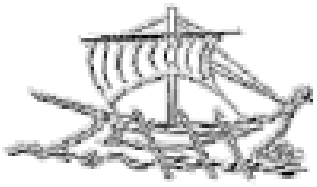


ΑΕΙ ΠΕΙΡΑΙΑ Τ.Τ.

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ Τ.Τ.

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μελέτη Πρωτοκόλλων Κρυπτογραφίας

Άννα Ελένη Κ. Γεωργοπούλου

Εισηγητής: Δρ Παναγιώτης Γιαννακόπουλος, Καθηγητής

ΑΘΗΝΑ
ΔΕΚΕΜΒΡΙΟΣ 2015

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μελέτη Πρωτοκόλλων Κρυπτογραφίας

Άννα Ελένη Κ. Γεωργοπούλου
Α.Μ. 39095

Εισηγητής:

Δρ Παναγιώτης Γιαννακόπουλος, Καθηγητής

Εξεταστική Επιτροπή:

Ημερομηνία εξέτασης

ΕΥΧΑΡΙΣΤΙΕΣ

Οφείλω να ευχαριστήσω τον επιβλέποντα καθηγητή μου , κύριο Γιαννακόπουλο Παναγιώτη για την πολύτιμη βοήθειά του και την άρτια επιστημονική καθοδήγηση ώστε να ολοκληρωθεί η παρούσα διπλωματική εργασία.

Επιπλέον, θα ήθελα να ευχαριστήσω τους γονείς μου, Κωνσταντίνο και Γεωργία, καθώς και τον αδερφό μου Γιώργο που με στήριξαν καθόλη τη διάρκεια των σπουδών μου.

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία ασχολείται με τη Κρυπτογραφία, αναλύοντας τις βασικές της έννοιες, τεχνικούς όρους καθώς και διάφορους αλγορίθμους (συμμετρικούς και ασύμμετρους) που έχουν αναπτυχθεί ιστορικά, κατά το πέρασμα των χρόνων. Επιπλέον, πραγματοποιείται καταγραφή των βασικών κρυπτογραφικών πρωτοκόλλων που εφαρμόζονται στις διανομές συμμετρικών και ασύμμετρων κλειδιών παραθέτοντας τις χρήσεις του κάθε πρωτοκόλλου, καθώς τα πλεονεκτήματα και τα μειονεκτήματά τους. Επίσης, περιγράφονται μέθοδοι και τεχνικές διασφάλισης απαιτήσεων όπως της εμπιστευτικότητας, της ακεραιότητας, της αυθεντικοποίησης και της αποποίησης. Στο τέλος, γίνεται μια προσπάθεια μελέτης της θεωρητικής κβαντικής κρυπτογραφίας με βασικά στοιχεία από αυτή. Όλα τα παραπάνω κρίνονται απαραίτητα στην επίτευξη ασφαλούς μεταφοράς δεδομένων τόσο στα δίκτυα όσο και στους ηλεκτρονικούς υπολογιστές.

ABSTRACT

This thesis deals with cryptography, analyzing its basic definitions and a variety of algorithms that have been developed historically, by the passage of time. Moreover, it lists their basic cryptographic protocols applicable to distributions of symmetric and asymmetric keys, quoting the uses of each protocol, as its advantages and disadvantages. Also, they are described the methods and the requirements assurance techniques such as confidentiality, integrity, authentication and disclaimers. In the end, there is an attempt to study theoretical quantum cryptography, examining the most important elements of it. All the above are deemed necessary to achieve safe data transfer in both networks and on computers.

ΕΠΙΣΤΗΜΟΝΙΚΗ ΠΕΡΙΟΧΗ: ΚΡΥΠΤΟΓΡΑΦΙΑ

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: συμμετρική, ασύμμετρη, κλειδί, αυθεντικοποίηση, κβαντοδυφίο

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

DES	Data Encryption Standard
TDES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
RC5	Rivest Cipher 5
RC6	Rivest Cipher 6
RSA	Ron **R**ivest, Adi **S**hamir, Len **A**dleman
RFC	Requests for Comments
IDEA	International Data Encryption Algorithm
CA	Certificate Authority
DSS	Digital Signature Standard
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECB	Electronic Code Book
CBC	Cipher Block Chaining
CFB	Cipher Feedback
OFB	Output Feedback
IV	Initialization Vector
KDC	Key Distribution Center
PKI	Public Key Infrastructure
FEP	Front-End Processor
EDE	Encryption - Decryption – Encryption
EEE	Encrypt – Encrypt – Encrypt
VPNs	Virtual Private Metworks
MAC	Message Authentication Code
HMAC	Hash Message Authentication Code
IP	Internet Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TCP	Transmission Control Protocol
HDLC	High-Level Data Link Control
NSA	National Security Agency
NIST	National Institute of Standards and Technology

IBM International Business Machines

EFF Electronic Frontier Foundation

ANSI American National Standards Institute

FIPS Federal Information Processing Standards

CNOT Controlled NOT gate

ATM Automated Teller Machine

ΚΕΦΑΛΑΙΟ 1

1. ΕΙΣΑΓΩΓΗ

Στο κεφάλαιο αυτό αναλύεται το αντικείμενο της πτυχιακής εργασίας, τη Κρυπτογραφία. Γίνεται μια ιστορική αναδρομή γύρω από τις μεθόδους και τους αλγορίθμους που έχουν αναπτυχθεί σε αυτή τη περιοχή.

1.1 Περιγραφή του αντικειμένου της πτυχιακής εργασίας

Αντικείμενο της παρούσας πτυχιακής εργασίας είναι η καταγραφή και ανάπτυξη των βασικότερων κρυπτογραφικών πρωτοκόλλων. Με τη βοήθεια αυτών των πρωτοκόλλων πραγματοποιούνται οι διανομές κλειδιών σε συμμετρικά και ασύμμετρα συστήματα κρυπτογραφίας. Επιπλέον, θα γίνει προσπάθεια να μελετηθούν τα βασικά στοιχεία της θεωρητικής κβαντικής κρυπτογραφίας η οποία αποτελεί το μέλλον της σύγχρονης κρυπτογραφίας.

1.2 Ιστορική αναδρομή

Πρώτη περίοδος κρυπτογραφίας

Η πρώτη περίοδος κρυπτογραφίας υπολογίζεται μεταξύ 1900 π.Χ – 1900 μ.Χ., κατά τη διάρκεια της οποίας αναπτύχθηκε ένας μεγάλος αριθμός μεθόδων και αλγορίθμων κρυπτογράφησης βασιζόμενοι κυρίως σε απλές αντικαταστάσεις γραμμάτων. Στις μέρες μας όμως, όλα αυτά τα συστήματα έχουν κρυπταναλυθεί και έχει αποδειχθεί ότι, εφόσον ένα μεγάλο κομμάτι του κρυπτογραφικού μηνύματος είναι γνωστό, τότε η επανάκτηση του αρχικού μηνύματος είναι σχετικά εύκολη.

Σύμφωνα με μια σφηνοειδή επιγραφή η οποία ανακαλύφθηκε στις όχθες του ποταμού τίγρη, οι πολιτισμοί που αναπτύχθηκαν στη Μεσοποταμία άρχισαν να ασχολούνται με την κρυπτογραφία ήδη από το 1500 π.Χ.. Η επιγραφή αυτή θεωρείται από τα αρχαιότερα κρυπτογραφικά μηνύματα, και περιγράφει το τρόπο κατασκευής σμάλτων για αγγειοπλαστική. Επιπλέον, το αρχαιότερο βιβλίο θεωρείται μια επιγραφή που ανακαλύφθηκε στη *Σούσα της Περσίας* και περιλαμβάνει τους αριθμούς 1-8 και 32-35, τοποθετημένους τον ένα κάτω από τον άλλον, και απέναντι τους βρίσκονται τα σφηνοειδή σύμβολα για το κάθε ένα αντίστοιχα.

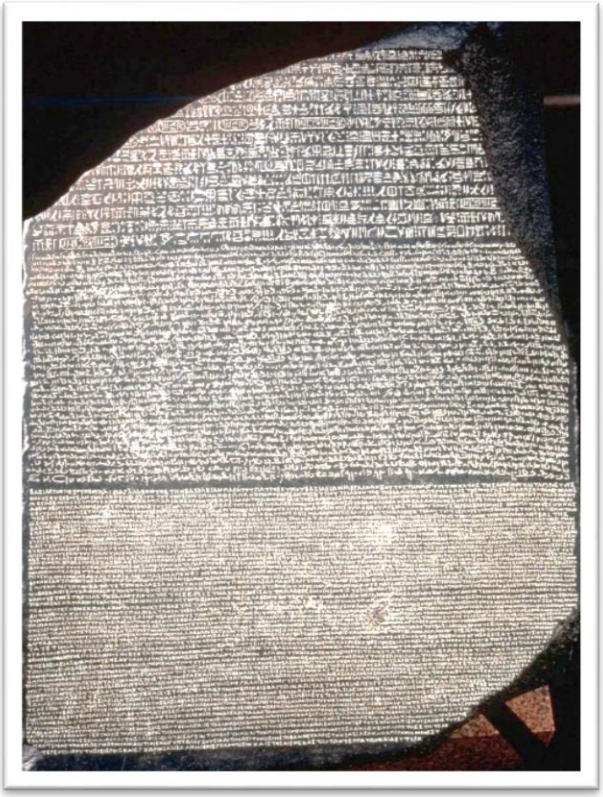
Η κρυπτογραφία χρησιμοποιήθηκε πρώτη φορά για στρατιωτικούς λόγους από τους Σπαρτιάτες. Γύρω στον 5ο αιώνα π.Χ ανακάλυψαν τη πρώτη κρυπτογραφική συσκευή, τη «σκυτάλη», στην οποία χρησιμοποίησαν την μέθοδο της μετάθεσης. Σύμφωνα με τον Πλούταρχο, η «Σπαρτιατική Σκυτάλη» ήταν μια ξύλινη ράβδος ορισμένης διαμέτρου, στην οποία βρισκόταν τυλιγμένη μια λωρίδα περγαμηνής. Το κείμενο ήταν γραμμένο σε στήλες, με ένα γράμμα σε κάθε έλικα, έτσι όταν δεν ξετύλιγαν τη λωρίδα, το κείμενο ήταν δυσνόητο εξαιτίας της αναδιάταξης των γραμμάτων. Το κλειδί για την αποκρυπτογράφηση ήταν η διάμετρος της σκυτάλης.

Εικόνα 0.1: *Σπαρτιατική σκυτάλη*

Τα συστήματα που χρησιμοποιήθηκαν κυρίως στην αρχαιότητα, ήταν βασισμένα περισσότερο στην στεγανογραφία και λιγότερο στην κρυπτογραφία. Αν και δεν γνωρίζουμε αν και πότε χρησιμοποιήθηκαν τα συστήματα γραπτής αντικατάστασης γραμμάτων, τα συναντάμε στην Ρωμαϊκή Αυτοκρατορία, κυρίως επί βασιλεία του Ιούλιου Καίσαρα, ο οποίος αλληλογραφούσε με τον Κικέρωνα και άλλους φίλους του, αντικαθιστώντας τα γράμματα του κειμένου, με γράμματα μετατοπισμένα κατά 3 θέσεις μετά, στο Λατινικό Αλφάβητο. Στις μέρες μας, τα συστήματα που στηρίζονται στην αντικατάσταση γραμμάτων με άλλα γράμματα που είναι μετατοπισμένα κατά ένα καθορισμένο αριθμό θέσεων δεξιά ή αριστερά της αλφαβήτου, ονομάζονται κρυπτοσύστημα ***αντικατάστασης του Καίσαρα***.

Κατά τη διάρκεια του Μεσαίωνα, η κρυπτολογία θεωρήθηκε ως μια μορφή μαύρης μαγείας, γεγονός που καθυστέρησε την ανάπτυξή της. Η συνέχιση της εξέλιξης της κρυπτογραφίας αλλά και των μαθηματικών, πραγματοποιήθηκε από τους Άραβες, οι οποίοι ήταν οι πρώτοι που εφηύραν και χρησιμοποίησαν μεθόδους

κρυπτανάλυσης. Επιπλέον πρέπει να τονίσουμε ότι ήταν αυτοί που επινόησαν τη χρησιμοποίηση των γραμμάτων κειμένου, σε συνδυασμό με τις συχνότητες εμφάνισης των γραμμάτων στα κείμενα των γραμμάτων της γλώσσας. Όμως, μεγάλη ανάπτυξη στον τομέα της κρυπτανάλυσης παρατηρείται μέσα στους επόμενους αιώνες λόγω των στρατιωτικών εξελίξεων. Το 1563 δημοσιεύθηκε από τον Ιταλό *Giovanni Batista Porta* σπουδαίο βιβλίο κρυπτολογίας «De furtivis literarum notis», το οποίο περιλάμβανε τα πολυαλφαβητικά συστήματα κρυπτογράφησης αλλά και τα διγραφικά, όπου δύο γράμματα αντικαθίστανται από ένα.



Εικόνα 0.2: *Στήλη της Ροζέτας*

Σπουδαίος εκπρόσωπος εκείνης της εποχής ήταν επίσης και ο Γάλλος Vigenere, του οποίου ο πίνακας πολυαλφαβητικής αντικατάστασης, χρησιμοποιείται μέχρι και σήμερα.

Ο C.Wheatstone, γνωστός μέσα από τις έρευνες του στον ηλεκτρισμό, παρουσίασε τη πρώτη μηχανή κρυπτοσυσκευή, που αποτέλεσε και τη βάση για την ανάπτυξη κρυπτομηχανών στη δεύτερη περίοδο της κρυπτογραφίας. Η αποκρυπτογράφηση των αιγυπτιακών ιερογλυφικών, ήταν ένα από τα μεγαλύτερα επιτεύγματα, καθώς επί αιώνες παρέμεναν μυστήριο για τους αρχαιολόγους. Τον 17ο αιώνα το

ενδιαφέρον για την αποκρυπτογράφηση ιερογλυφικών αναζωπυρώθηκε και το 1652 ο Γερμανός Αθανάσιος Κίρχερ δημοσίευσε ένα λεξικό ερμηνείας τους σε μια αποτυχημένη προσπάθεια να ερμηνεύσει τις αιγυπτιακές γραφές. Ωστόσο, αυτή η προσπάθεια άνοιξε το δρόμο για την σωστή ερμηνεία των ιερογλυφικών, που προχώρησε χάρη της ανακάλυψης της *«Στήλης της Ροζέτας»*. Η «Στήλη της Ροζέτας» ήταν μια μεγάλη πέτρινη στήλη που βρέθηκε στα στρατεύματα του Ναπολέοντα στην Αίγυπτο και πάνω της ήταν χαραγμένη η ίδια επιγραφή τρεις φορές, μια σε ιερογλυφικά, μια σε ιερατική γραφή και μια στα ελληνικά. Μέχρι να επινοηθεί το αλφάβητο, οι προϊστορικοί πληθυσμοί χρησιμοποίησαν τρεις γραφές οι οποίες κατατάσσονται χρονολογικά:

- 3000 – 1600 π.χ. : Εικονογραφική (Ιερογλυφική) γραφή
- 1850 – 1450 π.χ. : Γραμμική Α
- 1450 – 1200 π.χ. : Γραμμική Β

Η Κρητική εικονογραφική γραφή, δεν έχει αποκρυπτογραφηθεί ακόμη, όμως είμαστε σε θέση να γνωρίζουμε ότι δεν αποτελεί γραφή που χρησιμοποιεί εικόνες ως σημεία αλλά πρόκειται για μια φωνητική γραφή που εξαντλείται σε περίπου διακόσους σφραγιδόλιθους. Κάνει την εμφάνιση της στο *δίσκο της Φαιστού*, ο οποίος ανακαλύφθηκε το 1908. Ο δίσκος της Φαιστού είναι μια στρογγυλή πινακίδα που φέρει γραφή με τη μορφή δύο σπειρών. Τα σύμβολα δεν είναι χειροποίητα, αλλά έχουν χαραχθεί με τη βοήθεια σφραγίδων, καθιστώντας τον Δίσκο ως το αρχαιότερο δείγμα στοιχειοθεσίας. Μέχρι και σήμερα δεν έχει αποκρυπτογραφηθεί και αποτελεί τη πιο μυστηριώδης αρχαία ευρωπαϊκή γραφή.

Εικόνα 0.3: *Ο δίσκος της Φαιστού*

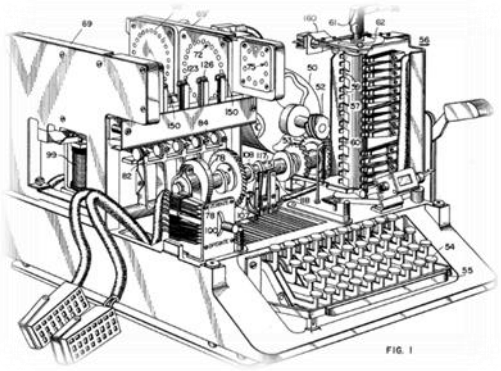
Δεύτερη περίοδος κρυπτογραφίας

Η δεύτερη περίοδος της κρυπτογραφίας χρονολογείται στις αρχές του 20ού αιώνα μέχρι το 1950. Επομένως, καλύπτει και τους δύο παγκοσμίους πολέμους οι οποίοι αποτέλεσαν και την αιτία, λόγω της ανάγκης για ασφαλή μετάδοση σημαντικών πληροφοριών, για την ραγδαία ανάπτυξη της κρυπτογραφίας. Εκείνη την περίοδο τα κρυπτοσυστήματα αρχίζουν να γίνονται πιο περίπλοκα και να αποτελούνται από μηχανικές και ηλεκτρομηχανικές κατασκευές, τις «κρυπτομηχανές». Για να μπορέσει να επιτευχθεί η κρυπτανάλυση αυτών των συστημάτων υπήρχε απαίτηση για μεγάλο αριθμό προσωπικού που θα εργαζόταν για μεγάλο χρονικό διάστημα, καθώς και μεγάλη υπολογιστική ισχύς. Παρά το γεγονός ότι τα συστήματα εκείνης της περιόδου ήταν αρκετά πολύπλοκα, η κρυπτανάλυση τους ήταν συνήθως επιτυχημένη. Οι Γερμανοί χρησιμοποιούσαν κυρίως ένα σύστημα που είναι γνωστό ως *Enigma* την οποία κατάφερε να παραβιάσει ο Marian Rejewski το 1932 στην Πολωνία, χρησιμοποιώντας θεωρητικά μαθηματικά.

Η αποκρυπτογράφηση μηνυμάτων που βασίζονταν στο Enigma, συνεχίστηκε από τους Πολωνούς μέχρι το 1939. Τότε, ο γερμανικός στρατός έκανε κάποιες αλλαγές, με αποτέλεσμα οι Πολωνοί να μην είναι σε θέση να παρακολουθήσουν, καθώς η αποκρυπτογράφηση πλέον απαιτούσε περισσότερους πόρους από αυτούς που είχαν διαθέσιμους. Έτσι, η γνώση τους μαζί με κάποιες μηχανές που είχαν κατασκευαστεί από τους ίδιους μεταβιβάστηκαν στους Γάλλους και τους

Βρετανούς. Ακόμη και ο Rejewski και οι μαθηματικοί του συνεργάστηκαν με τους Γάλλους και τους Βρετανούς, συνεργασία που ακολούθησαν και ο Alan Turing, Gordon Welchman και πολλούς άλλους, και οδήγησε σε ένα μεγάλο αριθμό αποκρυπτογραφήσεων διαφόρων παραλλαγών του Enigma, με την βοήθεια ενός υπολογιστή βρετανικής κατασκευής, του *Colossus*, ο οποίος καταστράφηκε μετά το τέλος του πολέμου.

Στον δεύτερο παγκόσμιο πόλεμο, χρησιμοποιήθηκαν από τους συμμάχους κρυπτομηχανές όπως το βρετανικό *TypeX* και το αμερικανικό *SIGABA*, τα οποία ήταν ηλεκτρομηχανικά σχέδια παρόμοια με το Enigma, αλλά με πολλές βελτιώσεις. Δεν έγινε γνωστό να παραβιάστηκε κάποιο από τα δύο κατά τη διάρκεια του πολέμου.



Εικόνα 0.4: *Κρυπτομηχανή SIGABA*

Επιπλέον πρέπει να τονιστεί ότι κατά τη διάρκεια του δευτέρου παγκοσμίου πολέμου επινοήθηκε από τις ένοπλες δυνάμεις των Η.Π.Α ο πιο επιτυχημένος κώδικας. Ο κώδικάς αυτός χρησιμοποιούσε Ινδιάνους Ναβάχο οι οποίοι μιλούσαν μεταξύ τους χρησιμοποιώντας συγκεκριμένες λέξεις δικές τους για τους στρατιωτικούς όρους. Η γλώσσα των Navajo είναι τονική, περίπλοκη, και δεν έχει γραπτή μορφή.

Τρίτη περίοδος κρυπτογράφησης

Αυτή η περίοδος χρονολογείται από το 1950 μέχρι σήμερα και χαρακτηρίζεται από την ραγδαία ανάπτυξη στους κλάδους των μαθηματικών, της μικροηλεκτρονικής και των υπολογιστικών συστημάτων. Η περίοδος της σύγχρονης κρυπτογραφίας ξεκινά με τον πατέρα των μαθηματικών συστημάτων κρυπτογραφίας όπως αποκαλέστηκε, τον *Claude Shannon*, ο οποίος δημοσίευσε

το έγγραφο *«Θεωρία επικοινωνίας των συστημάτων μυστικότητας»* και λίγο αργότερα το βιβλίο *«Μαθηματική Θεωρία της Επικοινωνίας»*.

Στα μέσα της δεκαετίας του 1970, πραγματοποιήθηκαν δύο σπουδαίες δημοσιεύσεις. Η πρώτη ήταν αυτή του σχεδίου προτύπου κρυπτογράφησης DES (Data Encryption Standard) το 1975. Ο DES χρησιμοποιήθηκε προκειμένου να αναπτυχθούν ασφαλείς ηλεκτρονικές εγκαταστάσεις επικοινωνίας σε μεγάλες επιχειρήσεις. Ο DES αποτέλεσε τον πρώτο προσιτό αλγόριθμο κρυπτογράφησης που εγκρίθηκε από μια εθνική αντιπροσωπεία όπως η NSA.

Μετά από αναγγελία του NIST (National Institute of Standards and Technology) ο DES αντικαταστάθηκε από τον AES το 2001. Αν και ο DES αλλά και οι παραλλαγές του χρησιμοποιούνται μέχρι και σήμερα, το μέγεθος του (56-bit) θεωρείται ανεπαρκές σε επιθέσεις ωμής βίας (μια τέτοια επίθεση κατάφερε να σπάσει το DES μέσα σε 56 ώρες). Επομένως, γίνεται κατανοητό ότι η χρήση του DES στα νέα κρυπτογραφικά συστήματα δεν είναι με βεβαιότητα ασφαλές, και μηνύματα που προστατεύονται από παλαιότερα συστήματα που χρησιμοποιούσαν DES, διατρέχουν κίνδυνο αποκρυπτογράφησης.

1.3 Ανασκόπηση της πτυχιακής εργασίας

Στο δεύτερο κεφάλαιο πραγματοποιείται μια εισαγωγή στη κρυπτογραφία, εξηγώντας αρχικά τους βασικούς τεχνικούς της όρους και παραθέτοντας στη συνέχεια τη χρησιμότητά της και τα πεδία που βρίσκει εφαρμογή στις μέρες μας. Επιπλέον, γίνεται μια σύντομη ανάλυση στους βασικότερους κρυπτογραφικούς αλγορίθμους και στην ισχύ αυτών.

Στο τρίτο και τέταρτο κεφάλαιο αναλύονται οι πιο σημαντικοί αλγόριθμοι κρυπτογράφησης μυστικού και δημόσιου κλειδιού αντίστοιχα, εξηγώντας το τρόπο λειτουργία τους και δίνοντας παραδείγματα για την καλύτερη κατανόησή τους. Ακολούθως, στο πέμπτο κεφάλαιο καταγράφονται και αναπτύσσονται κρυπτογραφικά πρωτόκολλα που χρησιμοποιούνται για τη διανομή τόσο δημόσιων όσο και ιδιωτικών κλειδιών.

Στο επόμενο κεφάλαιο γίνεται ανάλυση των ψηφιακών υπογραφών και πιστοποιητικών, καθώς επίσης σύγκριση και παρουσίαση των πιο αντιπροσωπευτικών τους κωδίκων. Στη συνέχεια, στο έβδομο κεφάλαιο,

παρουσιάζεται η αναλυτική λειτουργία μερικών από των πιο σημαντικών συναρτήσεων που χρησιμοποιούνται στη κρυπτογραφία.

Στο όγδοο και τελευταίο κεφάλαιο, γίνεται προσπάθεια να μελετηθούν κάποια βασικά στοιχεία της θεωρητικής κβαντικής κρυπτογραφίας όπως ο κβαντικός υπολογιστής και η στοιχειώδης μονάδα κβαντικής πληροφορίας.

ΚΕΦΑΛΑΙΟ 2ο

1. ΚΡΥΠΤΟΓΡΑΦΙΑ

2.1 Γενικές πληροφορίες

Η λέξη κρυπτογραφία (cryptography) είναι μια σύνθετη λέξη που αποτελείται από τα συνθετικά «κρυπτός» και «γράφω» και αποτελεί έναν διεπιστημονικό κλάδο που ασχολείται με τη μελέτη, την ανάπτυξη και τη χρήση τεχνικών *κρυπτογράφησης* (encryption) και *αποκρυπτογράφησης* (decryption) με στόχο την απόκρυψη περιεχομένων διαφόρων μηνυμάτων.

Η κρυπτογραφία είναι ένας από τους κλάδους ενός ευρύτερου διεπιστημονικού πεδίου, αυτού της Κρυπτολογίας όπου η κύρια ενασχόλησή της είναι η μελέτη της ασφαλούς επικοινωνίας. Σήμερα η κρυπτολογία θεωρείται μια επιστήμη που μπορεί να μελετηθεί ως όψη των εφαρμοσμένων μαθηματικών, της θεωρητικής πληροφορικής ή της επιστήμης ηλεκτρονικού μηχανικού. Άλλοι παρεμφερείς κλάδοι είναι η στεγανογραφία και η στεγανοανάλυση, αντίστοιχα.

Η σημασία της κρυπτολογίας είναι πολύ μεγάλη κυρίως στους τομείς της ασφάλειας υπολογιστικών συστημάτων και των τηλεπικοινωνιών. Ο βασικός σκοπός της είναι να παρέχει μηχανισμούς έτσι ώστε 2 ή περισσότερα άκρα επικοινωνίας, όπως π.χ. άνθρωποι, προγράμματα υπολογιστών κλπ., να μπορούν ανταλλάξουν μηνύματα, χωρίς κάποιος τρίτος να είναι σε θέση να διαβάσει την περιεχόμενη πληροφορία εκτός απ’ τα δύο αυτά άκρα.

Η κρυπτολογία αποτελείται από τα συνθετικά «κρυπτός» και «λόγος» και χωρίζεται σε δύο κλάδους: την *Κρυπτογραφία* (cryptography) και την *Κρυπτανάλυση* (cryptanalysis).

- **Κρυπτογραφία:** ο κλάδος όπου ασχολείται με μαθηματικούς μετασχηματισμούς προκειμένου να εξασφαλιστεί η ασφάλεια της πληροφορίας
- **Κρυπτανάλυση:** ο κλάδος που στόχο έχει την ανάλυση και την διάσπαση Κρυπτοσυστημάτων.

Ιστορικά, η κρυπτογραφία χρησιμοποιήθηκε προκειμένου να μετατραπεί η πληροφορία μηνυμάτων από μια κανονική και κατανοητή μορφή σε έναν γρίφο, με αποτέλεσμα στα μάτια ενός που δεν έχει γνώση του κρυφού μετασχηματισμού θα

παρέμενε ακατανόητος. Βασικό χαρακτηριστικό των παλαιότερων μορφών κρυπτογράφησης ήταν το γεγονός ότι η επεξεργασία πραγματοποιούταν στη γλωσσική δομή του μηνύματος, σε αντίθεση με τις νεότερες μορφές όπου η κρυπτογραφία χρησιμοποιεί το αριθμητικό ισοδύναμο.

2.2 Τεχνικοί όροι και έννοιες

Κρυπτογράφηση *(encryption)* ονομάζεται η διαδικασία κατά την οποία ένα μήνυμα μετασχηματίζεται με τη βοήθεια ενός κρυπτογραφικού αλγορίθμου σε μια ακατανόητη μορφή ούτως ώστε να μην μπορεί να διαβαστεί από κανέναν πέραν του νόμιμου παραλήπτη.

Η αντίστροφη διαδικασία κατά την οποία από το κρυπτογραφημένο κείμενο παράγεται το αρχικό μήνυμα ονομάζεται **αποκρυπτογράφηση (*decryption*)**.

Κρυπτογραφικός Αλγόριθμος (cipher) είναι η μέθοδος μετασχηματισμού δεδομένων σε τέτοια μορφή η οποία δεν επιτρέπει την αποκάλυψη των περιεχομένων τους από μη εξουσιοδοτημένα μέρη.

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

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

Κρυπτογραφημένο κείμενο (*ciphertext*) είναι το αποτέλεσμα που προκύπτει μετά την εφαρμογή ενός κρυπτογραφικού αλγόριθμου πάνω στο αρχικό κείμενο.

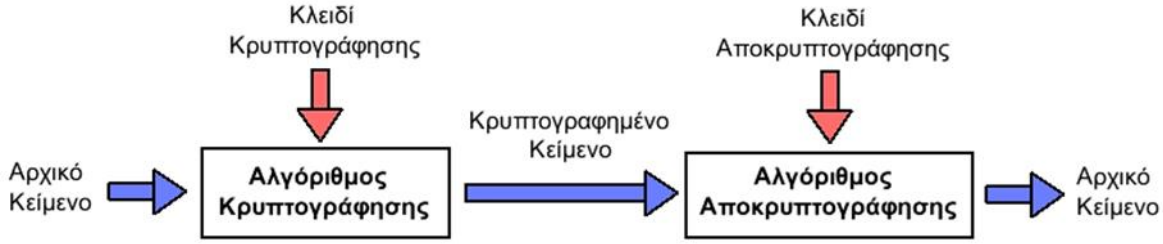
Κρυπτανάλυση (*cryptanalysis*) είναι η επιστήμη που ασχολείται με το "σπάσιμο" κάποιας κρυπτογραφικής τεχνικής έτσι ώστε χωρίς να είναι γνωστό το κλειδί της κρυπτογράφησης, το αρχικό κείμενο να μπορεί να αποκωδικοποιηθεί.

Η διαδικασία της κρυπτογράφησης και αποκρυπτογράφησης ενός μηνύματος πραγματοποιείται με τη βοήθεια ενός κρυπτογραφικού αλγορίθμου (cipher) και ενός κλειδιού κρυπτογράφησης (key). Συνήθως ο αλγόριθμος κρυπτογράφησης είναι γνωστός, επομένως η εμπιστευτικότητα του μεταδιδόμενου κρυπτογραφημένου μηνύματος βασίζεται κυρίως στη μυστικότητα του κλειδιού κρυπτογράφησης, το μέγεθος του οποίου μετριέται σε αριθμό bits. Γενικά ισχύει ο εξής κανόνας: όσο μεγαλύτερο είναι το κλειδί κρυπτογράφησης, τόσο δυσκολότερα μπορεί να αποκρυπτογραφηθεί το κρυπτογραφημένο μήνυμα από μη εξουσιοδοτημένα μέρη.

Διαφορετικοί αλγόριθμοι κρυπτογράφησης απαιτούν διαφορετικά μήκη κλειδιών προκειμένου να πετύχουν το ίδιο επίπεδο ανθεκτικότητας κρυπτογράφησης.

Ένας θεμελιώδης κανόνας της κρυπτογραφίας είναι ότι πρέπει πάντα να υποθέτουμε ότι οι μέθοδοι που χρησιμοποιούνται για την κρυπτογράφηση και αποκρυπτογράφηση είναι γνωστές στον κρυπταναλυτή. Η προσπάθεια που χρειάζεται για την επινόηση, τη δοκιμή, και την εγκατάσταση ενός νέου κρυπτογραφικού αλγορίθμου κάθε φορά που αποκαλύπτεται η παλιά μέθοδος, έκανε τη διατήρηση της μυστικότητας του αλγορίθμου μη πρακτική. Σ αυτό, λοιπόν, το σημείο είναι που χρειάζεται το κλειδί το οποίο, σε αντίθεση με τη γενική μέθοδο που μπορεί να αλλάζει κάθε κάποια χρόνια, είναι δυνατόν να αντικατασταθεί από κάποιο άλλο όσο συχνά απαιτείται. Έτσι, το βασικό μοντέλο είναι μια σταθερή και δημόσια γνωστή γενική μέθοδος η οποία παραμετροποιείται από ένα μυστικό και εύκολα μεταβαλλόμενο κλειδί. Η ιδέα ότι ο κρυπταναλυτής έχει γνώση του αλγορίθμου και ότι η μυστικότητα του αλγορίθμου βασίζεται στο κλειδί ονομάζεται ***αρχή του Kerckhoff.***

Η διαδικασία κρυπτογράφησης και αποκρυπτογράφησης παρουσιάζεται στο παρακάτω σχήμα:



Σχήμα 1.1: *Ένα τυπικό σύστημα κρυπτογράφησης – αποκρυπτογράφησης*

Ο βασικός και αντικειμενικός στόχος της κρυπτογραφίας είναι να δώσει τη δυνατότητα επικοινωνίας σε δύο πρόσωπα μέσα από ένα μη ασφαλές κανάλι με τέτοιο τρόπο έτσι ώστε ένα τρίτο, μη εξουσιοδοτημένο πρόσωπο (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*

Η συνάρτηση κρυπτογράφησης **E** δέχεται δύο παραμέτρους, μία από τον χώρο **P** και μία από τον χώρο **k** και παράγει μία ακολουθία η οποία ανήκει στον χώρο **C**.

Η συνάρτηση αποκρυπτογράφησης **D** δέχεται 2 παραμέτρους, τον χώρο **C** και τον χώρο **k** και παράγει μια ακολουθία που ανήκει στον χώρο **P**.

Το σύστημα του σχήματος λειτουργεί με τον εξής τρόπο :

1. Ο αποστολέας επιλέγει με τυχαίο τρόπο ένα κλειδί μήκους **n** από τον χώρο κλειδιών, όπου τα **n** στοιχεία του **K** είναι στοιχεία από ένα πεπερασμένο αλφάβητο.
2. Στη συνέχεια αποστέλλει το κλειδί στον παραλήπτη μέσα από ένα ασφαλές κανάλι.
3. Ο αποστολέας δημιουργεί ένα μήνυμα από τον χώρο μηνυμάτων.
4. Η συνάρτηση κρυπτογράφησης λαμβάνει τις δυο εισόδους (κλειδί και μήνυμα) και παράγει μια κρυπτοακολουθία συμβόλων (έναν γρίφο) η οποία αποστέλλεται μέσω ενός μη ασφαλούς καναλιού.
5. Η συνάρτηση αποκρυπτογράφησης λαμβάνει ως όρισμα τις δύο τιμές (κλειδί και γρίφο) και παράγει την ισοδύναμη ακολουθία μηνύματος.

Ο αντίπαλος που παρακολουθεί την επικοινωνία, ενημερώνεται για την κρυπτοακολουθία αλλά δεν έχει γνώση του κλειδιού που χρησιμοποιήθηκε με αποτέλεσμα να μην μπορεί να αναδημιουργήσει το μήνυμα. Στη περίπτωση που ο αντίπαλος επιλέξει να παρακολουθεί όλα τα μηνύματα θα προσανατολιστεί στην εξεύρεση του κλειδιού. Στη περίπτωση όμως που ενδιαφέρεται μόνο για το υπάρχον μήνυμα θα παράγει μια εκτίμηση για την πληροφορία του μηνύματος.

2.3. Βασικές κρυπτογραφικές αρχές

Υπάρχουν δύο βασικές αρχές στις οποίες στηρίζονται όλα τα συστήματα κρυπτογράφησης: ο πλεονασμός και η επικαιρότητα.

Πλεονασμός

Η **πρώτη βασική αρχή** είναι ότι όλα τα κρυπτογραφημένα μηνύματα πρέπει να περιέχουν κάποιον ***πλεονασμό***, δηλαδή πληροφορίες που δεν χρησιμεύουν για την κατανόηση του μηνύματος. Όλα τα μηνύματα πρέπει να περιέχουν σημαντικό

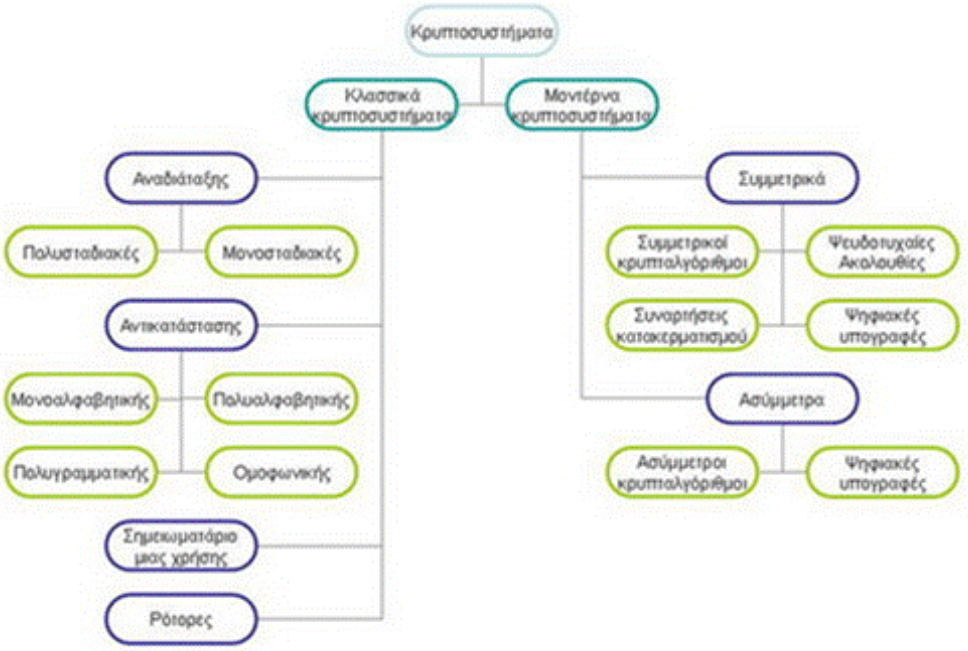
βαθμό πλεονασμού, έτσι ώστε οι ενεργητικοί εισβολείς να μην είναι σε θέση να στέλνουν ψεύτικα μηνύματα και να παραπλανούν τον δέκτη. Με άλλα λόγια, ο αποδέκτης του μηνύματος έχοντας αποκρυπτογραφήσει το μήνυμα, θα πρέπει να έχει τη δυνατότητα να διακρίνει την εγκυρότητα του μηνύματος με μια απλή εξέτασή του ή με την εκτέλεση κάποιου απλού υπολογισμού. Απ την άλλη μεριά όμως, ο πλεονασμός κάνει το σπάσιμο του συστήματος ευκολότερο, έτσι εδώ παρατηρούμε κάποια αντίφαση. Σ' αυτό το σημείο πρέπει να τονίσουμε ότι ο πλεονασμός δεν θα πρέπει να έχει μηδενικά στην αρχή και στο τέλος του μηνύματος γιατί έτσι σε μερικούς αλγορίθμους παραγάγει προβλέψιμα αποτελέσματα, συνεπώς κάνει τη δουλειά του κρυπταναλυτή πιο εύκολη.

Επικαιρότητα

Η **δεύτερη κρυπτογραφική αρχή** είναι ότι πρέπει να λαμβάνονται μέτρα ούτως ώστε να μπορεί να εξασφαλιστεί σε κάθε μήνυμα που λαμβάνεται η επαλήθευση της "επικαιρότητάς" του, δηλαδή ότι έχει σταλεί πρόσφατα. Αυτό το μέτρο έχει ως αποτέλεσμα την αποτροπή των εισβολέων να αναπαράγουν παλαιά έγκυρα μηνύματα.

2.4. Είδη κρυπτοσυστημάτων

Τα κρυπτοσυστήματα διακρίνονται σε δύο μεγάλες κατηγορίες τα **Κλασσικά Κρυπτοσυστήματα** και τα **Μοντέρνα Κρυπτοσυστήματα** (Συμμετρικά κρυπτοσυστήματα και Ασύμμετρα κρυπτοσυστήματα).



Εικόνα 1.1: *Χάρτης κρυπτοσυστημάτων*

2.4.1 Κλασικά κρυπτοσυστήματα

Στην κρυπτογραφία η διαδικασία κρυπτογράφησης και η αντίστοιχη διαδικασία αποκρυπτογράφησης, αποτελούν ένα κρυπτοσύστημα. Στα Κλασσικά κρυπτοσυστήματα ανήκουν τα κρυπτοσυστήματα αναδιάταξης και τα κρυπτοσυστήματα αντικατάστασης.

Τα κλασικά κρυπτοσυστήματα έχουν να κάνουν με την επεξεργασία γλωσσικών μηνυμάτων, δηλαδή μηνυμάτων που αποτελούνται από λέξεις όπου κάθε ψηφίο της λέξης αντιστοιχεί σε ένα από τα γράμματα αλφαβήτου, πχ 26 του αγγλικού. Για παράδειγμα η λέξη LAND μπορεί σε κάποιο σύστημα να κρυπτογραφείται LVNO. Η επεξεργασία πραγματοποιείται τόσο με αντικατάσταση του κάθε γράμματος με κάποιο άλλο γράμμα σύμφωνα με κάποια μέθοδο-κλειδί όσο και με αναδιάταξη στην σειρά-θέση στην οποία εμφανίζονται τα γράμματα σε μια λέξη.

2.4.1.1 Κρυπτοσυστήματα αντικατάστασης

Οι τεχνικές αντικατάστασης είναι αυτές όπου τα γράμματα αντικαθίστανται από άλλα γράμματα, σύμβολα ή αριθμούς. Υπάρχουν διάφορες τεχνικές αντικατάστασης όπως η μονοαλφαβητική αντικατάσταση, η ομοφωνική

αντικατάσταση, πολυγραμματική αντικατάσταση και η πολυαλφαβητική αντικατάσταση.

2.4.1.2 Κώδικας του Καίσαρα

Μία από τις παλαιότερες, απλούστερες αλλά και πιο γνωστές τεχνικές κωδικοποίησης είναι ο **Κώδικας του Καίσαρα**, η οποία πήρε το όνομα της από τον Ιούλιο Καίσαρα, καθώς ο ίδιος την χρησιμοποιούσε στην προσωπική του αλληλογραφία. Στη μέθοδο αυτή κάθε γράμμα της χρησιμοποιούμενης αλφαβήτου ολισθαίνει αριστερά κατά 3 και αντικαθίσταται από κάποιο άλλο γράμμα κάθε φορά. Συνεπώς, για παράδειγμα στο αγγλικό αλφάβητο, το γράμμα A θα αντικατασταθεί από το γράμμα D, το B από το γράμμα E, το C από το γράμμα F και ούτω καθεξής, με το τελευταίο γράμμα της αλφαβήτου το Z να αντικαθίσταται από το γράμμα C.

Παρ' όλα αυτά, η μέθοδος αυτή στη πιο γενικευμένη της μορφή επιτρέπει στο αλφάβητο να ολισθαίνει δεξιά ή αριστερά κατά k γράμματα αντί πάντα με 3 και αριστερά. Στην περίπτωση αυτή το k αποτελεί το κλειδί για τη γενική μέθοδο των κυκλικά μετατοπισμένων αλφαβήτων. Για παράδειγμα, έστω μετατόπιση k=7 αριστερά τότε:

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

Επομένως, σύμφωνα με το παραπάνω το κείμενο **RETREAT** θα μεταμφιεστεί ως **YLAYLHA**.

Την κρυπτογράφηση μπορούμε να την αναπαραστήσουμε με την χρήση αριθμητικής υπολοίπων αφού πρώτα μετασχηματίσουμε τα γράμματα σε αριθμούς, σύμφωνα με τον κανόνα, A=0, B=1, C=2, D=3 … Z=25, τότε ο αλγόριθμος για την παραπάνω περίπτωση μπορεί να εκφραστεί ως εξής:

$$C = E(k,p) = (p + k) \bmod 26 \qquad \textbf{(1.1)}$$

όπου *E()* αντιπροσωπεύει την κρυπτογράφηση και *k=7* η μετατόπιση. Ο τελεστής mod επιστρέφει το υπόλοιπο της ακεραίας διαίρεσης του *(p+7)* με το 26. Προκειμένου να λειτουργήσει αυτή η εξίσωση θα πρέπει όταν γίνεται αυτή η διαίρεση να κρατιέται το υπόλοιπο, ούτως ώστε η αρίθμηση του αλφαβήτου να είναι κυκλική, δηλαδή οι χαρακτήρες X, Y, Z να γίνουν E, F, G αντίστοιχα.

