



ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

Σχολή Τεχνολογίας

Τμήμα Ψηφιακών Συστημάτων

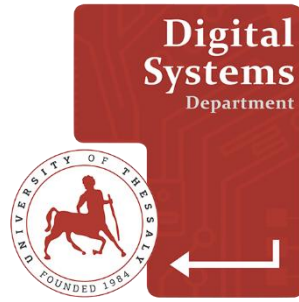
Αλγόριθμοι και εργαλεία Κρυπτογράφησης και Κρυπτανάλυσης

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Ονοματεπώνυμο: Ιωάννου Νικόλαος, ΑΜ3119086

Επιβλέπων: Ξενάκης Απόστολος, Επίκουρος Καθηγητής

ΛΑΡΙΣΑ, Μάρτιος 2025



UNIVERSITY OF THESSALY

School of Technology

Digital Systems Department

Algorithms and tools for Cryptography and Cryptanalysis

BACHELOR THESIS

Student Full Name: Ioannou Nikolaos, RN3119086

Supervisor: *Xenakis Apostolos, Assistant Professor*

LARISSA, March 2025

Υπεύθυνη Δήλωση περί Ακαδημαϊκής Δεοντολογίας και Πνευματικών Δικαιωμάτων

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ρητά ότι η παρούσα πτυχιακή εργασία, καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας, αποτελεί αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλει κάθε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχει έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον, και πληρούν τους κανόνες της επιστημονικής παράθεσης. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή.

Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο/Η Δηλών/ούσα

Ιωάννου Νικόλαος

5/3/2025

Εγκρίνεται από την Επιτροπή Εξέτασης:

Επιβλέπων/πουσα	Ξενάκης Απόστολος Επίκουρος Καθηγητής, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας
Μέλος Θεσσαλίας	Ηλίας Σάββας Καθηγητής, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο
Μέλος Πανεπιστήμιο Θεσσαλίας	Κωνσταντίνος Χαϊκάλης Αναπληρωτής Καθηγητής, Τμήμα Ψηφιακών Συστημάτων,

Ημερομηνία έγκρισης: 5/3/2025

Περίληψη

Η σημασία της ασφάλειας της επικοινωνίας και του απορρήτου ήταν πρωταρχικής σημασίας εδώ και πολύ καιρό. Τα άτομα έχουν αναζητήσει τη δυνατότητα να συνομιλούν χωρίς την κατανόηση τρίτων, είτε για προσωπικά, στρατιωτικά ή εμπορικά-οικονομικά κίνητρα. Η συγκεκριμένη εργασία μελετά το πλαίσιο των αλγορίθμων και των εργαλείων κρυπτογράφησης και κρυπτανάλυσης. Η εργασία διακρίνεται σε τέσσερα κεφάλαια: στην πλαισίωση της κρυπτογραφίας, στα εργαλεία κρυπτογράφησης και κρυπτανάλυσης, στη μελέτη του εργαλείου Cryptoool και στις ψηφιακές υπογραφές. Στόχος της συγκεκριμένης διπλωματικής εργασίας έγκειται η ανάδειξη της σημασίας της κρυπτογράφησης των δεδομένων.

Abstract

The importance of communication security and privacy has been of primary importance for a long time. Individuals have sought the ability to communicate without the understanding of third parties, whether for personal, military or commercial-economic motives. This specific work studies the framework of encryption and cryptanalysis algorithms and tools. The work is divided into four chapters: the framework of cryptography, encryption and cryptanalysis tools, the study of the Cryptool tool and digital signatures. The aim of this specific thesis is to highlight the importance of data encryption.

