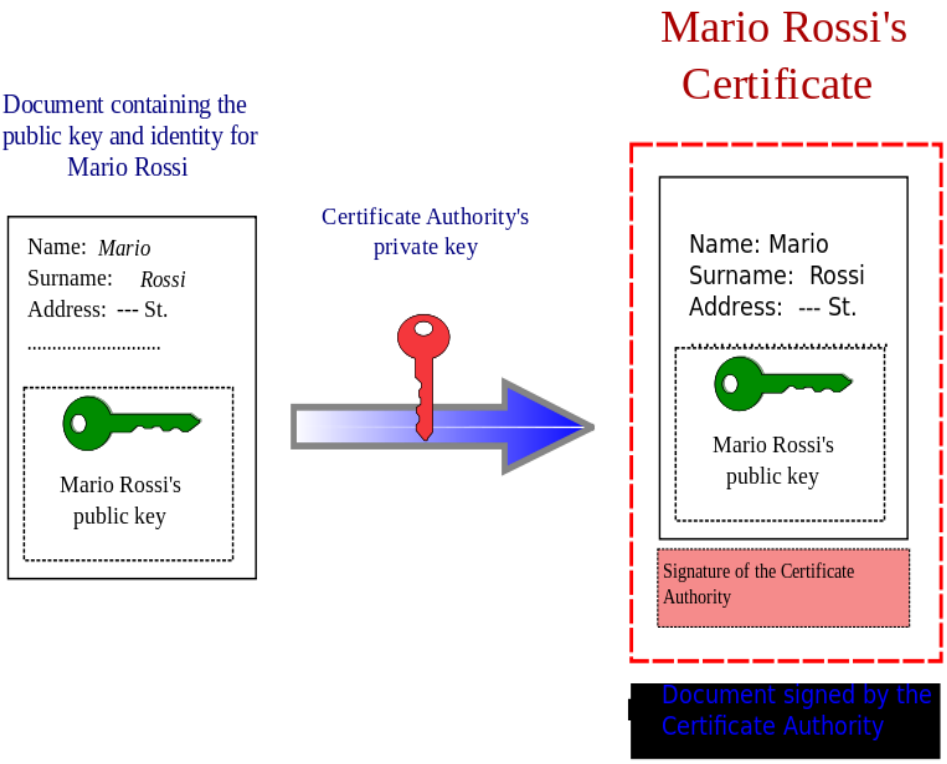
Όπως αναφέρθηκε και σε προηγούμενο κεφάλαιο, το πρόβλημα του διακριτού λογαρίθμου μπορεί να εφαρμοστεί και σε ελλειπτικές καμπύλες και συνεπώς και το συγκεκριμένο πρωτόκολλο θα μπορούσε να τα τροποποιηθεί προκειμένου να χρησιμοποιεί το πρόβλημα αυτό. [2] [4]

6.3 Πιστοποιητικά Δημοσίου Κλειδιού – Ψηφιακά Πιστοποιητικά

Ένα πιστοποιητικό δημοσίου κλειδιού (public key certificate) ή ψηφιακό πιστοποιητικό είναι μια δομή δεδομένων η οποία αντιστοιχίζει κάποιες ιδιότητες μιας φυσικής οντότητας στο δημόσιο κλειδί της. [2] Αποτελείται από δύο μέρη, το μέρος δεδομένων και το μέρος υπογραφής. Το μέρος δεδομένων περιλαμβάνουν τα στοιχεία της οντότητας καθώς και το δημόσιο κλειδί της, καθώς και πληροφορίες για τις κρυπτογραφικές συναρτήσεις που χρησιμοποιήθηκαν κατά την δημιουργία του. Το μέρος υπογραφής αποτελείται από την ψηφιακή υπογραφή μιας Αρχής Πιστοποίησης η οποία με χρήση μιας μονόδρομης συνάρτησης

δημιούργησε το πιστοποιητικό συναρτήσει μιας σύνοψης των μέρους των δεδομένων και του ιδιωτικού κλειδιού της. [4]

Η παραπάνω διαδικασία εμφανίζεται και στην Εικόνα 5.