Η αποκρυπτογράφηση θα εκφραζόταν από τη σχέση:

$$P = D(k,c) = (c - k) \bmod 26 \qquad \textbf{(1.2)}$$

όπου *k* είναι το μυστικό κλειδί (στο προηγούμενο παράδειγμα ήταν 7)

2.4.1.3. Μονοαλφαβητικοί αλγόριθμοι κρυπτογράφησης

Η επόμενη βελτίωση που επιδέχεται ο κώδικας του Καίσαρα είναι η αντιστοίχηση κάθε χαρακτήρα να πραγματοποιείται με μία τυχαία αντιμετάθεση των γραμμάτων του αλφάβητου. Δηλαδή:

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

Αυτό το γενικό σύστημα ονομάζεται **μονοαλφαβητική αντικατάσταση (monoalphabetic substitution),** με κλειδί να είναι ο συρμός των 26 γραμμάτων που αντιστοιχεί στο πλήρες αλφάβητο. Για το παραπάνω κλειδί, το κείμενο **RETREAT** θα γινόταν **VLHVLMH.**

Αυτό το σύστημα φαίνεται ασφαλές καθώς, ενώ ο κρυπταναλυτής έχει γνώση του γενικού συστήματος, δε γνωρίζει όμως ποιό από τα 26! ≈ 4 × 10^{26} πιθανά κλειδιά χρησιμοποιείται. Στη πραγματικότητα, σε αντίθεση με τον αλγόριθμο του Καίσαρα, το να δοκιμάσει κανείς όλα τα πιθανά κλειδιά δεν είναι και πολλά υποσχόμενη προσέγγιση γιατί ακόμα και με 1nsec ανά λύση, ένα εκατομμύριο υπολογιστές να τρέχουν παράλληλα θα χρειαστούν 10.000 χρόνια προκειμένου να δοκιμάσουν όλα τα κλειδιά. Εν τούτοις, στη περίπτωση που ο κρυπταναλυτής έχει στα χέρια του ένα μικρό κομμάτι του κρυπτοκειμένου, το σπάσιμο του αλγορίθμου είναι πολύ εύκολο. Η βασική μέθοδος επίθεσης χρησιμοποιεί τις στατιστικές ιδιότητες των φυσικών γλωσσών. Για παράδειγμα, στην αγγλική γλώσσα το γράμμα που εμφανίζεται πιο συχνά είναι το *e* ακολουθούμενο από τα t, o, a, n, I, κ.λπ. Οι πιο συχνοί συνδυασμοί δύο γραμμάτων ή **διγράμματα (digrams)** όπως ονομάζονται, είναι οι th, in, er, re, και an. Οι πιο συχνοί τριών γραμμάτων ή τριγράμματα (trigrams), είναι οι the, ing, and, και ion.

Ο κρυπταναλυτής που θα προσπαθήσει να σπάσει έναν μονοαλφαβητικό κώδικα θα ξεκινήσει μετρώντας τις σχετικές συχνότητες όλων των γραμμάτων στο κρυπτοκείμενο. Στη συνέχεια θα προσπαθούσε να αντιστοιχίσει το πιο συχνά εμφανιζόμενο γράμμα με το e, το αμέσως λιγότερο στο t κοκ. Μετά θα εξέταζε τα τριγράμματα ώστε να βρει ένα συνηθισμένο τρίγραμμα της μορφής tXe, που αυτό

θα σήμαινε ότι το X θα αντιστοιχούσε πιθανότατα στο γράμμα h. Με αυτή τη λογική, εάν εμφανίζεται συχνά το μοτίβο thYt, το Y πιθανόν αντιστοιχεί στο a. Έχοντας, λοιπόν, υπόψιν τις πληροφορίες αυτές, θα μπορούσε να ψάξει για τριγράμματα της μορφής aZW, το οποίο μάλλον είναι το and. Έτσι καταλήγουμε στο συμπέρασμα ότι μαντεύοντας τα συχνά γράμματα, διγράμματα και τριγράμματα και έχοντας γνώση των πιθανών μοτίβων των φωνηέντων και των συμφώνων, ο κρυπταναλυτής είναι σε θέση να χτίσει δοκιμαστικό κείμενο, γράμμα προς γράμμα.

Μια άλλη προσέγγιση είναι το να προσπαθήσει να μαντέψει μια πιθανή λέξη ή φράση. Ενδεικτικά, θεωρούμε το παρακάτω κρυπτοκείμενο από ένα λογιστικό γραφείο (ομαδοποιημένο σε ομάδες των πέντε χαρακτήρων):

CTBMN **B**YCTC BTJD**S** QXBNS GSTJC B**T**SWX **C**TQTZ CQVUJ
Q**J**SGS TJ**Q**ZZ MNQJS **V**LNSX VSZJU **J**DST**S** **J**QUUS **J**UBXJ
D**S**KSU JSNTK BGAQJ ZBGYQ TLCTZ BNYBN QJSW

Μια πιθανή λέξη σε ένα μήνυμα λογιστικού γραφείου αποτελεί η financial (οικονομικός). Γνωρίζοντας, επομένως, ότι ή λέξη financial αποτελείται από ένα επαναλαμβανόμενο γράμμα το i, με τέσσερα άλλα γράμματα ανάμεσα στις εμφανίσεις του, ψάχνουμε στο κρυπτοκείμενο για επαναλαμβανόμενα γράμματα με απόσταση τεσσάρων γραμμάτων ανάμεσα τους. Βρίσκουμε 12 περιπτώσεις, στις θέσεις 6, 15, 27, 31, 42, 48, 56, 66, 70, 71, 76, και 82. Όμως, μόνο δύο από αυτά, στις θέσεις 31 και 42 έχουν το επόμενο γράμμα τους να επαναλαμβάνεται στη σωστή θέση. Από αυτές τις δύο περιπτώσεις μόνο η 31 έχει το a στη σωστή θέση ούτως ώστε να είμαστε σε θέση να πούμε ότι απ' τη θέση 30 ξεκινά η λέξη financial. Από αυτό το σημείο και μετά, ο υπολογισμός του κλειδιού είναι πια εύκολος βάση των στατιστικών συχνοτήτων για το Αγγλικό κείμενο.

2.4.1.4. Κρυπταλγόριθμοι μετάθεσης

Η διαφορά μεταξύ των αλγορίθμων αντικατάστασης και μετάθεσης είναι ότι οι πρώτοι διατηρούν τη σειρά των συμβόλων του απλού κειμένου, αλλά συγκαλύπτουν τα σύμβολα, ενώ αντίθετα οι δεύτεροι αναδιατάσσουν τα γράμματα χωρίς όμως να τα συγκαλύπτουν. Στο παρακάτω παράδειγμα παρουσιάζεται ένας συνηθισμένος αλγόριθμος μετάθεσης, η ***μετάθεση στηλών*** (columnar transposition). Ο αλγόριθμος αυτός έχει ως κλειδί μια λέξη ή φράση που δεν

περιέχει επαναλαμβανόμενο γράμμα. Στο συγκεκριμένο παράδειγμα, το κλειδί είναι η λέξη MEGABUCK. Η χρησιμότητα του κλειδιού είναι ότι αριθμεί τις στήλες, τοποθετώντας τη στήλη 1 κάτω από το γράμμα του κλειδιού που βρίσκεται πλησιέστερα στην αρχή του αλφαβήτου, και ούτω καθεξής. Το απλό κείμενο οριζόντια σε γραμμές, συμπληρωμένο με κενά έτσι ώστε να γεμίζει τον πίνακα. Το κρυπτογραφημένο κείμενο διαβάζεται κατά στήλες, ξεκινώντας με τη στήλη που αντιστοιχεί στο χαμηλότερο γράμμα του κλειδιού.

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Απλό κείμενο:
pleasetransferonemilliondollarstomyswissbankaccountsixtwotwo

Κρυπτοκείμενο:
AFLLSKSOSELAWAIATOOSSCTCLNMOMANTESILYNTWRNNTSOWDPAEDOBUO

Προκειμένου να σπάσει ο κρυπταναλυτής έναν αλγόριθμο μετάθεσης, θα πρέπει να καταλάβει πρώτα απ' όλα ότι αντιμετωπίζει έναν τέτοιο αλγόριθμο. Εξετάζοντας τη συχνότητα των E, T, A, O, I, N κλπ., είναι εύκολο να αναγνωρίσει αν ταιριάζουν με τη συνηθισμένη κατανομή για το απλό κείμενο. Εφόσον συμβεί αυτό, ο κρυπταναλυτής αντιλαμβάνεται ότι πρόκειται για αλγόριθμο μετάθεσης- επειδή σε αυτούς τους αλγορίθμους, όπως αναφέραμε και πιο πάνω, τα σύμβολα δεν συγκαλύπτονται και ,επομένως, κάθε γράμμα αναπαριστά τον εαυτό του, γεγονός που καθιστά άθικτη την κατανομή συχνοτήτων.

Αμέσως μετά θα πρέπει να μαντέψουμε το πλήθος των στηλών. Συχνά μπορούμε να μαντέψουμε μια λέξη ή φράση από τα συμφραζόμενα. Λόγου χάρη, υποθέτουμε ότι ο κρυπταναλυτής υποπτεύεται ότι κάπου μέσα στο απλό κείμενο υπάρχει η φράση *milliondollars*. Παρατηρούμε ότι τα διγράμματα MO, IL, LL, LA, IR και OS εμφανίζονται στο κρυπτογραφημένο κείμενο λόγω της αναδίπλωσης της φράσης αυτής. Το γράμμα M στο κρυπτογράφημα ακολουθείται από το O (είναι δηλαδή κατακόρυφα γειτονικά στη στήλη 4), επειδή μέσα στη φράση απέχουν απόσταση ίση με το μήκος του κλειδιού. Στη περίπτωση που είχε χρησιμοποιηθεί κλειδί μήκους 7, θα εμφανίζονταν τα διγράμματα MD, IO, LL, LL, IA, OR, και NS. Ουσιαστικά ανάλογα με το μήκους κλειδιού που χρησιμοποιείται παράγεται και διαφορετικό

σύνολο διγραμμάτων. Έτσι, εξετάζοντας ο κρυπταναλυτής τις διάφορες δυνατότητες μπορεί να προσδιορίσει το μήκος του κλειδιού.

Το τελευταίο βήμα είναι η διάταξη των στηλών. Εάν το πλήθος των στηλών είναι μικρό, έχουμε δυνατότητα να εξετάσουμε κάθε ένα από τα *k(k-1)* δυνατά ζεύγη στηλών, για να ελέγξουμε αν οι συχνότητες των διγραμμάτων του ζεύγους ταιριάζουν με εκείνες που ισχύουν για το Αγγλικό απλό κείμενο. Υποθέτουμε ότι το ζεύγος με την καλύτερη ταύτιση έχει και τη σωστή διάταξη. Ύστερα ελέγχουμε κάθε στήλη που απομένει ως διάδοχο αυτού του ζεύγους Η στήλη της οποίας οι συχνότητες διγραμμάτων και τριγραμμάτων αποδίδουν την καλύτερη ταύτιση θεωρούμε ότι είναι σωστή. Η επόμενη στήλη βρίσκεται με τον ίδιο τρόπο. Όλη αυτή η διαδικασία επαναλαμβάνεται έως ότου βρεθεί μια πιθανή διάταξη.

2.4.2. Μοντέρνα κρυπτογραφία

Στις μέρες μας, όλοι οι καθιερωμένοι κρυπτογραφικοί αλγόριθμοι (συμμετρικοί ή ασύμμετροι), χρησιμοποιούν ένα κλειδί προκειμένου να παραμετροποιήσουν την κρυπτογράφηση αλλά και την αποκρυπτογράφηση ενός μηνύματος. Το κλειδί αυτό μπορεί να λαμβάνει μια τιμή, μέσα από ένα ευρύ φάσμα πιθανών τιμών, το οποίο ονομάζεται ***keyspace***. Σε αρκετούς αλγορίθμους το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση είναι διαφορετικό από αυτό το κλειδί της κρυπτογράφησης. Δεδομένου αυτής της παραδοχής, τα συστήματα κρυπτογράφησης μπορούν να χωριστούν σε δύο βασικές κατηγορίες: ***συμμετρικά, συμβατικά ή μυστικού κλειδιού (symmetric, conventional or secret key)*** όπου το κλειδί αποκρυπτογράφησης μπορεί να υπολογιστεί εφόσον γνωρίζουμε το κλειδί της κρυπτογράφησης, και **ασυμμετρικά ή δημοσίου κλειδιού (asymmetric or public key)** όπου το κλειδί της αποκρυπτογράφησης είναι υπολογιστικά ανέφικτο, αλλά όχι αδύνατον, να υπολογιστεί από το κλειδί κρυπτογράφησης.

2.4.2.1. Συμμετρική κρυπτογραφία

Ένας αλγόριθμος αποκαλείται συμμετρικός, όταν το κλειδί της κρυπτογράφησης και αποκρυπτογράφησης είναι το ίδιο. Συνεπώς αυτό σημαίνει, αφενός ότι το κλειδί αυτό θα πρέπει να γνωστοποιείται μόνο στα εξουσιοδοτημένα μέρη και αφετέρου απαιτείται ασφαλές μέσο για την μετάδοσή του. Επομένως, γίνεται κατανοητό ότι η εξασφάλιση της ασφαλούς μετάδοσης του κλειδιού, αποτελεί απαραίτητα προϋπόθεση για ένα τέτοιο κρυπτοσύστημα καθώς σε άλλη περίπτωση η συμμετρική κρυπτογραφία καθίσταται αναποτελεσματική. Εδώ πρέπει να σημειωθεί ότι το πιο σημαντικό πλεονέκτημα των συμμετρικών κρυπτοσυστημάτων είναι η ταχύτητά τους κι αυτός είναι ο λόγος που προτιμούνται σε περιπτώσεις που ο όγκος δεδομένων προς κρυπτογράφησης είναι μεγάλος.

Σχήμα 1.2: *Συμμετρικό Μοντέλο Κρυπτογράφησης*

2.4.2.2. Ασύμμετρη κρυπτογραφία

Στα ασύμμετρα κρυπτογραφικά συστήματα ή συστήματα δημοσίου κλειδιού όπως ονομάζονται, χρησιμοποιούνται διαφορετικά κλειδιά για τη διαδικασία της κρυπτογράφησης και αποκρυπτογράφησης, το **δημόσιο** (public key) και το **ιδιωτικό** (private key) κλειδί, αντίστοιχα. Τα κλειδιά αυτά παράγονται με τέτοιο τρόπο ώστε ένα κρυπτογραφημένο μήνυμα με το δημόσιο κλειδί να μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί. Επιπλέον, πρέπει να σημειωθεί, ότι δεν μπορεί το ένα κλειδί να προκύψει από το άλλο τόσο απλά. Αυτό που καθιστά τα ασύμμετρα κρυπτοσυστήματα ιδιαίτερα σημαντικά, είναι το γεγονός ότι εξαλείφουν το πρόβλημα της διανομής κλειδιών. Απ την άλλη, το βασικό τους μειονέκτημα αποτελεί η ταχύτητά τους, με αποτέλεσμα οι κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού να χρησιμοποιούνται κυρίως στην κρυπτογράφηση των κλειδιών των συμμετρικών συστημάτων, και όχι τον κύριο όγκο δεδομένων.

Η βασική αρχή της κρυπτογραφίας δημοσίου κλειδιού διατυπώθηκε από τους Whitfield Diffie και Martin Hellman το 1976. Συνήθως χρησιμοποιείται για την πραγματοποίηση της ανταλλαγής κλειδιών και όχι για την κρυπτογράφηση μηνυμάτων. Ένας αλγόριθμος θεωρείται ασφαλής στην περίπτωση που το μέγεθος των κλειδιών του είναι μεγάλο και οι γεννήτριες αριθμών που χρησιμοποιούνται είναι οι κατάλληλες.

2.5. Πλεονεκτήματα και μειονεκτήματα συμμετρικής και ασύμμετρης

Πλεονεκτήματα συμμετρικής κρυπτογράφησης

- Υψηλές ταχύτητες απόδοσης
- Τα κλειδιά που χρησιμοποιούνται είναι σχετικά μικρού μήκους

Μειονεκτήματα συμμετρικής κρυπτογράφησης

- Γνωστοποίηση κλειδιού
- Σε τέτοιου είδους κρυπτογραφήσεις υπαγορεύεται η συχνή αλλαγή του κλειδιού

Πλεονεκτήματα ασύμμετρης κρυπτογράφησης

- Το ιδιωτικό κλειδί δε χρειάζεται ποτέ να μεταδοθεί ή να αποκαλυφθεί σε οποιονδήποτε
- Παρέχουν επιπρόσθετα μια μέθοδο για ψηφιακές υπογραφές
- Ένα ζεύγος κλειδιών, μπορεί να παραμείνει το ίδιο και να επαναχρησιμοποιηθεί σε περισσότερες από μία συνόδους επικοινωνίας.
- Το κλειδί που χρησιμοποιείται για την δημόσια λειτουργία επαλήθευσης είναι πιο μικρό συγκριτικά με αυτό της συμμετρικής κρυπτογράφησης.

Μειονεκτήματα ασύμμετρης κρυπτογράφησης

- Χαμηλοί ρυθμοί απόδοσης
- Το μέγεθος των κλειδιών είναι μεγαλύτερα από αυτά της συμμετρικής.

2.6. Κρυπτογραφικές υπηρεσίες

Οι κρυπτογραφικές υπηρεσίες είναι αυτές οι οποίες κάνοντας χρήση της κρυπτογραφίας επιδιώκουν την αντιμετώπιση συγκεκριμένων απειλών. Οι υπηρεσίες είναι οι εξής:

- **Εμπιστευτικότητα (Confidentiality):** Είναι η προστασία της προς μετάδοσης πληροφορίας από μη εξουσιοδοτημένη πρόσβαση ή την γνωστοποίησή της. Η υπηρεσία αυτή υλοποιείται μέσω μηχανισμών ελέγχου πρόσβασης στην περίπτωση αποθήκευσης δεδομένων και κωδικοποιώντας τα δεδομένα κατά την αποστολή τους.
- **Ακεραιότητα (Integrity):** Προστασία των δεδομένων προκειμένου να αποφευχθεί η αλλοίωση ή η αντικατάσταση τους από μη εξουσιοδοτημένα μέλη και η δυνατότητα ανίχνευσης σε περίπτωση τροποποίησης τους. Η υπηρεσία παρέχεται από μηχανισμούς κρυπτογραφίας όπως η ψηφιακή υπογραφή.
- **Πιστοποίηση (Authentication):** Είναι η δυνατότητα επιβεβαίωσης της ταυτότητας ενός ατόμου καθώς επίσης της πηγής αποστολής αλλά και του προορισμού των πληροφοριών. Η πιστοποίηση μπορεί να πραγματοποιηθεί με τρείς βασικές μεθόδους:
    1. Με κάτι που γνωρίζουμε, όπως π.χ. το PIN μιας τραπεζικής κάρτας ή τον κωδικό ενός λογαριασμού (password).
    2. Με κάτι που βρίσκεται στην ιδιοκτησία μας, όπως π.χ. το κλειδί μιας πόρτας ή μια τραπεζική κάρτα.
    3. Με κάτι που έχουμε εκ γενετής, π.χ. φωνή, ίριδα του ματιού, δακτυλικά αποτυπώματα κτλ.
- **Μη Άρνηση Αποδοχής (Non-Repudiation):** Είναι η υπηρεσία κατά την οποία ο αποστολέας και ο παραλήπτης της πληροφορίας δεν μπορούν να απαρνηθούν την αυθεντικότητα της μετάδοσης ή της δημιουργίας της. Σ’ αυτήν την υπηρεσία συνδυάζονται οι υπηρεσίες της πιστοποίησης και της ακεραιότητας. Στην ασύμμετρη κρυπτογραφία παρέχονται ψηφιακές υπογραφές, τέτοιες ώστε μόνο ο αποστολέας του μηνύματος θα μπορούσε να έχει στην κατοχή του. Αυτό έχει ως αποτέλεσμα, ο οποιοσδήποτε, και συνεπώς και ο παραλήπτης, να βρίσκεται σε θέση να επιβεβαιώσει την ψηφιακή υπογραφή του αποστολέα.

2.7. Ισχύς κρυπτογραφικών αλγορίθμων

Θεωρητικά κανένα κρυπτογραφικό σύστημα δεν θεωρείται ασφαλές καθώς ο οποιοσδήποτε αλγόριθμος ο οποίος χρησιμοποιεί κλειδί κρυπτογράφησης, είναι δυνατόν να σπάσει κάνοντας δοκιμή όλων των πιθανών κλειδιών (brute force attack). Αυτό που κάνει ένα κρυπτογραφικό σύστημα να είναι ασφαλές είναι ο χρόνος που απαιτείται, κάνοντας χρήση της υπάρχουσας τεχνολογίας, ώστε να δοκιμαστούν όλα τα κλειδιά να είναι υπερβολικά μεγάλος. Έτσι, λοιπόν, γίνεται κατανοητό ότι το μέγεθος του κλειδιού παίζει καθοριστικό ρόλο στο βαθμό ασφάλειας που παρέχει ένα σύστημα. Η υπολογιστική δύναμη που απαιτείται για το σπάσιμο ενός συστήματος, αυξάνεται εκθετικά με το μέγεθος του κλειδιού.

Από την άλλη πλευρά, η συνεχής αύξηση της υπολογιστικής δύναμης των υπολογιστών αποτελεί δυνατό σύμμαχο της κρυπτανάλυσης. Λαμβάνοντας υπόψιν την ραγδαία εξέλιξη της τεχνολογίας, το πιο δύσκολο στάδιο κατά την διαδικασία ανάπτυξης ενός κρυπτογραφικού συστήματος είναι ο καθορισμός του μεγέθους του κλειδιού. Ο μόνος τρόπος για να αποφύγουμε, σε όσο δυνατόν μεγαλύτερο βαθμό, το σπάσιμο ενός αλγορίθμου μέσω της τεχνολογίας, είναι τα κλειδιά να έχουν μεγαλύτερο μέγεθος από αυτό που θεωρείται απαραίτητο.

Η μέθοδος που ακολουθείται στα συμμετρικά συστήματα, είναι η **brute force attack**. Για παράδειγμα, για ένα σύστημα με κλειδί 56-bit, χρειάζεται αρκετή προσπάθεια προκειμένου να σπάσει, καθώς τα πιθανά κλειδιά είναι 2^{56}. Παρ όλα' αυτά, όμως, με τη χρήση ειδικού hardware (ο οποίος μπορεί να αγοραστεί μόνο από εταιρείες, κυβερνήσεις, κτλ.), το σπάσιμό του γίνεται πιο εύκολο.

Από την άλλη στα ασύμμετρα συστήματα χρησιμοποιούνται κλειδιά που εκ φύσεως είναι πολύ μεγαλύτερα από εκείνα των συμμετρικών συστημάτων. Σ αυτά τα συστήματα το δύσκολο πλέον είναι να υπολογιστεί το ιδιωτικό κλειδί γνωρίζοντας το δημόσιο, κι όχι να βρεθεί το σωστό κλειδί.

Κάποιος θα μπορούσε να υποστηρίξει ότι "αφού όσο μεγαλύτερο το μέγεθος του κλειδιού τόσο ασφαλέστερο το σύστημα, γιατί να μην χρησιμοποιήσουμε ακόμα μεγαλύτερα;". Σίγουρα το μέγεθος του κλειδιού εξασφαλίζει ασφαλή συστήματα, αλλά θα πρέπει να σκεφτούμε ότι όσο πιο ισχυρή η κρυπτογραφία τόσο μεγαλύτερο το κόστος που απαιτείται σε υπολογιστική ισχύ και χρόνο. Η ισχύς ενός κρυπτογραφικού συστήματος δεν εξαρτάται μόνο από το μέγεθος του κλειδιού, καθώς πολλά συστήματα έχουν σπάσει και χωρίς να υπολογιστεί το κλειδί. Στη πραγματικότητα, ο λόγος για τον οποίο έχουν σπάσει είναι εξαιτίας του ασθενούς

σχήματος διαχείρισης κλειδιών (key management). Ένα σχήμα διαχείρισης κλειδιών περιλαμβάνει:

- **Δημιουργία κλειδιών (key generation):** Πόσο προβλέψιμοι και τυχαίοι είναι οι αριθμοί που θα χρησιμοποιηθούν για την δημιουργία του κλειδιού.
- **Αποθήκευση κλειδιών (key storage):** Τα κλειδιά αποθηκεύονται και φυλάσσονται σε tamper-resistant hardware, smart cards ή σε κάποιο άλλο token, ή κρυπτογραφούνται με κάποιο άλλο κλειδί και αποθηκεύονται σε μια βάση δεδομένων.
- **Αλλαγή κλειδιών (key change):** Ανά τι χρονικά διαστήματα αλλάζονται τα κλειδιά, ποιό σχήμα αντικατάστασης κλειδιών είναι διαθέσιμο σε περίπτωση που κάποιο από τα κλειδιά διαρρεύσει.
- **Καταστροφή κλειδιών (key destruction):** Ο τρόπος με τον οποίο καταστρέφονται μη χρησιμοποιούμενα κλειδιά και αν υπάρχει κίνδυνος ανάκτησής τους.
- **Χρήση και Διαχωρισμός κλειδιών (key usage and separation):** Τα κλειδιά διαχωρίζονται ανάλογα με τη χρήση τους (κλειδί αποθήκευσης δεδομένων, κλειδί διανομής άλλων κλειδιών κτλ.)

2.8. Εφαρμογές της κρυπτογραφίας

Στις μέρες μας η κρυπτογραφία χρησιμοποιείται από ένα μεγάλο εύρος εφαρμογών. Όσο αυξάνεται ο όγκος της πληροφορίας που πρέπει να αποθηκευτεί και να μεταδοθεί ηλεκτρονικά τόσο θα αυξάνεται και η σημαντικότητα της κρυπτογραφίας. Ενδεικτικά αναφέρονται παρακάτω μερικές από τις εφαρμογές όπου χρησιμοποιείται η κρυπτογραφία:

- **Ηλεκτρονικό ταχυδρομείο:** Τα δεδομένα ενός μηνύματος ηλεκτρονικού ταχυδρομείου αποστέλλονται μέσω μη ασφαλών καναλιών επικοινωνίας όπως είναι το internet. Η χρήση ή η κατάχρηση του Internet έχει καταστήσει απαραίτητη την κρυπτογράφηση στα μηνύματα που αποστέλλονται μέσω του ηλεκτρονικού ταχυδρομείου το οποίο χρησιμοποιείται όλο και πιο συχνά για την μετάδοση κρίσιμων πληροφοριών.
- **Ασφαλείς συναλλαγές στο Internet – Ψηφιακές Συναλλαγές (Digital transactions):** Δεδομένου ότι οι οικονομικές συναλλαγές

πραγματοποιούνται και μέσω δικτύου, η αυθεντικοποίησή τους παίζουν σημαντικό ρόλο στην αποφυγή εξαπάτησης ενός συναλλασσομένου.

- **Εθνική Ασφάλεια:** Η κρυπτογραφία και η κρυπτανάλυση όπως προαναφέρθηκε, παίζουν σημαντικό ρόλο σε στρατιωτικές υποθέσεις. Οι πρεσβείες των κρατών αποστέλλουν και δέχονται κρίσιμες πληροφορίες που απαιτούν εμπιστευτικότητα.
- **Έξυπνες κάρτες (Smart Cards):** Η κρυπτογραφία βρίσκει εφαρμογή στις έξυπνες κάρτες εξαιτίας της αυξανόμενης χρήσης της ως μηχανισμού ελέγχου λογικής και φυσικής πρόσβασης σε ευαίσθητες πληροφορίες και χώρους.
- **Πρόσβαση σε ασφαλείς δικτυακούς τόπους:** Η αποδοχή της Αρχής Πιστοποίησης έχει ως επακόλουθο την προσθήκη ψηφιακών πιστοποιητικών στον browser του χρήστη. Με δεδομένα τα χαρακτηριστικά του πιστοποιητικού, ο χρήστης μπορεί να επισκεφτεί ασφαλείς δικτυακούς τόπους και να προσπελάσει δεδομένα χωρίς αυτά να είναι δημοσιευμένα σε κοινή θέα.
- **Εικονικά Ιδιωτικά Δίκτυα (VPNs):** Τα routers και τα firewalls χρησιμοποιούν κρυπτογραφία προκειμένου να εξασφαλίσουν την ασφαλή σύνδεση ενός υπολογιστή σε ένα εταιρικό δίκτυο.
- **Κρυπτογράφηση αρχείων και αποθηκευτικών μέσων**

ΚΕΦΑΛΑΙΟ 3ο

3. ΑΛΓΟΡΙΘΜΟΙ ΜΥΣΤΙΚΟΥ Ή ΣΥΜΜΕΤΡΙΚΟΥ ΚΛΕΙΔΙΟΥ

Η σύγχρονη κρυπτογραφία βασίζεται στις ίδιες βασικές ιδέες που χρησιμοποιούνται και στην παραδοσιακή κρυπτογραφία (μετάθεση και αντικατάσταση), με τη διαφορά ότι στη σύγχρονη κρυπτογραφία η έμφαση δίνεται σε διαφορετικό σημείο. Σε αντίθεση με τους σύγχρονους, οι παραδοσιακοί αλγόριθμοι ήταν πολύ απλοί. Στις μέρες μας, όμως, ισχύει το αντίθετο, δηλαδή ο στόχος είναι ο αλγόριθμος να είναι τόσο περίπλοκος και μπλεγμένος έτσι ώστε, και στη περίπτωση που ο κρυπταναλυτής αποκτήσει κομμάτι ενός κρυπτογραφημένου κειμένου, να μην είναι σε θέση να καταλάβει τίποτα από αυτό χωρίς να γνωρίζει το κλειδί.

Όπως αναφέραμε και σε προηγούμενο κεφάλαιο, οι αλγόριθμοι της συμμετρικής κρυπτογράφησης κάνουν χρήση του ίδιου κλειδιού τόσο για τη διαδικασία της κρυπτογράφησης όσο και αποκρυπτογράφησης. Οι **αλγόριθμοι συμμετρικού κλειδιού** (symmetric-key algorithms) διακρίνονται σε δύο κατηγορίες: τους ***αλγορίθμους τμημάτων*** (block ciphers) και του ***αλγορίθμους στοιχειοσειράς*** (stream ciphers). Στους αλγορίθμους τμημάτων, όταν ένα μήνυμα κρυπτογραφείται, ο αλγόριθμος δεν κρυπτογραφεί κάθε ένα bit (δυαδικά ψηφία) του μηνύματος ξεχωριστά αλλά ολόκληρες ομάδες από bits. Αντιθέτως, στους αλγορίθμους στοιχειοσειράς, ο αλγόριθμος εφαρμόζεται σε μια στοιχειοσειρά από bits.

3.1. Κρυπτογράφημα τμημάτων (Block Cipher)

Αποτελεί αλγόριθμο συμμετρικής κρυπτογράφησης, ο οποίος μετατρέπει μια ομάδα απλού κειμένου (plaintext), καθορισμένου μήκους, σε ομάδα κρυπτογραφημένου κειμένου (ciphertext) του ίδιου μήκους. Ο μετασχηματισμός αυτός επιτυγχάνεται με τη χρήση ενός μυστικού κλειδιού. Η αποκρυπτογράφηση πραγματοποιείται ακολουθώντας την αντίστροφη διαδικασία μετασχηματισμού στο κρυπτογραφημένο κείμενο χρησιμοποιώντας το ίδιο μυστικό κλειδί. Το καθορισμένο μήκους ονομάζεται ***μέγεθος τμημάτων*** (block size) και για τους περισσότερους αλγορίθμους κρυπτογράφησης είναι 64 bits. Κάθε κείμενο στο οποίο εφαρμόζεται το κρυπτογράφημα τμήματος αποδίδει διαφορετικό κρυπτογραφημένο κείμενο.

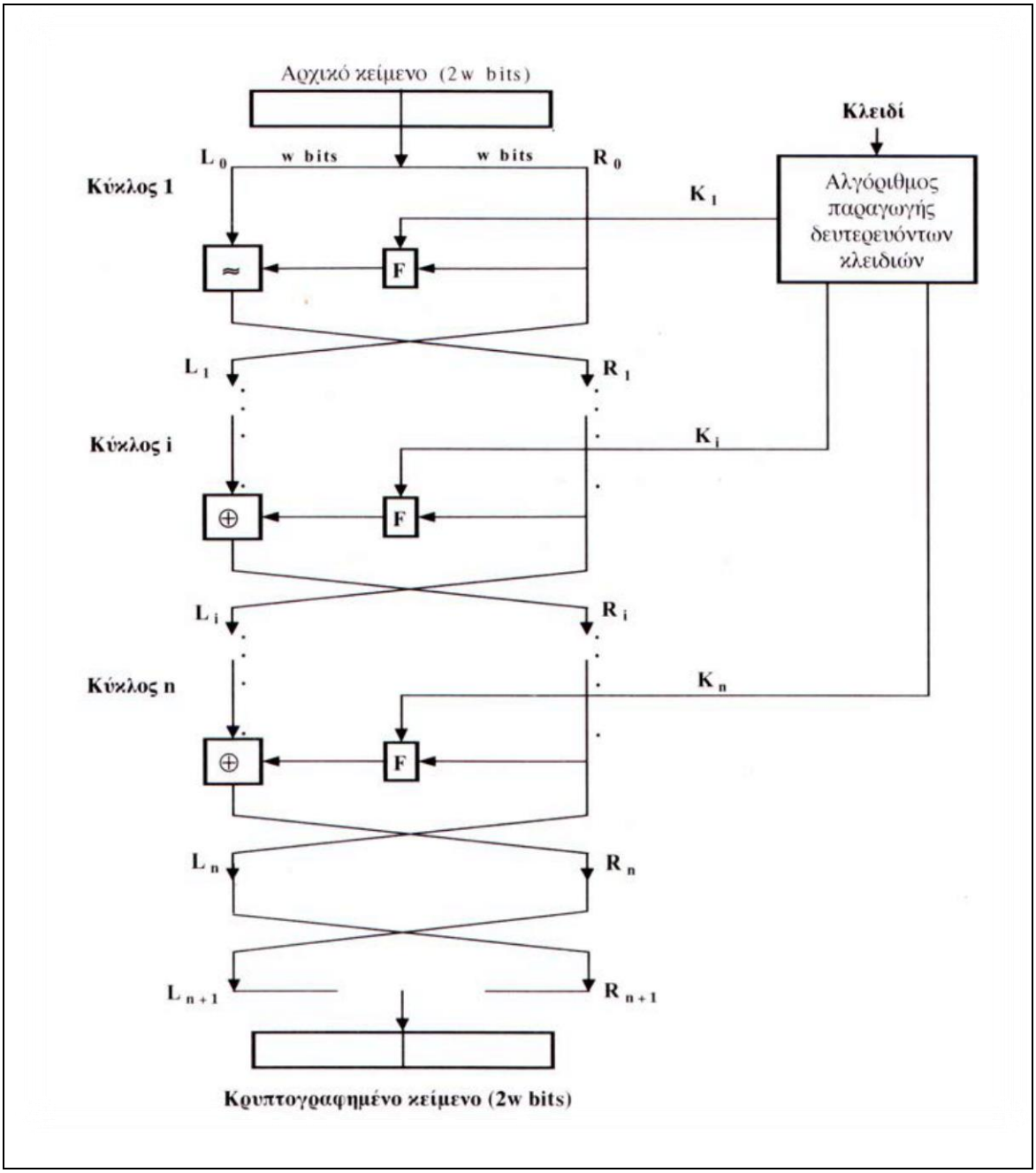
Όταν εφαρμόζουμε έναν τέτοιο αλγόριθμο σε ένα μήνυμα αυθαιρέτου μήκους προκειμένου να το κρυπτογραφήσουμε, χρησιμοποιούμε τεχνικές που ονομάζονται ***καταστάσεις λειτουργίας*** *(modes)*.

3.2. Δομές Feistel

Οι δομές Feistel αποτελούν τις βασικές δομές που εφαρμόζονται από τους αλγορίθμους τμημάτων. Η ιδέα του Feistel ήταν απλή και βασιζόταν στην απόδειξη της ασφάλειας ενός αλγορίθμου μέσω μη αντιστρέψιμων συναρτήσεων. Προσπάθησε να προωθήσει την ιδέα ότι τα μοντέλα των αλγορίθμων κρυπτογράφησης τμημάτων, πρέπει να είναι όσο το δυνατόν πιο απλά. Η πρόσθεση μερών που είναι ασφαλή, ανεξάρτητα το ένα από το άλλο, δεν συνεπάγεται ότι και όλο το σύστημα είναι ασφαλές.

Ακόμα και όταν πολλές φορές επιλέγουμε τμήματα να είναι αντιστρέψιμα, εισάγεται μια δομή στον αλγόριθμο που μπορεί να μην είναι προς όφελος της ασφάλειας ή της ταχύτητας αποκρυπτογράφησης αλλά του κρυπταναλυτή.

Έτσι λοιπόν, ο Feistel εισήγαγε δικές του δομές οι οποίες χρησιμοποιούνται από πολλούς σύγχρονους αλγορίθμους. Αρχικά μέσω μιας συνάρτησης g, μέσω της οποίας παράγονται τα κλειδιά κάθε γύρου K_i από το αρχικό κλειδί *K*. Σε αυτό το σημείο πρέπει να τονίσουμε ότι τα υποκλειδιά είναι διαφορετικά από το K αλλά και μεταξύ τους. Σε κάθε γύρο ενός αλγορίθμου τμήματος, η είσοδός του χωρίζεται στη μέση κι έτσι έχουμε το *δεξί* και το *αριστερό* τμήμα. Τα δύο αυτά τμήματα δεδομένων ακολουθούν n επαναληπτικά βήματα επεξεργασίας, και στη πορεία συνδυάζονται για να παράγουν το τμήμα του κρυπτογραφημένου κειμένου. Επομένως, αν υποθέσουμε ότι βρισκόμαστε στο γύρο *i*, έχουμε ως εισόδους τα R_{i-1} και L_{i-1} τα οποία παράγονται από τον προηγούμενο γύρο, καθώς επίσης και το υποκλειδί K_i (subkey), που παράγεται από το κλειδί *K.*



Σχήμα 3.1: *Δομή Feistel*

Τα επαναληπτικά βήματα ακολουθούν την ίδια δομή: Στα δεδομένα που βρίσκονται στην αριστερή πλευρά πραγματοποιείται μια αντικατάσταση. Η αντικατάσταση αυτή επιτυγχάνεται εφαρμόζοντας μια συνάρτηση F_i, που ονομάζεται ***συνάρτηση γύρου*** (round function), στα δεδομένα της δεξιάς πλευράς με τον λογικό τελεστή Exclusive-OR (XOR). Τότε ορίζουμε:

$$L_i = R_{i-1} \quad \textbf{(3.1)}$$

$$R_i = L_{i-1} \oplus f_i(K_i, R_{i-1}) \quad \textbf{(3.2)}$$

Η συνάρτηση F_i έχει την ίδια γενική δομή για κάθε γύρο, αλλά παραμετροποιείται από το υποκλειδί K_i του εκάστοτε γύρου. Ύστερα από αυτή την αντικατάσταση, πραγματοποιείται μια αντιμετάθεση των πλευρών των δεδομένων.

Στη παραπάνω δομή αν γνωρίζουμε το κλειδί και αντιστρέψουμε τα βήματα, θα προκύψει το αρχικό κείμενο από το κρυπτογράφημα. Άρα, καταλαβαίνουμε ότι η ασφάλεια του αλγόριθμου στηρίζεται στο να βρεθούν ασφαλείς οι συναρτήσεις γύρου F_i. Αν είναι αυτές ασφαλείς τότε και ο αλγόριθμος είναι εξίσου ασφαλής.

Αργότερα οι δομές Feistel γενικεύτηκαν από τους B. Schneier και J. Kelsey με τις μη ισορροπημένες δομές Feistel, προκειμένου να καλύπτουν περιπτώσεις όπου η είσοδος σε κάθε γύρο δε χωρίζεται στη μέση.

Η ακριβής υλοποίηση ενός δικτύου Feistel εξαρτάται από την επιλογή των παραμέτρων χαρακτηριστικών που περιγράφονται παρακάτω:

- **Μέγεθος των τμημάτων (block size):** Όσο μεγαλύτερο είναι το μέγεθος των τμημάτων τόσο αυξάνεται ο βαθμός ασφάλειας και μειώνεται η ταχύτητα κρυπτογράφησης και αποκρυπτογράφησης. Το τυπικό μέγεθος είναι 64 bit και αποτελεί το πιο συνηθισμένο στο σχεδιασμό τμημάτων κρυπτογράφησης.
- **Μέγεθος κλειδιού (key size):** Όσο μεγαλύτερο είναι το μέγεθος του κλειδιού εξασφαλίζεται υψηλότερος βαθμός ασφάλειας, αλλά μειώνεται η ταχύτητα κρυπτογράφησης και αποκρυπτογράφησης. Το τυπικό μέγεθος κλειδιού στους σύγχρονους αλγορίθμους είναι 128 bit.
- **Αριθμός κύκλων (number of rounds):** Το βασικό χαρακτηριστικό της δομής ενός δικτύου Feistel είναι ότι η ασφάλεια που προσφέρει ο κάθε κύκλος ανεπαρκής, αλλά η ασφάλεια που προσφέρει η διαδοχή των επαναληπτικών βημάτων είναι αυξημένη. Το τυπικό μέγεθος για τον αριθμό των κύκλων είναι 16 κύκλοι.
- **Αλγόριθμος παραγωγής δευτερευόντων κλειδιών (subkey generation algorithm):** Μεγαλύτερη πολυπλοκότητα στον αλγόριθμο πρέπει να συνεπάγεται με μεγαλύτερη δυσκολία κρυπτανάλυσης.
- **Συνάρτηση κύκλου (round cycle):** Μεγαλύτερη πολυπλοκότητα, σε γενικές γραμμές, σημαίνει και μεγαλύτερη αντίσταση σε κρυπταναλυτικές επιθέσεις.

Επιπλέον αναφέρονται δύο ακόμη παράμετροι οι οποίοι λαμβάνονται υπόψιν κατά το σχεδιασμό μιας δομής δικτύου Feistel:

- **Λογισμικό ταχείας κρυπτογράφησης και αποκρυπτογράφησης (fast software encryption and decryption):** Σε αρκετές περιπτώσεις η κρυπτογράφηση ενσωματώνεται στις εφαρμογές ή σε βοηθητικές συναρτήσεις με τέτοιο τρόπο ώστε να μην υπάρχει δυνατότητα υλοποίησης σε υλικό, κατά συνέπεια η ταχύτητα εκτέλεσης του αλγορίθμου αποτελεί σημαντικό παράγοντα.
- **Ευκολία ανάλυσης (ease analysis**): Αν και η επίτευξη υψηλού βαθμού δυσκολίας κατά τη διαδικασία της κρυπτανάλυσης ενός αλγορίθμου είναι επιθυμητή, υπάρχει σημαντικό όφελος εάν επιτευχθεί εύκολη ανάλυση του αλγορίθμου. Εάν υποθέσουμε ότι αλγόριθμος μπορεί να εξηγηθεί συνοπτικά και με σαφήνεια, τότε είναι πιο εύκολο να εξεταστεί για κρυπταναλυτικά σημεία ευπάθειας κατά συνέπεια να αναπτυχθεί υψηλότερο επίπεδο ασφάλειας.

  Η αποκρυπτογράφηση κατά Feistel ακολουθεί ουσιαστικά όμοια διαδικασία με αυτή της κρυπτογράφησης και ο κανόνας που ακολουθείται είναι ο εξής: Ως είσοδοι χρησιμοποιούνται το κρυπτογράφημα και τα υποκλειδιά K_i με αντίστροφη σειρά. Αναλυτικότερα, χρησιμοποιείται το K_n στον πρώτο κύκλο, το K_{n-1} στον δεύτερο κ.ο.κ μέχρι να χρησιμοποιηθεί το K_1 στον τελευταίο κύκλο. Το χαρακτηριστικό αυτό είναι πράγματι πολύ σημαντικό, καθώς δεν απαιτείται εφαρμογή δύο διαφορετικών αλγορίθμων, ενός για την κρυπτογράφηση και ενός άλλου για την αποκρυπτογράφηση.

3.3. Αλγόριθμος DES

Το κρυπτογραφικό σύστημα **DES** (Data Encryption Standard) ή **Πρότυπο Κρυπτογράφησης Δεδομένων** όπως ονομάζεται, αποτελεί τη πεμπτουσία των αλγορίθμων τμημάτων. Αν και είναι αρκετά παλιός, δεν μπορεί να πραγματοποιηθεί καμία συζήτηση για αλγορίθμους τμημάτων χωρίς να γίνει αναφορά σε αυτόν. Ο DES είναι ένας εξαιρετικά καλά-μηχανικής αλγόριθμος ο οποίος είχε ισχυρή επιρροή στην κρυπτογραφία. Βρίσκεται σε πολύ ευρεία χρήση, και κατά πάσα πιθανότητα θα είναι για τα επόμενα χρόνια. Κάθε φορά που χρησιμοποιούμε ένα μηχάνημα ATM, χρησιμοποιούμε DES.

Στις μέρες μας υπάρχουν αρκετοί αλγόριθμοι που βρίσκονται στην ίδια κατηγορία με τον DES ο οποίος αναπτύχθηκε από την IBM ως το βασικό της πρότυπο για τις μη απόρρητες πληροφορίες και υιοθετήθηκε τον Ιανουάριο του 1977 από τη κυβέρνηση των Η.Π.Α. Το κρυπτογραφικό σύστημα αυτό, χρησιμοποιήθηκε ευρύτατα στη βιομηχανία σε προϊόντα ασφαλείας και στον κλάδο των οικονομικών υπηρεσιών. Ο DES στην αρχική του μορφή δεν θεωρείται πια ασφαλής, αλλά εξακολουθούμε να τον χρησιμοποιούμε σε μια τροποποιημένη έκδοσή του, που ονομάζεται triple-DES.