Περιεχόμενα

ΠΕΡΙΛΗΨΗ	VII
ABSTRACT.....	IX
1 ΕΙΣΑΓΩΓΗ.....	1
2 ΚΡΥΠΤΟΓΡΑΦΙΑ	3
2.1 ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ.....	6
2.2 ΚΡΥΠΤΟΓΡΑΦΙΚΑ ΣΧΗΜΑΤΑ ΚΑΙ ΒΑΣΙΚΕΣ ΣΥΝΑΡΤΗΣΕΙΣ	7
2.3 ΚΡΥΠΤΟΓΡΑΦΙΚΑ ΣΥΣΤΗΜΑΤΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ	14
2.4 ΜΟΝΤΕΛΑ ΑΠΕΙΛΗΣ	21
3 ΕΡΓΑΛΕΙΑ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΚΑΙ ΚΡΥΠΤΑΝΑΛΥΣΗΣ	25
3.1 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ	25
3.2 ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΚΩΔΙΚΟΠΟΙΗΣΗ.....	27
3.3 ΨΗΦΙΑΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ ΚΑΙ ΚΡΥΠΤΟΓΡΑΦΙΑ	29
3.4 ΟΡΙΣΜΟΙ ΤΟΥ ΚΡΥΠΤΟΓΡΑΦΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ	31
3.5 Η ΔΥΝΑΜΗ ΤΟΥ ΚΡΥΠΤΟΓΡΑΦΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ	33
3.6 ΚΡΥΠΤΑΝΑΛΥΣΗ	35
4 ΑΛΓΟΡΙΘΜΟΙ ΚΑΙ ΕΡΓΑΛΕΙΑ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΚΑΙ ΚΡΥΠΤΑΝΑΛΥΣΗΣ.....	37
4.1 ΕΠΙΘΕΣΕΙΣ ΕΝΑΝΤΙΑ ΣΤΟΥΣ ΑΛΓΟΡΙΘΜΟΥΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ	37
4.2 ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ	37
4.3 ΚΡΥΠΤΑΛΓΟΡΙΘΜΟΙ ΤΜΗΜΑΤΟΣ (BLOCK CIPHERS)	39
5 CRYPTOOOL.....	47
5.1 ΤΟ ΠΡΟΓΡΑΜΜΑ CRYPTOOOL	47
5.2 ΠΕΡΙΓΗΓΗ ΣΤΟ ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ CRYPTOOOL.....	48
5.3 ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ ΜΕ ΤΟ CRYPTOOOL 1	50
5.4 CRYPTOOOL 2.0 ΚΑΙ ΚΡΥΠΤΟΓΡΑΦΗΜΑ ΚΑΙΣΑΡΑ	52
5.5 ΥΒΡΙΔΙΚΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΚΑΙ ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ.....	54
6 ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ	59

6.1	ΣΥΝΑΡΤΗΣΕΙΣ ΚΑΤΑΚΕΡΜΑΤΙΣΜΟΥ Η ΚΑΤΑΤΕΜΑΧΙΣΜΟΥ Η ΚΑΤΑΤΜΗΣΗΣ (HASH FUNCTIONS).....	61
6.2	ΔΙΑΧΕΙΡΙΣΗ ΚΛΕΙΔΙΩΝ: ΠΑΡΑΓΩΓΗ ΚΑΙ ΔΙΑΝΟΜΗ	64
6.3	Η ΥΠΟΔΟΜΗ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ – PUBLIC KEY INFRASTRUCTURE	68
6.4	ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΥΔΚ.....	80
7	ΣΥΜΠΕΡΑΣΜΑΤΑ.....	83
	ΒΙΒΛΙΟΓΡΑΦΙΑ.....	87

1 Εισαγωγή

Η σημασία της ασφάλειας της επικοινωνίας και του απορρήτου ήταν πρωταρχικής σημασίας εδώ και πολύ καιρό. Τα άτομα έχουν αναζητήσει τη δυνατότητα να συνομιλούν χωρίς την κατανόηση τρίτων, είτε για προσωπικά, στρατιωτικά ή εμπορικά-οικονομικά κίνητρα. Αυτή η αναγκαιότητα έχει αναγνωριστεί, οδηγώντας τα περισσότερα έθνη να ενσωματώσουν το απόρρητο της αλληλογραφίας και των τηλεφωνικών συζητήσεων στους νόμους τους, επιβάλλοντας αυστηρές κυρώσεις σε όσους παραβιάζουν αυτό το απόρρητο. Ωστόσο, υπάρχει ένα στοιχείο αντίθεσης: άτομα που προσπαθούν να διακυβέυσουν το απόρρητο και να υποκλέψουν επικοινωνίες για δικό τους όφελος. Πράγματι, κατά τη διάρκεια του πολέμου, τέτοιες οντότητες συχνά εμπλέκονται τόσο στην ασφάλεια των επικοινωνιών τους, ενώ ταυτόχρονα προσπαθούν να υποκλέψουν αυτές των αντιπάλων τους. Η αφήγηση της ανθρώπινης ιστορίας σχετικά με τις επικοινωνίες ήταν, μέχρι αυτό το σημείο, μια συνεχής μάχη για την καθιέρωση πιο ασφαλών μεθόδων αλληλεπίδρασης, ενώ ταυτόχρονα επιδιώκεται να «σπάσει» τα υπάρχοντα συστήματα και να τα καταστήσει λιγότερο ασφαλή.