Εικόνα 5 : Ψηφιακό Πιστοποιητικό

(Πηγή : Wikipedia, https://commons.wikimedia.org/wiki/File:PublicKeyCertificateDiagram_En.svg, άδεια CC Attribution-Share Alike 2.5 Generic, 2.0 Generic and 1.0 Generic)

6.3.1 Το πιστοποιητικό X.509

Το πιστοποιητικό X.509 είναι η τυποποίηση για κυριαρχεί στις υποδομές δημοσίου κλειδιού. Εμφανίστηκε για πρώτη φορά το 1988, ενώ το 2008 κυκλοφόρησε η έκδοση 3 η οποία και υιοθετήθηκε από τον IETF. [15] Η σημασία του διαφαίνεται από την χρήση του ως μέρος του Transport Layer Security (TLS) το οποίο χρησιμοποιείται εκτενώς για ασφαλή επικοινωνία στο Διαδίκτυο.

Τα πεδία του πιστοποιητικού παρουσιάζονται με μια σύντομη περιγραφή τους στον Πίνακα 1. [4] [15]

Όνομα Πεδίου	Χρήση
Version	Η έκδοση του προτύπου X.509.
Serial number	Ένας μοναδικός ακέραιος που καθορίζεται από την αρχή πιστοποίησης.
Signature algorithm identifier	Τα ονόματα και οι παράμετροι των κρυπτογραφικών συναρτήσεων που χρησιμοποιούνται.
Issuer name	Το όνομα της Αρχής Πιστοποίησης.
Period of validity	Η ημερομηνία ενεργοποίησης και λήξης του πιστοποιητικού.
Subject name	Το όνομα της οντότητας στην οποία ανήκει το πιστοποιητικό.
Algorithms	Το όνομα του κρυπταλγορίθμου που χρησιμοποιείται για την διανομή του δημοσίου κλειδιού της υπό πιστοποίηση οντότητας.
Parameters	Οι παράμετροι που καθορίζουν την λειτουργία του κρυπταλγορίθμου.
Subject’s public key	Το δημόσιο κλειδί της οντότητας.
Issuer unique identifier	Ένας αριθμός που σε συνδυασμό με το όνομα της Αρχής Πιστοποίησης την καθορίζει μονοσήμαντα
Subject unique identifier	Ένας αριθμός που σε συνδυασμό με το όνομα της οντότητας την καθορίζει μονοσήμαντα σε περίπτωση που εκδοθεί και άλλο πιστοποιητικό στο όνομα της

Extensions	Επιπλέον στοιχεία για απαιτήσεις της εφαρμογής
signature	Η ψηφιακή υπογραφή της Αρχής Πιστοποίησης η οποία έχει δημιουργηθεί με χρήση του ιδιωτικού κλειδιού της και συναρτήσει όλων των παραπάνω πληροφοριών.

Πίνακας 1 : Πεδία του πιστοποιητικού X.509

6.4 Υποδομές Δημόσιου Κλειδιού

Οι υποδομές δημόσιου κλειδιού (public key infrastructures, PKI) αποτελούν το σύνολο των πρωτοκόλλων και προτύπων που υποστηρίζουν την χρήση κρυπτογραφίας δημοσίου κλειδιού. Ο λόγος για τον οποίο δημιουργήθηκαν οι υποδομές αυτές είναι για να λύσουν το πρόβλημα της διανομής των δημοσίων κλειδιών των χρηστών, των οποίων ο αριθμός είναι πολύ μεγάλος. Λειτουργούν ως έμπιστη οντότητα και έτσι το δημόσιο κλειδί τους εξασφαλίζει την εγκυρότητα των δημοσίων κλειδιών των υπολοίπων. [2]

Πιο αναλυτικά, ένα PKI αποτελείται από :

- Αρχή Πιστοποίησης (Certification Authority). Είναι η οντότητα η οποία είναι υπεύθυνη για την πιστοποίηση των δημοσίων κλειδιών των χρηστών καθώς και την έκδοση πιστοποιητικών.
- Αρχή Καταχώρησης (Registration Authority). Αποτελεί μια συμπληρωματική στην Αρχή Πιστοποίησης οντότητα η οποία υλοποιεί ένα μέρος των λειτουργιών της. Συγκεκριμένα επαληθεύει την ταυτότητα των χρηστών, αρχικοποιεί την διαδικασία δημιουργίας πιστοποιητικού, δημιουργεί κλειδιά και αναφορές για ανάκληση πιστοποιητικών. Είναι σημαντικό να τονιστεί ότι δεν εκδίδει ούτε ανακαλεί πιστοποιητικά.
- Τελική Οντότητα (End – Entity). Είναι το υποκείμενο που πιστοποιείται από την Αρχή Πιστοποίησης. Μπορεί να είναι χρήστης ή ακόμα και εφαρμογή και αφού εκδοθεί πιστοποιητικό στο όνομα του πρέπει να εξασφαλίζει την ασφαλή του πρόσβαση στο ιδιωτικό του κλειδί, το όνομα της Αρχής Πιστοποίησης που εξέδωσε το πιστοποιητικό του καθώς και στο δημόσιο κλειδί του.