Ο DES είναι ένας block cipher με μέγεθος block n = 64 bits και χρησιμοποιεί ένα κλειδί μήκους k = 56 bits. Επιπλέον, αποτελείται από 16 γύρους που ονομάζονται **"Δίκτυο Feistel".** Ο DES μπορεί να χρησιμοποιηθεί προκειμένου να καταστήσει τα συστήματα ασφαλή από απλούς hackers, αλλά μπορεί να σπάσει εύκολα από hardware που είναι σε θέση να προμηθευτούν κυβερνήσεις ή οργανωμένοι εγκληματίες. Δεδομένου του ότι η υπολογιστική ισχύ των συμβατών συστημάτων αυξάνεται με ραγδαία ταχύτητα, δε θα πρέπει να χρησιμοποιούμε τον DES στο σχεδιασμό νέων συστημάτων. Μια από τις παραλλαγές του DES, που κρυπτογραφικά θεωρείται πιο ισχυρή, είναι ο Triple-DES ο οποίος βασίζεται στη χρήση του DES τρείς διαδοχικές φορές, χρησιμοποιώντας δύο ή τρία διαφορετικά κλειδιά.

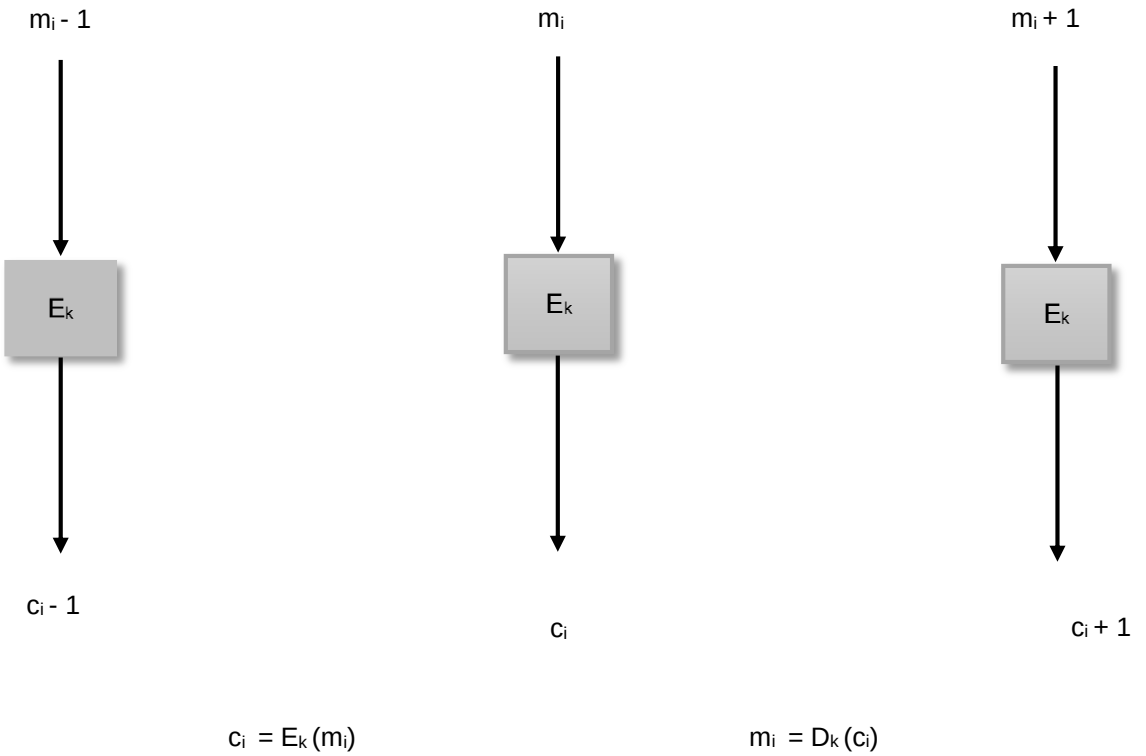
Το σίγουρο με τον DES ήταν ότι θα έπρεπε να αναθεωρείται κάθε πέντε χρόνια προκειμένου να ελεγχθεί κατά πόσον ή όχι θα πρέπει να επανεγκριθεί. Αν και υπήρχαν ισχυρισμοί ότι δεν θα έπρεπε να πιστοποιηθεί εκ νέου, ο αλγόριθμος επαναπιστοποιήθηκε ξανά και ξανά. Λαμβάνοντας υπόψιν την ηλικία του DES και την αύξηση της υπολογιστικής ισχύς των συστημάτων να φέρνει ολοένα και πιο κοντά το σπάσιμό του, το 1997 το National Institute for Standards & Technology (NIST) των ΗΠΑ προκήρυξε παγκόσμιο διαγωνισμό για τη δημιουργία και υιοθέτηση ενός νέου συμμετρικού αλγορίθμου κρυπτογράφησης. Από τους 15 αλγορίθμους, οι οποίοι ελέγχθηκαν λεπτομερώς από την αμερικανική κυβέρνηση και την διεθνή ακαδημαϊκή κοινότητα, επιλέχθηκε ο αλγόριθμος Rijndael που μετονομάστηκε αργότερα σε **Advanced Encryption Standard** (AES) και υιοθετήθηκε τελικά από την αμερικανική ομοσπονδιακή κυβέρνηση στις 26 Μαΐου 2002.

Προτού αρχίσουμε να περιγράφουμε το τρόπο λειτουργίας του αλγορίθμου DES, κρίνεται σκόπιμο να γίνει μια μικρή αναφορά των τεσσάρων τυπικών καταστάσεων

του αλγορίθμου, όπως έχουν δημοσιευθεί στο FIPS (Fedral Information Processing Standards Publications) το 1981, ενώ είναι γνωστές και ως ANSI X3.106. Οι καταστάσεις αυτές είναι οι εξής: *Electronic Code Book*, *Cipher Block Chaining, Cipher Feedback* και *Output Feedback*.

3.3.1. Κατάσταση λειτουργίας ηλεκτρονικού βιβλίου κωδικών

Στη μέθοδο ηλεκτρονικού βιβλίου κωδικών **(Electronic Code Book -ECB),** κάθε ομάδα απλού κειμένου κρυπτογραφείται ανεξάρτητα από το κρυπτογράφημα ομάδας. Η κρυπτογράφηση κάθε ομάδας των 64 bits της εισόδου πραγματοποιείται χρησιμοποιώντας το ίδιο κλειδί και το αποτέλεσμά της είναι μια καινούργια ομάδα από 64 bits. Η ECB μέθοδος εκτελεί απλή κρυπτογραφία, χρησιμοποιώντας μια ομάδα κάθε φορά, χωρίς να μπορεί να καθορίσει εάν έχουν προστεθεί ή αφαιρεθεί τμήματα από το αρχικό μήνυμα. Η απόδοσή του είναι αρκετά καλή σε περιπτώσεις που χρησιμοποιείται σε κανάλια μεταδόσεων με θόρυβο, καθώς η αλλαγή μερικών bits επηρεάζει μόνο μια ομάδα των 64 bits.



Σχήμα 3.2: *Η μέθοδος Electronic Code Book*

3.3.2. Κατάσταση λειτουργίας αλυσιδωτής σύνδεσης τμημάτων κρυπτογραφίας

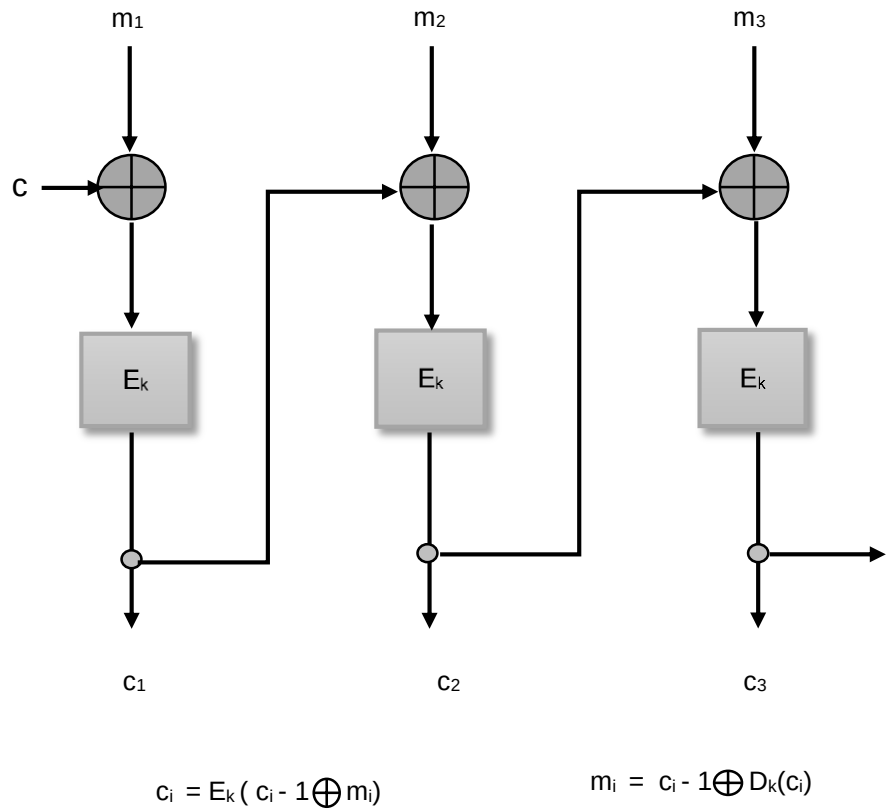
Στη μέθοδο αλυσιδωτής σύνδεσης τμημάτων κρυπτογραφίας **(Cipher Block Chaining - CBC)**, σε κάθε ομάδα κειμένου εφαρμόζεται η λογική συνάρτηση XOR με δεύτερο μέλος το κρυπτογράφημα της προηγούμενης ομάδας και στη συνέχεια η έξοδος αυτού κρυπτογραφείται χρησιμοποιώντας το κλειδί. Το ίδιο κλειδί χρησιμοποιείται σε κάθε τμήμα. Στην ουσία δεν υπάρχει λογική σύνδεση μεταξύ των επιμέρους τμημάτων του καθαρού κειμένου κατά την επεξεργασία τους. Η ομάδα απλού κειμένου που χρησιμοποιείται ως είσοδος της συνάρτησης κρυπτογράφησης, δεν αντιστοιχίζεται πια στην ίδια ομάδα κρυπτοκειμένου, με αποτέλεσμα οι επαναλαμβανόμενοι χαρακτήρες του αρχικού κειμένου να αποκρύπτονται και να μην εκτίθενται με τον ίδιο τρόπο.

Κατά την διαδικασία αποκρυπτογράφησης, ο αλγόριθμος αποκρυπτογράφησης επεξεργάζεται το κάθε κομμάτι και στο παραγόμενο αποτέλεσμα εφαρμόζεται η λογική συνάρτηση XOR με δεύτερο μέλος το προηγούμενο κομμάτι κρυπτογραφήματος, έτσι τελικά προκύπτει το αντίστοιχο τμήμα αρχικού κειμένου.

Αρχικά για τη παραγωγή της πρώτης ομάδας κρυπτοκειμένου, χρησιμοποιούμε ένα διάνυσμα αρχικοποίησης (Initialization Vector – IV) C_0 στο οποίο, μαζί με το πρώτο κομμάτι αρχικού κειμένου, εφαρμόζουμε τη λογική συνάρτηση XOR.

Το διάνυσμα αρχικοποίησης IV απαιτείται να γνωστοποιείται στον πομπό αλλά και τον δέκτη. Επιπλέον, για την επίτευξη της μέγιστης ασφαλείας, είναι απαραίτητο να διασφαλίζεται η μυστικότητα του διανύσματος αρχικοποίησης όπως συμβαίνει και με το κλειδί. Μάλιστα, θεωρείται απαραίτητο το διάνυσμα να είναι διαφορετικό για κάθε δύο μηνύματα που έχουν κρυπτογραφηθεί με το ίδιο κλειδί και προτείνεται η επιλογή του να γίνεται με τυχαίο τρόπο.

Εν κατακλείδι, η μέθοδος αλυσιδωτής κρυπτογράφησης τμημάτων είναι τόσο ασφαλής όσο και το κρυπτογράφημα ομάδας που χρησιμοποιείται. Το αρχικό, καθαρό κείμενο δεν μπορεί να αλλοιωθεί παρά μόνο σε περίπτωση αφαίρεσης τμημάτων από την αρχή ή το τέλος του κρυπτογραφήματος.



Σχήμα 3.3: *Η μέθοδος Cipher Block Chaining*

3.3.3. Μέθοδος Ανάδρασης κρυπτογραφημάτων

Στη μέθοδο ανάδρασης κρυπτογραφημάτων **(Cipher Feedback – CFB)** το προηγούμενο κρυπτοκείμενο επανακρυπτογραφείται (με την τιμή του κλειδιού του χρήστη εφαρμόζοντας τον τρόπο λειτουργίας ECB) και η έξοδος που προκύπτει συνδυασμένη με το τμήμα του καθαρού κειμένου χρησιμοποιώντας τη λογική συνάρτηση XOR αποτελεί την τρέχουσα κρυπτογραφημένη ομάδα.

Είναι εφικτό ένας αλγόριθμος τμήματος (block cipher) να μετατραπεί σε αλγόριθμο στοιχειοσειράς (stream cipher) εφαρμόζοντας σ' αυτή τη μέθοδο ανάδρασης κρυπτογραφημάτων. Η αξιοποίηση αλγορίθμου στοιχειοσειράς έχει ως αποτέλεσμα την εξάλειψη της αναγκαιότητας για συμπλήρωση ενός μηνύματος έτσι ώστε να αποτελείται από ακέραιο αριθμό τμημάτων, ενώ μπορεί να λειτουργήσει σε πραγματικό χρόνο. Αυτό σημαίνει ότι όταν μεταδίδεται μια σειρά χαρακτήρων, κάθε

ένας μπορεί να κρυπτογραφηθεί και να διαβαστεί αμέσως χρησιμοποιώντας έναν αλγόριθμο στοιχειοσειράς.

Μια σημαντική ιδιότητα των αλγορίθμων στοιχειοσειράς είναι η διατήρηση του ίδιου μήκους με το αρχικό κείμενο και στο κρυπτοκείμενο, γεγονός που αποτρέπει την άσκοπη χρήση εύρους του διαύλου μεταφοράς.

Κατά τη διαδικασία κρυπτογράφησης με τη CFB μέθοδο, η είσοδος της συνάρτησης κρυπτογράφησης είναι ένας καταχωρητής ολίσθησης 64 bit ο οποίος αρχικοποιείται με ένα διάνυσμα αρχικοποίησης C_0. Στα j αριστερά ψηφία, τα οποία αποτελούν τα σημαντικά ψηφία της εξόδου της συνάρτησης κρυπτογράφησης, εκτελείται η λογική συνάρτηση XOR με τη πρώτη ομάδα αρχικού κειμένου P_1, προκειμένου να παραχθεί η πρώτη ομάδα κρυπτογραφήματος C_1, η οποία στη συνέχεια αποστέλλεται. Ύστερα, τα περιεχόμενα του καταχωρητή ολίσθησης ολισθαίνουν αριστερά κατά j bit και το C_1 τοποθετείται δεξιά, στα λιγότερα σημαντικά ψηφία του καταχωρητή. Η διαδικασία αυτή επαναλαμβάνεται μέχρι να κρυπτογραφηθούν όλες οι ομάδες αρχικού κειμένου.

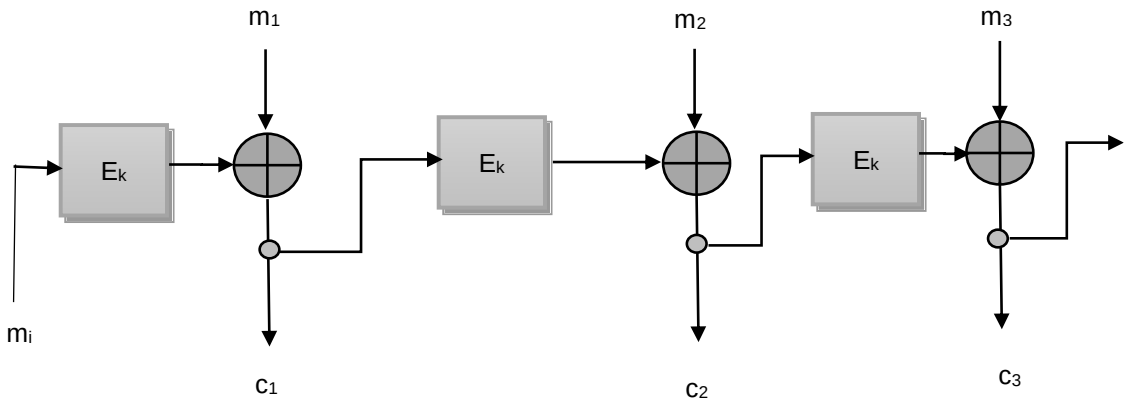
Για την αποκρυπτογράφηση ακολουθείται η ίδια ακριβώς διαδικασία με την κρυπτογράφηση, δηλαδή το περιεχόμενο του καταχωρητή κρυπτογραφείται αντί να αποκρυπτογραφείται, μόνο που στη λαμβανόμενη μονάδα κρυπτογραφημάτων εκτελείται η λογική πράξη XOR με την έξοδο της συνάρτησης κρυπτογράφησης, για την παραγωγή της μονάδας αρχικού κειμένου. Εάν θεωρήσουμε ότι το $S_j(X)$ ορίζεται ως τα j σημαντικότερα bit του X, τότε:

$$C_1 = P_1 \quad E_j\,(E \oplus (C_0)) \qquad \textbf{(3.3)}$$

Επομένως,

$$P_1 = C_1 \quad E_j\,(E \oplus (C_0)) \qquad \textbf{(3.4)}$$

Ένα πρόβλημα που διαπιστώνεται στη κατάσταση λειτουργίας κρυπτογραφίας ανάδρασης, είναι ότι σε περίπτωση που ένα bit στην ακολουθία του κρυπτοκειμένου αντιστραφεί κατά τη μετάδοση, τότε τα υπόλοιπα 8 byte που θα αποκρυπτογραφηθούν, θα είναι αλλοιωμένα, όσο βρίσκεται το προβληματικό byte στον καταχωρητή. Μόλις το προβληματικό byte αφαιρεθεί από τον καταχωρητή ολίσθησης, τότε θα παράγεται ξανά το σωστό απλό κείμενο. Έτσι, τα αποτελέσματα ενός μόνο αντεστραμμένου bit είναι τοπικά σχετικά, και δεν αλλοιώνουν το υπόλοιπο μήνυμα αλλά καταστρέφουν μόνο τα bit που αποτελούν
το πλάτος του καταχωρητή ολίσθησης.



Σχήμα 3.4: *Η μέθοδος Cipher Feedback*

3.3.4. Μέθοδος Ανάδρασης Εξόδου

Η μέθοδος ανάδρασης εξόδου (Output Feedback – OFB) μοιάζει με την CFB με τη διαφορά όμως ότι η ποσότητα πληροφορίας στην οποία εφαρμόζεται η λογική πράξη XOR με την ομάδα καθαρού κειμένου δημιουργείται ανεξάρτητα από το καθαρό κείμενο ή το κρυπτογράφημα.

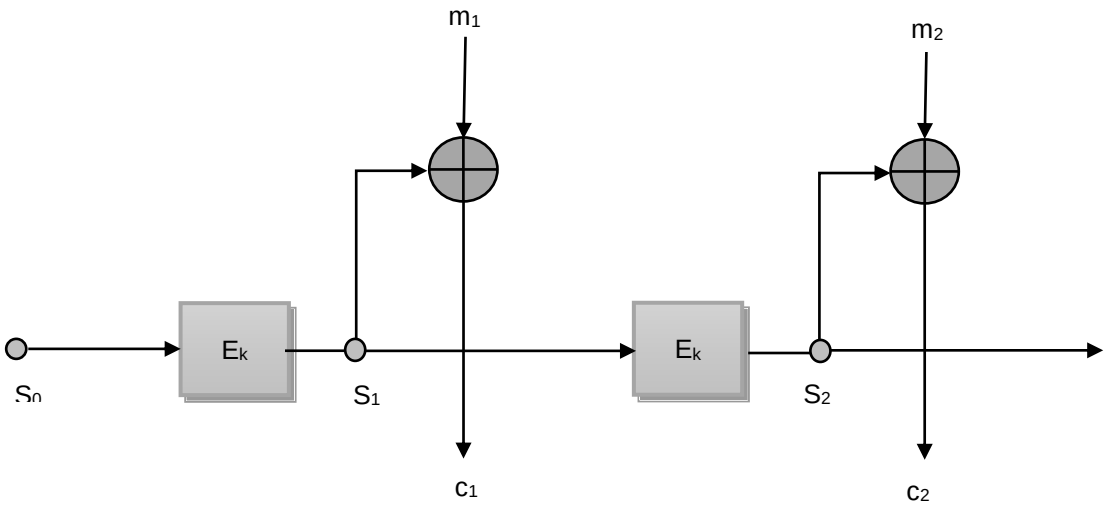
Και σε αυτή τη μέθοδο, το παραγόμενο αποτέλεσμα επανατροφοδοτείται στην είσοδο του μηχανισμού κρυπτογράφησης. Ένας καταχωρητής αρχικοποιείται με μια γνωστή τιμή και ύστερα κρυπτογραφείται με το κλειδί του χρήστη, εφαρμόζοντας τον ECB. Το αποτέλεσμα που προκύπτει από τη διαδικασία αυτή χρησιμοποιείται ως κλειδί προκειμένου να κρυπτογραφηθεί η ομάδα δεδομένων και αποθηκεύεται στον καταχωρητή για να χρησιμοποιηθεί στην επόμενη ομάδα.

Αναλυτικότερα, ένα διάνυσμα s_0 χρησιμοποιείται ως φύτρο για μια ακολουθία δεδομένων s_0, ενώ κάθε ομάδα s_j παράγεται από τη κρυπτογράφηση της προηγούμενης ομάδας δεδομένων s_{j-1}. Η κρυπτογράφηση της ομάδας του αρχικού κειμένου επιτυγχάνεται χρησιμοποιώντας τη λογική πράξη XOR ανάμεσα στο κομμάτι του καθαρού κειμένου και το σχετιζόμενο κομμάτι δεδομένων.

Το βασικό πλεονέκτημα που παρουσιάζει η μέθοδος OFB σε σχέση με τη CFB είναι η διασφάλιση ότι σε περίπτωση εμφάνισης σφαλμάτων κατά τη μετάδοση, έχει

περιορισμένη επίδραση και μόνο στα αντίστοιχα bits, άρα περιορίζεται η διάδοση σφαλμάτων.

Απ' την άλλη, θα μπορούσαμε να υποστηρίξουμε ότι μέθοδος OFB δεν είναι τόσο ασφαλής όσο οι υπόλοιπες τρείς λειτουργίες καθώς το αρχικό κείμενο μπορεί εύκολα να παραποιηθεί. Έστω ότι ο επιτιθέμενος γνωρίζει κάποιο κομμάτι καθαρού κειμένου m_i, έχει τη δυνατότητα να αντικαταστήσει αυτό το κομμάτι με κάποιο άλλο κομμάτι καθαρού κειμένου έστω x. Εφαρμόζοντας τη λογική συνάρτηση XOR (m_i x) στην αντίστοιχη ομάδα κρυπτογράφησης C_i.



$c_i = m_i \oplus s_i$ $\quad m_i = c_i \oplus s_i$ $\quad s_i = E_K (s_i -1)$

Σχήμα 3.5: *Η μέθοδος Output Feedback*

3.3.5. Λειτουργία του DES

Ο αλγόριθμος DES είναι ένας αλγόριθμος ομάδας, όπως αναφέραμε και πιο πάνω, που σημαίνει ότι κατά τη διαδικασία κρυπτογράφησης ενός μηνύματος δεν κρυπτογραφεί το κάθε ένα bit ξεχωριστά, αλλά ολόκληρες ομάδες των 64 bits (16 δεκαεξαδικά ψηφία). Για τη διαδικασία της κρυπτογράφησης αλλά και αποκρυπτογράφησης ο DES χρησιμοποιεί κλειδιά με μήκος 64 bits. Όμως, όλα τα bits που βρίσκονται στις θέσεις 8, 16, 24, 32, 40, 48, 56 και 64 αγνοούνται από τον αλγόριθμο με αποτέλεσμα το τελικό ενεργό μήκος του κλειδιού να είναι 56 bits. Ωστόσο, υπάρχουν περιπτώσεις όπου το μήκος του μηνύματος δεν είναι ίσο ή ακέραιο πολλαπλάσιο των 64 bits και θα πρέπει στο τέλος του μηνύματος να προστεθούν κάποια bytes. Αυτά τα επιπλέον bytes, δεν επηρεάζουν το περιεχόμενο του μηνύματος, καθώς, όταν αποκρυπτογραφηθεί το μήνυμα, αυτά θα

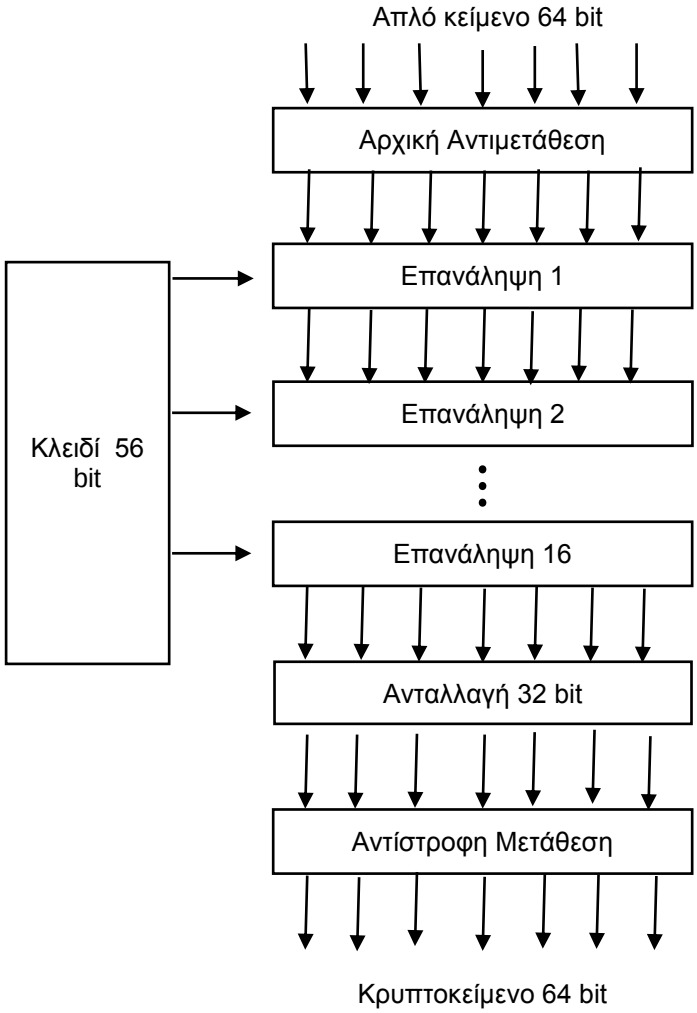
αφαιρεθούν. Υπάρχουν πολλοί τρόποι για να συμπληρωθούν τα επιπλέον bytes στο μήνυμα. Ο πιο απλός είναι να προστεθούν στο τέλος του μηνύματος αρκετά μηδενικά, ώστε το συνολικό μήκος του μηνύματος να είναι πολλαπλάσιο των 8 bytes (64 bits).

Ο αλγόριθμος, λοιπόν, που υλοποιεί τον DES δέχεται ως είσοδο ένα απλό κείμενο το οποίο κρυπτογραφείται σε τμήματα των 64 bit,που με τη σειρά τους παράγουν 64 bit κρυπτογραφημένου κειμένου, και ένα κλειδί 56 bits. Αρχικά , εφαρμόζεται στο απλό κείμενο μια συγκεκριμένη αντιμετάθεση των ψηφίων του, το αποτέλεσμα της οποίας χωρίζεται σε δύο τμήματα των 32 bits, το δεξί και το αριστερό. Στη συνέχεια, εκτελεί 16 φορές έναν μετασχηματισμό ο οποίος χρησιμοποιεί τη λογική συνάρτηση XOR (Exclusive or), μια ειδική συνάρτηση f, και διαφορετικά κάθε φορά υποσύνολα του αρχικού κλειδιού. Στο τέλος, αφού ολοκληρωθεί αυτή η διαδικασία, το αποτέλεσμα της υπόκειται σε μια ακόμη αντιμετάθεση των ψηφίων, η οποία στην ουσία αποκαθιστά τη σειρά των ψηφίων του αρχικού μηνύματος, την οποία αλλοίωσε η αρχική μετάθεση.

Για να κατανοήσουμε καλύτερα τη λειτουργία του θα εξηγήσουμε τα σχεδιαγράμματα που ακολουθούν και αποτελούν:

a. Τη γενική διάρθρωση του DES και

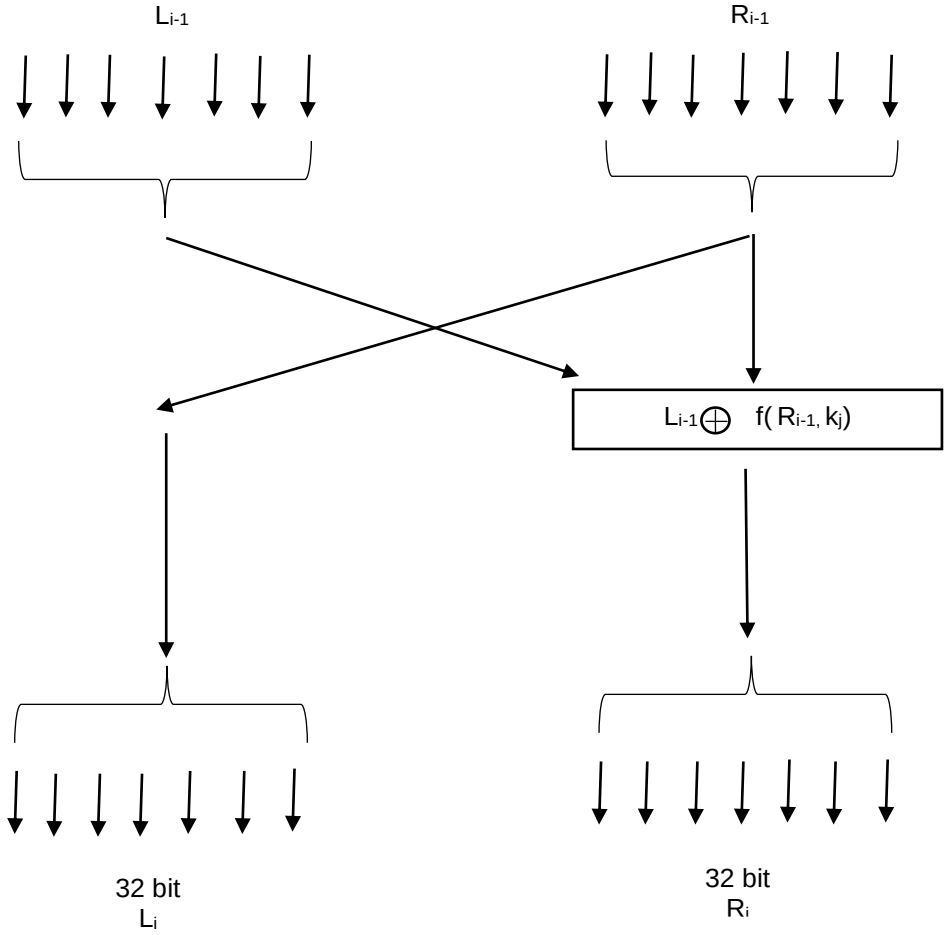
b. Τη λεπτομέρεια μιας επανάληψης



Σχήμα 3.6: *Γενική Διάρθρωση*

Το κείμενο κρυπτογραφείται σε τμήματα των 64 bit τα οποία αποδίδουν 64 bit κρυπτογραφημένου κειμένου. Ο αλγόριθμος παραμετροποιείται με ένα κλειδί 56 bit και αποτελείται από 19 διακριτά στάδια. Στο πρώτο στάδιο πραγματοποιείται μετάθεση των δυαδικών ψηφίων του αρχικού μη κρυπτογραφημένου κειμένου, η οποία είναι ανεξάρτητη από το κλειδί. Το τελευταίο στάδιο αποτελεί το αντίστροφο της αρχικής μετάθεσης στο πρώτο στάδιο. Στο προτελευταίο στάδιο πραγματοποιείται ανταλλαγή των 32 bits στα αριστερά με τα 32 bits στα δεξιά. Τα υπόλοιπα 16 στάδια που απομένουν είναι παρόμοια, με τη διαφορά ότι παραμετροποιούνται με διαφορετικές συναρτήσεις του κλειδιού. Το σύστημα αυτό έχει δημιουργηθεί έτσι ώστε η αποκρυπτογράφηση να επιτυγχάνεται

χρησιμοποιώντας το ίδιο κλειδί με της κρυπτογράφησης, μόνο που τα βήματα εκτελούνται αντίστροφα.



Σχήμα 3.7: *Λεπτομέρεια μιας επανάληψης*

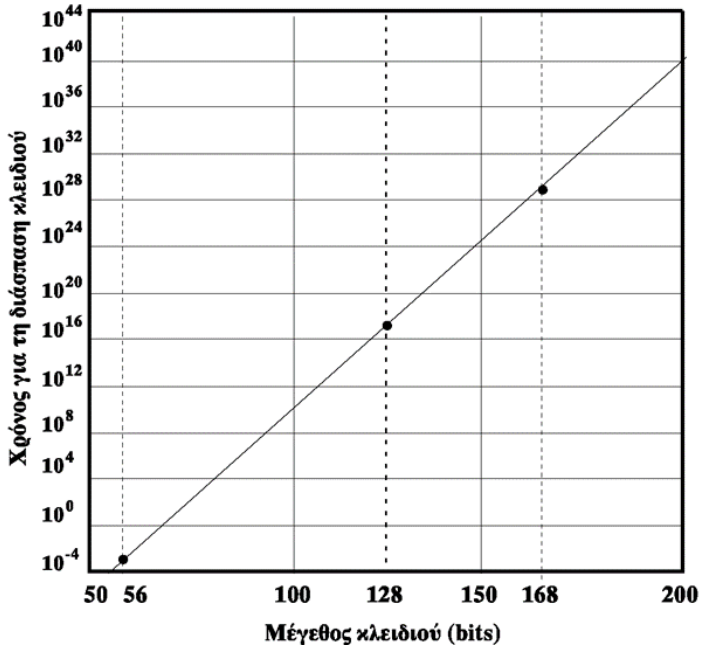
3.3.6. Η Ισχύς του Αλγορίθμου DES

Όσον αναφορά την ισχύ του αλγορίθμου DES, υπήρχε μια ανησυχία που στηριζόταν σε δύο αιτίες: αιτίες σχετιζόμενες με τον ίδιο τον αλγόριθμο και αιτίες σχετιζόμενες με τη χρήση κλειδιού με μέγεθος 56 bit.

Η πρώτη κατηγορία αιτιών ανησυχίας στηριζόταν στην πιθανότητα να επιτευχθεί η κρυπτανάλυση του αλγορίθμου μέσω της εκμετάλλευσης κάποιων χαρακτηριστικών του. Παρ' όλα αυτά, αν και έχουν πραγματοποιηθεί πολλές προσπάθειες για την εύρεση και εκμετάλλευση αδυναμιών του DES, δεν ανακαλύφθηκαν ή τουλάχιστον δεν δημοσιεύτηκαν, αδυναμίες σημαντικής κλίμακας, γεγονός που τον καθιστά ως τον εκτενέστερα μελετημένο ρωμαλέο αλγόριθμο κρυπτογράφησης.

Η δεύτερη κατηγορία αιτιών ανησυχίας στηριζόταν στο μήκος του κλειδιού. Ήδη από τα τέλη της δεκαετίας του ’70 ειδικοί σε θέματα ασφάλειας προειδοποιούσαν ότι το χρονικό διάστημα κατά το οποίο ο DES με μέγεθος κλειδιού 56 bit θεωρείται ασφαλής, φτάνει προς το τέλος του, λαμβάνοντας πάντα υπόψιν τις διαφαινόμενες τάσεις αύξησης της ταχύτητας των επεξεργαστών και ταυτόχρονης μείωσης των τιμών του υλικού. Τον Ιούλιο του 1998, το Ίδρυμα Electronic Frontier Foundation – EFF ανακοίνωσε ότι κατόρθωσε εντός τριών ημερών να κρυπταναλύσει ένα DES κρυπτομήνυμα χρησιμοποιώντας μια μηχανή ειδικού σκοπού αποκαλούμενη DES cracker, που το κόστος της ήταν μικρότερο από 250.000 USD. Το EFF δημοσίευσε μια λεπτομερή περιγραφή της μηχανής, προσφέροντας τη δυνατότητα σε όποιον άλλο ήθελε να δημιουργήσει αντίστοιχες ατομικές μηχανές.

Αξίζει να σημειώσουμε ότι δεν είναι μια απλή επίθεση αναζήτησης κλειδιού, όπου δοκιμάζονται με επιθέσεις, τύπου εξαντλητικής αναζήτησης, όλα τα πιθανά κλειδιά για να βρεθεί το κατάλληλο. Σε περίπτωση που δεν δίνετε γνωστό αρχικό κείμενο, ο αναλυτής πρέπει να μπορεί να αναγνωρίσει το αρχικό κείμενο ως πράγματι αρχικό κείμενο. Έστω ότι το μήνυμα είναι απλό-κοινό κείμενο στην Αγγλική γλώσσα, τότε το αποτέλεσμα παράγεται εύκολα, διότι η αναγνώριση των κειμένων στην Αγγλική γλώσσα έχει αυτοματοποιηθεί. Εάν, όμως, το κείμενο έχει συμπιεστεί πριν από τη διαδικασία της κρυπτογράφησης, τότε η αναγνώριση γίνεται πιο δύσκολη. Κατά συνέπεια, για να πραγματοποιηθεί η κρυπτανάλυση απαιτείται και κάποια γνώση για το είδος του αρχικού κειμένου. Η προσέγγιση του EFF έχει εξετάσει το ζήτημα αυτό και εισήγαγε μερικές αυτοματοποιημένες τεχνικές οι οποίες θα μπορούσαν να είναι αποτελεσματικές σε αρκετά κείμενα.



Εικόνα 3.1: Χρόνος που απαιτείται για τη διάσπαση ενός κώδικα (υποθέτοντας 10^6 αποκρυπτογραφήσεις/μs)

Ιδιαίτερο ενδιαφέρον παρουσιάζει το εξής σημείο: Έστω ότι η μόνη μορφή επίθεσης που θα μπορούσε να δεχτεί ένας κρυπτογραφικός αλγόριθμος είναι η επίθεση τύπου εξαντλητικής αναζήτησης κλειδιών, τότε ο τρόπος αντιμετώπισης των επιθέσεων αυτών θα ήταν η χρήση κλειδιών με ακόμη μεγαλύτερο μέγεθος. Εάν υποθέσουμε ότι η μηχανή διάσπασης είναι σε θέση να πραγματοποιήσει 106 αποκρυπτογραφήσεις ανά μs, τότε 10 ώρες περίπου αρκούν προκειμένου να κρυπταναλυθεί ένα κείμενο κρυπτογραφημένο με το σύστημα DES. Το γεγονός αυτό οδηγεί σε 7 φορές ταχύτερα αποτελέσματα από εκείνα που επιτεύχθηκαν από το EFF. Με αυτό το ρυθμό, στο παραπάνω σχήμα παρουσιάζεται ο απαιτούμενος χρόνος που χρειάζεται για να διασπαστεί ένας αλγόριθμος τύπου DES σε σχέση με το μέγεθος του κλειδιού. Ένα κλειδί μεγέθους 128 bit, το οποίο μέγεθος χρησιμοποιείται πλέον στους σύγχρονους αλγορίθμους, θα χρειαζόταν περισσότερα από 1018 χρόνια για να παραβιαστεί κάνοντας χρήση της μηχανής διάσπασης του EFF. Επιπλέον, αν μπορούσαμε να επιταχύνουμε τη διάσπαση με συντελεστή της τάξης του 1012, θα απαιτούσε περισσότερα από 106 χρόνια προκειμένου να διασπαστεί ο κώδικας. Κατά συνέπεια, ένα κλειδί 128 bit αποτελεί εγγύηση για έναν αλγόριθμο έναντι σε επιθέσεις τύπου εξαντλητικής αναζήτησης κλειδιών.

3.4. Τριπλό DES

Ήδη από το 1979, η IBM αντιλήφθηκε ότι το μέγεθος του κλειδιού του DES ήταν πολύ μικρό και γι' αυτό το λόγο επινόησε έναν τρόπο για την ουσιαστική αύξησή του, χρησιμοποιώντας τριπλή κρυπτογράφηση. Το TDES (Triple Data Encryption Standard) ή TDEA ή συνηθέστερα 3DES προτάθηκε αρχικά από τον W. Tuchman και το 1985 προτυποποιήθηκε στο ANSI X9.17, έτσι ώστε να χρησιμοποιηθεί σε οικονομικές εφαρμογές. Το 1999, με την δημοσίευση του με το όνομα FIPS PUB 46-3, το TDES ενσωματώθηκε ως μέρος της προτυποποίησης κρυπτογράφησης δεδομένων DES.

Το TDES χρησιμοποιεί τρία κλειδιά και τρείς εκτελέσεις του αλγορίθμου DES. Ο αλγόριθμος ακολουθεί τα εξής στάδια: κρυπτογράφηση, αποκρυπτογράφηση, κρυπτογράφηση (EDE- Encryption - Decryption – Encryption)

$$C = E_{K3}[\,D_{K2}[\,E_{K1}[P]]] \qquad \textbf{(3.4)}$$

Όπου:

C = κρυπτογράφημα

P = αρχικό κείμενο

$E_K[X]$ = κρυπτογράφηση του X χρησιμοποιώντας το κλειδί K

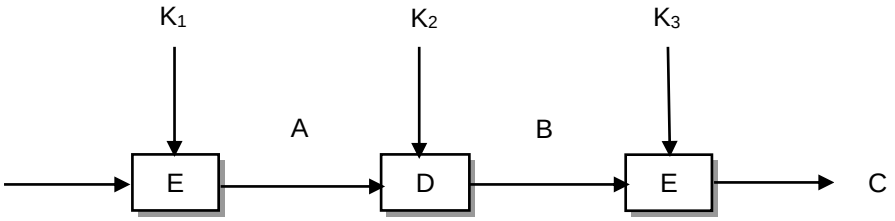
$D_K[Y]$ = αποκρυπτογράφηση του X χρησιμοποιώντας το κλειδί K

Σχετικά με τα κλειδιά το πρότυπο ANSI X9.52 ορίζει τρείς διαφορετικές περιπτώσεις:

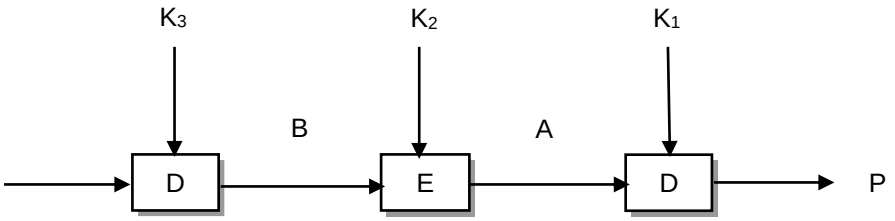
- Τα τρία κλειδιά K_1, K_2, K_3 είναι ανεξάρτητα
- Τα κλειδιά K_1 και K_2 είναι ανεξάρτητα αλλά $K_1 = K_3$
- $K_1 = K_2 = K_3$

Κατά την αποκρυπτογράφηση ακολουθείται όμοια διαδικασία με την κρυπτογράφηση με τα κλειδιά, όμως, σε αντίστροφη χρήση.

$$P = D_{K1}[E_{K2}[D_{K3}[C]]] \qquad \textbf{(3.5)}$$



(α) Κρυπτογράφηση



(β) Αποκρυπτογράφηση

Σχήμα 3.8: *TDES*

Ο λόγος για τον οποίο εφαρμόζεται η σειρά κρυπτογράφηση, αποκρυπτογράφηση, κρυπτογράφηση είναι η συμβατότητα προς τα πίσω με τα ήδη υπάρχοντα συστήματα DES ενός κλειδιού. Οι συναρτήσεις κρυπτογράφησης και αποκρυπτογράφησης αποτελούν και τις δυο αντιστοιχίσεις ανάμεσα σε σύνολα 64μπιτων αριθμών. Από την πλευρά της κρυπτογραφίας, οι δύο αυτές αντιστοίχισης είναι το ίδιο ισχυρές. Όταν όμως εφαρμόζεται η σειρά EDE, ένας υπολογιστής ο οποίος χρησιμοποιεί τριπλή κρυπτογράφηση μπορεί να επικοινωνήσει με έναν υπολογιστή που κάνει χρήση μονής κρυπτογράφησης ορίζοντας απλά $K_1 = K_2$. Η ιδιότητα αυτή επιτρέπει την σταδιακή εισαγωγή της τριπλής κρυπτογράφησης.

Το TDES, έχοντας την υποστήριξη τριών διαφορετικών κλειδιών, διαθέτει κλειδί μεγέθους 168 bit. Στα πλαίσια του FIPS 46-3 επιτρέπεται η χρήση δύο κλειδιών K_1, K_2, με $K_1 = K_3$. Έτσι εξασφαλίζεται κλειδί μεγέθους 112 bit. Το FIPS 46-3 περιλαμβάνει τις οδηγίες που αναφέρονται παρακάτω για το TDES:

- Το TDES είναι ένας εγκεκριμένος συμβατικός αλγόριθμος κρυπτογράφησης ως FIPS.

- Το DES, ο οποίος κάνει χρήση ενός και μοναδικού κλειδιού των 56 bit, επιτρέπεται στα συστήματα διαχείρισης δικτύων για επίτευξη συμβατότητας προς τα κάτω. Τα νέα συστήματα, όμως, απαιτείται να είναι συμβατά με τον TDES
- Οι κυβερνητικές οργανώσεις των Η.Π.Α που χρησιμοποιούν DES ενθαρρύνονται για τη μετάβαση σε TDES
- Αναμένεται ότι το TDES και το Advanced Encryption Standard – AES θα συνυπάρξουν ως FIPS εγκεκριμένοι αλγόριθμοι, μέχρι ότου γίνει οριστική μετάβαση στο AES

Γενικότερα υπάρχουν τέσσερις παραλλαγές για τον triple-DES:

- DES-EEE3 (Encrypt – Encrypt – Encrypt): πραγματοποιούνται τρεις συνεχόμενες κρυπτογραφήσεις με τρία διαφορετικά κλειδιά.
- DES-EDE3 (Encrypt – Decrypt - Encrypt): το μήνυμα διαδοχικά κρυπτογραφείται, αποκρυπτογραφείται, κρυπτογραφείται με τη χρήση τριών διαφορετικών κλειδιών
- DES-EE2: αποτελεί την ίδια διαδικασία με τη πρώτη με τη διαφορά ότι απαιτούνται δύο διαφορετικά κλειδιά
- DES-EDE2: αποτελεί την ίδια διαδικασία με τη δεύτερη με τη διαφορά ότι απαιτούνται δύο κλειδιά

Ο TDES αποτελεί έναν σπουδαίο αλγόριθμο και επειδή προέρχεται από τον DES παρουσιάζει την ίδια ισχυρή αντίσταση με αυτόν στις κρυπταναλυτικές επιθέσεις. Επίσης, χρησιμοποιώντας κλειδί μήκους 168 bit, οι επιθέσεις τύπου εξαντλητικής αναζήτησης είναι πρακτικά ατελέσφορες. Άρα αναμένεται ο TDES να αξιοποιηθεί ολοένα και περισσότερο μέσα στα επόμενα χρόνια, μέχρι να γίνει η ολοκληρωτική μετάβαση στον AES.

3.5. Advanced Encryption Standard (AES)

Λαμβάνοντας υπόψιν όσων αναφέρθηκαν παραπάνω, αν η ασφάλεια ήταν το μοναδικό κριτήριο επιλογής ενός αλγορίθμου, τότε ο TDES θα αποτελούσε μια εξαιρετικά καλή επιλογή για έναν τυποποιημένο κρυπτογραφικό αλγόριθμο για τα επόμενα χρόνια.

Το κυριότερο μειονέκτημα του TDES αποτελεί το γεγονός ότι ο αλγόριθμος είναι σχετικά αργός σε υλοποιήσεις με χρήσεις λογισμικού. Το σύστημα DES σχεδιάστηκε τη δεκαετία του ’70 για υλοποίηση με χρήση υλικού αλλά δε παράγει αποδοτικό κώδικα λογισμικού. Ο TDES, είναι πολύ πιο βραδύτερος από τον DES καθώς οι γύροι που περιλαμβάνει είναι τρεις φορές περισσότεροι. Ένα άλλο μειονέκτημα είναι η απαίτηση που εμφανίζουν οι DES και TDES να χρησιμοποιούν τμήματα μεγέθους 64 bit το οποίο μέγεθος, για γενικότερους λόγους αποδοτικότητας και ασφάλειας, είναι επιθυμητό να είναι μεγαλύτερο. Επομένως, καταλήγουμε στο συμπέρασμα ότι ο TDES δεν μπορεί να θεωρηθεί αποτελεσματικός.

Προκειμένου να αντιμετωπιστούν τα προβλήματα αυτά, ήδη από το 1997 το NIST προκήρυξε παγκόσμιο διαγωνισμό για τη δημιουργία ενός νέου **Προηγμένου Προτύπου Κρυπτογράφησης (Advanced Encryption Standard - AES)**, διάδοχο του DES και προσδιόρισε ότι το AES θα πρέπει να αποτελεί κωδικοποιητή τμημάτων με συμμετρικό σύστημα κρυπτογράφησης, μήκος τμήματος 128 bit και να υποστηρίζει κλειδιά μήκους 128 bit, 192 bit και 256 bit. Τα κριτήρια συγκριτικής αξιολόγησης των υποψήφιων αλγορίθμων χωρίστηκαν σε τρείς κατηγορίες:

- **Στην ασφάλεια των αλγορίθμων:** τα κριτήρια που περιλαμβάνονται σε αυτή τη κατηγορία σχετίζονταν με τη ρωμαλεότητα των αλγορίθμων σε κρυπταναλυτικές επιθέσεις, την ορθότητα του μαθηματικού φορμαλισμού, τη συγκριτική ασφάλεια του αλγορίθμου σε σχέση με τους υπόλοιπους υποψήφιους αλγορίθμους και την τυχαιότητα της συμπεριφοράς της εξόδου. Σε γενικές γραμμές τα χαρακτηριστικά ασφαλείας που παρουσίαζαν οι αλγόριθμοι, θα έπρεπε να είναι τουλάχιστον ισοδύναμα με τους TDES, αλλά ταυτόχρονα να χαρακτηρίζονται από σημαντικά βελτιωμένη αποδοτικότητα.
- **Στο κόστος:** τα κριτήρια που ανήκουν σε αυτή τη κατηγορία περιλάμβαναν τις απαιτήσεις μνήμης και υπολογιστικής ισχύος του αλγορίθμου, καθώς επίσης και τις απαιτήσεις που σχετίζονταν με τη προστασία των δικαιωμάτων πνευματικής ιδιοκτησίας και πατέντες έτσι ώστε το πρότυπο που βρισκόταν υπό ανάπτυξη να είναι δυνατόν να αξιοποιηθεί σε διεθνή κλίμακα.
- **Στην απλότητα:** τα κριτήρια που ανήκουν σε αυτή τη κατηγορία σχετίζονταν με την απλότητα, την ευελιξία – με άλλα λόγια με το πόσο ικανός είναι ο αλγόριθμος να χειριστεί μεγέθη μυστικών κλειδιών και τμημάτων μη

κρυπτογραφημένου κειμένου που είναι μεγαλύτερα από τα ελάχιστα τεθέντα – τη δυνατότητα υλοποίησης του αλγορίθμου σε διάφορα περιβάλλοντα όπως για παράδειγμα λογισμικό, υλικό, υλικό λογισμικό (firmware), αλλά επιπλέον και την παροχή συμπληρωματικών λειτουργιών.

Στον πρώτο κύκλο αξιολόγησης έγιναν αποδεκτοί 15 αλγόριθμοι και στον δεύτερο κύκλο έγιναν αποδεκτοί μόνο οι 5 αλγόριθμοι. Οι αλγόριθμοι αυτοί είναι οι εξής: MARS, RC6, Rijndael, Serpent, Twofish. Εν τέλει, επισήμως επιλέχθηκε ως AES ο αλγόριθμος Rijndael, τον οποίο είχαν υποβάλει οι Βέλγοι κρυπτογράφοι J. Daemen και V. Rijmen, και έλαβε την τελική του μορφή στο τέλος του καλοκαιριού του 2001.

Παρακάτω αναφέρονται συνοπτικά τα βασικότερα χαρακτηριστικά του κάθε ένα αλγορίθμου που είχε περάσει στον τελευταίο κύκλο αξιολόγησης και ήταν υποψήφιος για AES:

- **Ο αλγόριθμος MARS**

Ο αλγόριθμος MARS περιλαμβάνει 32 κύκλους μετασχηματισμών. Από τους κύκλους αυτούς μόνο οι 16 στηρίζονται στο μυστικό κλειδί και οι πράξεις που πραγματοποιούνται είναι ο πολλαπλασιασμός, η πρόσθεση με τα κλειδιά των 32 bit και η ολίσθηση ή περιστροφή των δεδομένων. Οι υπόλοιποι 16 κύκλοι που απομένουν αξιοποιούν 8 S-boxes των 32 bit με πράξεις πρόσθεσης και XOR.

- **Ο αλγόριθμος RC6**

Ο αλγόριθμος RC6 αποτελείται από 20 κύκλους μετασχηματισμών. Σε όλους τους κύκλους πραγματοποιείται μεταβλητή περιστροφή δεδομένων και οι πράξεις που διεξάγονται είναι ο πολλαπλασιασμός, η πρόσθεση, η λογική πράξη XOR και η πρόσθεση υποκλειδιών.

- **Ο αλγόριθμος Serpent**

Ο αλγόριθμος Serpent αποτελείται από 32 κύκλους μετασχηματισμών. Στον αλγόριθμο εφαρμόζεται μια αρχική και μια τελική μετάθεση, οι οποίες διευκολύνουν εναλλακτικούς τρόπους λειτουργίας. Ο κάθε ένας κύκλος περιλαμβάνει τρία επιμέρους επίπεδα μετασχηματισμών: η λογική πράξη XOR με το υποκλειδί, 32 παράλληλες εφαρμογές ενός από τα 8 S-boxes και ένας γραμμικός μετασχηματισμός.

- **Ο αλγόριθμος Twofish**

Ο αλγόριθμος Twofish αποτελείται από 16 κύκλους, στον καθένα εκ των οποίων εφαρμόζονται 4 S-boxes τα οποία εξαρτώνται από το μυστικό κλειδί. Στα επόμενα

στάδια περιλαμβάνονται η αξιοπιστία των σταθερών S-boxes, η διενέργεια μετασχηματισμού pseudo-Hadamard και η πρόσθεση του υποκλειδιού.

- **Ο αλγόριθμος Rijndael**

Ο αλγόριθμος Rijndael, που επιλεχθεί ως AES, χαρακτηρίζεται από απλότητα, ευελιξία, ρωμαλεότητα σε όλες τις κρυπταναλυτικές επιθέσεις και υψηλή ταχύτητα λειτουργίας

Όσον αναφορά το σχεδιαστικό κομμάτι, ο αλγόριθμος Rijndael δεν ακολουθεί τη κλασική δομή Feistel, αλλά κάθε κύκλος λειτουργίας αποτελείται από τρεις όμοιους μετασχηματισμούς, με όρους ισότιμης αντιμετώπισης κάθε ξεχωριστού bit, που ονομάζονται επίπεδα (layers):

- Το επίπεδο γραμμικής ανάμιξης (linear mixing layer) επιτυγχάνει υψηλή διάχυση σε πολλαπλούς κύκλους
- Το μη γραμμικό επίπεδο (non-linear layer) έχει να κάνει με την παράλληλη εφαρμογή S-boxes τα οποία εμφανίζουν εξαιρετικές μη γραμμικές ιδιότητες για το ενδεχόμενο χειρότερης περίπτωσης (optimum worst-case nonlinarity properties)
- Το επίπεδο πρόσθεσης κλειδιού (key addition layer) αφορά στη συσχέτιση του αποτελέσματος που προκύπτει ενδιάμεσα με το υποκλειδί του κύκλου, με την λογική πράξη XOR.

Ο αλγόριθμος Rijndael αποτελείται από 10, 12 ή 14 κύκλους ανάλογα με το μήκος του μυστικού κλειδιού. Ο κάθε κύκλος αποτελείται από τέσσερις μετασχηματισμούς οι οποίοι είναι εξής: ByteSub, ShiftRow, MixColumn, AddKeyRound. Ο ByteSub μετασχηματισμός βρίσκει εφαρμογή σε όλα τα bytes του τμήματος. Οι μετασχηματισμοί ShiftRow και MixColumn υποστηρίζουν τη γραμμική ανάμειξη των δεδομένων του τμήματος. Ο μετασχηματισμός AddKeyRound συσχετίζει τα bytes του τμήματος με τα bytes των υποκλειδιών με την λογική πράξη XOR. Επίσης, ο μετασχηματισμός αυτός εκτελείται ακόμη μια φορά στη φάση αρχικοποίησης πριν τον πρώτο κύκλο, ενώ στον τελευταίο κύκλο παραλείπεται ο μετασχηματισμός MixColumn.

3.6. Λοιποί Συμμετρικοί Κωδικοποιητές Τμημάτων

Όλοι οι εναλλακτικοί συμβατικοί αλγόριθμοι τμημάτων κρυπτογράφησης στηρίζονται στη βασική δομή τμημάτων του Feistel. Η δομή του Feistel γίνεται εύκολα κατανοητή και καθιστά την εκτίμηση της κρυπτογραφικής ισχύος ενός νέου

αλγορίθμου ευκολότερη. Σε αντίθετη περίπτωση όπου γίνετε εφαρμογή μιας εντελώς διαφορετικής δομής, η νέα αυτή δομή είναι πιθανό να παρουσιάζει κάποια αδυναμία η οποία δε γίνεται εύκολα διακριτή και συνεπώς δεν θα γινόταν αμέσως αντιληπτή από το σχεδιαστή

Αλγόριθμος	Μήκος Κλειδιού	Αριθμός κύκλων	Μαθηματικές Πράξεις	Εφαρμογές
DES	56 bits	16	XOR, σταθερά S-boxes	SET, Kerberos
Triple DES	112 ή 168	48	XOR, σταθερά S-boxes	Financial key management, PGP, S/MIME
IDEA	128	8	XOR, πρόσθεση. πολλαπλασιασμός	PGP
Blowfish	Μεταβλητό μέχρι 448 bits	16	XOR, μεταβλητά S-boxes, πρόσθεση	
RC5	Μεταβλητό μέχρι 2048 bits	Μεταβλητό μέχρι 255	πρόσθεση, αφαίρεση, XOR, περιστροφή	
CAST-128	40 μέχρι 128 bits	16	πρόσθεση, αφαίρεση, XOR, περιστροφή, σταθερά S-boxes	PGP

Πίνακας 3.1: Συμβατικοί αλγόριθμοι κρυπτογράφησης

3.6.1. International Data Encryption Algorithm (IDEA)

Ο αλγόριθμος International Data Encryption Algorithm – IDEA αποτελεί συμμετρικό κωδικοποιητή τμημάτων, που αναπτύχθηκε από τους X. Lai και J. Massey, στο Swiss Federal Institute of Technology, το 1991. Το κλειδί που χρησιμοποιείται από τον IDEA είναι μεγέθους 128 bit και διαφέρει με τον DES στη συνάρτηση F αλλά και στη συνάρτηση παραγωγής των υποκλειδιών. Όσον αναφορά τη συνάρτηση F, ο IDEA δε χρησιμοποιεί S-boxes, αλλά βασίζεται σε τρεις διαφορετικές λειτουργίες οι οποίες είναι: η δυαδική λογική πράξη XOR, τη δυαδική πρόσθεση ακεραίων των 16 bit και τον δυαδικό πολλαπλασιασμό ακεραίων των 16 bit.

Οι συναρτήσεις συνδυάζονται με τέτοιο τρόπο έτσι ώστε να δημιουργηθεί ένας περίπλοκος μετασχηματισμός που αναλύεται δύσκολα, με αποτέλεσμα το έργο της κρυπτανάλυσης να καθίσταται πιο δύσκολο. Ο αλγόριθμος παραγωγής δευτερευόντων κλειδιών στηρίζεται στην εφαρμογή κυκλικών μετατοπίσεων, οι οποίες χρησιμοποιούνται πολύπλοκο τρόπο για να παραχθούν συνολικά έξι δευτερεύοντα κλειδιά για καθέναν από τους οχτώ γύρους του IDEA. Ο IDEA ήταν

ένας από τους προτεινόμενους 128 bit αντικαταστάτες του DES, έχει διερευνηθεί διεξοδικά και εμφανίζεται ανθεκτικός σε κρυπταναλυτικές επιθέσεις.

3.6.2. Blowfish

Ο αλγόριθμος Blowfish αναπτύχθηκε το 1993 από τον κρυπτογράφο B. Schneier και καθιερώθηκε ως μια από τις δημοφιλέστερες εναλλακτικές λύσεις του DES. Ο Blowfish δημιουργήθηκε με τέτοιο τρόπο ώστε να είναι εύκολο να υλοποιηθεί και να παρουσιάζει μεγάλη ταχύτητα εκτέλεσης. Πρόκειται για έναν συνεπτυγμένο αλγόριθμο που μπορεί να εκτελεστεί σε μνήμη μικρότερη από 5K. Ένα απ' τα χαρακτηριστικά που παρουσιάζει ιδιαίτερο ενδιαφέρον είναι το μήκος του κλειδιού, το οποίο είναι μεταβλητό και μπορεί να λάβει τιμές έως 448 bit, αν και πρακτικά χρησιμοποιούνται κλειδιά των 128 bit. Ο Blowfish αποτελείται από 16 γύρους.

Όπως ο αλγόριθμος DES έτσι και ο Blowfish χρησιμοποιεί X-boxes, XOR και δυαδική πρόσθεση. Αντίθετα, όμως, με τον DES που χρησιμοποιεί σταθερά X-boxes, ο Blowfish χρησιμοποιεί δυναμικά S-boxes τα οποία παράγονται ως συνάρτηση του κλειδιού. Τα υποκλειδιά και τα S-boxes αυτού του αλγορίθμου παράγονται από την επανειλημμένη εφαρμογή του ίδιου του Blowfish στο κλειδί. Συνολικά χρειάζονται 521 εκτελέσεις του αλγορίθμου προκειμένου να παραχθούν τα υποκλειδιά και τα S-boxes. Βάση των χαρακτηριστικών αυτών καταλήγουμε στο συμπέρασμα ότι ο Blowfish δεν είναι κατάλληλος για εφαρμογές που απαιτούν συχνή αλλαγή του μυστικού κλειδιού.

Ο Blowfish αποτελεί έναν από τους πιο καλούς συμβατικούς αλγόριθμους κρυπτογράφησης που έχουν εφαρμοστεί καθώς τα κλειδιά και τα S-boxes είναι αποτέλεσμα επανειλημμένων εφαρμογών του ίδιου του Blowfish στον εαυτό του. Οι επαναλήψεις αυτές τροποποιούν εξ' ολοκλήρου τα δυαδικά ψηφία και καθιστούν το έργο της κρυπτανάλυσης εξαιρετικά δύσκολο. Οι μέχρι σήμερα προσπάθειες για κρυπτανάλυση του Blowfish δεν αναφέρουν πρακτικές αδυναμίες.

3.6.3. RC5

Ο RC5 αναπτύχθηκε το 1994 από τον R. Rivest, ένας από τους σχεδιαστές του αλγορίθμου δημοσίου κλειδιού RSA. Ο RC5 προσδιορίζεται στο RFC 2040 και σχεδιάστηκε ώστε να υποστηρίζει τα παρακάτω χαρακτηριστικά:

- **Κατάλληλο για υλοποίηση σε υλικό ή λογισμικό:** ο RC5 χρησιμοποιεί μόνο βασικές υπολογιστικές λειτουργίες, που συνήθως περιλαμβάνονται στους μικροεπεξεργαστές.
- **Ταχύς:** έτσι ώστε να επιτευχθεί υψηλή ταχύτητα, ο αλγόριθμος RC5 είναι ένας απλός αλγόριθμος που στηρίζεται στη λέξη (word). Οι βασικές του λειτουργίες βασίζονται σε πλήρεις λέξεις δεδομένων ανά στιγμή.
- **Προσαρμόσιμος σε επεξεργαστές διαφορετικών μήκους λέξης***:* Στον RC5 ο αριθμός των δυαδικών ψηφίων μιας λέξης αποτελεί βασική παράμετρο, καθώς διαφορετικά μήκη λέξης παράγουν διαφορετικούς αλγορίθμους.
- **Μεταβλητό μήκος γύρων:** Ο αριθμός των γύρων αποτελεί δεύτερη βασική παράμετρο του RC5. Αυτή η παράμετρος επιτρέπει την εναλλαγή μεταξύ υψηλότερης ταχύτητας και υψηλότερης ασφάλειας.
- **Μεταβλητό μήκος κλειδιού:** Το μήκος του κλειδιού αποτελεί τη τρίτη βασική παράμετρο του RC5. Κι αυτή η παράμετρος εξίσου επιτρέπει την εναλλαγή μεταξύ υψηλότερης ταχύτητας και υψηλότερης ασφάλειας.
- **Απλός:** Η απλή δομή του RC5 επιτρέπει την εύκολη υλοποίησή του και διευκολύνει τον υπολογισμό της ισχύος του αλγορίθμου.
- **Χαμηλή απαίτηση μνήμης:** Η χαμηλή απαίτηση μνήμης κάνει τον αλγόριθμο κατάλληλο για αξιοποίηση σε έξυπνες κάρτες και άλλες συσκευές περιορισμένης μνήμης.
- **Υψηλή ασφάλεια:** Ο προορισμός του RC5 είναι να παρέχει υψηλή ασφάλεια με προσδιορισμό των κατάλληλων παραμέτρων.
- **Περιστροφές εξαρτώμενες από τα δεδομένα:** Ο RC5 ενσωματώνει τις περιστροφές, δηλαδή κυκλικές μετατοπίσεις δυαδικών ψηφίων, ο αριθμός των οποίων εξαρτάται από τα δεδομένα. Αυτό έχει ως αποτέλεσμα την ενίσχυση του αλγορίθμου ενάντια στις κρυπταναλυτικές επιθέσεις.

3.6.4. CAST-128

Το CAST αναπτύχθηκε20 1997 από τους C. Adams και S. Tavares της εταιρίας Entrust Technologies και αποτελεί μια διαδικασία σχεδίασης συμμετρικών αλγορίθμων κρυπτογράφησης. Ένας αλγόριθμος ο οποίος αναπτύχθηκε ως τμήμα του προγράμματος CAST είναι ο CAST-128. Το μέγεθος του κλειδιού που χρησιμοποιείται σ' αυτόν τον αλγόριθμο παίρνει τιμές μεταξύ 40 bit και 128 bit, με βήματα των 8 bit. Το CAST αποτελεί το προϊόν μιας μεγάλης χρονικά διαδικασίας έρευνας και ανάπτυξης και έχει ενσωματώσει σειρά σχολίων από κρυπταναλυτές.

Το CAST χρησιμοποιεί σταθερά S-boxes, αλλά μόνο αυτά που είναι αρκετά μεγαλύτερα από αυτά που χρησιμοποιούνται στον DES. Τα S-boxes έχουν σχεδιαστεί με τέτοιο τρόπο ώστε να μην παρουσιάζουν γραμμικότητα μεταξύ εισόδου κι εξόδου, με αποτέλεσμα να είναι ανθεκτικά σε επιθέσεις κρυπτανάλυσης. Η διαδικασία με την οποία παράγονται τα υποκλειδιά στον CAST-128 είναι διαφορετική σε σχέση με αυτήν που χρησιμοποιείται στους υπόλοιπους συμβατικούς αλγορίθμους κρυπτογράφησης τμημάτων. Οι σχεδιαστές του CAST προσπάθησαν να δημιουργήσουν κλειδιά που θα είναι πιο ανθεκτικά σε γνωστές κρυπταναλυτικές επιθέσεις. Θεωρήθηκε ότι η παραγωγή κλειδιών από το βασικό κλειδί με τη χρήση μη γραμμικών S-boxes, θα μπορούσε να παρέχει αυτή τη δυνατότητα. Σπουδαίο χαρακτηριστικό του CAST-128 αποτελεί η συνάρτηση κύκλου F, η οποία είναι διαφορετική σε κάθε κύκλο, καθιστώντας με αυτόν τον τρόπο τον αλγόριθμο κρυπταναλυτικά ανθεκτικότερο.

3.7. Κρυπτογραφήματα στοιχειοσειράς (Stream Chipher)

Το κρυπτογράφημα στοιχειοσειράς είναι ένα είδος συμμετρικού αλγορίθμου κρυπτογράφησης. Τα κρυπτογραφήματα αυτά είναι δυνατόν να σχεδιαστούν με τέτοιο τρόπο ώστε να είναι πολύ γρήγορα, γρηγορότερα από οποιοδήποτε κρυπτογράφημα ομάδας. Αντίθετα με τα κρυπτογραφήματα ομάδας που λειτουργούν σε μεγάλες ομάδες δεδομένων, τα κρυπτογραφήματα στοιχειοσειράς εφαρμόζονται σε πιο μικρές ομάδες κειμένου, συνήθως σε επίπεδο δυαδικών ψηφίων (bits). Η κρυπτογράφηση ενός απλού κειμένου με κρυπτογράφημα ομάδας, θα είχε αποτέλεσμα το ίδιο κρυπτογράφημα στη περίπτωση που χρησιμοποιούνταν το ίδιο κλειδί. Αντίθετα, όμως, με το κρυπτογράφημα στοιχειοσειράς ο μετασχηματισμός των μικρών μονάδων απλού κειμένου θα διαφέρει.

Το κρυπτογράφημα στοιχειοσειράς δημιουργεί αυτό που ονομάζεται ***στοιχειοσειρά κλειδιού*** (keystream), δηλαδή μια ακολουθία από bits που χρησιμοποιείται ως κλειδί. Η κρυπτογράφηση πραγματοποιείται συνδυάζοντας τη στοιχειοσειρά κλειδιού με το απλό κείμενο συνήθως με τη συνάρτηση XOR. Η δημιουργία της στοιχειοσειράς κλειδιού μπορεί να είναι ανεξάρτητη από το απλό κείμενο και το κρυπτογράφημα, κι αυτό ονομάζεται "σύγχρονο κρυπτογράφημα στοιχειοσειράς" ή μπορεί να εξαρτάται από τα δεδομένα και την κρυπτογράφησή τους, όπου τότε κάνουμε αναφορά για αυτό-συγχρονιζόμενο κρυπτογράφημα στοιχειοσειράς.

Το καινούργιο ενδιαφέρον στα κρυπτοσυστήματα στοιχειοσειράς έχει να κάνει με τα θεωρητικά χαρακτηριστικά του λεγόμενου "παραγεμίσματος της μιας φοράς" (one-time pad). Το one-time pad, που συχνά αναφέρεται και ως κρυπτογράφημα Verman χρησιμοποιεί μια σειρά από bits που παράγεται τυχαία. Το κλειδί στοιχειοσειράς διαθέτει το ίδιο μέγεθος με το μήνυμα του απλού κειμένου και συνδυάζεται με τη βοήθεια της συνάρτησης XOR με το καθαρό κείμενο προκειμένου να παραχθεί ο κρυπτογραφημένο. Εξαιτίας του ότι όλη η στοιχειοσειρά κειμένου είναι τυχαία, ακόμα και ένας κρυπταναλυτής που θα είχε στη διάθεσή του άπειρους υπολογιστικούς πόρους, το μόνο που θα μπορούσε είναι να μαντέψει το αρχικό κείμενο με βάση το κρυπτογραφημένο. Ένα τέτοιο κρυπτογράφημα, θεωρείται ότι μπορεί να προσφέρει τέλεια ασφάλεια, παρά το γεγονός ότι το μέγεθος του μυστικού κλειδιού (το οποίο μπορεί να χρησιμοποιηθεί μόνο για μια φορά) είναι τόσο μεγάλο όσο και το καθαρό κείμενο, δημιουργώντας έτσι προβλήματα στη διαχείριση του κλειδιού. Έτσι γίνεται αντιληπτό ότι, αν και είναι εξαιρετικά ασφαλές για το one-time pad, ωστόσο δεν είναι δυνατή η πρακτική χρησιμοποίησή του.

Στις μέρες μας, δεν υπάρχει κάποιο κρυπτογράφημα στοιχειοσειράς. Το πιο ευρέως διαδεδομένο κρυπτογράφημα στοιχειοσειράς είναι το RC4.

ΚΕΦΑΛΑΙΟ 4ο

4. ΑΛΓΟΡΙΘΜΟΙ ΔΗΜΟΣΙΟΥ ΄Η ΑΣΥΜΜΕΤΡΟΥ ΚΛΕΙΔΙΟΥ

Κατά την ιστορική αναδρομή της κρυπτογραφίας παρατηρούμε ότι η μεγαλύτερη αδυναμία των περισσότερων κρυπτοσυστημάτων (cryptosystems) ήταν πάντα η διανομή των κλειδιών. Αν ένας εισβολέας, ανεξάρτητα από το πόσο ισχυρό ήταν το κρυπτοσύστημα, μπορούσε να υποκλέψει το κλειδί, τότε το σύστημα αυτό ήταν άχρηστο. Οι κρυπτολόγοι είχαν πάντα ως δεδομένο ότι το κλειδί της κρυπτογράφησης και της αποκρυπτογράφησης πρέπει να είναι ταυτόσημα ή τουλάχιστον ότι θα μπορεί το ένα να προκύπτει εύκολα απ' το άλλο. Απ' την άλλη, όμως, το κλειδί έπρεπε να μοιραστεί σε όλους τους χρήστες του συστήματος. Αυτό είχε, λοιπόν, ως αποτέλεσμα τη δημιουργία ενός εγγενούς προβλήματος καθώς τα κλειδιά αφενός έπρεπε να προστατευτούν αλλά, αφετέρου, έπρεπε και να μοιραστούν.

Οι ερευνητές Diffie και Helman στο Πανεπιστήμιο της Στάνφορντ το 1976, πρότειναν ένα διαφορετικό είδος κρυπτοσυστήματος, όπου το κλειδί της κρυπτογράφησης ήταν διαφορετικό από αυτό της αποκρυπτογράφησης και το κλειδί της αποκρυπτογράφησης δεν μπορούσε να προκύψει από εκείνο της κρυπτογράφησης. Σύμφωνα με την πρότασή τους, οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης με τα κλειδιά *E* και *D* αντίστοιχα, έπρεπε να ικανοποιούν τις παρακάτω τρείς απαιτήσεις οι οποίες μπορούν να οριστούν ως εξής:

1. $D(E(P)) = P$
2. Είναι εξαιρετικά δύσκολα να προκύψει το *D* από το *E*.
3. Ο *E* δεν μπορεί να σπάσει με μια επίθεση επιλεγμένου απλού κειμένου

Πιο απλά, η πρώτη απαίτηση λέει ότι αν εφαρμόσουμε τον αλγόριθμο κρυπτογράφησης D σε ένα κρυπτογραφημένο κείμενο E(P) θα παράγουμε το αρχικό καθαρό μήνυμα P. Χωρίς αυτή την ιδιότητα, ο νόμιμος παραλήπτης δε θα μπορούσε να αποκρυπτογραφήσει το κρυπτογραφημένο κείμενο. Η δεύτερη απαίτηση είναι αυτονόητη. Η τρίτη απαίτηση κρίνεται απαραίτητη γιατί οι εισβολείς έχουν τη δυνατότητα να πειραματιστούν με τον αλγόριθμο όσο επιθυμούν. Επομένως, αν ισχύουν αυτές οι τρεις συνθήκες τότε ο αλγόριθμος κρυπτογράφησης και το κλειδί μπορούν να δημοσιευτούν, απ' όπου προέρχεται και το όνομα ***κρυπτογραφία δημόσιου κλειδιού*** (public key cryptography). Η κρυπτογραφία

δημόσιου κλειδιού χρησιμοποιείται κυρίως για αυθεντικοποίηση μηνυμάτων και διανομή μυστικών κλειδιών.

4.1. Δομή Κρυπτοσυστημάτων Δημοσίου Κλειδιού

Οι κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού βασίζονται σε μαθηματικές συναρτήσεις και όχι σε απλές πράξεις με bits. Μάλιστα, η κρυπτογραφία δημοσίου κλειδιού είναι ασύμμετρη (asymmetric) καθώς χρησιμοποιεί ένα ζευγάρι ξεχωριστών κλειδιών (key pair), σε σύγκριση με τη συμμετρική κρυπτογράφηση που κάνει χρήση ενός μόνο κλειδιού. Η χρήση δύο κλειδιών συνεπάγεται με σημαντικές τροποποιήσεις τόσο σε θέματα που αφορούν την εμπιστευτικότητα και την αυθεντικότητα, όσο και τη διανομή κλειδιών.

Αρχικά, είναι απαραίτητο να γίνει αναφορά σε κάποιες λανθασμένες αντιλήψεις σχετικά με την κρυπτογράφηση δημοσίου κλειδιού. Η πρώτη λάθος αντίληψη αφορά την εντύπωση πως η ασύμμετρη κρυπτογράφηση είναι πιο ασφαλής συγκριτικά με τη συμμετρική κρυπτογράφηση, ως ανθεκτικότερη σε επιθέσεις κρυπτανάλυσης. Στη πραγματικότητα, όμως, η ασφάλεια οποιουδήποτε κρυπτογραφικού συστήματος εξαρτάται από το μέγεθος του κλειδιού και από την απαιτούμενη υπολογιστική ισχύ που έχει στη διάθεσή του ένας κρυπταναλυτής ώστε να κατορθώσει να παραβιάσει και να αποκαλύψει με επιτυχία ένα κρυπτογραφικό μήνυμα. Η δεύτερη εσφαλμένη αντίληψη σχετίζεται με την επικράτηση της ασύμμετρης κρυπτογραφίας σε βάρος της συμμετρικής. Έτσι λοιπόν, σ’ αυτό το σημείο πρέπει να ξεκαθαρίσουμε ότι και τα δύο συστήματα χρησιμοποιούνται εξίσου και δε προβλέπεται με κανένα τρόπο η εγκατάλειψη του συμμετρικού συστήματος, ειδικά όταν είναι γνωστή η σημαντική χρονική επιβάρυνση που απαιτείται για την ολοκλήρωση των εκτελούμενων εργασιών σε περιβάλλον ασύμμετρου κρυπτοσυστήματος. Επίσης, επικρατεί η άποψη ότι η διανομή κλειδιών είναι ευκολότερη στην ασύμμετρη κρυπτογραφία σε σχέση με τις επιπλέον χειραψίες (handshaking) που είναι απαραίτητες με τα κέντρα διανομής κλειδιών (key distribution centers) για τη συμμετρική κρυπτογράφηση. Στην πράξη, στα συστήματα δημοσίου κλειδιού είναι απαραίτητη η εκτέλεση κάποιων πρωτοκόλλων, εμπλέκεται κάποιος ενδιάμεσος αντιπρόσωπος, ο οποίος θεωρείται έμπιστος, και οι διαδικασίες που παρεμβάλλονται δεν είναι απλούστερες ή

περισσότερο αποδοτικές από αυτές που απαιτούνται για τη συμμετρική κρυπτογράφηση.

4.2. Μέθοδος Λειτουργίας

Όπως υποδεικνύει το όνομά τους, το δημόσιο κλειδί αποσκοπεί σε δημόσια χρήση, ενώ το ιδιωτικό κλειδί χρησιμοποιείται αποκλειστικά από τον κάτοχό του. Ένας γενικής χρήσης αλγόριθμος κρυπτογράφησης/αποκρυπτογράφησης στηρίζεται σε ένα δημόσιο κλειδί για την κρυπτογράφηση και σε ένα άλλο, διαφορετικό αλλά μοναδικά συσχετιζόμενο κλειδί, το ιδιωτικό κλειδί, για την αποκρυπτογράφηση.

Παρακάτω περιγράφονται τα βήματα που ακολουθούνται:

- Κάθε χρήστης παράγει ένα ζεύγος κλειδιών που θα χρησιμοποιηθούν κατά τη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης των μηνυμάτων.
- Κάθε χρήστης τοποθετεί το δημόσιο κλειδί σε μια βάση δεδομένων ενός φορέα ή σε κάποιο προσβάσεως αρχείο. Το ιδιωτικό κλειδί, διαφυλάσσεται διατηρώντας τη μυστικότητα. Για επίτευξη στοιχειώδους λειτουργικότητας, είναι απαραίτητο κάθε χρήστης να μπορεί να ανακτήσει εύκολα τα δημόσια κλειδιά των άλλων.
- Έστω ότι ο Bob επιθυμεί να αποστείλει ένα μήνυμα στην Alice και αποτελεί τεθείσα απαίτηση (requirement) η διασφάλιση της εμπιστευτικότητας του μηνύματος, τότε ο Bob κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί της Alice.
- Η Alice λαμβάνει το μήνυμα και το αποκρυπτογραφεί με το ιδιωτικό της κλειδί. Το μήνυμα αυτό δε μπορεί να αποκρυπτογραφηθεί από κανέναν άλλο, καθώς μόνο η Alice γνωρίζει το ιδιωτικό της κλειδί το οποίο είναι μοναδικά συσχετιζόμενο με το αντίστοιχο δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση.

Αναλυτικότερα: Έστω η Alice, ένα άτομο που επιθυμεί να λάβει ένα μυστικό μήνυμα, επινοεί αρχικά δύο αλγόριθμους οι οποίοι ικανοποιούν τις παραπάνω απαιτήσεις. Ο αλγόριθμος κρυπτογράφησης και το κλειδί της Alice δημοσιεύονται. Προκειμένου να δηλώσουμε τον αλγόριθμο κρυπτογράφησης με παράμετρο το **δημόσιο κλειδί** της Alice θα χρησιμοποιήσουμε τη σημειογραφία E_A. Όμοια, ο

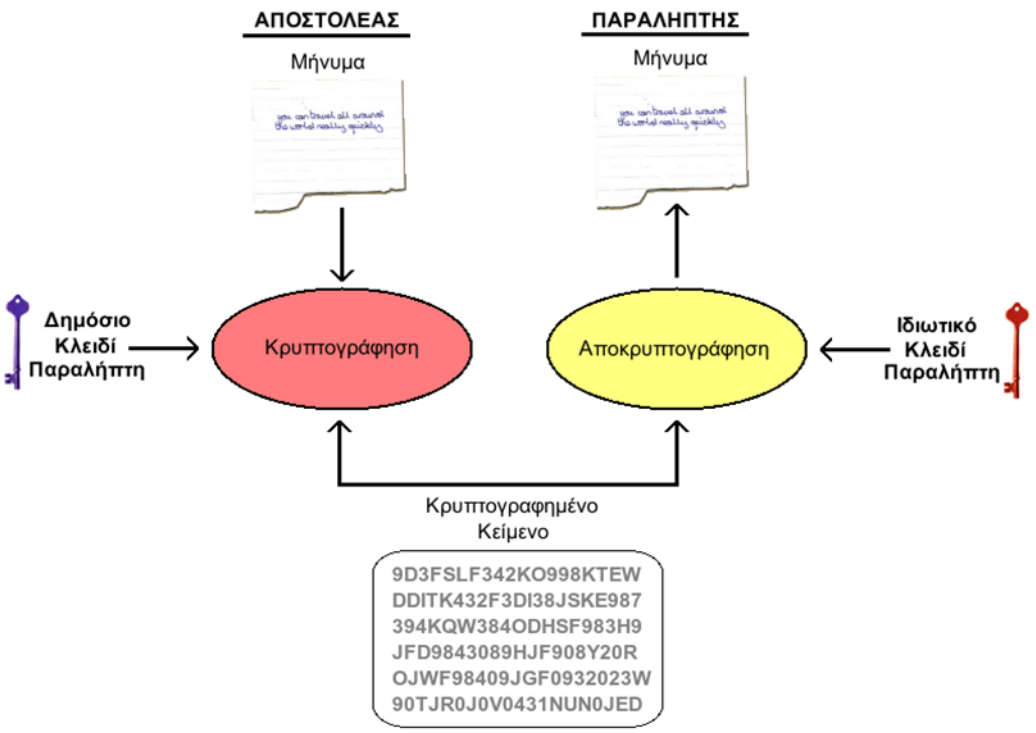
αλγόριθμος αποκρυπτογράφησης με παράμετρο το **ιδιωτικό κλειδί** της Alice συμβολίζεται με D_A. Ο Bob κάνει το ίδιο πράγμα, δημοσιεύοντας το E_B αλλά κρατώντας μυστικό το D_B.

Έστω ότι η Alice και ο Bob δεν είχαν καμία επικοινωνία στο παρελθόν, η εγκαθίδρυση ενός ασφαλούς καναλιού ανάμεσά τους πραγματοποιείται ως εξής: Θεωρούμε ότι το κλειδί κρυπτογράφησης της Alice E_A αλλά και του Bob E_B είναι τοποθετημένα σε αρχεία αναγνώσιμα από όλους. Η Alice λαμβάνει το πρώτο μήνυμα P, υπολογίζει το E_B (P), και το στέλνει στον Bob, ο οποίος το αποκρυπτογραφεί χρησιμοποιώντας το μυστικό κλειδί του D_B, δηλαδή υπολογίζει $D_B (E_B (P)) = P$. Κανείς άλλος δε είναι σε θέση να διαβάσει το κρυπτοκείμενο $E_B (P)$, διότι υποθέσαμε ότι το κρυπτογραφικό σύστημα είναι αρκετά ισχυρό και άρα είναι δύσκολο να υπολογιστεί το D_B από το δημόσια γνωστό E_B. Για να μπορέσει να στείλει απάντηση R, ο Bob μεταδίδει το $E_A(R)$. Τώρα η Alice και ο Bob μπορούν να επικοινωνήσουν με ασφάλεια.

Προϋπόθεση αυτής της προσέγγισης είναι τα δημόσια κλειδιά να είναι προσβάσιμα σε όλους τους συμμετέχοντες, ενώ τα ιδιωτικά να παράγονται τοπικά για τον κάθε συμμετέχοντα προκειμένου να εξασφαλίζεται η μυστικότητά τους. Ένας χρήστης έχει τη δυνατότητα να αλλάξει το ιδιωτικό του κλειδί ανά πάσα στιγμή και ταυτόχρονα να γνωστοποιήσει το αντίστοιχο νέο δημόσιο κλειδί, ώστε να αντικατασταθεί το προηγούμενο, μη πλέον ισχύον δημόσιο κλειδί.

Το κλειδί που χρησιμοποιείται στη συμμετρική κρυπτογράφηση αναφέρεται ως μυστικό κλειδί (secret). Το ζεύγος κλειδιών (key pair) που χρησιμοποιείται στην ασύμμετρη κρυπτογράφηση εμπεριέχει το δημόσιο κλειδί (public key) και το ιδιωτικό κλειδί (private key), το οποίο παραμένει μυστικό αλλά προκειμένου να αποφευχθεί εννοιολογική σύγχυση με τη συμμετρική κρυπτογράφηση, αναφέρεται ως ιδιωτικό κι όχι μυστικό κλειδί.

Στο παρακάτω σχήμα αναπαριστάται η γενική μορφή υλοποίησης ενός ασύμμετρου συστήματος:



Σχήμα 4.1: *Γενική αναπαράσταση ενός συστήματος δημοσίου κλειδιού*

4.3. Εφαρμογές Κρυπτοσυστημάτων δημοσίου κλειδιού

Στα κρυπτοσυστήματα δημοσίου κλειδιού, ανάλογα με τις απαιτήσεις ασφάλειας, το είδος της εφαρμογής και της υπηρεσίας που βρίσκεται υπό σχεδιασμό και υλοποίηση, ο αποστολέας χρησιμοποιεί είτε το δικό του ιδιωτικό κλειδί, είτε το δημόσιο κλειδί του παραλήπτη, είτε και τα δύο προκειμένου να υλοποιήσει κάποιο τύπο κρυπτογραφικών λειτουργιών

Το ζεύγος του δημόσιου και ιδιωτικού κλειδιού σε αυτά τα συστήματα, βρίσκουν εφαρμογή σε τρείς περιπτώσεις, οι οποίες είναι οι εξής:

- ***Κρυπτογράφηση/Αποκρυπτογράφηση (Encryption/Decryption)***: Το μήνυμα κρυπτογραφείται από τον πομπό χρησιμοποιώντας το δημόσιο κλειδί του αποδέκτη ο οποίος με τη σειρά του αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί.
- ***Ψηφιακή Υπογραφή (Digital Signature)****:* Ο αποστολέας κάνοντας χρήση του ιδιωτικού του κλειδιού, υπογράφει ένα μήνυμα. Η υπογραφή αυτή δημιουργείται εφαρμόζοντας έναν κρυπτογραφικό αλγόριθμο στο μήνυμα ή συνηθέστερα στη σύνοψη (hash) του μηνύματος. Ο αποδέκτης αυθεντικοποιεί τον αποστολέα χρησιμοποιώντας το δημόσιο κλειδί του.

- ***Ανταλλαγή κλειδιών (Key Exchange):*** Δύο πρόσωπα συνεργάζονται προκειμένου να ανταλλάξουν ένα κλειδί συνόδου (session key). Για την επίτευξη της ανταλλαγής κλειδιών είναι πιθανό να πραγματοποιηθούν ένα σύνολο διαφόρων ενεργειών, που αξιοποιούν το ιδιωτικό κλειδί του ενός ή και των δύο προσώπων που συμμετέχουν.

Αλγόριθμος	Κρυπτογράφηση/ Αποκρυπτογράφηση	Ψηφιακή Υπογραφή	Ανταλλαγή Κλειδιών
RSA	x	x	x
Diffie - Hellman	-	-	x
DSS	-	x	-
Elliptic Curve	x	x	x

Πίνακας 4.1: Αλγόριθμοι δημοσίου κλειδιού και υποστηριζόμενες εφαρμογές

Κάποιοι αλγόριθμοι είναι κατάλληλοι και για τις τρεις εφαρμογές, κάποιοι άλλοι μόνο για δύο και άλλοι μόνο για μία από αυτές.

4.4. Αλγόριθμος RSA

Το 1977, λίγο μετά την παρουσίαση της ιδέας του συστήματος με δημόσιο κλειδί, αναπτύχθηκε στο MIT ένα από τα πρώτα ασύμμετρα κρυπτογραφικά συστήματα από τους μαθηματικούς R. Rivest, A. Shamir και L. Adleman, το οποίο δημοσιεύτηκε για πρώτη φορά το 1978. Από εκείνη τη στιγμή ο RSA επικράτησε ως ο πλέον αποδεκτός και προσεγγιστικά εύκολα υλοποιήσιμος αλγόριθμος για ασύμμετρα κρυπτοσυστήματα. Στον αλγόριθμο του RSA το αρχικό και το κρυπτοκείμενο είναι ακέραιοι αριθμοί με τιμές μεταξύ 0 και n-1, για κάποιο n.