- Χώρος Αποθήκευσης (Repository Site). Αποτελεί το σύστημα που είναι υπεύθυνο για την αποθήκευση των πιστοποιητικών και των λιστών ανακληθέντων πιστοποιητικών. Ουσιαστικά είναι μια υπηρεσία καταλόγου με την οποία επικοινωνούν οι χρήστες όταν θέλουν να παραλάβουν το δημόσιου κλειδί μιας Τελικής Οντότητας. [2] [4] [16]

6.5 Δημιουργία, Χρήση και Ανάκληση Πιστοποιητικού Δημοσίου Κλειδιού

6.5.1 Δημιουργία και διανομή πιστοποιητικού δημοσίου κλειδιού

Στόχος του πιστοποιητικού είναι να αντιστοιχιστεί ένα όνομα με ένα δημόσιο κλειδί ή πιο πρακτικά να δημιουργηθεί ένα ζεύγος ιδιωτικού και δημοσίου κλειδιού όπου το δεύτερο θα κατατεθεί στην Αρχή Πιστοποίησης μαζί με τα στοιχεία του χρήστη. Η δημιουργία του ζεύγους κλειδιών γίνεται με δυο εναλλακτικές :

- Δημιουργία Κλειδιών από την Αρχή Πιστοποίησης: Σε αυτή την περίπτωση η Αρχή Πιστοποίησης δημιουργεί το δημόσιο κλειδί και το αντιστοιχεί σε μια οντότητα. Έπειτα, εκδίδει το πιστοποιητικό συναρτήσει των στοιχείων της οντότητας και του δημοσίου κλειδιού που δημιούργησε και ο χρήστης το παραλαμβάνει, αφού πρώτα ταυτοποιηθεί με φυσικό τρόπο, μέσα από ένα ασφαλές κανάλι επικοινωνίας. Η μέθοδος αυτή επιτρέπει την ασφαλή αποθήκευση των κλειδιών στην Αρχή Πιστοποίησης, γεγονός που από τη μια επιτρέπει την ανάκτηση του σε περίπτωση απώλειας από το μέρος του χρήστη, αλλά αφετέρου εγείρει θέματα ασφάλειας σε περίπτωση επιτυχούς επίθεσης στην Αρχή.
- Δημιουργία Κλειδιών από την Οντότητα: Στην περίπτωση αυτή, η δημιουργία του ζεύγους κλειδιών είναι ίδια με την παραπάνω και η μόνη διαφοροποίηση έγκειται στο γεγονός ότι ο χρήστης είναι υπεύθυνος για την δημιουργία των κλειδιών. Η αποστολή στην Αρχή Πιστοποίησης γίνεται μέσα από ένα ασφαλές κανάλι το οποίο εγγυάται την αυθεντικότητα του μηνύματος.

Η Αρχή Πιστοποίησης μετά την δημιουργία των πιστοποιητικών, έχει τρεις τρόπους για να τα διανείμει. Η πρώτη μέθοδος είναι εκείνη της δημοσίευσης σε ένα δημόσιο κατάλογο στον οποίο όλοι οι χρήστες έχουν δικαίωμα ανάγνωσης. Κατά την δεύτερη μέθοδο, υιοθετείται ένα προωθητικό μοντέλο κατά το οποίο είτε όλα μαζί, είτε περιοδικά, στέλνονται σε όλους

τους χρήστες τα πιστοποιητικά. Η τρίτη μέθοδος βασίζεται στους χρήστες οι οποίοι προμηθεύουν σε όποιον το αιτείται το πιστοποιητικό τους. [2] [4]

6.5.2 Χρήση και Επιβεβαίωση πιστοποιητικού δημοσίου κλειδιού

Έστω ένα σενάριο στο οποίο δυο οντότητες, η Α και η Β, θέλουν να επικοινωνήσουν και η οντότητα Β θέλει να ελέγξει την αυθεντικότητα του πιστοποιητικού της οντότητας Α.