Η κρυπτογράφηση για ένα κείμενο M και αποκρυπτογράφηση για ένα κρυπτοκείμενο C συμβολίζεται ως εξής:

$C = M^e \bmod n$ **(4.1)**

$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$ **(4.2)**

Οι τιμές των *n* και *e* θα πρέπει να είναι γνωστοποιημένες τόσο στον αποστολέα όσο και στον παραλήπτη. Την τιμή *d* αντιθέτως, πρέπει να τη γνωρίζει μόνο ο παραλήπτης. Στην ουσία ο RSA είναι ένας αλγόριθμος ασύμμετρου κρυπτοσυστήματος με δημόσιο κλειδί KU = { e,n } και ιδιωτικό κλειδί KR = {d,n}. Παρακάτω παρατίθενται οι απαιτήσεις που πρέπει να πληρεί ο αλγόριθμος αυτός ώστε να καθίσταται ικανοποιητικός:

- Επιλογή δύο μεγάλων πρώτων αριθμών, p και q (συνήθως των 1024)
- Υπολογισμός των n = p x q και φ(n) = (p-1)(q-1)
- Επιλογή ενός αριθμού που είναι αμοιβαία πρώτος με το *φ(n),* τον οποίο ονομάζουμε *d.*
- Εντοπισμός το e και e x d = 1 mod φ(n)

Στον παρακάτω πίνακα περιγράφεται συνοπτικά ο RSA αλγόριθμος. Στην αρχή, για την παραγωγή των κλειδιών κρυπτογράφησης, επιλέγονται δυο αριθμοί *p,q* οι οποίοι πρέπει να είναι μεγάλοι και να κρατιούνται μυστικοί, και ύστερα υπολογίζεται το γινόμενό τους *n = p x q*, το οποίο αποτελεί βασικό παράγοντα για τη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης.

Παραγωγή κλειδιών	
Επέλεξε *p,q*	*p* και *q* κι οι δυ'ο πρώτοι
Υπολόγισε *n = p x q*	
Υπολόγισε φ(n) = (p – 1)(q – 1)	
Επέλεξε ακέραιο e	gcd(φ(n),e) = 1;1 < e< φ(n)
Υπολόγισε d	$d = e^{-1} \bmod \varphi(n)$
Δημόσιο κλειδί	KU = { e,n }
Ιδιωτικό κλειδί	KR = { d,n }
Αποκρυπτογράφηση	
Κρυπτοσύστημα:	C
Αρχικό κείμενο:	$M = C^d \ (mod\ n)$
Κρυπτογράφηση	
Κρυπτογράφημα:	M < n
Αρχικό κείμενο:	$C = M^d \ (mod\ n)$

Πίνακας 4.2: *Αλγόριθμος RSA*

Στη συνέχεια εφαρμόζεται η τιμή της συνάρτησης *φ(n),* που είναι γνωστή ως συνάρτηση του ***Euler*** για το *n (φ(n) = (p-1)(q-1)),*και η οποία δείχνει το πλήθος των θετικών ακέραιων αριθμών που είναι μικρότεροι από n και πρώτοι με αυτόν. Στη συνέχεια επιλέγεται ένας αριθμός *e* ώστε να είναι μικρότερος του *n*. Ο αριθμός αυτός δε είναι απαραίτητο να είναι πρώτος αριθμός αλλά πρέπει οπωσδήποτε να είναι περιττός. Επιπλέον, ο αριθμός *e* πρέπει να είναι πρώτος ως προς το *φ(n),* δηλαδή ο μέγιστος κοινός διαιρέτης του *e* και του *φ(n)* να είναι το 1. Στο τέλος υπολογίζεται ο *d*, ως φυσικός αντίστροφος αριθμός e modulo *φ(n),* από τη σχέση $d=e^{-1} \bmod \varphi(n)$. Ο *d* ονομάζεται *πολλαπλασιαστική ανάστροφος (multiplicative inverse)* του *e.*

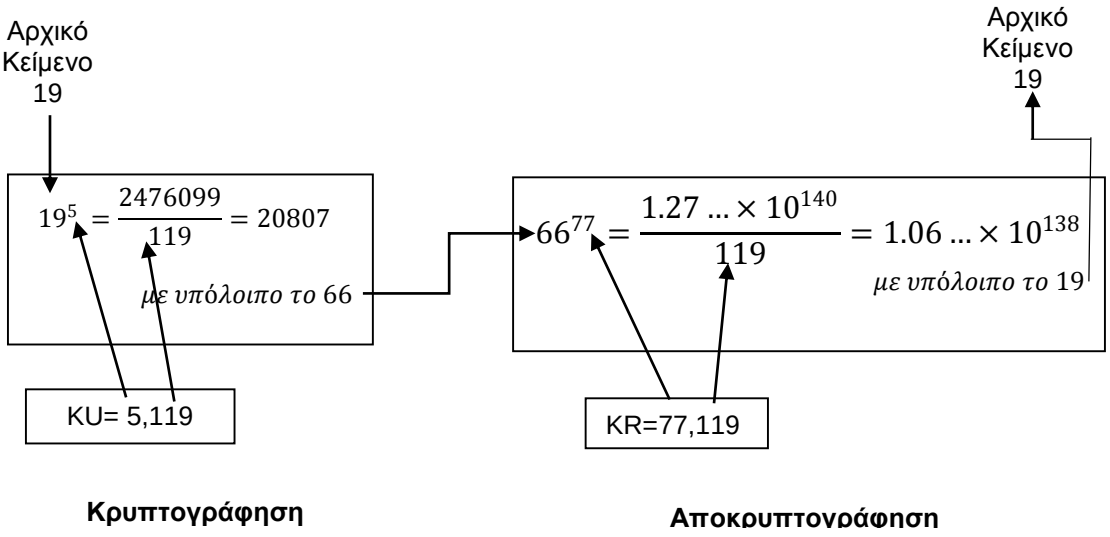
Ας υποθέσουμε ότι ο χρήστης Α έχει γνωστοποιήσει το δημόσιο κλειδί του στον χρήστη Β ο οποίος επιθυμεί να στείλει ένα μήνυμα *M* στον Α.

- Αρχικά το μήνυμα *M* (το οποίο θεωρούμε ως μια ακολουθία bits) παριστάνεται με έναν ακέραιο αριθμό που βρίσκεται εντός της περιοχής [0,n-1]. Σε περίπτωση που το μήνυμα *M* είναι μεγάλο, διαιρείται σε μικρότερα τμήματα.
- Ακολούθως, κάθε ένα τμήμα του μηνύματος αναπαρίσταται με έναν ακέραιο αριθμό που βρίσκεται εντός της περιοχής [0,n-1]. Σ' αυτό το σημείο πρέπει να τονίσουμε ότι ο αριθμός αυτός είναι διαφορετικός για κάθε τμήμα του μηνύματος αλλά έχει το ίδιο σταθερό μήκος για όλα τα τμήματα.

΄Υστερα ο Β κρυπτογραφεί κάθε τμήμα του μηνύματος με βάση την παράσταση $C=M^e \bmod n$ και μεταδίδει το *C*. Για την αποκρυπτογράφηση του μηνύματος, ο χρήστης Α υπολογίζει την παράσταση $M=C^d \bmod n$.

Παράδειγμα:

1. Στο σχήμα 4.2 παρουσιάζεται ένα σχετικό παράδειγμα:
2. Επιλέχθηκαν δύο πρώτοι αριθμοί, *p=7* και *q=17*
3. Υπολογίστηκε η τιμή του *n=pq=7*17=119*
4. Υπολογίστηκε η τιμή του *φ(n)=(p-1)(q-1)=96*
5. Επιλέχθηκε το *e*, το οποίο είναι πρώτος αριθμός ως προς το *φ(n)=96* και μικρότερο του *φ(n).* Στην περίπτωση αυτή *e=5.*
6. Προσδιορίστηκε το *d* έτσι, ώστε *de=1* mod 96 και *d<96*. Η σωστή τιμή του d είναι 77, γιατί *77*5=385=4*96+1*.



Σχήμα 4.2: *Παράδειγμα αλγορίθμου RSA*

Με τη παραπάνω διαδικασία υπολογίσαμε το δημόσιο κλειδί KU = { 5,119} αλλά και το ιδιωτικό KR = { 77,119}. Στο παράδειγμα παρουσιάζεται η χρήση των κλειδιών αυτών για ένα αρχικό κείμενο με *M = 19*. Κατά τη διαδικασία της κρυπτογράφησης το 19 υψώνεται στην 5η δύναμη δίνοντας αποτέλεσμα 2.476.099. Αφού το διαιρέσουμε με το 119 δίνει υπόλοιπο 66. Στη συνέχεια, 19^5 *66 mod 199* και το κρυπτοκείμενο είναι *C=66.* Κατά τη διαδικασία της αποκρυπτογράφησης προκύπτει ότι $66^{77} \equiv 19 \bmod 119$.

Υπάρχουν δύο πιθανοί τρόποι με τους οποίους είναι εφικτό να προκληθεί επιτυχημένη επίθεση στον RSA. Ο πρώτος τρόπος είναι μέσω της εξαντλητικής αναζήτησης κατά την οποία δοκιμάζονται όλα τα πιθανά κλειδιά. Έτσι διαπιστώνεται ότι όσο μεγαλύτερο μέγεθος (bits) έχουν τα e,d, τόσο πιο ασφαλής είναι ο αλγόριθμος. Όμως, λαμβάνοντας υπόψιν ότι κατά τη δημιουργία κλειδιών καθώς και κατά τη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης απαιτούνται πολύπλοκοι υπολογισμοί, όσο μεγαλύτερο είναι το μέγεθος των κλειδιών τόσο πιο αργός θα είναι ο ρυθμός λειτουργίας του συστήματος.

Η περισσότερη προσοχή, όμως, όσον αναφορά την κρυπτανάλυση του RSA, έχει στραφεί στη εύρεση δύο πρώτων αριθμών που να είναι παράγοντες του n. Για ένα μεγάλο αριθμό n, η διαδικασία αυτή αποτελεί δύσκολο πρόβλημα αλλά όχι τόσο όσο τα προηγούμενα χρόνια. Για παράδειγμα, τον Ιανουάριο του 1977 οι σχεδιαστές του RSA ζήτησαν από τους αναγνώστες του περιοδικού Scientific American να αποκρυπτογραφήσουν ένα κρυπτοκείμενο που είχε δημοσιευτεί σε

στήλη του περιοδικού. Θεωρούσαν πως ήταν τόσο αδύνατον να αποκρυπτογραφηθεί το κείμενο στα επόμενα 40 τετράκις εκατομμύρια χρόνια που προσέφεραν και αμοιβή 100 δολαρίων για την αποκρυπτογράφηση μιας μόνο πρότασης του κρυπτογραφημένου κειμένου. Όμως τον Απρίλιο του 1994, μία ερευνητική ομάδα που εργαζόταν αξιοποιώντας την υπολογιστική ισχύ 1600 υπολογιστών στο Internet κέρδισε το βραβείο μετά από 8 μήνες προσπάθεια. Σε αυτήν την περίπτωση, έγινε χρήση δημόσιου κλειδιού με μέγεθος 129 δεκαδικών ψηφίων (μήκος του n), δηλαδή 428 bits περίπου. Μάλιστα, το 1996 αναλύθηκε σε γινόμενο πρώτων παραγόντων ένας αριθμός 130 ψηφίων με 10 φορές λιγότερες πράξεις από αυτές που απαιτούνται κατά την ανάλυση ενός αριθμού με 129 ψηφία. Αυτά τα αποτελέσματα σηματοδοτούν ότι πρέπει να χρησιμοποιούνται μεγαλύτερα μεγέθη κλειδιών, χωρίς όμως αυτό να σημαίνει ότι οι δυνατότητες του RSA μειώνονται. Για τις σημερινές εφαρμογές ένα κλειδί μεγέθους 2048 θεωρείται ισχυρό.

4.5. Κρυπτογραφία Ελλειπτικής Καμπύλης

Στα περισσότερα προϊόντα και πρότυπα που χρησιμοποιούνται τα ασύμμετρα κρυπτοσυστήματα για κρυπτογράφηση και ψηφιακή υπογραφή, εφαρμόζουν τον αλγόριθμο RSA. Τα τελευταία χρόνια, έχει παρατηρηθεί σημαντική αύξηση του πλήθους των bits που χρησιμοποιείται για ασφαλή χρήση του RSA, με αποτέλεσμα να επιβαρύνονται με σημαντικό επιπλέον επεξεργαστικό φόρτο όλες οι αντίστοιχες εφαρμογές. Το πρόβλημα αυτό, εμφανίζεται εντονότερα στις ιστοσελίδες εφαρμογών ηλεκτρονικού εμπορίου, καθώς εκεί λαμβάνουν χώρα πολλές ασφαλείς δοσοληψίες. Τα τελευταία χρόνια, όμως, έχει αρχίσει να αναπτύσσεται ένα ανταγωνιστικό σύστημα του RSA, η Κρυπτογραφία Ελλειπτικής Καμπύλης (Elliptic Curve Cryptography – ECC).

Ο βασικός λόγος για τον οποίο ο ECC καθίσταται πιο ελκυστικός συγκριτικά με τον αλγόριθμο του RSA, είναι ότι προσφέρει το ίδιο επίπεδο ασφάλειας για μικρότερο πλήθος bits, μειώνοντας έτσι σημαντικά τον υπολογιστικό χρόνο και φόρτο εργασίας που απαιτείται. Σύμφωνα με σχετικά πρόσφατες επιστημονικές ανακοινώσεις, επιτεύχθηκε η κρυπτανάλυση του ECC με μέγεθος κλειδιού 109 bits χρησιμοποιώντας την αδιάκοπη επεξεργαστική ισχύ 10.000 υπολογιστών επί 549 ημέρες. Σε αυτή τη φάση, ο αλγόριθμος μπορεί να θεωρηθεί ασφαλής, αρκεί το

μέγεθος του κλειδιού να είναι τουλάχιστον 163 bits. Από την άλλη όμως, ενώ η θεωρία του ECC ήταν γνωστή για αρκετό καιρό, σχετικά πρόσφατα άρχισαν να κάνουν την εμφάνισή τους προϊόντα που χρησιμοποιούν ECC. Από αυτό γίνεται κατανοητή η έλλειψη εμπιστοσύνης προς τον ECC, σχετικά με τον RSA. Η αξιοποιηθείσα τεχνική του ECC, στηρίζεται στην εφαρμογή ενός μαθηματικού μοντέλου, που ονομάζεται *ελλειπτική καμπύλη*.

ΚΕΦΑΛΑΙΟ 5ο

5. ΚΡΥΠΤΟΓΡΑΦΙΚΑ ΠΡΩΤΟΚΟΛΛΑ

5.1. Διανομή Κρυπτογραφικών Κλειδιών

Προκειμένου την επίτευξη της αποτελεσματικής λειτουργίας στη συμβατική κρυπτογράφηση, θα πρέπει τα δυο συμβαλλόμενα μέρη να μοιράζονται το ίδιο κλειδί, το οποίο δε θα είναι προσιτό σε τρίτους. Επίσης, απαραίτητες είναι οι συχνές αλλαγές του κλειδιού έτσι ώστε να περιοριστούν τα δεδομένα που πιθανόν να αποκαλυφθούν σε περίπτωση που κάποιος ανακαλύψει το κλειδί. Έτσι, λοιπόν, η ισχύς οποιουδήποτε συστήματος κρυπτογράφησης βασίζεται στην τεχνική διανομής των κλειδιών (key distribution), ένας όρος ο οποίος αναφέρεται στον τρόπο διανομής ενός κλειδιού μεταξύ δυο συμβαλλόμενων μερών που επιθυμούν να ανταλλάξουν δεδομένα, χωρίς να επιτρέπουν σε τρίτους να ανακαλύψουν το μυστικό αυτό κλειδί. Η διανομή κλειδιών μπορεί να πραγματοποιηθεί με διάφορους τρόπους.

Για δυο συμβαλλόμενα μέρη Α και Β:

- Ένα κλειδί θα μπορούσε να επιλεγεί από τον Α και να παραδοθεί στον Β με φυσικό τρόπο.
- Το κλειδί θα μπορούσε να επιλεγεί από έναν έμπιστο τρίτο ο οποίος θα παραδώσει το κλειδί στους Α και Β με φυσικό τρόπο.
- Αν ο Α και ο Β έχουν χρησιμοποιήσει πρόσφατα κάποιο κλειδί που παραμένει μυστικό, έχουν τη δυνατότητα ο μετάδοσης του καινούργιου κλειδιού ο ένας στον άλλο, κρυπτογραφώντας το νέο κλειδί με το παλαιό.
- Εάν οι Α και Β διατηρούν μια κρυπτογραφημένη σύνδεση με έναν τρίτο Γ, τότε ο τελευταίος θα ήταν σε θέση να διαβιβάσει ένα κλειδί μέσω της κρυπτογραφημένης σύνδεσης στους Α και Β.

Οι δυο πρώτοι τρόποι αναφέρονται στη λογική της μη αυτοματοποιημένης μετάδοσης ενός κλειδιού. Για την κρυπτογράφηση ζεύξης αποτελεί μια λογική απαίτηση, καθώς κάθε συσκευή κρυπτογράφησης ζεύξης θα ανταλλάξει δεδομένα μόνο με την άλλη πλευρά της ζεύξης. Για την κρυπτογράφηση, όμως, από άκρη σε άκρη η μη αυτοματοποιημένη διανομή δεν είναι επαρκής. Σε ένα κατανεμημένο σύστημα, ο οποιοσδήποτε σταθμός είναι δυνατόν ανά πάσα στιγμή να χρειαστεί να επικοινωνήσει με πολλούς άλλους σταθμούς, με αποτέλεσμα κάθε συσκευή να

χρειάζεται έναν αριθμό κλειδιών τα οποία θα μεταβιβάζονται άμεσα και δυναμικά. Το πρόβλημα είναι αρκετά δύσκολο σε ένα ευρέως κατανεμημένο σύστημα.

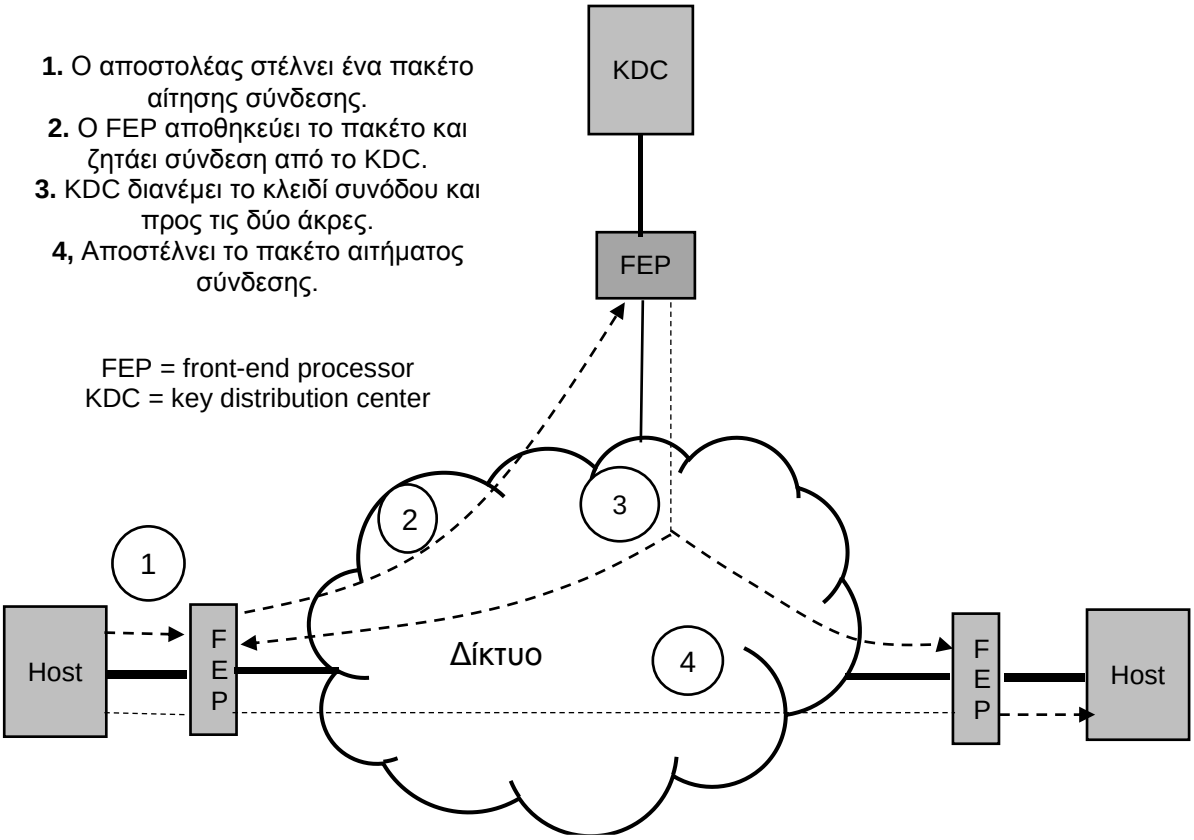
Ο τρίτος τρόπος είναι δυνατόν να λάβει χώρα είτε στην κρυπτογράφηση ζεύξης, είτε στην κρυπτογράφηση από-άκρη-σε-άκρη, αλλά αν ένας επιτιθέμενος κατορθώσει και αποκτήσει πρόσβαση σε ένα κλειδί τότε αποκαλύπτονται όλα τα επόμενα κλειδιά. Ακόμη και αν γίνονται συχνές αλλαγές στα κλειδιά κρυπτογράφησης ζεύξης, αυτές θα πρέπει να γίνουν μη αυτοματοποιημένα.

Ο τέταρτος τρόπος θεωρείται ο πιο κατάλληλος για τη διανομή κλειδιών στη κρυπτογράφηση από-άκρη-σε-άκρη. Στο παρακάτω σχήμα βλέπουμε μια σχετική εφαρμογή. Σε αυτό τη σχήμα αγνοείται η κρυπτογράφηση ζεύξης, καθώς μπορεί να προστεθεί ή να παραληφθεί ανάλογα με τις απαιτήσεις. Για τη λειτουργία του σχήματος 5.1, προσδιορίζονται δύο είδη κλειδιών:

- **Κλειδί συνόδου (session key):** Όταν δύο συστήματα όπως για παράδειγμα σταθμοί, τερματικά κλπ. θέλουν να επικοινωνήσουν από-άκρη-σε-άκρη καθιερώνουν μια λογική σύνδεση. Καθ' όλη τη διάρκεια της λογικής αυτής σύνδεσης, όλα τα δεδομένα των χρηστών κρυπτογραφούνται με ένα κλειδί συνόδου μιας χρήσης όπου στο τέλος της σύνδεσης το κλειδί αυτό καταστρέφεται.
- **Μόνιμο κλειδί (permanent key):** Μόνιμο κλειδί ονομάζεται το κλειδί εκείνο που χρησιμοποιείται μεταξύ δυο οντοτήτων με σκοπό την ασφαλή μετάδοση κλειδιών συνόδου.

Η διαμόρφωση (configuration) αποτελείται από τα ακόλουθα στοιχεία:

- **Κέντρο διανομής κλειδιού (key distribution center – KDC):** Το κέντρο διανομής κλειδιών KDC προσδιορίζει τα συστήματα που επιτρέπεται να επικοινωνήσουν μεταξύ τους. Όταν δοθεί η άδεια εγκατάστασης σύνδεσης σε δυο συστήματα, το KDC παρέχει ένα κλειδί συνόδου μιας χρήσης για την πραγματοποίηση της συγκεκριμένης επικοινωνίας.
- **Μετωπικός Επεξεργαστής (front-end processor – FEP):** Ένας μετωπικός επεξεργαστής πραγματοποιεί την κρυπτογράφηση από-άκρη-σε-άκρη και λαμβάνει τα κλειδιά συνόδου για λογαριασμό του σταθμού.



Σχήμα 5.1: *Αυτόματη διανομή κλειδιών σε πρωτόκολλο προσανατολισμένο στη σύνδεση*

Η εγκαθίδρυση μιας σύνδεσης περιλαμβάνει τα ακόλουθα βήματα:

Βήμα 1. Όταν ένας σταθμός επιθυμεί να εγκαταστήσει μια σύνδεση με έναν άλλον σταθμό, αποστέλλει ένα πακέτο αίτησης σύνδεσης (connection-request packet).

Βήμα 2. Το πακέτο αποθηκεύεται στον FEP ο οποίος αποστέλλει και μια αίτηση στο KDC για τη δημιουργία σύνδεσης

Βήμα 3. Η επικοινωνία μεταξύ των FEP και KDC κρυπτογραφείται εφαρμόζοντας ένα κύριο κλειδί το οποίο είναι γνωστό μόνο στους FEP και KDC. Εάν ο τελευταίος κάνει δεκτό το αίτημα σύνδεσης, δημιουργεί το κλειδί συνόδου και το μεταδίδει στους δυο κατάλληλους FEP εφαρμόζοντας ένα μοναδικό μόνιμο κλειδί για κάθε FEP.

Βήμα 4. Ο FEP που στέλνει το αίτημα σύνδεσης, μπορεί να αποστείλει το πακέτο αιτήματος σύνδεσης και να δημιουργήσει μια σύνδεση ανάμεσα των δύο συστημάτων. Τα δεδομένα του χρήστη, τα οποία μεταδίδονται

μεταξύ των συστημάτων, κρυπτογραφούνται από τους αντίστοιχους FEP χρησιμοποιώντας το κλειδί συνόδου μιας χρήσης.

Η αυτοματοποιημένη διανομή κλειδιών προσφέρει ιδιαίτερη ευελιξία και όλα τα δυναμικά χαρακτηριστικά που είναι απαραίτητα προκειμένου ένας αριθμός χρηστών να μπορούν να προσπελάσουν διαφόρους σταθμούς εργασίας, ενώ ταυτόχρονα δίνει τη δυνατότητα στους σταθμούς εργασίας να ανταλλάξουν δεδομένα μεταξύ τους.

Εναλλακτική προσέγγιση για τη διανομή κλειδιών μπορεί να πραγματοποιηθεί αξιοποιώντας τις δυνατότητες της ασύμμετρης κρυπτογράφησης και την υιοθέτηση ψηφιακών φακέλων (digital envelopes).

5.2. Διαχείριση Δημοσίων Κλειδιών

Ένα από τα πιο σημαντικά προβλήματα που παρατηρείται στα ασύμμετρα κρυπτοσυστήματα είναι η διανομή των δημοσίων κλειδιών. Στη διανομή των κλειδιών, υπάρχουν δύο περιπτώσεις οι οποίες παρουσιάζουν ιδιαίτερο ενδιαφέρον:

i. Η διανομή δημοσίων κλειδιών

ii. Η χρήση του ασύμμετρου κρυπτογραφικού συστήματος για τη διανομή των μυστικών κλειδιών, δηλαδή των κλειδιών που χρησιμοποιούνται στα συμμετρικά κρυπτοσυστήματα.

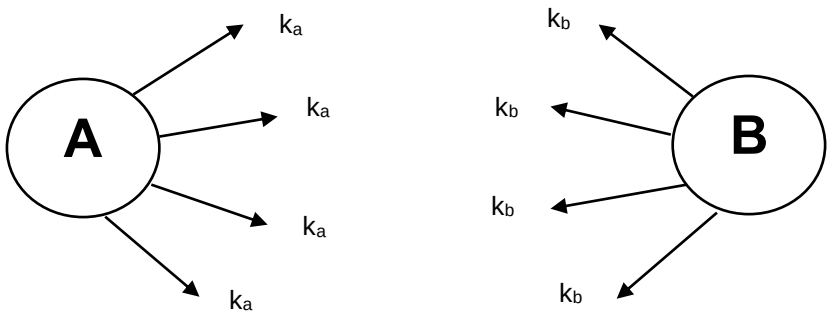
5.2.1. Διανομή Δημοσίων Κλειδιών

Η διανομή δημοσίων κλειδιών (Distribution of Public Keys) μπορεί να πραγματοποιηθεί με έναν από τους παρακάτω τρόπους:

- Δημόσια ανακοίνωση (public announcement)
- Δημόσια διαθέσιμος κατάλογος (publicly available directory)
- Αρχή δημοσίου κλειδιού (public-key authority)
- Πιστοποιητικά δημοσίου κλειδιού (public-key certificates)

a. Δημόσια Ανακοίνωση (public announcement)

- Οι χρήστες διανέμουν τα δημόσια κλειδιά στους αποδέκτες με τους οποίους επιθυμούν να επικοινωνήσουν ή τα εκπέμπουν
- Κύριο μειονέκτημα η πλαστογραφία
  - Κάθε χρήστης έχει τη δυνατότητα δημιουργίας κλειδιού, το οποίο μπορεί να το εκπέμψει ισχυριζόμενος ότι είναι κάποιος άλλος.
  - Επομένως, μπορεί να προσποιείται κάποιον άλλον έως ότου ανακαλυφθεί η πλαστογραφία



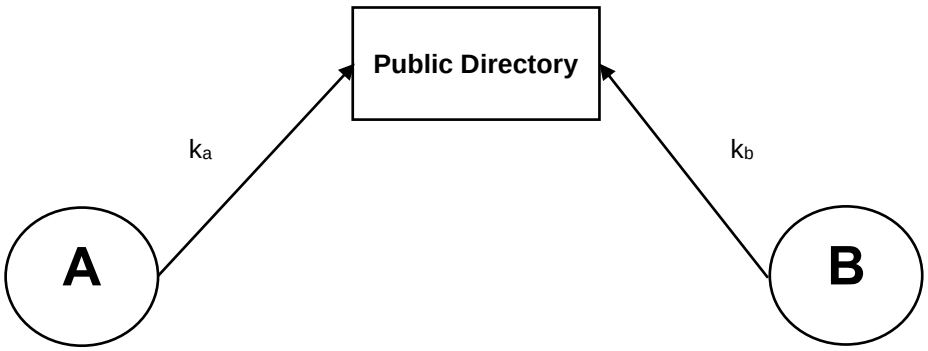
Σχήμα 5.2: *Δημόσια Ανακοίνωση*

b. Δημόσια διαθέσιμος κατάλογος (publicly available directory)

- Προϋποθέτει την ύπαρξη ενός αξιόπιστου κέντρου το οποίο θα είναι υπεύθυνο για τη συντήρηση και διανομή των δημοσίων κλειδιών
- Επίτευξη μεγαλύτερης ασφάλειας, εγγράφοντας τα κλειδιά σε έναν κατάλογο
- Ο κατάλογος μπορεί να θεωρηθεί αξιόπιστος εφόσον πληρεί τις παρακάτω ιδιότητες:
  - Περιέχει εγγραφές της μορφής {όνομα, δημόσιο κλειδί}
  - Οι συμμετέχοντες γράφουν με ασφάλεια στον κατάλογο.

- Οι συμμετέχοντες έχουν τη δυνατότητα αντικατάστασης του κλειδιού τους οποιαδήποτε στιγμή.
- Ο κατάλογος δημοσιεύεται περιοδικά.
- Ο κατάλογος μπορεί να προσπελαστεί ηλεκτρονικά

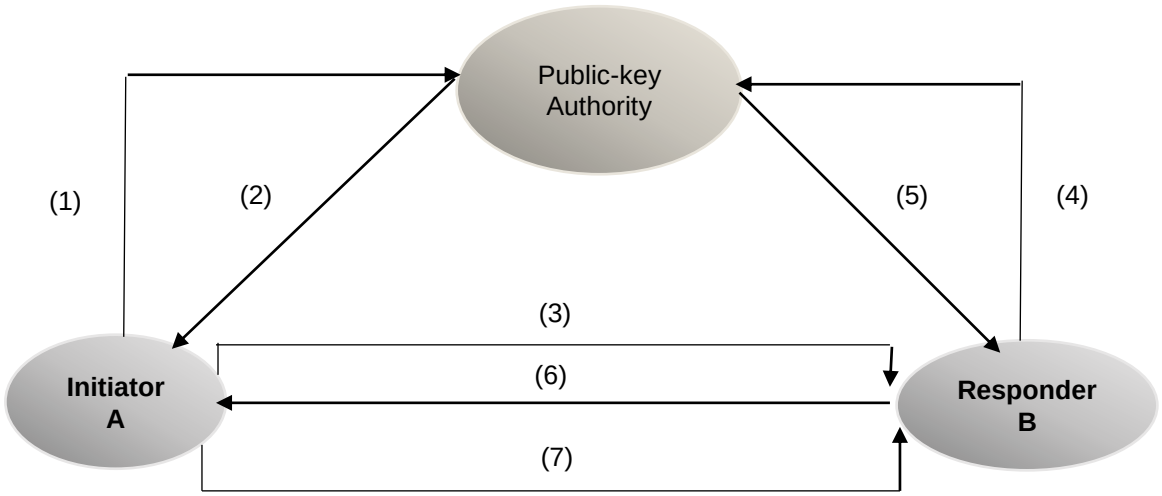
- Ο κίνδυνος της πλαστογραφίας παραμένει
  - Σε περίπτωση που κάποιος αντίπαλος, με κάποιο τρόπο, αποκτήσει ή υπολογίσει το μυστικό κλειδί του Δημόσιου Καταλόγου, μπορεί να προσποιηθεί οποιονδήποτε χρήστη που είναι εγγεγραμμένος στον Κατάλογο.



Σχήμα 5.3: *Δημόσιος Διαθέσιμος Κατάλογος*

c. Αρχή δημοσίου κλειδιού (public-key authority)

- Πραγματοποιείται αυστηρότερος έλεγχος στη διανομή κλειδιών, βελτιώνοντας έτσι την ασφάλεια.
- Διαθέτει ιδιότητες του καταλόγου
- Οι χρήστες είναι απαραίτητο να γνωρίζουν το δημόσιο κλειδί του καταλόγου.
- Τότε οι χρήστες επικοινωνούν με τον κατάλογο και λαμβάνουν γνώση οποιουδήποτε δημοσίου κλειδιού επιθυμούν με ασφάλεια
  - Επιβάλλεται πρόσβαση σε **πραγματικό χρόνο** στον κατάλογο όταν χρειάζονται τα κλειδιά



Όπου:

(1) Request [T_1]

(2) E_{KRauth} [K_B, Request \ T_1]

(3) E_{kb} [ID_A, N_1]

(4) Request [T_2]

(5) E_{KRauth} [K_A, Request \ T_2]

(6) E_{ka} [N_1, N_2]

(7) E_{kb} [N_2]

και **KRauth** είναι το μυστικό κλειδί της Αρχής Έκδοσης (Authority's Private Key)

Σχήμα 5.4: *Αρχή Δημοσίου Κλειδιού*

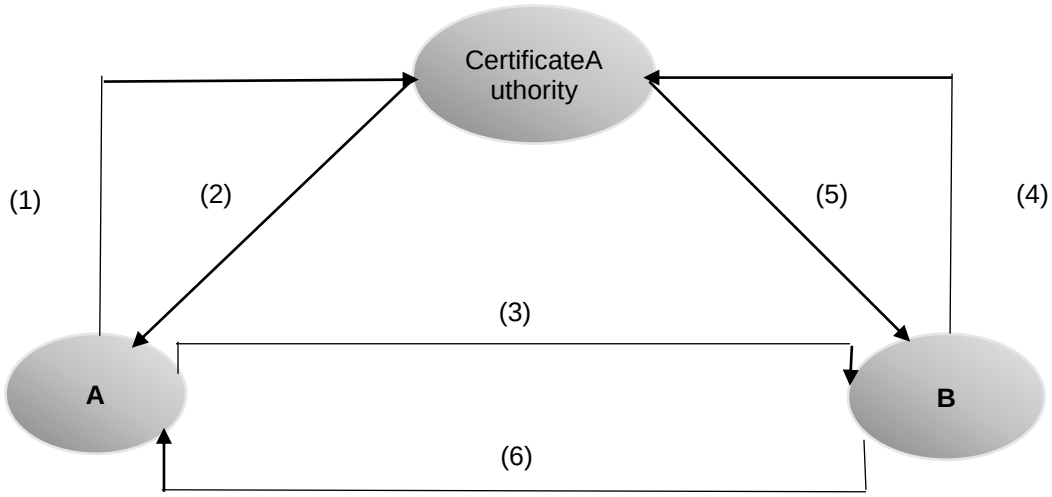
Ύστερα από τα βήματα **(1) – (5)** οι Α και Β μπορούν πλέον να επικοινωνήσουν με ασφάλεια. Με τα βήματα **(6)** και **(7)** ο Β βεβαιώνει τον Α ότι είναι αυτός με τον οποίο επιθυμεί να επικοινωνήσει καθώς και το αντίστροφο.

d. Πιστοποιητικά δημοσίου κλειδιού (public-key certificates)

- Τα πιστοποιητικά επιτρέπουν την ανταλλαγή κλειδιού χωρίς real-time πρόσβαση όπως στην Αρχή Δημοσίου Κλειδιού
- Ένα πιστοποιητικό συνδέει την οντότητα με το δημόσιο κλειδί
  - Συνήθως το δημόσιο κλειδί συνοδεύεται και από άλλη πληροφορία όπως για παράδειγμα η περίοδος εγκυρότητας, τα δικαιώματα χρήσης, κλπ.

- Το περιεχόμενο υπογράφεται από την έμπιστη Αρχή Δημοσίου Κλειδιού ή Αρχή Πιστοποιητικών ή Αρχή Πιστοποίησης (Certificate Authority, CA)

$$CA = E_{KRauth}[T, ID_a, K_a]$$



Όπου:

(1) K_a Δημόσιο κλειδί

(2) $C_A = E_{KRauth}[T_1 \setminus ID_A, K_a]$

(3) C_A Πιστοποιητικό

(4) K_b Δημόσιο κλειδί

(5) $C_B = E_{KRauth}[T_2 \setminus ID_B, K_b]$

(6) C_B Πιστοποιητικό

και **KRauth** είναι το μυστικό κλειδί της Αρχής Έκδοσης (Authority's Private Key)

Σχήμα 5.5: *Πιστοποιητικά δημοσίου κλειδιού*

5.2.2. Διανομή Συμμετρικού Κλειδιού με χρήση Δημοσίου Κλειδιού

Όπως αναφέρθηκε σε προηγούμενες παραγράφους, για την επίτευξη της επικοινωνίας μεταξύ δύο χρηστών σε ένα συμμετρικό κρυπτογραφικό σύστημα είναι απαραίτητο και οι δύο χρήστες να γνωρίζουν το μυστικό κλειδί. Έστω, για παράδειγμα, ότι ο Β επιθυμεί να κατασκευάσει μια εφαρμογή η οποία θα του επιτρέπει να ανταλλάσει μηνύματα με τον Α χρησιμοποιώντας την υπηρεσία του ηλεκτρονικού ταχυδρομείου, εφαρμόζοντας συμμετρικό κρυπτοσύστημα. Πρέπει να βρεθεί ένας τρόπος προκειμένου ο Β να αποστείλει το μυστικό κλειδί στον Α.

Ένας από τους πιο διαδεδομένους τρόπους είναι η αξιοποίηση ψηφιακού φακέλου (digital envelope), δηλαδή ο Β να χρησιμοποιήσει ασύμμετρο κρυπτοσύστημα για να αποστείλει το μυστικό κλειδί. Έτσι, είναι φανερό ότι η χρήση των πιστοποιητικών και η λειτουργία **PKI - Public Key Infrastructure** (Υποδομή δημόσιου κλειδιού) είναι απαραίτητη, προκειμένου να εξασφαλιστεί η αυθεντικότητα του αποστολέα Α και η ακεραιότητα του μηνύματος. Τα γενικά βήματα που πρέπει να ακολουθηθούν σε μια τέτοια περίπτωση είναι τα εξής:

Ο Β ετοιμάζει το προς αποστολή μήνυμα

1. Ο Β κρυπτογραφεί το μήνυμα με συμβατικό (συμμετρικό)κρυπτοσύστημα, χρησιμοποιώντας ένα μυστικό κλειδί που δημιούργησε ο ίδιος
2. Ο Β κρυπτογραφεί το μυστικό κλειδί με το δημόσιο κλειδί του Α.
3. Ο Β επισυνάπτει το κρυπτογραφημένο κλειδί στο μήνυμα και το αποστέλλει στον Α.

Ο Α είναι ο μόνος που μπορεί να αποκρυπτογραφήσει το μήνυμα και να διαβάσει το αρχικό κείμενο. Αν ο Β έχει ανακτήσει το δημόσιο κλειδί του Α μέσω πιστοποιητικού από κάποια Έμπιστη Τρίτη Οντότητα, τότε ο Β είναι βέβαιος ότι το μυστικό κλειδί είναι ορθό.

a. Απλή διανομή Μυστικού Κλειδιού (Simple Secret Key Distribution)

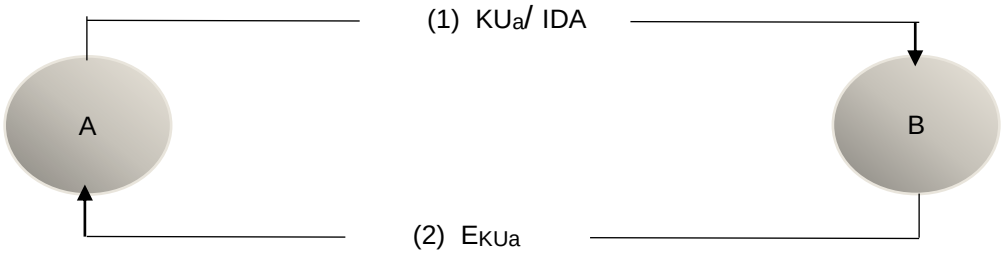
Αν κάποιος χρήστης Α θέλει να επικοινωνήσει με έναν χρήστη Β ακολουθεί τη παρακάτω διαδικασία:

I. Ο Α κατασκευάζει τα κλειδιά (KU_a, KR_a) και αποστέλλει στο Β το μήνυμα (K_{ua} [IDA]…).

II. Ο Β κατασκευάζει ένα Μυστικό Κλειδί Ks και το στέλνει στον Α αφού πρώτα το έχει κρυπτογραφήσει με το Δημόσιο Κλειδί KU_a.

III. Ο Α υπολογίζει το D_{KRa} [E_{KUa} (Ks)]

IV. Ο Α διαγράφει τα KU_a, KRa και ο Β διαγράφει το KU_a.

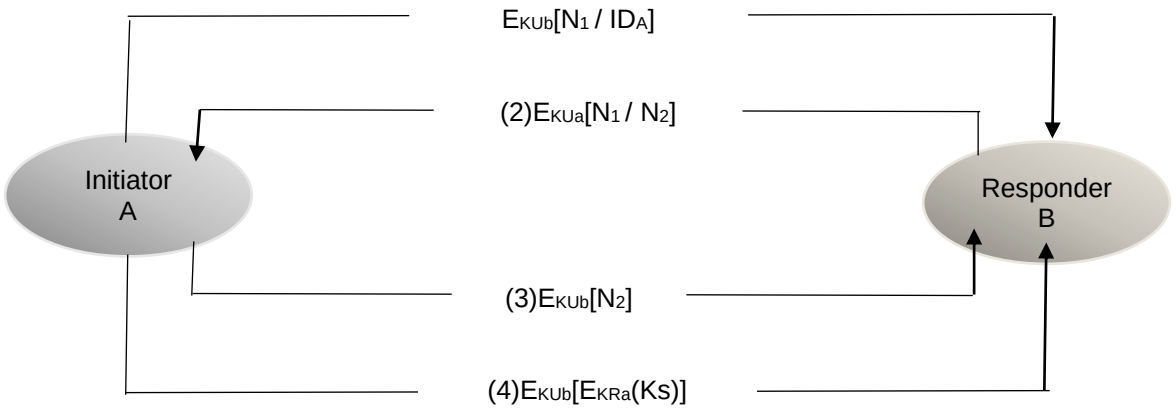


Σχήμα 5.6: *Απλή διανομή Μυστικού Κλειδιού*

Στη συνέχεια οι A και B μπορούν να επικοινωνήσουν με ασφάλεια ως προς τους παθητικούς ωτακουστές – passive attack – χρησιμοποιώντας το κλειδί Ks και συμβατική κρυπτογράφηση (π.χ. DES).

b. Διανομή Μυστικού Κλειδιού με Εμπιστευτικότητα και Πιστοποίηση Αυθεντικότητας

Οι Needham και Schoeder πρότειναν ένα σύστημα που παρέχει προστασία από ενεργούς και παθητικούς παρεμβολείς. Αρχικά, είναι απαραίτητη η διανομή δημοσίων κλειδιών μεταξύ των A και B με ένα από τα σχήματα που έχουν περιγραφεί. Στη συνέχεια ακολουθείται η εξής διαδικασία:



KU – Δημόσιο κλειδί
KR – Μυστικό κλειδί

Σχήμα 5.7: *Διανομή Μυστικού Κλειδιού με Εμπιστευτικότητα και Πιστοποίηση Αυθεντικότητας*

5.2. Ανταλλαγή κλειδιών κατά Diffie – Hellman

Ο πρώτος αλγόριθμος για ασύμμετρο κρυπτογραφικό σύστημα δημοσιεύτηκε στην εργασία των Diffie – Hellman που όριζε την κρυπτογραφία με ασύμμετρο κρυπτογραφικό σύστημα και είναι γνωστός ως ανταλλαγή κλειδιών κατά Diffie – Hellman (Diffie – Hellman key exchange).

Στόχος του αλγορίθμου είναι η εφικτή και ασφαλή ανταλλαγή, μεταξύ δυο χρηστών, ενός μυστικού κλειδιού, το οποίο στη συνέχεια θα χρησιμοποιηθεί για κρυπτογράφηση μηνυμάτων. Ο αλγόριθμος περιορίζεται ακριβώς στην ανταλλαγή κλειδιών.

Η αποτελεσματικότητα του αλγορίθμου στηρίζεται στη δυσκολία που εμφανίζεται κατά τον υπολογισμό διακριτών λογαρίθμων. Εν συντομία, ο διακριτός λογάριθμος ορίζεται ως εξής: Στην αρχή προσδιορίζεται μια πρωτογενής (primitive) ρίζα ενός πρώτου αριθμού p, τέτοιου ώστε οι δυνάμεις του να παράγουν όλους τους ακέραιους από το 0 ως το p-1. Έτσι ,λοιπόν, εάν a είναι μια ρίζα του πρώτου αριθμού p, τότε οι αριθμοί: $a \bmod p$, $a^2 \bmod p$, …, $a^{p-1} \bmod p$ αποτελούν τους ακέραιους από 1 ως το p-1 με κάποια μετάθεση.

Για οποιοδήποτε ακέραιο b και για μια πρωτογενή ρίζα a ενός πρώτου αριθμού p, μπορεί να βρεθεί ένας μοναδικός πρώτος αριθμός i, τέτοιος ώστε $b = a^i \bmod p$ όπου $0 \leq i \leq (p-1)$.

Ο εκθέτης *i* ονομάζεται ***διακριτός λογάριθμος*** ή ***δείκτης*** (index) του b για βάση a, mod p και συμβολίζεται $i = ind_{a,p}(b)$.

Έτσι, σύμφωνα με τα παραπάνω μπορεί να οριστεί η ανταλλαγή κλειδιών κατά Diffie – Hellman. Για την τεχνική αυτή είναι απαραίτητη η ύπαρξη δύο δημοσίως γνωστών αριθμών. Ένας πρώτος αριθμός q και ένας ακέραιος αριθμός a που αποτελεί την πρωτογενής ρίζα του q.

Καθολικά δημόσια στοιχεία	
q	πρώτος αριθμός
a	a < q και α μια πρώτη ρίζα του q
Παραγωγή κλειδιού για το χρήστη Α	
Επίλεξε ιδιωτικό κλειδί X_A	$X_A < q$
Υπολόγισε δημόσιο Y_A	$Y_A = a^{X_A} \bmod q$
Παραγωγή κλειδιού για το χρήστη Β	
Επίλεξε ιδιωτικό κλειδί X_B	$X_B < q$
Υπολόγισε δημόσιο Y_B	$Y_B = a^{X_B} \bmod q$
Παραγωγή μυστικού κλειδιού από το χρήστη Α	
$K = (Y_B)^{X_A} \bmod q$	
Παραγωγή μυστικού κλειδιού από το χρήστη Β	
$K = (Y_A)^{X_B} \bmod q$	

Πίνακας 5.1: *Ανταλλαγή κλειδιών κατά Diffie-Hellman*

Έστω ότι δυο χρήστες Α και Β θέλουν να ανταλλάξουν ένα κλειδί. Ο Α διαλέγει τυχαία έναν ακέραιο αριθμό X_A με $X_A < q$ και υπολογίζει το $Y_A = a^{X_A} \bmod q$. Παρομοίως, ο Β διαλέγει ανεξάρτητα από τον Α, τυχαία έναν ακέραιο αριθμό X_B με $X_B < q$ και υπολογίζει το $Y_B = a^{X_B} \bmod q$. Ο κάθε χρήστης διατηρεί μυστική την αντίστοιχη τιμή του Χ, δηλαδή X_A και X_B, και γνωστοποιεί την αντίστοιχη τιμή του Υ

στην άλλη πλευρά. Ο χρήστης Α υπολογίζει το κλειδί σύμφωνα με τη σχέση $K=(Y_B)^{XA} \bmod q$, όπως επίσης και ο Β σύμφωνα με τη σχέση $K=(Y_A)^{XB} \bmod q$. Όπως αποδεικνύεται παρακάτω, αυτές οι δύο σχέσεις παράγουν το ίδιο αποτέλεσμα:

$$\begin{aligned}
\mathbf{K} &= (Y_B) \bmod q = {}^{XA} \\
&= (a^{XB} \bmod q)^{XA} \bmod q = \\
&= (a^{XB})^{XA} \bmod q = \\
&= a^{XBXA} \bmod q = \\
&= (a^{XA})^{XB} \bmod q = \\
&= (a^{XA} \bmod q)^{XB} \bmod q = \\
&= (Y_A)^{XB} \bmod q \qquad \textbf{(5.1)}
\end{aligned}$$

Με αυτή τη διαδικασία πραγματοποιείται η ανταλλαγή ενός μυστικού κλειδιού και στις δυο πλευρές. Με τη προϋπόθεση ότι τα X_A και X_B παραμένουν μυστικά, ένας επιτιθέμενος έχει μόνο τα ακόλουθα στοιχεία στη διάθεσή του για να αποπειραθεί να κρυπταναλύσει τον αλγόριθμο: q, a, Y_A, Y_B. Επομένως, θα πρέπει να υπολογίσει ένα διακριτό λογάριθμο προκειμένου να υπολογίσει το κλειδί.

Η ασφάλεια της ανταλλαγής κλειδιού κατά Diffie – Hellman βασίζεται στο ότι ενώ θεωρείται υπολογιστικά εύκολο να υπολογιστεί η ποσότητα δύναμη mod πρώτου αριθμού, είναι πολύ δύσκολο να υπολογιστούν οι διακριτοί λογάριθμοι. Και για μεγάλους πρώτους αριθμούς το πρόβλημα θεωρείται ανέφικτο να επιλυθεί.

Ένα τυπικό αριθμητικό παράδειγμα περιλαμβάνει τα ακόλουθα βήματα: Η ανταλλαγή κλειδιών στηρίζεται στη χρήση του πρώτου αριθμού q = 71 και μιας πρωτογενούς ρίζας του 71, έστω την a = 7. Οι χρήστες Α και Β διαλέγουν τυχαία ως ιδιωτικά κλειδιά τα X_A = 5 και X_B = 12 αντίστοιχα. Τα δημόσια κλειδιά υπολογίζονται χωριστά από κάθε χρήστη ως εξής:

$$Y_A = 7^5 = 51 \bmod 71 \qquad \textbf{(5.2)}$$

$$Y_B = 7^{12} = 4 \bmod 71 \qquad \textbf{(5.3)}$$

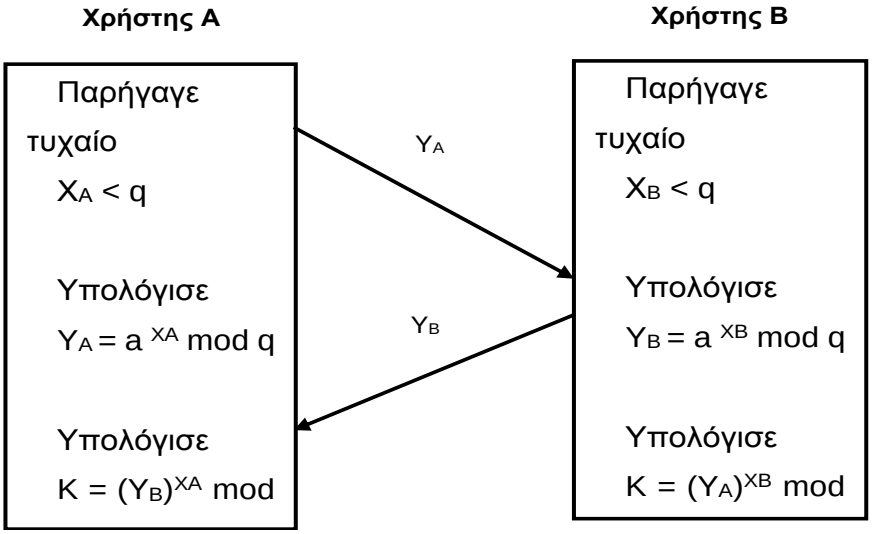
Εφόσον τα δημόσια κλειδιά έχουν υπολογιστεί, κάθε πλευρά μπορεί να υπολογίσει το κοινό μυστικό κλειδί ως ακολούθως:

$$K = (Y_B)^{XA} \bmod 71 = 4^5 = 30 \bmod 71 \qquad \textbf{(5.4)}$$

$$K = (Y_A)^{XB} \bmod 71 = 51^{12} = 30 \bmod 71 \qquad \textbf{(5.5)}$$

Από τη γνώση των {51, 4} ένας επιτιθέμενος δεν μπορεί εύκολα να υπολογίσει το κοινό μυστικό κλειδί 30.

Στο παρακάτω σχήμα παρουσιάζεται ένα απλό πρωτόκολλο που χρησιμοποιεί την τεχνική Diffie –Hellman. Υποθέτουμε ότι ο Α θέλει να εγκαταστήσει επικοινωνήσει με τον Β και χρησιμοποιεί ένα μυστικό κλειδί ώστε να κρυπτογραφεί τα μηνύματα σε αυτή τη σύνδεση. Ο Α μπορεί να παράγει ένα ιδιωτικό κλειδί X_A. Ύστερα υπολογίζει το Y_A και το αποστέλλει στον Β. Ο Β απαντά παράγοντας το μυστικό κλειδί X_B, υπολογίζοντας το Y_B και αποστέλλοντάς το στον Α. Και οι δύο πλευρές είναι πλέον σε θέση να υπολογίσουν το κοινό μυστικό κλειδί Κ. Τα απαραίτητα δημόσια στοιχεία q και a θα πρέπει να είναι γνωστά από την αρχή. Εναλλακτικά, ο Α θα μπορούσε να επιλέξει τιμές για τα q και a και να τα συμπεριλάβει στο πρώτο μήνυμα.



Σχήμα 5.8: *Παράδειγμα ανταλλαγής κλειδιών κατά Diffie - Hellman*

ΚΕΦΑΛΑΙΟ 6ο

6. ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ ΚΑΙ ΠΙΣΤΟΠΟΙΗΤΙΚΑ

6.1. Ψηφιακά Πιστοποιητικά

Η κρυπτογράφηση δημοσίου κλειδιού από μόνη της δε μπορεί να εξασφαλίσει την αυθεντικότητα του συντάκτη ενός κειμένου σε ένα ανοικτό δίκτυο όπως το Διαδίκτυο, καθώς οι πιθανότητες να πέσουμε θύματα παραπλάνησης ως προς το πραγματικό κλειδί του Α είναι μεγάλες. Με άλλα λόγια, αν κάποιος τρίτος θελήσει να μας παραπλανήσει μπορεί να το επιτύχει απλά δίνοντας μας το δικό του δημόσιο κλειδί ισχυριζόμενος ότι είναι του Β. Το μόνο που διασφαλίζει την αυθεντικότητα (authentication) των μερών που επικοινωνούν είναι το γεγονός ότι το δημόσιο και το ιδιωτικό κλειδί του αποστολέα είναι συμπληρωματικό ζευγάρι κλειδιών. Η διαδικασία αυτή της αντιστοίχησης και δέσμευσης ενός δημοσίου κλειδιού σε μια οντότητα, ονομάζεται **πιστοποίηση (certification).** Κατ' αναλογία, ονομάζονται **πιστοποιητικά δημόσιου κλειδιού (public key certificates)** ή απλά **πιστοποιητικά.**

Το πρόβλημα, λοιπόν, της πιστοποίησης της ιδιοκτησίας του δημόσιου κλειδιού από τον συγκεκριμένο ιδιοκτήτη αντιμετωπίζεται με τα ψηφιακά πιστοποιητικά που εκδίδει και υπογράφει ψηφιακά η Αρχή Πιστοποίησης **(Cerification Authority - CA).** Το ψηφιακό πιστοποιητικό είναι ένα ηλεκτρονικό έγγραφο που χρησιμοποιείται για τη ταυτοποίηση μιας οντότητας (φυσικό πρόσωπο, εξυπηρετητής, οργανισμός, κ.ο.κ.) και την ανάκτηση του δημόσιου κλειδιού της. Πιο συγκεκριμένα, τα ψηφιακά πιστοποιητικά αποτελούνται από μια ακολουθία χαρακτήρων στην οποία δηλώνονται τα εξής:

- Το όνομα του ιδιοκτήτη
- Το δημόσιο κλειδί του (public key)
- Άλλα πιθανά στοιχεία του ιδιοκτήτη όπως διεύθυνση, εταιρία, κ.λπ.
- Τα στοιχεία της Αρχής Πιστοποίησης που εξέδωσε το πιστοποιητικό
- Τον αυξάνοντα αριθμό (serial number) και το τύπο του πιστοποιητικού
- Την ημερομηνία έκδοσης (valid from) και ημερομηνία λήξης (valid to) του πιστοποιητικού
- Την ψηφιακή υπογραφή της αρχής πιστοποίησης που το εξέδωσε και τον αλγόριθμο που χρησιμοποιήθηκε (signature algorithm).

Το ψηφιακό πιστοποιητικό χρησιμοποιείται προκειμένου να επιβεβαιωθεί από τρίτους τόσο η ταυτότητα της αρχής πιστοποίησης, αφού είναι υπογεγραμμένο από αυτή, όσο και η ορθότητα της αντιστοίχησης του δημοσίου κλειδιού με τον ιδιοκτήτη του.

Σε αυτό το σημείο είναι απαραίτητο να επισημάνουμε ότι παρ' όλο που το ψηφιακό πιστοποιητικό εκδίδεται πάντα από κάποια γνωστή και έγκυρη αρχή πιστοποίησης (CA), η δημιουργία του ζεύγους των κλειδιών δεν πραγματοποιείται απαραίτητα από το CA. Υπάρχουν δύο τρόποι δημιουργίας ζευγών δημοσίων-ιδιωτικών κλειδιών

Ο πρώτος τρόπος είναι η έκδοση τους από την αρχή πιστοποίησης CA, η οποία παραδίδει στον ιδιοκτήτη το ζεύγος των κλειδιών και το πιστοποιητικό του δημοσίου κλειδιού

Ο δεύτερος τρόπος είναι το ζεύγος των κλειδιών να εκδίδεται από εξοπλισμό (Ηλεκτρονικό Υπολογιστή) του ίδιου του χρήστη ο οποίος στη συνέχεια αποστέλλει το δημόσιο κλειδί που κατασκεύασε στην πιστοποιούσα αρχή για να του χορηγηθεί το ψηφιακό πιστοποιητικό. Το πλεονέκτημα αυτής της μεθόδου έγκειται στο γεγονός ότι το ιδιωτικό κλειδί δημιουργείται, υπάρχει και παραμένει σε ένα και μοναδικό μέρος (ιδιοκτήτης) αλλά μειονεκτεί στο ότι ο χρήστης πρέπει να έχει στη διάθεσή του μηχανισμό έκδοσης και διαχείρισης των κλειδιών.

6.2. Αυθεντικοποίηση Μηνυμάτων

Στόχος της κρυπτογραφίας είναι η προστασία αφενός από παθητικές επιθέσεις (passive attacks) που στόχο έχουν την παραβίαση της εμπιστευτικότητας των μηνυμάτων (eavesdropping), αφετέρου από ενεργητικές επιθέσεις (active attacks) κατά τον μεταδιδόμενων δεδομένων και των δοσοληψιών (falsification of data and transactions). Η υπηρεσία ασφάλειας που παρέχει τη δυνατότητα προστασίας από τέτοιες κατηγορίες επιθέσεων, είναι γνωστή ως ***αυθεντικοποίηση μηνυμάτων (message authentication).***

Η αυθεντικοποίηση μηνυμάτων αποτελεί μια διαδικασία που καθιστά τους επικοινωνούντες ικανούς να προστατέψουν τόσο την ακεραιότητα (integrity), δηλαδή τη μη τροποποίηση των δεδομένων του μηνύματος, όσο και την αυθεντικότητα (authenticity) της πηγής μετάδοσης. Στη περίπτωση που το μήνυμα περιέχει και χρονοσήμανση (timestamp) διασφαλίζεται το γεγονός ότι το μήνυμα

δεν έχει καθυστερήσει πέραν ενός “φυσιολογικού” χρονικού ορίου και ότι δεν αποτελεί αναμετάδοση παλαιότερου μηνύματος.

- Αυθεντικοποίηση χρησιμοποιώντας Συμβατική Κρυπτογράφηση

Είναι εφικτή η πραγματοποίηση αυθεντικοποίησης απλά με χρήση συμβατικής κρυπτογραφίας. Εάν υποθέσουμε ότι οι μόνοι που μοιράζονται ένα μυστικό κλειδί είναι ο αποστολέας και ο παραλήπτης, τότε μόνο ο πραγματικός αποστολέας θα είναι σε θέση να κρυπτογραφήσει ένα μήνυμα με επιτυχία. Επιπλέον, εάν το μήνυμα περικλείει και κώδικα ανίχνευσης σφάλματος (error detection code) και αριθμό ακολουθίας (sequence number), τότε ο νόμιμα εξουσιοδοτημένος παραλήπτης διαβεβαιώνεται πως το μήνυμα δεν έχει υποστεί καμία παραβίαση της ακεραιότητας του και ότι η ακολουθία είναι η ορθή. Εάν το μήνυμα εμπεριέχει επιπλέον και χρονοσήμανση, ο παραλήπτης έχει τη δυνατότητα επιβεβαίωσης ότι το μήνυμα δεν έχει υποστεί καμία καθυστέρηση, πέραν της αναμενόμενης, που προβλέπεται κατά τη μετάδοση δεδομένων στο δίκτυο.

- Αυθεντικοποίηση μηνυμάτων χωρίς κρυπτογράφηση

Στη βιβλιογραφία αναφέρονται ορισμένες προσεγγίσεις αυθεντικοποίησης μηνυμάτων που δε στηρίζονται στην κρυπτογράφηση. Σε όλες αυτές τις περιπτώσεις, παράγεται μία ετικέτα αυθεντικοποίησης μηνύματος (authentication tag), η οποία ενσωματώνεται στο προς μετάδοση μήνυμα το οποίο δεν είναι κρυπτογραφημένο και μπορεί να είναι αναγνώσιμο ανεξάρτητα από τη μέθοδο αυθεντικοποίησης στον προορισμό.

Οι προσεγγίσεις που αναφέρουμε σε αυτή τη παράγραφο δεν περιλαμβάνουν κρυπτογράφηση του μηνύματος, επομένως γίνεται κατανοητό ότι η σχετική απαίτηση για εμπιστευτικότητα δεν ικανοποιείται.

Παρακάτω προτείνονται τρείς περιπτώσεις όπου η αυθεντικοποίηση μηνύματος χωρίς εμπιστευτικότητα είναι προτιμητέα:

- Σε ορισμένες εφαρμογές το ίδιο μήνυμα προωθείται σε πολλούς παραλήπτες (broadcast), όπως για παράδειγμα για ειδοποίηση

των χρηστών ενός δικτύου για επικείμενη μη διαθεσιμότητα ή για προώθηση ενός σήματος συναγερμού από ένα κέντρο ελέγχου. Προκειμένου, λοιπόν, να διασφαλιστεί η αυθεντικοποίηση του μηνύματος, τότε το μήνυμα προωθείται σε μη

κρυπτογραφημένη μορφή, αλλά συνοδεύεται από μία ετικέτα αυθεντικοποίησης μηνύματος αυθεντικοποίηση πραγματοποιείται από ένα συγκεκριμένο σύστημα που έχει δημιουργηθεί για αυτό το σκοπό. Εάν παρατηρηθεί κάποια παραβίαση, τα υπόλοιπα συστήματα προορισμού ενημερώνονται μέσω ενός συγκεκριμένου τύπου σήματος συναγερμού.

- Το πιο συνηθισμένο σενάριο είναι μια ανταλλαγή δεδομένων, κατά τη διάρκεια της οποίας η μια πλευρά έχει σημαντικό φόρτο να διαχειριστεί και δεν είναι σε θέση να ανταπεξέλθει στο μεγάλο χρόνο που χρειάζεται για την αποκρυπτογράφηση όλων των εισερχόμενων μηνυμάτων. Σε αυτή τη περίπτωση, η αυθεντικοποίηση πραγματοποιείται σε επιλεκτική βάση και τα μηνύματα για έλεγχο επιλέγονται τυχαία.
- Ενδιαφέρον παρουσιάζει η αυθεντικοποίηση ενός προϊόντος λογισμικού που βρίσκεται σε μη κρυπτογραφημένη μορφή. Το πρόγραμμα θα πρέπει να μπορεί να εκτελεστεί, χωρίς φυσικά να χρειάζεται αποκρυπτογράφηση κάθε φορά, γεγονός που θα οδηγούσε σε απώλεια υπολογιστικού χρόνου του συστήματος. Όμως, αν μια ετικέτα ενός μηνύματος αυθεντικοποίησης επισυνάπτεται στο μήνυμα, θα πρέπει να μπορεί να ελέγχεται όποτε απαιτείται διαβεβαίωση για την ακεραιότητα του προγράμματος.

6.3. Κώδικας αυθεντικοποίησης μηνυμάτων

Μια συχνά χρησιμοποιούμενη τεχνική αυθεντικοποίησης ονομάζεται ***Κώδικας Αυθεντικοποίησης Μηνυμάτων*** (Message Authentication Code – MAC). Στην τεχνική αυτή είναι απαραίτητη η χρήση ενός μυστικού κλειδιού, προκειμένου να παραχθεί ένα μικρό τμήμα δεδομένων που θα προσαρτηθεί στη συνέχεια στο μήνυμα. Για παράδειγμα, έστω ότι υπάρχουν δύο οντότητες Α και Β που θέλουν να επικοινωνήσουν και είναι γνώστες ενός μυστικού κλειδιού K_{AB}. Όταν ο Α θελήσει να στείλει ένα μήνυμα στον Β υπολογίζει το MAC ως συνάρτηση του μηνύματος και του μυστικού κλειδιού: $MAC_M = f(K_{AB}, M)$.

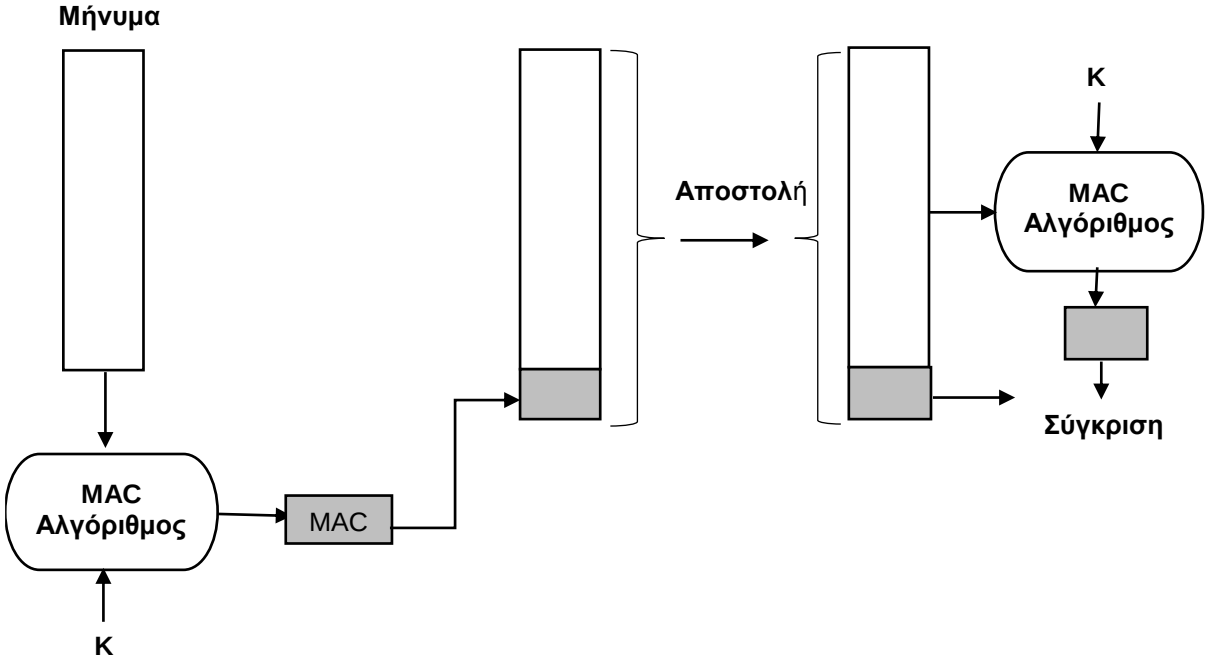
Το MAC προσαρτάται στο μήνυμα και αποστέλλεται στο Β, ο οποίος ακολουθώντας τον ίδιο υπολογισμό στο μήνυμα που έλαβε, χρησιμοποιώντας το

ίδιο μυστικό κλειδί, παράγει ένα νέο MAC. Όπως φαίνεται στο παρακάτω σχήμα, που παραλήφθηκε συγκρίνεται με αυτό που έχει υπολογιστεί στην πλευρά του παραλήπτη. Υποθέτοντας ότι το μυστικό κλειδί είναι γνωστό μόνο στον αποστολέα και τον παραλήπτη και ότι τα MAC είναι ίσα, τότε συνάγονται τα ακόλουθα:

- Ο παραλήπτης επιβεβαιώνει ότι το μήνυμα δεν υπέστη κάποια τροποποίηση κατά τη μετάδοση. Σε περίπτωση που το μήνυμα έχει υποστεί κάποια αλλοίωση από έναν επιτιθέμενο, τότε κατά τον υπολογισμό του MAC από τον παραλήπτη θα προκύψει διαφορά με το αντίστοιχο MAC του αποστολέα. Επειδή ο επιτιθέμενος δε γνωρίζει το μυστικό κλειδί, δεν μπορεί να αλλάξει το MAC ώστε να ανταποκρίνεται στις αλλαγές του μηνύματος.
- Ο παραλήπτης μπορεί να επιβεβαιώσει ότι το μήνυμα προέρχεται από τον συγκεκριμένο αποστολέα. Αυτή η διαβεβαίωση πηγάζει από το ότι κανείς, εκτός του αποστολέα και του νόμιμα εξουσιοδοτημένου παραλήπτη, δε γνωρίζει το μυστικό κλειδί, κατά συνέπεια κανένας άλλος δεν μπορεί να προετοιμάσει ένα μήνυμα με το κατάλληλο MAC.
- Εάν το μήνυμα περιλαμβάνει αριθμό ακολουθίας, όπως αυτοί που χρησιμοποιούνται στα πρωτόκολλα X.25, HDLC και TCP, τότε ο παραλήπτης είναι σε θέση να επιβεβαιώσει την ορθότητα της σωστής ακολουθίας, επειδή ο επιτιθέμενος δεν μπορεί να τροποποιήσει με επιτυχία έναν αριθμό ακολουθίας.

Στα σύγχρονα συστήματα, οι MAC παράγονται χρησιμοποιώντας αρκετούς αλγορίθμους. Το US National Bureau of Standards στο κείμενο με τίτλο DES Modes of Operation συστήνει τη χρήση του DEA για παραγωγή του MAC. Το DEA χρησιμοποιείται για τη παραγωγή κρυπτογραφημένης έκδοσης του μηνύματος και τα τελευταία 16 ή 32 bits του κρυπτογραφημένου κειμένου χρησιμοποιούνται ως MAC.

Η διαδικασία που περιγράψαμε παραπάνω είναι αντίστοιχη με εκείνης της κρυπτογράφησης. Η βασική τους διαφορά τους έγκειται στο γεγονός ότι ένας αλγόριθμος αυθεντικοποίησης δεν πρέπει να είναι αντιστρέψιμος, ενώ αντίθετα η συνάρτηση κρυπτογράφησης θα πρέπει να μπορεί να αντιστραφεί στη πλευρά του παραλήπτη.



Σχήμα 6.1: *Αυθεντικοποίηση μηνύματος με χρήση MAC*

6.4. Ψηφιακές Υπογραφές

Μια άλλη επέκταση της χρήσης της κρυπτογράφησης με την τεχνική του δημόσιου και ιδιωτικού κλειδιού, είναι η ψηφιακή υπογραφή. Η χρήση του ιδιωτικού κλειδιού, το οποίο είναι μοναδικό και φυλάσσεται πολύ καλά από τον ιδιοκτήτη του για την κρυπτογράφηση ενός κειμένου, αποτελεί την προσωπική ψηφιακή του υπογραφή. Έστω ότι ο Β επιθυμεί να στείλει ένα μήνυμα στον Α. Στις καταγραφείσες απαιτήσεις δεν περιλαμβάνεται πλέον η εμπιστευτικότητα του κειμένου, αλλά ο παραλήπτης Α θέλει να είναι βέβαιος για τη πηγή του μηνύματος, με άλλα λόγια απαιτείται αυθεντικοποίηση του αποστολέα Β του μηνύματος. Έτσι, λοιπόν, ο Β κρυπτογραφεί με το ιδιωτικό του κλειδί το κείμενο, το οποίο μόλις το παραλάβει ο Α το αποκρυπτογραφεί με το δημόσιο κλειδί του Β, εξασφαλίζοντας με αυτό το τρόπο ότι το αρχικό κείμενο κρυπτογραφήθηκε από τον Β. Κανένας άλλος δεν έχει στη διάθεσή του και δεν γνωρίζει το ιδιωτικό κλειδί του Β με αποτέλεσμα, κανένας να μη μπορεί να δημιουργήσει κρυπτογράφημα που θα αποκρυπτογραφείται με το δημόσιο κλειδί του Β. Έτσι, όλο το κρυπτογραφημένο κείμενο αποτελεί μία ***ψηφιακή υπογραφή*** (digital signature). Επιπλέον, γίνεται άμεσα αντιληπτό ότι το μήνυμα δε μπορεί να τροποποιηθεί από κάποιον τρίτο χωρίς να γνωρίζει το ιδιωτικό

κλειδί του Β, επομένως εξασφαλίζεται η αυθεντικοποίηση του αποστολέα, αλλά και η ακεραιότητα των δεδομένων.

Σε αυτό το σημείο είναι συνετό να αναφέρουμε ότι ένα μεγάλο σε μήκος κείμενο απαιτεί πολύ χρόνο επεξεργασίας προκειμένου να κρυπτογραφηθεί και να αποκρυπτογραφηθεί με την τεχνική του ιδιωτικού και δημόσιου κλειδιού. Επίσης, σε αυτή τη περίπτωση παρουσιάζεται ένα πρόβλημα που σχετίζεται με το χώρο αποθήκευσης. Πιο συγκεκριμένα, κάθε μήνυμα είναι απαραίτητο να αποθηκεύεται σε μη κρυπτογραφημένη μορφή για πρακτικούς λόγους, καθώς και να φυλάσσεται ένα αντίγραφο του μηνύματος σε κρυπτογραφημένη μορφή έτσι ώστε, σε περίπτωση αμφισβήτησης και διαφωνίας, να είναι δυνατό να προσδιοριστούν η πηγή και τα περιεχόμενα του. Ένας άλλος τρόπος που θα επιφέρει τα ίδια αποτελέσματα ευκολότερα, θα ήταν να κρυπτογραφηθεί μικρό τμήμα από bits, το οποίο θα αποτελεί συνάρτηση του κειμένου. Αυτό το τμήμα ονομάζεται **αυθεντικοποιητής** (authenticator), και ένα μήνυμα δε θα μπορεί να αλλοιωθεί χωρίς να αλλάξει ο αυθεντικοποιητής. Αν ο αυθεντικοποιητής κρυπτογραφηθεί με το ιδιωτικό κλειδί του αποστολέα, τότε χαρακτηρίζεται ως ***ψηφιακή υπογραφή*** (digital signature).

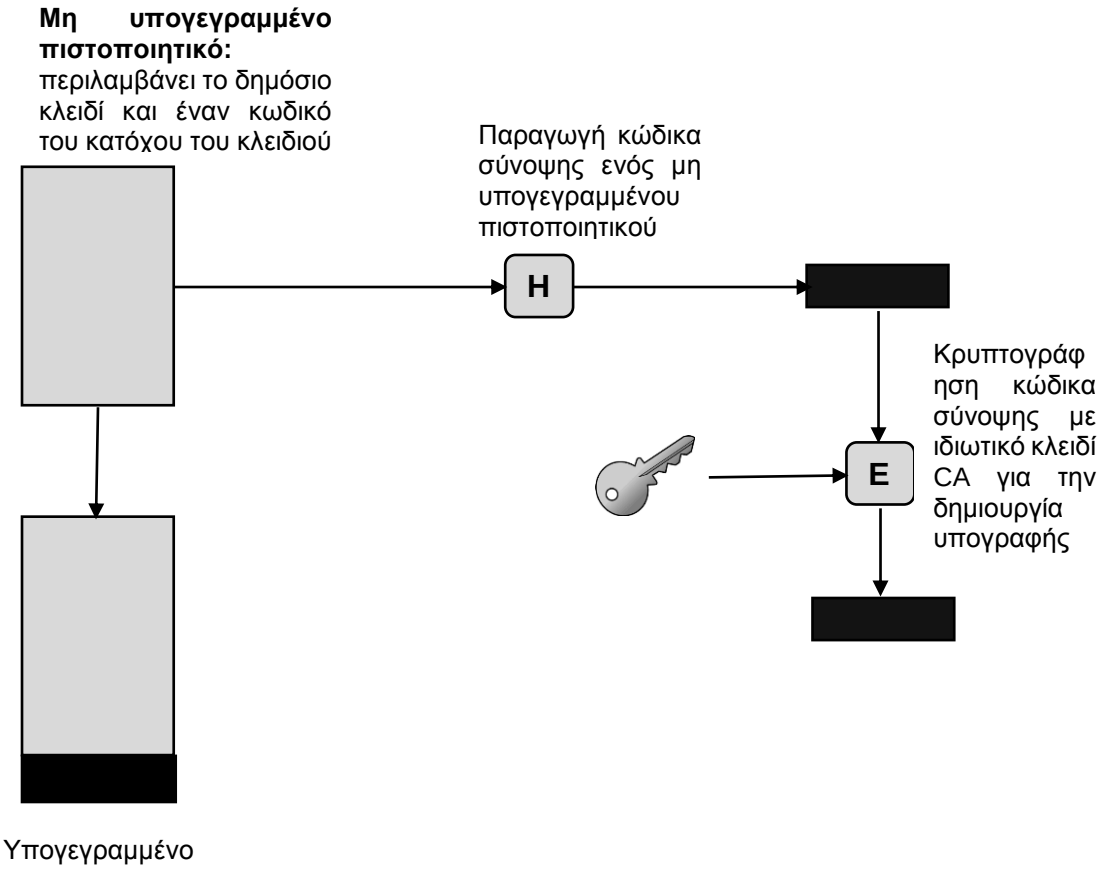
Πιο αναλυτικά, προκειμένου να αποφευχθούν τα προβλήματα που αναφέρθηκαν παραπάνω κατασκευάζεται, με τη βοήθεια της τεχνικής **hash** που περιγράφεται παρακάτω, μια ακολουθία bit μικρού μήκους η οποία είναι μοναδική και αντιπροσωπεύει το μεγάλο κείμενο και ονομάζεται **digest**. Η κρυπτογράφηση αυτής της ακολουθίας (κι όχι όλου του κειμένου) με το ιδιωτικό κλειδί χρησιμοποιείται ως ψηφιακή υπογραφή (digital signature).

Ο γνωστότερος τρόπος για τη δημιουργία του digest ενός κειμένου είναι η χρήση ειδικών αλγορίθμων που ονομάζονται μονοσήμαντες συναρτήσεις **hash** (one-way hash functions). Οι συναρτήσεις αυτές δεν κάνουν χρήση κλειδιών, παρά εφαρμόζονται σε ένα μεγάλου μήκους μήνυμα και παράγουν μονοσήμαντα, μια μικρότερη ακολουθία χαρακτήρων συγκεκριμένου μήκους (π.χ. 16 byte). Ουσιαστικά, αυτή η τεχνική επιβεβαιώνει ότι το μήνυμα δεν έχει υποστεί κάποια αλλοίωση, αφού η παραμικρή αλλαγή στο κείμενο συνεπάγεται με διαφορετικό digest.

Έτσι με την ψηφιακή υπογραφή εκπληρώνουμε δύο στόχους:

1) Την **πιστοποίηση** του υπογράφοντα, με τη χρήση του ιδιωτικού κλειδιού και
2) Την πιστοποίηση **μη αλλοίωσης** του μηνύματος, με τη χρήση του digest που το συνοδεύει.

Υποθέτουμε ότι ο Α θέλει να αποστείλει ένα μήνυμα στον Β. Πριν στείλει το μήνυμα δημιουργεί το digest του κειμένου εφαρμόζοντας μια συνάρτηση hash σε αυτό. Ύστερα κρυπτογραφεί το digest με το ιδιωτικό του κλειδί, δημιουργώντας με αυτό το τρόπο τη ψηφιακή υπογραφή που στη ουσία είναι το κρυπτογραφημένο digest. Εφόσον η ψηφιακή υπογραφή έχει ενσωματωθεί στο τέλος του κειμένου, αυτό αποστέλλεται στον παραλήπτη Β. Αρχικά, αφού ο Β έχει διαχωρίσει τη ψηφιακή υπογραφή από το μήνυμα, στη συνέχεια την αποκρυπτογραφεί με τη βοήθεια του δημοσίου κλειδιού του Α, αποκαλύπτοντας το digest που έχει αποσταλεί από τον Α. Ταυτόχρονα, εφαρμόζει την ίδια συνάρτηση hash πάνω στο κείμενο κατασκευάζοντας ένα νέο digest, το οποίο πρέπει να είναι ταυτόσημα με αυτό που αποκαλύφθηκε από την ψηφιακή υπογραφή. Σε περίπτωση που ένα από τα δύο digest είναι διαφορετικό, αυτό σημαίνει ότι το μήνυμα τροποποιήθηκε κατά τη μετάδοση ή ότι η υπογραφή του δεν είναι γνήσια.



Σχήμα 6.2: *Ψηφιακές υπογραφές*

Είναι απαραίτητο να επισημάνουμε 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.

6.4.1. Πρότυπο ψηφιακής υπογραφής DSS (Digital Signature Standard)

Ένας σημαντικός αλγόριθμος παραγωγής ψηφιακών υπογραφών, εκτός του RSA, αποτελεί ο **DSS**, που δημοσιεύτηκε από το Εθνικό Ινστιτούτο Προτυποποίησης και Τεχνολογίας (NIST) των Η.Π.Α. Πρώτη φορά δημοσιεύτηκε το 1991, ενώ αναθεωρήθηκε αργότερα το 1993. Το DSS χρησιμοποιεί τη συνάρτηση σύνοψης SHA-1 και εφαρμόζει μια καινούργια τεχνική ψηφιακών υπογραφών – τον αλγόριθμο δημοσίου κλειδιού **DSA** (Digital Signature Algorithm).

6.4.2. Αλγόριθμος ψηφιακής υπογραφής DSA (Digital Signature Algorithm)

Ο αλγόριθμος DSA αποτελεί έναν αλγόριθμο δημόσιου κλειδιού και αναπτύχθηκε από το γραφείο Εθνικής Ασφάλειας των Η.Π.Α (NSA) για την παραγωγή ψηφιακών υπογραφών. Το Εθνικό Ινστιτούτο Προτυποποίησης και Τεχνολογίας (NIST) δημοσίευσε τον αλγόριθμο στο Πρότυπο Ψηφιακής Υπογραφής (Digital Signature Standard – DSS) έτσι ώστε να αποτελέσει το πρότυπο ψηφιακής πιστοποίησης της αμερικανικής κυβέρνησης. Η προτυποποίηση του αλγορίθμου πραγματοποιήθηκε το Μάιο του 1994.

Ο DSA στηρίζεται στη δυσκολία που παρουσιάζει ο υπολογισμός των διακριτών λογαρίθμων. Συγκριτικά με τον RSA που μπορεί να εφαρμοστεί τόσο για κρυπτογράφηση όσο και για ψηφιακές υπογραφές, ο DSA μπορεί να χρησιμοποιηθεί μόνο για ψηφιακές υπογραφές.

Με τον DSA η παραγωγή υπογραφών πραγματοποιείται γρηγορότερα σε σχέση με την επαλήθευσή τους, γεγονός που για αρκετούς αποτελεί μεγάλο πλεονέκτημα. Αντιθέτως στον RSA, η επαλήθευση των υπογραφών πραγματοποιείται πιο γρήγορα σε σχέση με τη παραγωγή τους. Ωστόσο, ένα έγγραφο υπογράφεται μια φορά, αλλά χρειάζεται να επαληθευτεί πολλές φορές, γεγονός που παρέχει συγκριτικό πλεονέκτημα στον RSA.

ΚΕΦΑΛΑΙΟ 7ο

7. ΣΥΝΑΡΤΗΣΕΙΣ

7.1. Συναρτήσεις Κατακερματισμού

Ο όρος συναρτήσεις κατακερματισμού (hash functions) υποδηλώνει έναν μετασχηματισμό που λαμβάνει ως είσοδο ένα μήνυμα m ανεξαρτήτου μήκους και επιστρέφει στην έξοδο μια ακολουθία χαρακτήρων h περιορισμένου μήκους που ονομάζεται hash value, δηλαδή ισχύει $h = H(m)$. Οι συναρτήσεις κατακερματισμού είναι συναρτήσεις της μορφής $H(x) = y$, και διαθέτουν τις παρακάτω ιδιότητες:

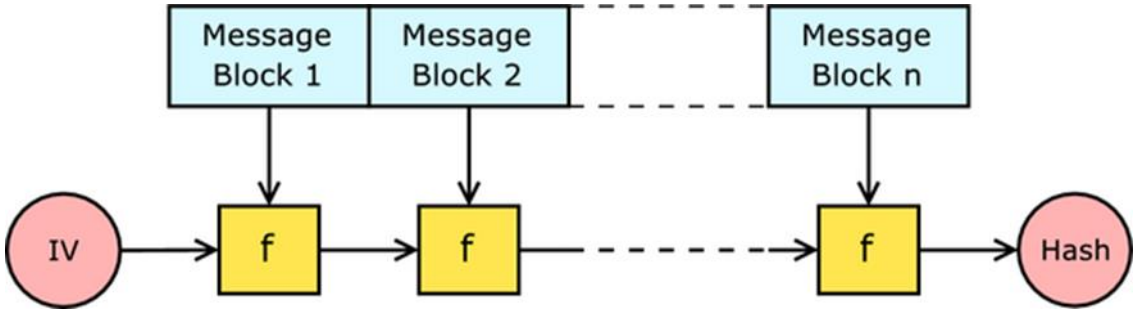
- Η είσοδος μπορεί να είναι οπουδήποτε μήκους,
- Η έξοδος έχει συγκεκριμένο μήκος,
- Δεδομένου του x, το y υπολογίζεται εύκολα,
- Η H(x) είναι μη αντιστρέψιμη,
- Η H(x) είναι αμφιμονοσήμαντη συνάρτηση.

Λέγοντας ότι μια συνάρτηση Η είναι μη αντιστρέψιμη εννοούμε πως δίνοντας μια τιμή κατακερματισμού h είναι υπολογιστικά αδύνατο να βρεθεί ένα μήνυμα τέτοιο ώστε H(x) = h. Μια συνάρτηση κατακερματισμού μπορεί να χαρακτηριστεί ως ″ισχυρώς ελευθέρα συγκρούσεων″ (strongly collision-free) αν δεν είναι δυνατό να βρεθούν δύο διαφορετικά μηνύματα x, y τέτοια ώστε να ισχύει H(x) = H(y).

Εξαιτίας του ότι οι συναρτήσεις κατακερματισμού είναι πιο γρήγορες συγκριτικά με τους αλγορίθμους κρυπτογράφησης και τις ψηφιακές υπογραφές, έχει καθιερωθεί η υπογραφή των μηνυμάτων να παράγεται εφαρμόζοντας κρυπτογραφικές διαδικασίες στο συγχωνευμένο μήνυμα, που είναι πιο μικρό και επομένως πιο εύκολο στη διαχείριση. Επιπλέον ένα συγχωνευμένο μήνυμα μπορεί να δημοσιευτεί χωρίς να αποκαλύπτει τα περιεχόμενα του αυθεντικού κειμένου. Η παραπάνω ιδιότητα παίζει ιδιαίτερο ρόλο στις ψηφιακές χρονοσφραγίδες, όπου χρησιμοποιώντας συναρτήσεις κατακερματισμού, μπορούν να αποδοθούν χρονοσφραγίδες σε έγγραφα χωρίς να αποκαλυφθεί το περιεχόμενο τους στην υπηρεσία έκδοσης χρονοσφραγίδων.

Εικόνα 7.1: *Κρυπτογράφηση μηνύματος με hash function*

Οι Damgard και Merkle επηρέασαν ιδιαίτερα το σχεδιασμό κρυπτογραφικών συναρτήσεων κατακερματισμού εισάγοντας την έννοια της ***συμπίεσης***. Μια συνάρτηση συμπίεσης λαμβάνει ως είσοδο ένα μήνυμα σταθερού μεγέθους και παράγει στην έξοδο ένα μήνυμα σταθερού μεγέθους αλλά μικρότερο. Σύμφωνα με τους Damgard και Merkle, έχοντας δώσει μια συνάρτηση συμπίεσης, μια συνάρτηση κατακερματισμού μπορεί να οριστεί μέσω επαναληπτικών εφαρμογών στης συνάρτησης συμπίεσης μέχρι να επεξεργαστεί ολόκληρο το κείμενο. Βάση αυτής της διαδικασίας, ένα μήνυμα αυθαιρέτου μεγέθους σπάει σε ομάδες, το μέγεθος των οποίων καθορίζεται από τις προδιαγραφές της συνάρτησης συμπίεσης που χρησιμοποιείται και συμπληρώνεται, προκειμένου το μέγεθος του μηνύματος να γίνει πολλαπλάσιο του μεγέθους ομάδας. Ύστερα, οι ομάδες επεξεργάζονται σειριακά η μια μετά την άλλη και παράγουν στην έξοδο την τιμή κατακερματισμού για το συγκεκριμένο μήνυμα.