Αρχικά, η οντότητα Β αποκτάει το δημόσιο κλειδί της Αρχής Πιστοποίησης και το δημόσιο κλειδί της οντότητας Α καθώς και το πιστοποιητικό της οντότητας Α. Στη συνέχεια, εκτελούνται τρεις ενέργειες ελέγχου. Η πρώτη ενέργεια αφορά τον έλεγχο των στοιχείων του πιστοποιητικού και τον συσχετισμό με τα στοιχεία του Α. Η δεύτερη ενέργεια είναι η εξέταση της χρονικής περιόδου εγκυρότητας του πιστοποιητικού και κατά πόσο αυτό θεωρείται επίκαιρο. Τέλος, εξετάζεται αν το πιστοποιητικό της οντότητας Α έχει ανακληθεί. Αν η οντότητα Β εκτελέσει με επιτυχία τους παραπάνω ελέγχους είναι σε θέση να επιβεβαιώσει την ταυτότητας της οντότητας Α και να προχωρήσει σε επικοινωνία με χρήση ασύμμετρης κρυπτογραφίας. [2] [4]

6.5.3 Ανάκληση πιστοποιητικών δημοσίου κλειδιού

Κάθε πιστοποιητικό που δημιουργείται έχει μια προκαθορισμένη διάρκεια ζωής. Υπάρχουν, όμως, περιπτώσεις κατά τις οποίες η Αρχή Πιστοποίησης είναι αναγκασμένη να ανακαλέσει ένα πιστοποιητικό πριν την λήξη του κύκλου της ζωής του.

Οι περιπτώσεις αυτές μπορούν να κατηγοριοποιηθούν σε δύο επιμέρους. Στην πρώτη περίπτωση, μια οντότητα μπορεί να υποψιάζεται την υποκλοπή του ιδιωτικού της κλειδιού, ενώ στην δεύτερη μπορεί η οντότητα να κάνει κακή χρήση του πιστοποιητικού, μη προβλεπόμενη δηλαδή από την Αρχή Πιστοποίησης.

Η ανάκληση ενός πιστοποιητικού δημοσίου κλειδιού μπορεί να γίνει με τέσσερις εναλλακτικές μεθόδους :

- Χειροκίνητα. Στην περίπτωση αυτή όλοι οι χρήστες ειδοποιούνται μέσα από ένα κανάλι για το ανακληθέν πιστοποιητικό.
- Με χρήση Δημοσίου Φακέλου Ανακληθέντων. Υπάρχει ένας δημόσιος φάκελος ανακληθέντων πιστοποιητικών ο οποίος πρέπει να ελέγχεται πριν από τη χρήση ενός δημοσίου κλειδιού
- Με χρήση Λιστών Ανακληθέντων Πιστοποιητικών. Αυτή η λύση είναι μια μέθοδος διαχείρισης ενός δημοσίου φακέλου ανακληθέντων.

- Με χρήση Πιστοποιητικών Ανάκλησης. Αποτελούν πιστοποιητικά δημοσίου κλειδιού τα οποία έχουν ένα πεδίο με όνομα σημαία ανάκλησης και χρόνος ανάκλησης και κάθε φορά εισάγονται στη θέση του ανακληθέντος πιστοποιητικού.

Στις υποδομές δημοσίου κλειδιού που περιγράφηκαν παραπάνω, χρησιμοποιούνται οι λίστες ανακληθέντων πιστοποιητικών. Σε αυτή την λίστα, η οποία είναι ψηφιακά υπογεγραμμένη από την Αρχή Αυθεντικοποίησης, κάθε εγγραφή περιλαμβάνει τον σειριακό αριθμό, τη χρονική στιγμή ανάκλησης καθώς και τον λόγο της ανάκλησης ενός πιστοποιητικού

Παράλληλα, υπάρχει μια ειδική λίστα με όνομα Λίστα Ανακληθέντων Πιστοποιητικών Αρχής η οποία καταγράφει τα πιστοποιητικά διαπιστοποίησης μεταξύ Αρχών Πιστοποίησης.