Εικόνα 7.2: *Η επαναληπτική δομή Damgard / Merkle για συναρτήσεις κατακερματισμού. F είναι μια συνάρτηση συμπίεσης*

7.2. Γενικές Αρχές Ασφαλών Συναρτήσεων Σύνοψης

Όπως και στη περίπτωση των συμμετρικών κρυπτογραφικών συστημάτων, οι σχεδιαστές συναρτήσεων δεν ήταν πρόθυμοι να αποχωριστούν μια ικανοποιητική λύση. Το DES στηρίζεται στον αλγόριθμο του Feistel. Τα συμμετρικά κρυπτογραφικά συστήματα στην πλειοψηφία τους ακολούθησαν τον σχεδιασμό του Feistel διότι προσέφερε τη δυνατότητα προσαρμογής έτσι ώστε να αντιστέκονται σε νεοεμφανιζόμενες κρυπταναλυτικές απειλές. Αν οι σχεδιαστές αξιοποιούσαν μια καινούργια δομή για τα συμμετρικά κρυπτοσυστήματα, θα επικρατούσε μια συνεχής αναστάτωση καθώς η ίδια η δομή, ως μη καλά ελεγμένη, θα μπορούσε να προκαλέσει καινούργια ρήγματα για ανύπαρκτες μέχρι τότε κρυπταναλυτικές επιθέσεις.

Σε αυτή τη κατεύθυνση, οι σύγχρονες συναρτήσεις σύνοψης βασίζονται στην επαναληπτική συνάρτηση σύνοψης που προτάθηκε για πρώτη φορά από τον R. Merkle. Το κίνητρο για την αξιοποίηση της επαναληπτικής δομής βασίστηκε στις παρατηρήσεις των R. Merkle και I. Damgard ότι αν η συνάρτηση συμπίεσης είναι ανθεκτική στις συγκρούσεις (collision resistant), τότε και η επαναληπτική συνάρτηση σύνοψης (iterated hash function) είναι το ίδιο ανθεκτική. Άρα η δομή αυτή μπορεί να χρησιμοποιηθεί ώστε να παράγει μία ασφαλή συνάρτηση σύνοψης (secure hash function) που λειτουργεί για οποιοδήποτε μήνυμα, ανεξαρτήτως μήκους. Το πρόβλημα κατασκευής μιας ασφαλούς συνάρτησης σύνοψης ανάγεται σε πρόβλημα σχεδίασης μιας συνάρτησης συμπίεσης που θα είναι ανθεκτική σε συγκρούσεις και η οποία λειτουργεί με εισόδους καθορισμένου μεγέθους. Στις παρακάτω παραγράφους περιγράφονται δύο ακόμη συναρτήσεις σύνοψης, οι MD5 και RIPEMD-160, οι οποίες μαζί με την SHA-1 χαίρουν ευρείας εμπορικής αποδοχής.

	MD5	SHA-1	RIPEMD-160
Μήκος Σύνοψης	128 bits	160 bits	160 bits
Βασική μονάδα επεξεργασίας	512 bits	512 bits	512 bits
Αριθμός βημάτων	64 (4 rounds of 16)	80 (4 rounds of 20)	160 (5 paired rounds of 16)
Μέγιστο μέγεθος μηνύματος	a	$2^{64} – 1$ bits	a
Αρχική τυπική συνάρτηση	4	4	5
Επιπλέον χρησιμοποιούμενες σταθερές	64	4	9

Πίνακας 7.1: *Συγκριτική παρουσίαση των αλγορίθμων σύνοψης MD5, SHA-1, RIPEMD-160*

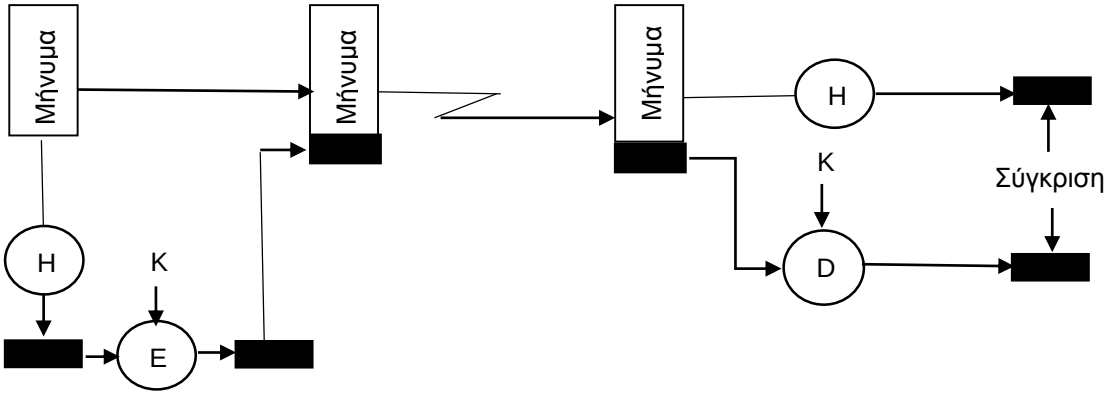
7.3. Μονόδρομες συναρτήσεις σύνοψης

Μια παραλλαγή του κώδικα αυθεντικοποίησης μηνυμάτων που παίζει σημαντικό ρόλο στις σύγχρονες κρυπτογραφικές εφαρμογές, είναι η αξιοποίηση μονόδρομης συνάρτησης σύνοψης (one-way hash function). Όπως και στον κώδικα αυθεντικοποίησης, έτσι και μια συνάρτηση σύνοψης λαμβάνει ως είσοδο ένα μεταβλητού μεγέθους μήνυμα M και στην έξοδο παράγει μια σύνοψη (hash ή digest) σταθερού μήκους *H(M)*. Αντίθετα με το MAC, μια συνάρτηση σύνοψης δε χρειάζεται μυστικό κλειδί στην είσοδο. Προκειμένου νε επιτευχθεί αυθεντικοποίηση του μηνύματος, η σύνοψη H(M) αποστέλλεται έτσι ώστε η σύνοψη μηνύματος να είναι αυθεντική.

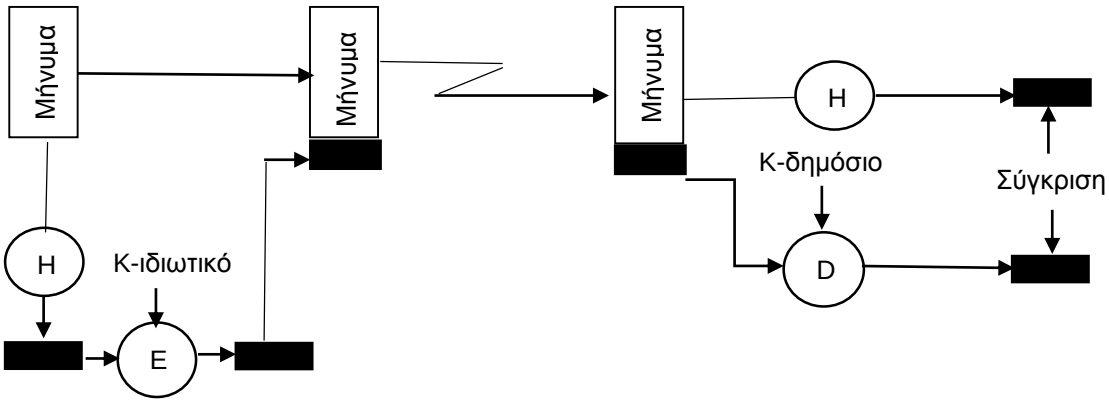
Στο παρακάτω σχήμα απεικονίζονται τρεις τρόποι με τους οποίους μπορεί να αυθεντικοποιηθεί ένα μήνυμα.

Στο σχήμα 7.1α εξηγείται ο τρόπος με τον οποίο η σύνοψη του μηνύματος μπορεί να κρυπτογραφηθεί με χρήση συμμετρική κρυπτογράφηση. Υποθέτοντας ότι ο αποστολέας και ο νόμιμα εξουσιοδοτημένος παραλήπτης είναι οι μοναδικοί που γνωρίζουν το μυστικό κλειδί κρυπτογράφησης, τότε διασφαλίζεται η αυθεντικότητα.

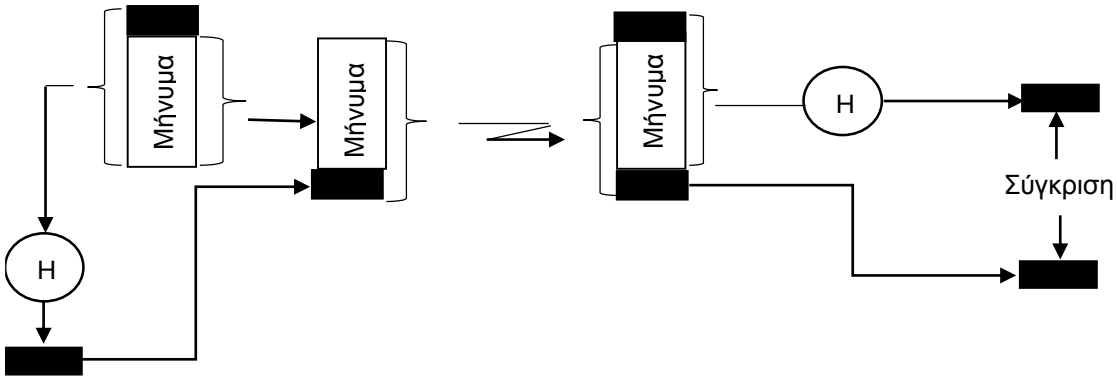
Στο σχήμα 7.1β το μήνυμα μπορεί να κρυπτογραφηθεί χρησιμοποιώντας κρυπτογράφηση δημοσίου κλειδιού. Η προσέγγιση δημοσίου κλειδιού έχει ως βασικό πλεονέκτημα ότι παρέχει τη δυνατότητα λήψης υπηρεσιών ψηφιακής υπογραφής και αυθεντικοποίησης μηνύματος, χωρίς να χρειάζεται διαμοιρασμό μυστικών κλειδιών στα επικοινωνούντα μέρη.



α) Χρησιμοποιώντας συμμετρική κρυπτογράφηση



β) Χρησιμοποιώντας κρυπτογράφηση δημοσίου κλειδιού



γ) Χρησιμοποιώντας συνάρτηση σύνοψης

Σχήμα 7.1: *Αυθεντικοποίηση μηνύματος με χρήση μονόδρομης συνάρτησης σύνοψης*

Αυτές οι προσεγγίσεις, συγκριτικά με τις προσεγγίσεις που κρυπτογραφούν όλο το μήνυμα, παρέχουν σημαντικό πλεονέκτημα καθώς οι απαιτήσεις σε υπολογιστική ισχύ είναι πολύ μικρότερες.

Ωστόσο, ιδιαίτερο ενδιαφέρον εξακολουθεί να παρουσιάζει η ανάπτυξη τεχνικών που αποφεύγουν την κρυπτογράφηση. Οι αιτίες, μεταξύ άλλων, περιλαμβάνουν:

- Το λογισμικό κρυπτογράφησης είναι σχετικά αργό. Παρ' ότι το μέγεθος των δεδομένων που απαιτούν κρυπτογράφηση ανά μήνυμα έχει μειωθεί σημαντικά, εξακολουθεί να υπάρχει χρονοβόρα ροή εισερχόμενων και εξερχόμενων μηνυμάτων από το σύστημα.
- Το κόστος του υλικού κρυπτογράφησης είναι αρκετά μεγάλο. Διατίθενται χαμηλού κόστους υλοποιήσεις σε υλικό για γνωστά κρυπτογραφικά συστήματα, όπως του DES, αλλά το κόστος αυξάνεται σημαντικά, καθώς όλοι οι κόμβοι ενός δικτύου πρέπει να παρέχουν αυτή τη δυνατότητα.
- Στις περιπτώσεις που η κρυπτογράφηση πραγματοποιείται σε υλικό βελτιώνεται σημαντικά η απόδοση κατά την εφαρμογή σε μεγάλου όγκου δεδομένα. Όμως, για μικρά τμήματα δεδομένων δαπανάται σημαντικός χρόνος για την απαιτούμενη αρχικοποίηση.
- Οι αλγόριθμοι κρυπτογράφησης καλύπτονται από πατέντες (patents), γεγονός που, αν και απολύτως θεμιτό, έχει ως συνέπεια τη συνολική αύξηση του κόστους.
- Μέχρι πριν λίγο καιρό οι αλγόριθμοι ισχυρής (strong) κρυπτογράφησης, όπως οι DES και TDES για μεγάλο μέγεθος κλειδιών, υπόκεινταν σε έλεγχο εξαγωγών από τις ΗΠΑ.

Στο σχήμα 7.1γ παρουσιάζεται μία τεχνική που χρησιμοποιεί συνάρτηση σύνοψης, αλλά όχι κρυπτογράφηση για την αυθεντικοποίηση ενός μηνύματος. Η τεχνική αυτή απαιτεί τη γνωστοποίηση της κοινής μυστικής τιμής S_{AB} (secret value) από τον αποστολέα Α και τον παραλήπτη Β, που επικοινωνούν. Όταν ο αποστολέας Α θέλει να στείλει ένα μήνυμα στον Β, εισάγει στη συνάρτηση σύνοψης τη συνένωση (concatenation) της κοινής μυστικής τιμής και του μηνύματος: $MD_M = H\ (S_{AB} \,||\, M)$ και ακολούθως στέλνει στο Β το $[M \,||\, MD_M]$. Έχοντας στη κατοχή του ο Β το S_{AB} έχει τη δυνατότητα να επαναϋπολογίσει το $H\ (S_{AB} \,||\, M)$ και να επαληθεύσει το MD_M. Λόγω του ότι η μυστική τιμή δεν γνωστοποιείται αυτόνομη, μπορεί κάποιος

επιτιθέμενος να αλλοιώσει το μήνυμα που θα έχει καταφέρει να υποκλέψει. Όσο, όμως, διασφαλίζεται η μυστικότητα του S_{AB} δεν έχει τη δυνατότητα ο επιτιθέμενος να τροποποιήσει το μήνυμα χωρίς η πράξη του να γίνει αντιληπτή από τον παραλήπτη.

Μια παραλλαγή της τρίτης τεχνικής ονομάζεται **HMAC** και έχει ιδιαίτερη πρακτική σημασία αφού έχει υιοθετηθεί για την ασφάλεια του IP, για το SSL, ενώ αποτελεί και προδιαγραφή για το SNMPv3.

7.4. Ασφαλείς συναρτήσεις σύνοψης και HMAC

Η μονόδρομη συνάρτηση σύνοψης είναι σημαντική, όχι μόνο για την επίτευξη της αυθεντικοποίησης μηνυμάτων, αλλά και για τη δημιουργία και επαλήθευση ψηφιακών υπογραφών. Παρακάτω αναφέρονται οι απαιτήσεις για μια μονόδρομη συνάρτηση σύνοψης και ακολούθως αναλύονται τα βασικά χαρακτηριστικά των πιο σημαντικών συναρτήσεων σύνοψης

• Απαιτήσεις Συναρτήσεων Σύνοψης

Σκοπός μιας συνάρτησης σύνοψης είναι η κατασκευή ενός αποτυπώματος (digital fingureprint) ενός αρχείου, ενός μηνύματος ή άλλης μορφής δεδομένων. Μία συνάρτηση σύνοψης *H* προκειμένου να μπορεί να χρησιμοποιηθεί στην αυθεντικοποίηση μηνυμάτων πρέπει να ικανοποιεί τις ακόλουθες απαιτήσεις:

1. Η συνάρτηση *H* πρέπει να μπορεί να εφαρμοστεί σε τμήμα δεδομένων οποιουδήποτε μεγέθους.
2. Η συνάρτηση *H* πρέπει να παράγει έξοδο συγκεκριμένου μικρού σταθερού μήκους.
3. Η συνάρτηση *H(x)* πρέπει να μπορεί να υπολογιστεί εύκολα για δοθέν x, καθιστώντας πρακτική την υλοποίηση είτε με λογισμικό είτε με υλικό.
4. Για οποιοδήποτε h που έχει δοθεί πρέπει να είναι υπολογιστικά ανέφικτο (computationally infeasible) να βρεθεί x, τέτοιο ώστε H(x)=h.
5. Για ένα τμήμα δεδομένων x που έχει δοθεί, πρέπει να είναι υπολογιστικά αδύνατο να βρεθεί κάποιο y ≠x, τέτοιο ώστε *H(y)=H(x).*
6. Πρέπει να είναι υπολογιστικά αδύνατο να βρεθεί ζεύγος (x,y) τέτοιο ώστε *H(x)=H(y).*

Οι τρεις πρώτες ιδιότητες αποτελούν βασικές απαιτήσεις για την πρακτική εφαρμογή μιας συνάρτησης σύνοψης στην αυθεντικοποίηση μηνυμάτων. Η τέταρτη ιδιότητα αποτελεί βασικό χαρακτηριστικό μιας μονόδρομης συνάρτησης (one-way). Είναι απαραίτητο να μπορεί να παραχθεί εύκολα η σύνοψη ενός μηνύματος, αλλά ουσιαστικά να είναι ανέφικτο να παραχθεί το μήνυμα της δοθείσας σύνοψης. Αυτή η ιδιότητα είναι πολύ σημαντική αν η τεχνική αυθεντικοποίησης περιέχει τη χρήση μυστικής τιμής (Σχήμα 7.1γ). Η μυστική τιμή δεν αποστέλλεται αυτόνομη. Παρ' όλα' αυτά εάν η συνάρτηση σύνοψης δεν ήταν μονόδρομη, ένας επιτιθέμενος θα ήταν σε θέση να ανακαλύψει εύκολα τη μυστική τιμή, σύμφωνα με την ακόλουθη διαδικασία: υποθέτοντας ότι ο επιτιθέμενος μπορούσε να παρατηρήσει ή να ανακόψει τη πορεία μετάδοσης ενός μηνύματος, τότε ο επιτιθέμενος θα μπορούνε να υποκλέψει το μήνυμα M και τον κωδικό σύνοψης.

$$MD_M = H\,(S_{AB} \,||\, M) \qquad \textbf{(7.1)}$$

΄Υστερα ο επιτιθέμενος θα αντέστρεφε τη συνάρτηση σύνοψης για να αποκτήσει το:

$$S_{AB} \,||\, M = H^{-1}\,(MD_M) \qquad \textbf{(7.2)}$$

Επειδή, όμως, ο επιτιθέμενος θα είχε στη κατοχή του και το *M* και το $S_{AB} \,||\, M$, θα ήταν εύκολο πλέον να ανακαλύψει το S_{AB}.

Η Πέμπτη ιδιότητα εξασφαλίζει ότι είναι ανέφικτο να βρεθεί κάποιο άλλο μήνυμα που θα παράγει την ίδια τιμή σύνοψης με το δοθέν μήνυμα. Αυτό έχει ως αποτέλεσμα να αποτρέπεται η πλαστογράφηση κατά τη χρήση ενός κρυπτογραφημένου κωδικού σύνοψης (Σχήμα 7.1α και 7.1β). Εάν αυτή η ιδιότητα δεν ίσχυε, ο επιτιθέμενος θα μπορούσε να πραγματοποιήσει διαδοχικά τις παρακάτω ενέργειες: Στην αρχή να παρατηρήσει ή να υποκλέψει ένα μήνυμα και την κρυπτογραφημένη σύνοψη, στη πορεία να κατασκευάσει μια κρυπτογραφημένη σύνοψη από το μήνυμα και ακολούθως να δημιουργήσει ένα άλλο μήνυμα με την ίδια σύνοψη. Μία συνάρτηση σύνοψης που πληροί τις πέντε πρώτες απαιτήσεις καλείται ***αδύναμη συνάρτηση σύνοψης*** (weak hash function). Εάν πληρείται και η έκτη ιδιότητα καλείται ***ισχυρή συνάρτηση σύνοψης*** (strong hash function). Η έκτη ιδιότητα προστατεύει από ιδιαίτερα έξυπνες κλάσεις επιθέσεων, γνωστές στη βιβλιογραφία ως επιθέσεις τύπου γενεθλίων (birthday attack).

Επίσης, με την παροχή αυθεντικοποίησης, η μέθοδος αυτή παρέχει υπηρεσία ακεραιότητας δεδομένων: αν κάποια bits στο μήνυμα αλλοιωθούν κατά τη

μετάδοση, τότε η σύνοψη που θα έχει ενσωματωθεί στο τέλος του μηνύματος δε θα αντιστοιχεί με το μήνυμα.

- Απλές Συναρτήσεις Σύνοψης

Το σύνολο των συναρτήσεων σύνοψης λειτουργεί βασιζόμενο στις δύο γενικές αρχές που περιγράφονται παρακάτω: Η είσοδος (μήνυμα, αρχείο κλπ.) αντιμετωπίζεται σαν μια ακολουθία από τμήματα μήκους n-bit, τα οποία τα επεξεργάζεται ένα-ένα τμήμα κάθε φορά, με επαναληπτικό τρόπο, ώστε να παραχθεί μία τιμή σύνοψης μήκους n-bit.

Μία από τις πιο απλές συναρτήσεις σύνοψης είναι η συνάρτηση σύνοψης *Ψηφίο – Προς – Ψηφίο XOR* (bit-by-bit XOR) για κάθε τμήμα. Για τη συνάρτηση αυτή ισχύουν:

$C_i = b_{i1} \oplus b_{i2} \oplus \ldots \oplus b_{im}$ **(7.3)**

όπου:

C_i = το i bit της σύνοψης, $1 \leq i \leq n$

b_{ij} = το i bit του τμήματος j

m = ο αριθμός των n-bit τμημάτων στην είσοδο

$\oplus$ = η πράξη XOR

Στο Πίνακας 7.2 περιγράφεται η λειτουργία της συνάρτησης σύνοψης, κατά την οποία παράγεται μία απλή ισοτιμία (parity) σε κάθε θέση bit, γνωστή ως longitudinal redundancy check. Αποτελεί μια αποτελεσματική συνάρτηση για έλεγχο ακεραιότητας τυχαίων δεδομένων. Κάθε συνδυασμός bits, δηλαδή κάθε τιμή ως σύνοψη, έχει την ίδια πιθανότητα να προκύψει. Έτσι η πιθανότητα να προκύψει λάθος ενώ η τιμή της σύνοψης παραμένει η ίδια, είναι 2^{-n}. Η συνάρτηση, όμως, δεν είναι το ίδιο αποτελεσματική για μη τυχαία δεδομένα. Για παράδειγμα, στα περισσότερα αρχεία κειμένου το υψηλής προτεραιότητας bit κάθε byte είναι πάντα μηδέν. Έτσι λοιπόν, έστω ότι χρησιμοποιείται τιμή σύνοψης μεγέθους 128 bit, η πιθανότητα σφάλματος μειώνεται από 2^{-128} σε 2^{-112}.

	Bit 1	**Bit 2**	**...**	**Bit n**
Block 1	b_{11}	b_{21}		b_{n1}
Block 2	b_{12}	b_{22}		b_{n2}
	⋮	⋮	⋮	⋮
Block m	b_{1m}	b_{2m}		b_{nm}
Κώδικας σύνοψης	C_1	C_2		C_n

Πίνακας 7.2: *Λειτουργία μιας συνάρτησης σύνοψης με bit-by-bit XOR*

Ένας απλός τρόπος βελτίωσης αυτής της μεθόδου είναι η αριστερή κυκλική ολίσθηση ενός bit (one-bit circular shift), ή περιστροφή (rotation) της τιμής σύνοψης μετά την επεξεργασία κάθε τμήματος. Η διαδικασία αυτή επιτυγχάνει είσοδο με μεγαλύτερη τυχαιότητα και μπορεί να συνοψισθεί ως ακολούθως:

Βήμα 1. Αρχικοποίηση της n-bit τιμής σύνοψης με μηδενική τιμή.

Βήμα 2. Εκτέλεση των ακόλουθων βημάτων για κάθε τμήμα δεδομένων n-bit:

Βήμα 2.1 Αριστερή κυκλική ολίσθηση κατά ένα bit της τρέχουσας τιμής σύνοψης

Βήμα 2.2 Εφαρμογή της XOR στο τμήμα της τιμής σύνοψης

Αν και η δεύτερη διαδικασία φαίνεται υποβοηθητική για τη προστασία της ακεραιότητας των δεδομένων, στην πραγματικότητα αποτελεί μια ενέργεια ανώφελη για την προστασία των δεδομένων όταν χρησιμοποιείται κρυπτογραφημένη σύνοψη σε μη κρυπτογραφημένο κείμενο (Σχήμα 7.1α και 7.2β). Δοθέντος ενός μηνύματος, είναι πια εύκολο να δημιουργηθεί εναλλακτικό μήνυμα που θα παράγει την ίδια σύνοψη, αφού ο δυνητικός κρυπταναλυτής με απλή προετοιμασία του εναλλακτικού μηνύματος και προσάρτηση ενός τμήματος n-bit μπορεί να παραγάγει την επιθυμητή σύνοψη.

Παρόλο ότι μία απλή XOR ή R-XOR δεν είναι επαρκής στη περίπτωση που είναι κρυπτογραφημένη μόνο η σύνοψη, η μέθοδος είναι ιδιαίτερα χρήσιμη όταν αναφερόμαστε και σε κρυπτογραφημένο μήνυμα. Μία τεχνική που προτάθηκε αρχικά από το US National Bureau of Standards εφάρμοζε μία απλή XOR σε τμήμα μεγέθους 64-bit ενός μηνύματος και στη συνέχεια κρυπτογραφούσε όλο το μήνυμα με τη μέθοδο της Αλυσιδωτής Κρυπτογράφησης Τμημάτων CBC.

Αναλυτικότερα, η τεχνική είχε ως εξής:

Δοθέντος ενός μηνύματος, που αποτελείται από τμήματα των 64-bit $X_1,X_2,\ldots,X_n$, ορίζεται ως σύνοψη *C* το *XOR* όλων των επιμέρους τμημάτων και επισυνάπτεται η σύνοψη ως το τελευταίο τμήμα.

$$C = X_{n+1} = X_1 \oplus X_2 \oplus \ldots \oplus X_n \qquad \textbf{(7.4)}$$

Στη συνέχεια, όλο το μήνυμα μαζί με τη σύνοψη κρυπτογραφούνται, εφαρμόζοντας τη μέθοδο CBC, προκειμένου να παραχθεί το κρυπτογραφημένο μήνυμα $Y_1,Y_2,\ldots Y_{n+1}$. Στη βιβλιογραφία αναφέρονται αρκετοί τρόποι για τη μετατροπή του κρυπτογραφημένου κειμένου του μηνύματος, ώστε να μην ανιχνεύονται από τη σύνοψη. Για παράδειγμα, από τον ορισμό του CBC έχουμε :

$X_1=IV \oplus D_K(Y_1)$

$Xi=Y_{i-1} \oplus D_K(Y_i)$

$X_{n+1}= Y_n \oplus D_K(Y_{n+1})$ **(7.5)**

Όμως, το X_{n+1} είναι η σύνοψη:

$X_{n+1} = X_1 \oplus X_2 \oplus \ldots \oplus X_n$

$= (IV \oplus D_K(Y_1)) \oplus (Y_2 \oplus D_K(Y_2)) \oplus \ldots \oplus (Y_n \oplus D_K(Y_{n+1}))$ **(7.6)**

Επειδή οι όροι στην προηγούμενη εξίσωση μπορούν να υποστούν XOR με οποιαδήποτε σειρά, η σύνοψη δεν αλλάζει εάν μετατεθεί η σειρά των τμημάτων του κρυπτογραφημένου κειμένου.

7.5. Συνάρτηση Σύνοψης SHA–1

Ο αλγόριθμος Secure Algorithm – SHA αναπτύχθηκε από το US National Institute of Standards and Technology και δημοσιεύτηκε ως Federal Information Processing Standard FIPS PUB 180 το 1993. Το 1995 δημοσιεύθηκε μια αναθεωρημένη έκδοσή του FIPS PUB 180-1, η οποία έχει γίνει γνωστή και αποδεκτή ως SHA-1

Ο SHA-1 αλγόριθμος λαμβάνει στην είσοδο ένα μήνυμα, μέγιστο μήκους του οποίου μπορεί να είναι 2^{64} bits και δίνει ως έξοδο μια σύνοψη μεγέθους 160 bits. Για να πραγματοποιηθεί επεξεργασία της εισόδου πρέπει, αρχικά, να σπάσουμε το μήνυμα σε τμήματα των 512 bits.

Στο Σχήμα 7.2 απεικονίζεται η διαδικασία παραγωγής σύνοψης ενός μηνύματος, η οποία αποτελείται από τα ακόλουθα βήματα:

Βήμα 1: Επισύναψη Επιπρόσθετων Ψηφίων

Στο μήνυμα προσθέτονται κάποια bits έτσι ώστε να διατηρείται το μέγεθος του ίσο με 448 mod 512 και κατά συνέπεια το μέγεθος του μηνύματος να είναι πάντα 64 bits μικρότερο από οποιοδήποτε πολλαπλάσιο του 512. Η προσάρτηση αυτών των bits πραγματοποιείται σε κάθε περίπτωση, ακόμη κι όταν το μήνυμα διαθέτει το επιθυμητό μήκος. Το πλήθος των bits που προσαρτώνται είναι μεταξύ 1 έως 512 bits. Η προσάρτηση ψηφίων αποτελείται από ένα 1-bit και ακολουθείται από τον απαιτούμενο αριθμό των 0-bits.

Βήμα 2: Επισύναψη του Μήκους του Μηνύματος

Προσαρτάται στο μήνυμα ένα τμήμα 64 bits, το οποίο παίζει το ρόλο ενός μη προσημασμένου ακέραιου αριθμού 64 bit, με το σημαντικότερο byte πρώτο, που δηλώνει το μέγεθος του αρχικού μηνύματος, σαφώς πριν την προσάρτηση των πρόσθετων ψηφίων. Προσαρτώντας τη τιμή του μήκους έχει ως αποτέλεσμα τη μείωση των πιθανοτήτων επίτευξης ενός είδους επίθεσης, γνωστής ως επίθεση τύπου επισύναψης (padding attack).

Το παραγόμενο αποτέλεσμα των δύο πρώτων βημάτων είναι ένα μήνυμα με μήκος έναν ακέραιο πολλαπλάσιο των 512 bits. Στο Σχήμα 7.2 το επαυξημένο μήνυμα απεικονίζεται με μία ακολουθία τμημάτων $Y_0\ Y_1 \ldots Y_{L-1}$ των 512 bits το καθένα, προκειμένου το συνολικό μέγεθος του μηνύματος να είναι *L*512* bits. Ισοδύναμα, το αποτέλεσμα είναι πολλαπλάσιο των 16 λέξεων των 32 bits η καθεμία. Αν οι λέξεις του παραγόμενου μηνύματος είναι *M[0…N-1]* με N ακέραιο πολλαπλάσιο του 16, τότε *N=L*16.*

Βήμα 3: Αρχικοποίηση του Καταχωρητή MD

Τα ενδιάμεσα αλλά και τα τελικά αποτελέσματα της συνάρτησης σύνοψης αποθηκεύονται σε ένα καταχωρητή (buffer) των 160 bits, ο οποίος μπορεί να αναπαρασταθεί με 5 μικρότερους καταχωρητές (registers) των 32 bits (A, B, C, D, E). Η αρχικοποίηση των καταχωρητών αυτών επιτυγχάνεται καταχωρώντας σε αυτούς τις παρακάτω δεκαεξαδικές τιμές:

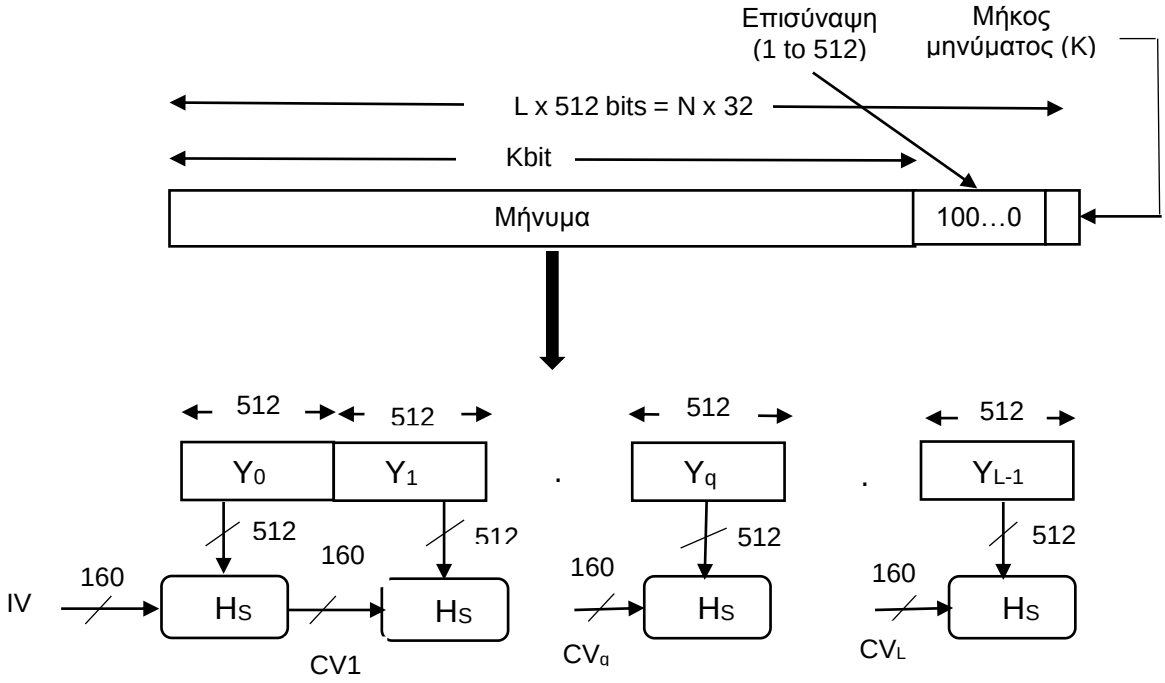
A = 67452301

B = EFCDAB89

C = 98BADCFE

D = 10325476

E = C3D2E1F0

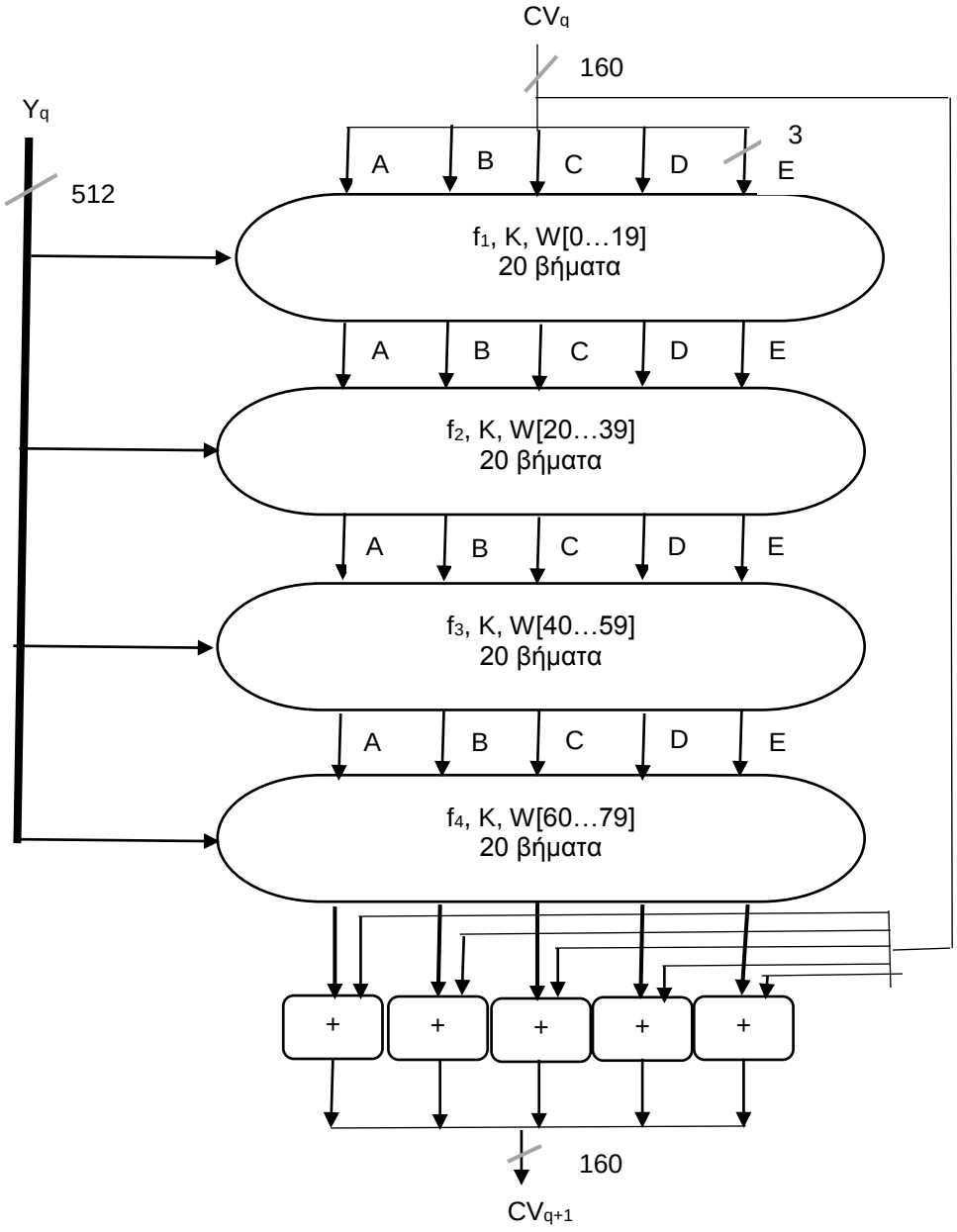


Σχήμα 7.2: *Διαδικασία παραγωγής σύνοψης μηνύματος*

Βήμα 4: Επεξεργασία Μηνύματος σε Τμήματα των 512 bits ή ισοδύναμα των 16 λέξεων

Το σημαντικότερο συστατικό του αλγορίθμου αποτελεί ένα τμήμα κώδικα που καλείται συνάρτηση συμπίεσης (compression function), η οποία συντίθεται από 4 κύκλους επεξεργασίας των 20 βημάτων ο καθένας. Η λογική της συνάρτησης περιγράφεται στο Σχήμα 7.3. Όλοι οι κύκλοι διαθέτουν παρόμοια δομή, αλλά ο κάθε ένας εφαρμόζει διαφορετικές λογικές συναρτήσεις τις f_1, f_2, f_3, f_4. Ο κάθε κύκλος δέχεται ως είσοδο το τρέχων τμήμα των 512 bits που επεξεργάζεται (έστω Y_q το τρέχον τμήμα) και την τιμή ABCDE που βρίσκεται στον καταχωρητή των 160 bit και ενημερώνει τα περιεχόμενα του. Επιπλέον, κάθε κύκλος χρησιμοποιεί μία πρόσθετη σταθερά K_t, όπου $0 \leq t \leq 79$, η οποία υποδεικνύει κάποιο από τα 80 βήματα των 5 κύκλων. Στην ουσία υπάρχουν μόνο 4 διακριτές σταθερές που χρησιμοποιούνται. Οι τιμές αυτές στο δεκαδικό και στο δεκαεξαδικό σύστημα είναι:

Αριθμός Βημάτων	**Δεκαεξαδικό**	**Λήψη τμήματος ακεραίου:**
0 ≤ t ≤ 19	K_t = 5A827999	$[2^{30} \times \sqrt{2}\ ]$
20 ≤ t ≤ 39	K_t = 6ED9EBA1	$[2^{30} \times \sqrt{3}\ ]$
40 ≤ t ≤ 59	K_t = 8F1BBCDC	$[2^{30} \times \sqrt{5}\ ]$
60 ≤ t ≤ 79	K_t = CA62C1D6	$[2^{30} \times \sqrt{10}\ ]$



Σχήμα 7.3: *Λειτουργία συνάρτησης συμπίεσης*

Η έξοδος του τέταρτου κύκλου, ή ισοδύναμα του 80ου βήματος, προστίθεται στην είσοδο του πρώτου κύκλου (CVq) ώστε να παραχθεί το CVq+1. Η πρόσθεση γίνεται ανεξάρτητα για καθεμία από τις 5 λέξεις του καταχωρητή για την καθεμία από τις λέξεις στο *CVq*, χρησιμοποιώντας πρόσθεση υπολοίπου 2^{32}.

Βήμα 5: Έξοδος

Εφόσον όλα τα τμήματα L έχουν υποστεί την απαιτούμενη επεξεργασία, η έξοδος που προκύπτει από το τελευταίο στάδιο αποτελεί τη σύνοψη των 160 bits του αρχικού μηνύματος.

Ο SHA–1 αλγόριθμος διαθέτει την ιδιότητα όλα τα bits του κωδικού σύνοψης να είναι αποτέλεσμα εφαρμογής συνάρτησης σε όλα τα bits της εισόδου. Η πολύπλοκη επανάληψη της βασικής συνάρτησης *f* παράγει καλά-ανομοιογενή (well–mixed) αποτελέσματα. Για παράδειγμα, είναι ανέφικτο δύο τυχαία επιλεγμένα μηνύματα, ακόμη και αν παρουσιάζουν όμοια κανονικότητα, να παράγουν την ίδια σύνοψη. Στο βαθμό που δεν υπάρχει κάποια εγγενής σχεδιαστική αδυναμία του αλγορίθμου SHA-1, ή που δεν έχει ακόμη αποκαλυφθεί ή δημοσιευτεί, η δυσκολία να υπάρξουν δύο μηνύματα με την ίδια σύνοψη είναι της τάξεως των 2^{80} λειτουργιών, ενώ η δυσκολία ανεύρεσης του μηνύματος δοθείσης μιας σύνοψης είναι της τάξεως των 2^{160} λειτουργιών.

7.6. Αλγόριθμος MD5

Ο αλγόριθμος MD5 (Message Digest) αναπτύχθηκε από τον R. Rivest και περιγράφεται στο RFC 1321. Μέχρι πρόσφατα ο MD5 ήταν ο πιο διαδεδομένος ασφαλής αλγόριθμος σύνοψης, γεγονός που όμως άλλαξε όταν το ενδιαφέρον για εξαντλητική αναζήτηση κλειδιών και κρυπτανάλυση άρχισε να αυξάνεται με ραγδαία ταχύτητα. Ο αλγόριθμος δέχεται ως είσοδο μήνυμα οποιουδήποτε μεγέθους και παράγει ως έξοδο μία σύνοψη των 128 bits. Η είσοδος επεξεργάζεται τμήματα των 512 bits.

Όσο οι ταχύτητες των επεξεργαστών αυξάνονταν, τόσο πιο πολύ αμφισβητήσιμη θεωρούταν η ασφάλεια που προερχόταν από μια σύνοψη των 128 bits. Μπορεί να αποδειχθεί ότι η δυσκολία να υπάρξει ίδια MD5 σύνοψη για δύο διαφορετικά μηνύματα είναι της τάξης των 2^{64} πράξεων, ενώ η δυσκολία αποκάλυψης ενός μηνύματος με τη βοήθεια της MD5 σύνοψης του είναι της τάξης των 2^{128} πράξεων.

Στις μέρες μας και οι δυο αυτές τιμές θεωρούνται μικρές ως προς την παροχή ασφαλείας. Επίσης, έχουν κάνει την εμφάνισή τους αρκετές μορφές κρυπταναλυτικών επιθέσεων που στηρίζονται σε αδυναμίες και εγγενή σημεία ευπάθειας που παρουσιάζει ο MD5.

7.7. Συνάρτηση σύνοψης RIPEMD – 160

Ο αλγόριθμος σύνοψης μηνυμάτων RIPEMD–160 αναπτύχθηκε στα πλαίσια του ευρωπαϊκού έργου RIPE - RACE Integrity Primitives Evaluation από ομάδα ερευνητών που είχαν επιχειρήσει και καταφέρει επιθέσεις στους αλγορίθμους *MD4* και *MD5*. Στην αρχή, αναπτύχθηκε η έκδοση RIPEM με 128 bits. ΄Υστερα από την ολοκλήρωση του έργου RIPE, ο H. Dobbertin που δεν είχε πάρει μέρος στο έργο RIPE, εφήυρε κάποιες επιθέσεις για το RIPEMD και αργότερα για το MD4 και MD5. Στη πορεία, κάποια από τα μέλη του RIPE αποφάσισαν να αναβαθμίσουν το RIPEMD και προχώρησαν σε νέο σχεδιασμό από κοινού με τον H. Dobbertin.

Η δομή του RIPEMD-160 είναι παρόμοια με αυτή του SHA-1. Ο αλγόριθμος δέχεται ως είσοδο ένα μήνυμα οποιουδήποτε μήκους και παράγει ως έξοδο μία σύνοψη του μηνύματος των 160 bits. Η είσοδος χωρίζεται σε τμήματα των 512 bits για να επεξεργαστεί.

7.8. Hash-based message authentication code (HMAC)

Τα τελευταία χρόνια, είχε αναπτυχθεί ιδιαίτερο ενδιαφέρον για τη δημιουργία MAC από κρυπτογραφική σύνοψη, όπως αυτή που παράγεται από τον SHA-1. Τα σημαντικότερα κίνητρα ήταν τα εξής:

- Οι κρυπτογραφικές συναρτήσεις σύνοψης, εκτελούνται γρηγορότερα χρησιμοποιώντας το κατάλληλο λογισμικό απ’ ότι οι συμβατικοί αλγόριθμοι κρυπτογραφίας, όπως ο DES.
- Οι βιβλιοθήκες κώδικα για κρυπτογραφικές συναρτήσεις σύνοψης είναι ευρέως διαθέσιμες.
- Δεν υπάρχουν πλέον νομικοί περιορισμοί εξαγωγής κρυπτογραφικών συναρτήσεων σύνοψης ούτε από τις ΗΠΑ, ούτε από άλλη χώρα, όπως συνέβαινε λίγα χρόνια πριν με τους συμβατικούς αλγορίθμους κρυπτογραφίας, ακόμα και αυτούς που έβρισκαν εφαρμογή στη δημιουργία MAC.

Η συνάρτηση σύνοψης SHA–1 δεν σχεδιάστηκε και δεν είναι σε θέση να χρησιμοποιηθεί για δημιουργία MAC, διότι δε στηρίζεται σε μυστικό κλειδί. Υπήρχαν πολλές προτάσεις για ενσωμάτωση μυστικού κλειδιού σε ήδη υπάρχοντα αλγόριθμο σύνοψης, με επικρατέστερη πρόταση το HMAC. Όπως περιγράφεται στο RFC 2104, το HMAC επιλέχθηκε ως υποχρεωτικό προς υλοποίηση MAC για IP Security και εφαρμόζεται σε πολλά πρωτόκολλα ασφαλείας στο Internet όπως στο TLS/SSL και στο SET.

- Σχεδιαστικοί στόχοι HMAC

Στο RFC 2014 αναλύονται οι παρακάτω σχεδιαστικοί στόχοι για το HMAC:

- Να εφαρμοστούν χωρίς αλλαγές ήδη υπάρχουσες συναρτήσεις σύνοψης, δηλαδή συναρτήσεις σύνοψης που λειτουργούν καλά σε επίπεδο λογισμικού και για τις οποίες ο κώδικας είναι δωρεάν και ευρέως διαθέσιμος
- Να μπορεί να πραγματοποιηθεί γρήγορα και εύκολα αντικατάσταση της ενσωματωμένης συνάρτησης σύνοψης που υπάρχει στο HMAC, σε περίπτωση που αναπτυχθεί κάποια πιο γρήγορη ή ασφαλείς συνάρτηση ή απαιτείται για οποιονδήποτε άλλο λόγο.
- Η αρχική απόδοση της συνάρτησης σύνοψης να διασώζεται, χωρίς την ύπαρξη επιπτώσεων που έχουν ως αποτέλεσμα τον υποβιβασμό της.
- Να γίνεται χρήση κλειδιών και η διαχείρισή τους να επιτυγχάνεται εύκολα.
- Να υπάρχει σαφής κρυπτογραφική ανάλυση των δυνατοτήτων του μηχανισμού αυθεντικοποίησης, στηριζόμενη σε λογικές υποθέσεις σχετικά με την όποια ενσωματωμένη συνάρτηση σύνοψης που υπάρχει στο HMAC.

Οι δύο πρώτοι στόχοι παίζουν σημαντικό ρόλο στην οργάνωση ενός πλαισίου ευρείας αποδοχής του HMAC. Το HMAC χρησιμοποιεί τη συνάρτηση σύνοψης ως μαύρο κουτί (black box). Αυτό έχει δύο πλεονεκτήματα:

- Η υλοποίηση του HMAC μπορεί να επιτευχθεί βασιζόμενη σε υλοποίηση συνάρτησης σύνοψης που ήδη υπάρχει. Αυτό έχει ως συνέπεια, το κύριο μέρος του κώδικα του HMAC να είναι προκατασκευασμένο και έτοιμο να χρησιμοποιηθεί χωρίς καμία μετατροπή.

- Εάν απαιτηθεί αντικατάσταση της συνάρτησης σύνοψης του HMAC, το μόνο που χρειάζεται είναι η αφαίρεση του υπάρχοντος κώδικα στης συνάρτησης και η αντικατάστασή του με το νέο κώδικα. Αυτό μπορεί να συμβεί είτε επειδή απαιτείται γρηγορότερη συνάρτηση σύνοψης, είτε επειδή η ασφάλεια που προσφέρει η ενσωματωμένη συνάρτηση σύνοψης είναι ελλιπής.

Ο τελευταίος σχεδιαστικός στόχος αποτελεί το σημαντικότερο πλεονέκτημα του HMAC συγκριτικά με όλα τα υπόλοιπα προτεινόμενα συστήματα που στηρίζονται σε συναρτήσεις σύνοψης: το HMAC μπορεί να αποδειχθεί ότι προσφέρει ασφάλεια, σύμφωνα με τις κρυπτογραφικές δυνατότητες της ενσωματωμένης συνάρτησης σύνοψης.

- Αλγόριθμος HMAC

Στο Σχήμα 7.4 παρουσιάζεται η λειτουργία του HMAC. Η επεξήγηση των συμβόλων έχει ως εξής:

H = ενσωματωμένη συνάρτηση σύνοψης (π.χ. SHA-1)

M = μήνυμα που αποτελεί είσοδο στο HMAC, συμπεριλαμβανομένου και του πλήθους των bits που έχουν προσαρτηθεί σύμφωνα με την H

Yi = i τμήμα του M, με $0 \leq i \leq L-1$

L = αριθμός τμημάτων του M

B = αριθμός bits ενός τμήματος

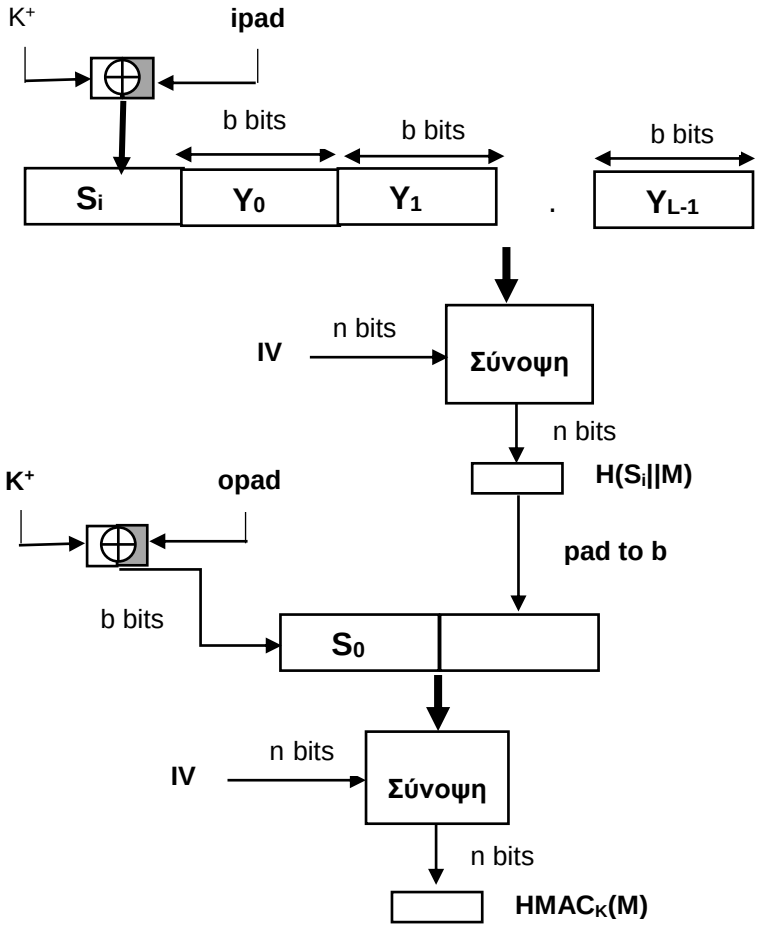
N = το μήκος της σύνοψης που παράγεται από την ενσωματωμένη συνάρτηση σύνοψης

K = το μυστικό κλειδί. Αν το μήκος του κλειδιού είναι μεγαλύτερο από το b, το κλειδί είναι είσοδος στη συνάρτηση σύνοψης ώστε να παραχθεί ένα κλειδί n-bits. Ως προτεινόμενο μήκος αναφέρεται ότι πρέπει να είναι μεγαλύτερο ή ίσο του n.

K+ = το K μετά από προσάρτηση μηδενικών από τα αριστερά, έτσι ώστε το αποτέλεσμα να είναι b bits σε μήκος.

ipad = 00110110 (36 στο δεκαεξαδικό) επαναλαμβανόμενο b/8 φορές

opad = 01011100 (5C στο δεκαεξαδικό) επαναλαμβανόμενο b/8 φορές



Σχήμα 7.4: *Λειτουργία του HMAC*

Σύμφωνα με τα παραπάνω, το HMAC μπορεί να εκφραστεί ως:

$$HMAC_K = H\,[(K^+ \oplus opad) \,||\, H\,[(K^+ \oplus ipad) \,||\, M]] \qquad \textbf{(7.7)}$$

Αναλυτικά :

Βήμα 1. Προσθήκη μηδενικών στο K από τα αριστερά για να δημιουργηθεί μία συμβολοσειρά K+μήκους b bits (για παράδειγμα, αν το K έχει μήκος 160 bits και b=512, τότε στο K θα προστεθούν 44 μηδενικά bytes 0x00).

Βήμα 2. Εφαρμογή XOR στο K+□ και στο ipad για να παραχθεί το τμήμα Si από b bits**.**

Βήμα 3. Προσάρτηση του M στο Si.

Βήμα 4. Εφαρμογή της H στο αποτέλεσμα του βήματος 3.

Βήμα 5. Εφαρμογή XOR στο K+ και στο opad για να παραχθεί το τμήμα So από b bits.

Βήμα 6. Προσάρτηση του αποτελέσματος του βήματος 4 στο So.

Βήμα 7. Εφαρμογή της H στο αποτέλεσμα του βήματος 6. Η έξοδος της H είναι το τελικό αποτέλεσμα του αλγόριθμου.

Σημειώνεται ότι το XOR με ipad και opad έχει ως συνέπεια την αλλαγή των μισών bits του K, με τη διαφορά όμως, ότι στη δεύτερη περίπτωση η τροποποίηση πραγματοποιείται σε διαφορετική ομάδα bits. Επομένως, εισάγοντας τα S_0 και S_i, από τον αλγόριθμο σύνοψης παράγονται ψευδοτυχαία δύο κλειδιά από το K.

Το HMAC απαιτεί για τη λειτουργία, κατά προσέγγιση, τον ίδιο χρόνο με την ενσωματωμένη συνάρτηση σύνοψης για μεγάλα μηνύματα. Παρ' όλα' αυτά, έχει το μειονέκτημα ότι επιβραδύνει τη συνολική λειτουργία με τις τρεις παραπάνω εκτελέσεις συγκριτικά με τη κύρια συνάρτηση σύνοψης, για το S_0 και S_i, και το τμήμα που παράγεται από την εσωτερική σύνοψη.

ΚΕΦΑΛΑΙΟ 8Ο

8. ΚΒΑΝΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

8.1. Εισαγωγή

Για πολλά χρόνια, οι μαθηματικοί ερευνούσαν για ένα σύστημα που θα καθιστούσε την μετάδοση πληροφοριών μεταξύ δύο οντοτήτων απόλυτα ασφαλή. Το 1940 ο Claude Shannon απέδειξε ότι αυτό είναι αδύνατο, εκτός κι αν τα δύο επικοινωνούντα μέρη μοιράζονται ένα τυχαίο μυστικό κλειδί, το μήκος του οποίου ισούται με το μήκος του μηνύματος που θέλουν να αποστείλουν. Επίσης αυτό το κλειδί μπορεί να χρησιμοποιηθεί μόνο μια φορά.

Το εμπόδιο αυτό, όμως, στη κβαντική κρυπτογραφία μπορεί να ξεπεραστεί αν εκμεταλλευτούμε αφενός την αδυναμία ακριβής μέτρησης της κβαντικής πληροφορίας, αφετέρου τη διαταραχή που δημιουργείται από τέτοιες μετρήσεις. Πληροφορία που έχει κωδικοποιηθεί κατάλληλα σε κβαντικές καταστάσεις, κάθε πιθανή προσπάθεια πρόσβασης σε αυτή, περιέχει το κίνδυνο να καταστραφεί η πληροφορία δια παντός. Το αποτέλεσμα αυτό, μπορεί να ανιχνευτεί από τους νόμιμους χρήστες της, παρέχοντας τη δυνατότητα εγκατάστασης μιας ασφαλούς σύνδεσης, χωρίς να χρειάζεται να ανταλλάξουν ένα κοινό μυστικό κλειδί.

Σε αυτό το σημείο είναι σημαντικό να σημειώσουμε πως οι κβαντικοί υπολογιστές απειλούν τα πιο πολλά από τα κρυπτοσυστήματα που χρησιμοποιούνται σήμερα, αλλά η κβαντική κρυπτογραφία παρέχει μια ασφαλή εναλλακτική λύση χωρίς προϋποθέσεις.

8.1.1. Η πρώτη ιδέα

Σε μια εργασία του ο Stephen Wiesner γύρω στο 1970 ότι τα κβαντικά φαινόμενα ήταν δυνατό να χρησιμοποιηθούν για να παράγουμε τραπεζογραμμάτια που δεν θα μπορούσαν να πλαστογραφηθούν. Επειδή η κβαντική πληροφορία δε μπορεί να κλωνοποιηθεί, ο Wiesner αντιλήφθηκε ότι ένα χαρτονόμισμα που περιείχε κβαντική πληροφορία, ήταν ανέφικτο να αντιγραφεί.

Ο μόνος που έδωσε σημασία σε αυτή την ιδέα ήταν ο Charles Bennett, η οποία τον οδήγησε ύστερα από πολλά χρόνια στην ανακάλυψη της κβαντικής πληροφορίας. Το 1989 ο Bennet μαζί με τους John A. Smolin και Gilles Brassard

επιχείρησαν ένα πείραμα το οποίο επιδείκνυε ένα καινούργιο τρόπο κρυπτογράφησης στηριζόμενο στις αρχές της κβαντικής μηχανικής.

Η πιο πάνω ομάδα συναρμολόγησε μια πειραματική διάταξη όπου τα φωτόνια διέσχιζαν ένα κανάλι μήκους 30 εκατοστών σε ένα φωτογενές κουτί που το ονόμασαν *φέρετρο της θείας Μάρθας*. Η διεύθυνση κατά την οποία ταλαντωνόταν το ηλεκτρικό πεδίο των φωτονίων, η πόλωσή τους, αναπαριστούσε το 0 και 1 μιας ακολουθίας κβαντικών bit που είναι γνωστά ως ***qubit***. Τα qubit περιείχαν ένα κρυπτογραφικό κλειδί που μπορούσε να χρησιμοποιηθεί για την κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος. Το κλειδί αυτό προστατεύεται από τους υποκλοπείς μέσω της αρχής της αβεβαιότητας του Heisenberg – η βασική αρχή της κβαντικής φυσικής που ορίζει ότι η μέτρηση μιας φυσικής ιδιότητας σε μια κβαντική κατάσταση, θα διαταράξει κάποια άλλη ιδιότητα. Σε ένα κβαντικό σύστημα κρυπτογραφίας, ο υποκλοπέας εάν προσπαθούσε να διαβάσει κάποια από τα φωτόνια θα τα μετέβαλε με αποτέλεσμα η παρεμβολή ενός τρίτου να γινόταν αντιληπτή και από τα δύο επικοινωνούντα μέρη.

8.1.2. Πρακτική εφαρμογή

Ένας τρόπος μετάδοσης ενός κβαντικού κλειδιού κρυπτογράφησης, απαιτεί την ύπαρξη ενός λέιζερ που θα μπορεί να εκπέμπει μεμονωμένα φωτόνια πολωμένα με δύο διαφορετικούς τρόπους. Κατά το πρώτο τρόπο, τα φωτόνια έχουν κατακόρυφη ή οριζόντια πόλωση (ορθός τρόπος), κατά το δεύτερο τρόπο, η πόλωση των φωτονίων σχηματίζει με την κατακόρυφο γωνία ± 45 μοιρών (πλάγιος τρόπος). Και στους δύο τρόπους, οι δυο αμοιβαίως ορθογώνιες πολώσεις αναπαριστούν το ψηφίο 0, η μία, και το ψηφίο 1, η άλλη. Ο αποστολέας, αποστέλλει μια ακολουθία bit, επιλέγοντας τυχαία με ποιόν από τους δύο παραπάνω τρόπους, ορθό ή πλάγιο, θα μεταδοθούν τα φωτόνια. Αντίστοιχα, ο αποδέκτης επιλέγει τυχαία ποιό τρόπο θα χρησιμοποιήσει για να μετρήσει τα εισερχόμενα bit. Η αρχή της αβεβαιότητας του Heisenberg δεν δίνει στον αποδέκτη τη δυνατότητα μέτρησης των εισερχόμενων φωτονίων και με του δύο τρόπους, παρά μόνο με έναν από τους δύο. Από όλα τα φωτόνια, μόνο εκείνα που μέτρησε ο παραλήπτης με τον ίδιο τρόπο που μεταδόθηκαν από τον αποστολέα είναι σίγουρο πως θα έχουν και για τους δυο αφενός την ίδια πόλωση, αφετέρου ότι τα bit θα συμπίπτουν.

Μετά τη μετάδοση, ο παραλήπτης επικοινωνεί με τον αποστολέα, χωρίς να χρειάζεται αυτή η επικοινωνία να είναι κρυφή, και τον ενημερώνει ποιον από τους δύο τρόπους (ορθό ή πλάγιο) επέλεξε για να λάβει το κάθε φωτόνιο. Όμως, δεν αναφέρει ποιά τιμή, 0 ή 1, αναπαριστούσε το κάθε ένα φωτόνιο από αυτά. Στη συνέχεια ο αποστολέας αποκαλύπτει τον παραλήπτη ποια φωτόνια μετρήθηκαν σωστά και αυτά που μετρήθηκαν με λάθος τρόπο αγνοούνται και από τους δύο. Τα σωστά μετρημένα bit αποτελούν το κλειδί που θα χρησιμοποιηθεί ως είσοδος για τον αλγόριθμο με τον οποίο θα κρυπτογραφηθεί ή θα αποκρυπτογραφηθεί το μήνυμα.

Σε περίπτωση που κάποιος τρίτος, προσπαθήσει να υποκλέψει το κλειδί, τότε πάλι εξαιτίας της αρχής της αβεβαιότητας, δε θα μπορέσει να χρησιμοποιήσει και τους 2 τρόπους για τις μετρήσεις. Αν υποθέσουμε ότι πραγματοποιεί τη μέτρηση με λάθος τρόπο, ακόμα κι αν αποστείλει στον παραλήπτη τα bit όπως ακριβώς τα μέτρησε, αναπόφευκτα θα εισαγάγει κάποια σφάλματα. Οι νόμιμοι παραλήπτης και αποστολέας έχουν τη δυνατότητα να ανακαλύψουν τυχόν απόπειρες υποκλοπής διαλέγοντας ορισμένα bit και συγκρίνοντάς τα προκειμένου να ανακαλύψουν τα σφάλματα.

8.2. Κβαντικός υπολογιστής

Κβαντικός υπολογιστής ονομάζεται μια υπολογιστική συσκευή που εκμεταλλεύεται χαρακτηριστικές ιδιότητες της κβαντομηχανικής, όπως η αρχή της υπέρθεσης και της διεμπλοκής καταστάσεων, προκειμένου να μπορέσει να επεξεργαστεί δεδομένα και να πραγματοποιήσει υπολογισμούς.

Σε έναν συμβατικό ψηφιακό υπολογιστή (κατά κανόνα ηλεκτρονικό), η στοιχειώδης μονάδα πληροφορίας είναι το bit, ενώ σε έναν κβαντικό υπολογιστή το qubit. Η βασική αρχή της κβαντικής υπολογιστικής επιστήμης είναι το γεγονός ότι οι κβαντομηχανικές ιδιότητες της ύλης μπορούν να χρησιμοποιηθούν για την αναπαράσταση και τη δόμηση των δεδομένων, καθώς επίσης μπορούν να επινοηθούν και να κατασκευαστούν μηχανισμοί βασισμένοι στη κβαντομηχανική για την επεξεργασία αυτών των δεδομένων.

8.2.1. Βασικές αρχές

Η μνήμη ενός συμβατικού ψηφιακού υπολογιστή αποτελείται από bit τα οποία αναπαριστούν την τιμή 0 ή 1. Ένα qubit μπορεί να αναπαραστήσει την τιμή 0, 1 ή οποιαδήποτε υπέρθεση αυτών των δύο. Δυο qubits είναι δυνατόν να αναπαραστήσουν οποιαδήποτε υπέρθεση τεσσάρων δυνατών καταστάσεων, τα 3 qubits οποιαδήποτε υπέρθεση 8 καταστάσεων κ.ο.κ. Γενικότερα, ένας κβαντικός υπολογιστής με n qubits μπορεί να βρίσκεται σε αυθαίρετη υπέρθεση των έως 2^n πιθανών καταστάσεων ταυτόχρονα, ενώ αντίθετα ο κλασικός υπολογιστής μπορεί να βρίσκετε μόνο σε μια από αυτές τις καταστάσεις κάθε στιγμή. Ο κβαντικός υπολογιστής λειτουργεί θέτοντας τα qubits σε μια ελεγχόμενη αρχική κατάσταση που αναπαριστά το αρχικό πρόβλημα και χειρίζεται τα qubits κάνοντας χρήση λογικών κβαντικών πυλών. Η αλληλουχία των πυλών που χρησιμοποιούνται αποκαλείται **κβαντικός αλγόριθμος.**

Υπάρχουν αρκετά κβαντικά συστήματα δύο καταστάσεων που μπορούν να χρησιμοποιηθούν ως qubits. Ένα παράδειγμα εφαρμογής των qubits σε έναν κβαντικό υπολογιστή θα ξεκινούσε χρησιμοποιώντας σωματίδια με δύο καταστάσεις περιστροφής (spin): πάνω και κάτω (τυπικά γράφεται $|\downarrow\rangle$ και $|\uparrow\rangle$, ή $|0\rangle$ και $|1\rangle$). Ενδεικτικά, η κατάσταση του spin ½ , μπορεί να θεωρηθεί ως qubit, όπου το spin - ½ αντιστοιχεί στη κατάσταση $|0\rangle$ και το spin + ½ στη κατάσταση $|1\rangle$. Γενικότερα, κβαντικό σύστημα μπορεί να θεωρηθεί ένα ατομικό ή υποατομικό σύστημα που διέπεται από τις αρχές της κβαντομηχανικής

8.2.2. Μειονεκτήματα – Πλεονεκτήματα

Πλεονεκτήματα

- Μεγάλη ταχύτητα
- Τεράστια μνήμη
- Απεριόριστη ισχύς
- Λύση πολλών σύνθετων προβλημάτων

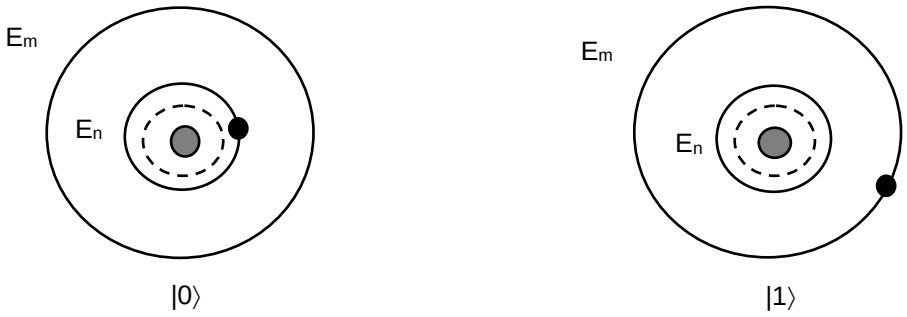
Μειονεκτήματα

- Δεν μπορούν να πραγματοποιήσουν όλα αυτά που κάνει ο σημερινός (συμβατικός) υπολογιστής όπως π.χ. επεξεργασία κειμένου ή web surfing). Είναι «εξειδικευμένοι» στην πολυεπεξεργασία δεδομένων.

- Έλλειψη κατάλληλων ανθεκτικών υλικών για την υλοποίηση της ιδέας του κβαντικού υπολογιστή. Τα μέχρι σήμερα υλικά, δεν είναι σε θέση να αντέξουν τις πολύ μεγάλες θερμοκρασίες που αναπτύσσονται λόγω των τεράστιων ταχυτήτων μεταφοράς δεδομένων, που έχει ως αποτέλεσμα τη μεγάλη «τριβή» των υλικών.
- Εξαιτίας της μεγάλης αλληλεπίδρασης των qubits με το περιβάλλον είναι δύσκολο να απομονωθούν αυτά τα υλικά και κατά συνέπεια να είναι λειτουργικά καθώς η αλληλεπίδραση των qubits με το περιβάλλον οδηγεί στη κατάρρευση της υπέρθεσης των καταστάσεων που περιγράφεται από μια κυματοσυνάρτηση την εξίσωση Schrodinger).

8.3. Η στοιχειώδης μονάδα κβαντικής πληροφορίας

Στο επιστημονικό πεδίο του κβαντικού υπολογισμού και στην τεχνολογία των ψηφιακών κβαντικών υπολογιστών, το κβαντικό bit ή το qubit (quantum bit) όπως συνηθίζεται να το αποκαλούν, αποτελεί τη στοιχειώδη μονάδα κβαντικής πληροφορίας.



Σχήμα 8.1: *Αναπαράσταση ενός qubit από δύο διακριτά ενεργειακά επίπεδα E_m και E_n σε ένα άτομο*

Για παράδειγμα, η πόλωση ενός φωτονίου μπορεί να αναπαραστήσει ένα qubit, όπου η οριζόντια πόλωση αντιστοιχεί στη κατάσταση |0⟩ και η κάθετη στη κατάσταση |1⟩. Όπως φαίνεται και στο παραπάνω σχήμα, ένα qubit είναι δυνατόν να αναπαρασταθεί κι από δύο ενεργειακά επίπεδα, E_m και E_n, σε ένα άτομο. Η παρουσία ενός ηλεκτρονίου με ενέργεια ίση με E_m αντιστοιχει στη κατάσταση |1⟩ και η παρουσία ενός ηλεκτρονίου με ενέργεια ίση με E_n αντιστοιχεί στη κατάσταση |0⟩.

Η διαφορά μεταξύ δυαδικού ψηφίου (bit) και του κβαντικού δυαδικού ψηφίου qubit είναι το ότι ενώ το πρώτο μπορεί να πάρει μόνο μια από τις δύο τιμές (είτε 0 είτε 1), το qubit αποτελεί μια υπέρθεση (άθροισμα) και των δύο καταστάσεων ταυτόχρονα.

1 qubit = $\alpha \bullet |1\rangle + b \bullet |0\rangle$ όπου: $|\alpha|^2 + |b|^2 = 1$ **(8.1)**

Οι δύο βασικές καταστάσεις του qubit μπορούν να αναπαρασταθούν και ως πίνακες:

$$|0\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \text{και} \quad |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

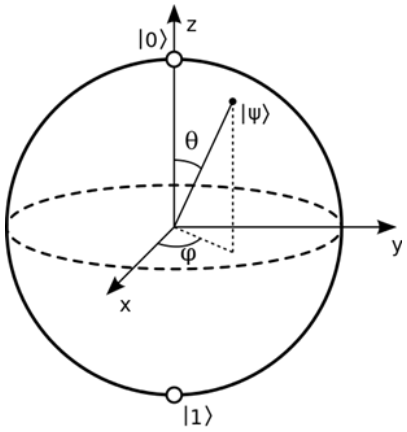
Οι αριθμοί α και b, που ονομάζονται ω ***πλάτη πιθανότητας***, είναι μιγαδικοί αριθμοί και το διάνυσμα κατάστασης $|\psi\rangle$ του qubit είναι ένα διάνυσμα στο χώρο Hlbert που έχει δύο διαστάσεις.

Μια χρήσιμη αναπαράσταση για το qubit, η οποία απεικονίσει σχεδόν όλα τα χαρακτηριστικά του, είναι η σφαίρα Bloch. Η σφαίρα Bloch έχει ακτίνα ίση με 1 και το διάνυσμα κατάστασης $|\psi\rangle$ του qubit, έχει την αρχή του στο κέντρο της σφαίρας και το τέλος του σε κάποιο σημείο στην επιφάνεια ττης σφαίρας. Επομένως το διάνυσμα $|\psi\rangle$ ισούτε με τη μονάδα.

Εφόσον λοιπόν τα πλάτη πιθανότητας *α* και *b* είναι μιγαδικοί αριθμοί, μπορούμε να γράψουμε την παραπάνω εξίσωση ως εξής:

$$|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\varphi}\sin(\theta/2)\,|1\rangle \qquad \textbf{(8.2)}$$

Όπου οι γωνίες *θ* και *φ* ανήκουν στους πραγματικούς αριθμούς και ορίζουν ένα σημείο της επιφάνειας της σφαίρας. Το σημείο αυτό είναι το τέλος του διανύσματος $|\psi\rangle$. Η γωνία θ καθορίζει τις τιμές των πλατών πιθανότητας. Η γωνία φ ονομάζεται ***γωνία φάσης.***



Εικόνα 8.1: *Μια αναπαράσταση qubit από μια σφαίρα Bloch*

8.3.1. Σύγκριση bits και qubits

Ένας υπολογιστής με έναν αριθμό qubits είναι εντελώς διαφορετικός από έναν συμβατικό ψηφιακό υπολογιστή με τον ίδιο αριθμό bits. Έστω, λοιπον, ότι θέλουμε να αναπαραστήσουμε την κατάσταση ενός συστήματος με n qubits σε έναν συμβατικό υπολογιστή θα χρειαστεί να αποθηκεύσουμε 2^n μιγαδικούς συντελεστες. Από αυτό καταλαβαίνουμε ότι τα qubits έχουν τη δυνατότητα να αποθηκεύσουν εκθετικά περισσότερη πληροφορία συγκριτικά με τα «απλά» bits, δε πρέπει όμως να ξεχνάμε ότι τα qubits είναι μια πιθανολογική υπέρθεση όλων των πιθανών καταστάσεών τους. Με άλλα λόγια, όταν μετρήσουμε την τελική τους κατάστση θα βρίσκονται μόνο σε έναν από τους πιθανούς σχηματισμούς που βρίσκονταν πριν τη μέτρηση.

Ενδεικτικά, έστω ένας συμβατικός υπολογιστής που λειτουργεί σε έναν καταχωρητή με 3 bits. Η κατάσταση του υπολογιστή οποιαδήποτε στιγμή είναι μια πιθανότητα κατανεμημμένη σε 2^3=8 διαφορετικές 3-bites ακολουθίες: 000, 001, 010, 011,100, 101, 110, 111. Στη περίπτωση που ο υπολογιστής είναι ντετερμινιστικός, θα πρέπει να βρίσκεται σε μια από αυτές καταστάσεις με πιθανότητα 1. Αν είναι πιθανολογικός, υπάρχει πιθανότητα να βρίσκεται σε μια πληθώρα καταστάσεων. Αυτή την πιθανολογική κατάσταση μπορούμε να την περιγράψουμε με οχτώ μη αρνητικούς αριθμούς A, B, C, D, E, F, G, H (όπου A=η πιθανότητα ο υπολογιστής να βρίσκεται στη κατάσταση 000, B= η πιθανότητα να βρίσκεται στη κατάσταση 001, κ.ο.κ). Το άθροισμα των πιθανοτήτων είναι 1.

Η κατάσταση ενός 3-bit-ου κβαντικού υπολογιστή περιγράφεται από ένα διάνυσμα με οχτώ διαστάσεις (a, b, c, d, e, f, g, h) που ονομάζεται **ket**. Αντί, όμως, το άθροισμά τους να είναι 1, πρέπει το τετράγωνο των συντελεστών $|\alpha|^2 + |b|^2 + |c|^2 + |d|^2 + |e|^2 + |f|^2 + |g|^2 + |h|^2$ να είναι 1. Το απόλυτο τετράγωνο των συντελεστών υποδηλώνει το πλάτος πιθανότητας των δοθέντων καταστάσεων, ενώ η φάση μεταξύ οποιονδήποτε δύο συντελεστών (καταστάσεις) αναπαριστά μια πολύ σημαντική παράμετρο, η οποία αποτελεί μια θεμελιώδη διαφορά ανάμεσα στους κβαντικούς υπολογιστές και τους πιθανολογικούς συμβατικούς υπολογιστές.

8.4. Κβαντικές πύλες και κυκλώματα

Η λειτουργία ενός κβαντικού υπολογιστή, θα πραγματοποιείται με κατάλληλους χειρισμούς πάνω στα κβαντοδυφία που συνιστούν τη μνήμη ή αλλιώς τον καταχωρητή του. Επειδή τα κβαντοδυφία είναι, ασφαλώς, κβαντικά αντικείμενα, ο χειρισμός τους, δηλαδή η πρόκληση επιθυμητών αλλαγών στη κατάστασή τους, θα επιτυγχάνεται με τις δύο μόνο διαδικασίες που προβλέπει η κβαντική θεωρία. Τη μοναδιαία εξέλιξη *μέσω της εξίσωσης Schrodinger* – που προκαλείται με την άσκηση κατάλληλων ηλεκτρομαγνητικών παλμών – καθώς επίσης και *τη διαδιακασία της μέτρησης.* Επειδή, όμως, η διαδικασία της μέτρησης, εκτός κάποιων εξαιρέσεων, πραγματοπιείται στο τέλος της υπολογιστικής διαδικασίας (και στοχεύει στην *ανάγνωση* του αποτελέσματος) οι δυνατοί χειρισμοί επί των κβαντοδυφίων θα πρέπει να είναι υποχρεωτικά μοναδιαίοι. Ο καθιερωμένος όρος γι' αυτές τις μοναδιαίες «πράξεις» είναι *κβαντικές πύλες* ή για τους κλασικούς υπολογιστές απλώς *πύλες*.

Οι κβαντικές πύλες εκτός από το ότι μιμούνται τη λειτουργία των απλών πυλών, δέχονται ως είσοδο qubits που βρίσκονται σε υπέρθεση. Επίσης, η κβαντική πληροφορία δεν διέρχεται μέσα από τις κβαντικές πύλες αλλά είναι αποθηκευμένη σε qubits ή σε κβαντικούς καταχωρητές και παραμένει εκεί.

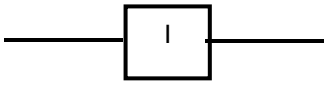
Ένα άλλο χαρακτηριστικό των κβαντικών πυλών είναι το ότι είναι αντιστρέψιμες. Δηλαδή, ως έξοδοι της μπορούν να δωθούν και πάλι οι αρχικοί είσοδοι. Αυτό θεωρείται απαραίτητο προκειμένου να διατηρηθεί η κβαντική κατάσταση. Ο αριθμός των εισόδων, πρέπει να είναι ίδιος με αυτών των εξόδων, έτσι ώστε οι πύλες να παραμείνουν αντιστρέψιμες.

Παρακάτω παρουσιάζεται μια λιστα με τις βασικές κβαντικές λογικές πύλες:

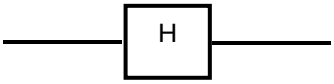
1. Κβαντική πύλη Hadamard
2. Κβαντική πύλη αδράνειας
3. Κβαντικές πύλες μετατόπισης φάσης
4. Ελεγχόμενες κβαντικές πύλες
    - Πύλη ελεγχόμενης άρνησης (CNOT)
    - Πύλη ελεγχόμενης μετατόπισης φάσης
    - Πύλη διπλά ελεγχόμενης άρνησης (CCNOT)
5. Pauli – X κβαντική πύλη
6. Pauli – Y κβαντική πύλη
7. Pauli – Z κβαντική πύλη
8. Κβαντική πύλη Fredkin
9. Κβαντική πύλη Toffoli

8.4.1. Πύλες που δρούν μόνο πάνω σε ένα κβαντοδυφίο

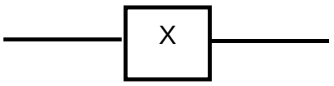
Οι πύλες αυτού του τύπου δρούν πάνω στις καταστάσεις ενός μόνο κβαντοδυφίου, δηλαδή στο δισδιάστατο χώρο διανυσμάτων α •|0⟩ + b • |1⟩. Παρακάτω απεικονίζονται το κυκλωματικό σύμβολο και το όνομα κάθε πύλης.

Μονάδα 

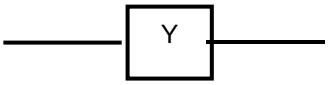
$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Hadamard 

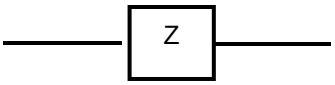
$$H = 1\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Pauli X 

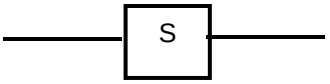
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Pauli Y 

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

Pauli Z 

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Φάση S 

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

Σχήμα 8.2: *Κυκλωματικό σύμβολο και όνομα κάθε πύλης*

8.4.2. Πύλες που δρουν σε δύο κβαντοδυφία

Η βασική πύλη αυτού του είδους είναι η Controlled–NOT ≡ CNOT και η δράση της πάνω σε μια τυχαία κατάσταση |x,y⟩ ≡ |x⟩ |y⟩ περιγράφεται από τις σχέσεις:

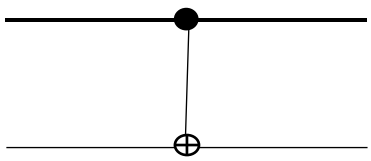
$$\mathrm{CNOT}\,|0\rangle\,|\mathrm{y}\rangle = |0\rangle\,|y\rangle, \qquad \textbf{(8.3)}$$

$$\mathrm{CNOT}\,|1\rangle\,|\mathrm{y}\rangle = |1\rangle\,|\bar{\mathrm{y}}\rangle \qquad \textbf{(8.4)}$$

Οι παραπάνω εξισώσεις μας πληροφορούν ότι στη περίπτωση που το πρώτο κβαντοδυφίο βρίσκετε στη κατάσταση |0⟩, η πύλη CNOT δε κάνει τίποτε στο δεύτερο, ενώ αν το πρώτο βρίσκεται στη κατάσταση |1⟩ η πύλη CNOT αναστρέφει το δεύτερο. Άρα το πρώτο κβαντοδυφίο αποτελεί το *κβαντοδυφίο ελέγχου* (control qubit) και το δεύτερο το *κβαντοδυφίο στόχος* (target qubit) και από το τρόπο λειτουργίας πήρε το όνομα της αυτή η πύλη. Ως προς τη αναπαράστασή της με τη μορφή μήτρας:

$$\mathrm{Wcnot}=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix} \qquad \textbf{(8.5)}$$

Ως προς τον κυκλωματικό συμβολισμό της, η πύλη CNOT διαφέρει από τις άλλες πύλες, αφού τα κβαντοδυφία που εμπλέκονται είναι δύο και επομένως απαιτούνται δύο ευθείες γραμμές αντί για ένα ευθύγραμμο τμήμα και το σύμβολο της πύλης στο κέντρο του.



Σχήμα 8.3: Κυκλωματικό σύμβολο της πύλης CNOT

όπου η βαρεία τελεία υποδηλώνει το κβαντοδυφίο ελέγχου και το «σταυρωμένο» κυκλάκι το κβαντοδυφίο στόχο.

ΚΕΦΑΛΑΙΟ 9Ο

9. ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΠΡΟΟΠΤΙΚΕΣ

9.1. Σύνοψη πτυχιακής εργασίας

Η κρυπτογράφηση και η Κρυπτανάλυση ασχολούνται με τη μελέτη, την ανάλυση, την ανάπτυξη αλλά και την επαλήθευση κρυπτογραφικών μεθόδων, τεχνικών, συστημάτων και πρωτοκόλλων. Από αυτές τις δύο επιστήμες συντίθεται το πεδίο της Κρυπτολογίας, ένας πολύ σπουδαίος τομέας στη προσπάθεια διασφάλισης απαιτήσεων όπως της εμπιστευτικότητας, της ακεραιότητας, της αυθεντικοποίησης και της αποποίησης. Οι κρυπτογραφικές εφαρμογές αποτελούν το πιο σημαντικό υπόβαθρο σε περιβάλλον δικτύων υπολογιστών για την υλοποίηση των μέτρων αντιμετώπισης επιθέσεων, όπως είναι η υποκλοπή ή η τροποποίηση δεδομένων, η παράνομη αναπαραγωγή ψηφιακών υπογραφών και η παραβίαση της ιδιωτικότητας στο ραγδαία αναπτυσσόμενο περιβάλλον της Κοινωνίας της Πληροφορίας. Στηριζόμενοι, λοιπόν, στην ανάγκη για επίτευξη όσο το δυνατόν μεγαλύτερης ασφάλειας, η σύγχρονη κρυπτογραφία εκμεταλλευόμενη τις αρχές της κβαντομηχανικής αλλά και τα πλεονεκτήματα που απορρέουν από αυτήν, πραγματοποιεί προσπάθειες για την υλοποίηση τόσο ασφαλέστερων όσο και ταχύτερων κβαντικών κρυπτογραφικών συστημάτων.

9.2. Προοπτικές

Η πτυχιακή αυτή θα μπορούσε να αποτελέσει βάση για τη συγγραφή τυχών μελλοντικών πτυχιακών εργασιών που το θέμα τους θα μπορούσε να είναι ενδεχομένως ένα από τα παρακάτω:

1. Εξέταση και ανάλυση επιθέσεων που έχουν προταθεί όπως RSA, Diffie – Hellman) και των μεθόδων προστασίας.
2. Εξέταση και ανάλυση επιθέσεων κατά συναρτήσεων διασποράς (Hash Functions).
3. Με τη χρήση βιβλιοθηκών σε Java να κατασκευαστεί μια Αρχή Πιστοποίησης (Certificate Authority – CA) η οποία θα εκδίδει και θα διαχειρίζεται ψηφιακά πιστοποιητικά.

References

[1] *Cryptography and Network Security.* (2015, 7 16). Ανάκτηση από University of Cyprus: Department of Computer Science: https://www.cs.ucy.ac.cy/

[2] *Faculty of Mathematics .* (2015, 7). Ανάκτηση από UNIVERSITY OF CAMBRIDGE: https://www.maths.cam.ac.uk/

[3] *Qubit*. (2015, 9). Ανάκτηση από ΒΙΚΙΠΑΙΔΕΙΑ: https://el.wikipedia.org/wiki/Qubit

[4] TANENBAUM, A. (2003). *Computer Networks,.* Amsterdam: The Netherlands: Pearson Education, Inc.

[5] Αλεξόπουλος, Αριστείδης; Λαγογιάννης Γεώργιος. (2003). *Τηλεπικοινωνίες και Δίκτυα Υπολογιστών.* Αθήνα.

[6] Άνδρέας Πομπότσης, Γ. Π. (2003). *Ασφάλεια Δικτύων Υπολογιστών. Τζιόλας, Α.*

[7] *Βασικές έννοιες της κρυπτογραφίας*. (2015, 6 22). Ανάκτηση από Εύδοξος: https://static.eudoxus.gr/

[8] Εργαζάκης, Δ. (2015, 4 14). *Βασικές εισαγωγικές αρχές κρυπτογραφίας.* Ανάκτηση από Communication Solutions: http://www.comsol.gr/

[9] Καλλονιάτης, Χ. (2015, 6 6). *Βασικά θέματα κρυπτογραφίας.* Ανάκτηση από Τμήμα Πολιτισμικής Τεχνολογίας & Επικοινωνίας Πανεπιστημίου Αιγαίου: http://www.ct.aegean.gr/index.php

[10] Καραφυλλίδης, Ι. (2005). *Κβαντικοί Υπολογιστές Βασικές Έννοιες.* Κλειδάριθμος.

[11] *Κβαντικοί Υπολογιστές*. (2015, 9). Ανάκτηση από Google: ttps://sites.google.com/site/icsdkvantikoiypologistes/home

[12] *Κβαντικός Υπολογιστής*. (2015, 10). Ανάκτηση από ΒΙΚΙΠΑΙΔΕΙΑ: https://el.wikipedia.org/wiki/Κβαντικός_υπολογιστής

[13] *Κλασσικές Τεχνικές Κρυπτογράφησης*. (2015, 10). Ανάκτηση από Skytal.es: https://skytal.es/wiki/Κλασικές_τεχνικές_κρυπτογράφησης

[14] *Κρυπτανάλυση*. (2015, 6). Ανάκτηση από ΒΙΚΙΠΑΙΔΕΙΑ: https://el.wikipedia.org/wiki/Κρυπτανάλυση

[15] *Κρυπτογραφία*. (2015, 6). Ανάκτηση από ΒΙΚΙΠΑΙΔΕΙΑ: https://el.wikipedia.org/wiki/Κρυπτογραφία

[16] Στέφανος., Τ. (2008). *ΚΒΑΝΤΟΜΗΧΑΝΙΚΗ ||. .* Πανεπιστηνιακές Εκδόσεις Κρήτης.

[17] Χειλάς. (2015, 5 4). *Κρυπτογραφία Δημόσιου Κλειδιού.* Ανάκτηση από Τ.Ε.Ι Κεντρικής Μακεδονίας (ΣΕΡΡΕΣ): http://www.teicm.gr/

[18] *Ψηφιακό Πιστοποιητικό*. (2015, 8). Ανάκτηση από ΒΙΚΙΠΑΙΔΕΙΑ: ttps://el.wikipedia.org/wiki/Ψηφιακό_πιστοποιητικό