Για λόγους απόδοσης και κόστους, καθώς το μέγεθος των λιστών αυτών μπορεί να μεγαλώσει ταχύτατα, οι παραπάνω λίστες διασπώνται σε τμήματα και διανέμονται στους χρήστες. Οι τεχνικές με τις οποίες επιτυγχάνεται αυτό είναι τρείς. Κατά την πρώτη, κάθε νέα ενημέρωση της λίστας περιλαμβάνει μόνο νέες εγγραφές ανακληθέντων πιστοποιητικών και κάθε χρήστης καλείται να διατηρεί παλαιότερες και ενημερωμένες μορφές της λίστας. Στη δεύτερη μέθοδο, η λίστα διασπάται σε μέρη ανάλογα με τον λόγο ανάκλησης του πιστοποιητικού. Τέλος, η τρίτη μέθοδος είναι αυτή κατά την οποία κάθε λίστα διασπάται σε υπο-λίστες και κατά την δημιουργία ενός πιστοποιητικού αυτό αντιστοιχίζεται σε μια από αυτές . Οι υπο-λίστες αυτές έχουν ένα άνω φράγμα στην χωρητικότητα τους το οποίο μόλις ξεπεραστεί δημιουργείται μια νέα υπο-λίστα. [2] [4]

ΚΕΦΑΛΑΙΟ 7: ΒΙΒΛΙΟΓΡΑΦΙΑ

7.1 Βιβλιογραφία

[1] S. Singh, The Code Book, Εκδοτικός Οίκος Π.ΤΡΑΥΛΟΣ, 1999.

[2] M. Burmester, Σ. Γκρίτζαλης, Σ. Κάτσικας και Β. Χρυσακόπουλος, Σύχγρονη Κρυπτογραφία : Θεωρία και Εφαρμογές, Αθήνα: Εκδόσεις Παπασωτηρίου, 2011.

[3] A. S. Tanenbaum, Computer Networks, Prentice Hall, 2003.

[4] Β. Α. Κάτος και Γ. Χ. Στεφανίδης, Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης, Θεσσαλονίκη: Εκδόσεις Ζυγός, 2003.

[5] J. Daemen και V. Rijmen, *AES Submission document on Rijndael,* 1999.

[6] A. Popov, «IETF,» Internet Engineering Task Force, February 2015. [Ηλεκτρονικό]. Available: https://tools.ietf.org/html/rfc7465. [Πρόσβαση 19 December 2016].

[7] K. Thorsten, A. Kazumaro, F. Jens, L. Arjen, T. Emmanuel, B. Joppe, G. Pierrick, K. Alexander, M. Peter, A. O. Dag, t. R. Herman, T. Andrey και Z. Paul, «Factorization of a 768-bit RSA modulus,» 2010.

[8] U. S. D. o. Commerce, «FEDERAL INFORMATION PROCESSING STANDARDS - Secure Hash Standard (SHS),» Gaithersburg, 2012.

[9] B. Schneier, «Cryptanalysis of SHA-1,» 18 February 2005. [Ηλεκτρονικό]. Available: https://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html. [Πρόσβαση 20 December 2016].

[10] D. Christoph, E. Maria και M. Florian, «Analysis of SHA-512/224 and SHA-512/256,» Graz University of Technology, Austria, 2016.

[11] S. J. Chang, «Announcing Approval of Federal Information Processing Standard (FIPS) 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, and Revision of the Applicability Clause of FIPS 180-4, Secure Hash Standard,» National Institute of Standards and Technology, Gaithersburg, 2015.

[12] P. Barreto, «Whirlpool Page,» 25 November 2008. [Ηλεκτρονικό]. Available: http://www.larc.usp.br/~pbarreto/WhirlpoolPage.html. [Πρόσβαση 20 December 2016].

[13] U. S. D. o. Commerce, «FEDERAL INFORMATION PROCESSING STANDARDS - Digital Signature Standard (DSS),» National Institute of Standards and Technology, Gaithersburg, 2013.

[14] C. Neuman, T. Yu, S. Hartman και K. Raeburn, «The Kerberos Network Authentication Service (V5) [RFC 4120],» IETF, July 2005.

[15] D. Cooper, S. Santesson, F. Farreli, S. Boeyen, R. Housley και W. Polk, «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [RFC 5280],» IETF, 2008.

[16] Microsoft, «Public Key Infrastructure,» Microsoft, [Ηλεκτρονικό]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/bb427432%28v=vs.85%29.aspx?f=255&MSPPError=-2147217396. [Πρόσβαση 13 January 2017].