Ο όγκος των πληροφοριών που μοιράζονται σήμερα έχει αυξηθεί δραματικά, χάρη σε ένα ευρύτερο φάσμα μεθόδων επικοινωνίας που καλύπτουν ένα διευρυνόμενο φάσμα θεμάτων, με αποτέλεσμα μια άνευ προηγουμένου ζήτηση για ασφάλεια επικοινωνίας. Έχουν προκύψει πολυάριθμες νέες εφαρμογές, συμπεριλαμβανομένων των διαδικτυακών συστημάτων πληρωμών, των λύσεων αποθήκευσης cloud, των ψηφιακών υπογραφών και των εφαρμογών για τη διαχείριση ηλεκτρονικών καταστημάτων, οι οποίες χρησιμοποιούν ηλεκτρονική μετάδοση δεδομένων που ενδέχεται να υποκλαπούν από μη εξουσιοδοτημένα μέρη. Για την αντιμετώπιση αυτού του ζητήματος, χρησιμοποιούνται αλγόριθμοι κρυπτογράφησης για την ασφάλεια των δεδομένων που μεταδίδονται, καθιστώντας τα ακατανόητα σε όποιον προσπαθεί να αποκρυπτογραφήσει το νόημά τους.

Η συγκεκριμένη εργασία μελετά το πλαίσιο των αλγορίθμων και των εργαλείων κρυπτογράφησης και κρυπτανάλυσης. Η εργασία διακρίνεται σε τέσσερα κεφάλαια: στην παισίωση της κρυπτογραφίας, στα εργαλεία κρυπτογράφησης και κρυπτανάλυσης, στη μελέτη του εργαλείου Cryptool και στις ψηφιακές υπογραφές. Στόχος της συγκεκριμένης

διπλωματικής εργασίας έγκειται η ανάδειξη της σημασίας της κρυπτογράφησης των δεδομένων.

2 Κρυπτογραφία

Η πρακτική της «κρυφής γραφής», γνωστή ως κρυπτογραφία, μπορεί να υπερηφανεύεται για μια πλούσια ιστορία που εκτείνεται σε αιώνες, που προέρχεται από την εποχή που τα άτομα άρχισαν να χρησιμοποιούν γραπτή επικοινωνία για να κρύψουν το περιεχόμενο του μηνύματος από τους ξένους. Στα χρόνια της δημιουργίας της, η κρυπτογράφηση περιλάμβανε την αλλαγή ή την αναδιάταξη των συμβόλων γραφής με συγκεκριμένους τρόπους - τη δημιουργία ενός κώδικα για τη δημιουργία ενός μηνύματος που θα ήταν ακατανόητο - του κωδικοποιημένου μηνύματος. Η επιδίωξη της αποκρυπτογράφησης αυτού του κώδικα για την ανάκτηση του αρχικού μηνύματος αναφέρεται ως κρυπτανάλυση. Μαζί, η κρυπτογραφία και η κρυπτανάλυση αποτελούν το πεδίο της κρυπτολογίας (Stallings, 2017).

Ιστορικά, η κρυπτογραφία χρησίμευε ως εργαλείο για τους κατασκόπους, τους διπλωμάτες και το στρατιωτικό προσωπικό για να επικοινωνούν κρυφά, βασιζόμενοι σε χειρωνακτικές μεθόδους με μολύβι και χαρτί που απαιτούσαν σημαντική προσπάθεια κατά περίπτωση. Ωστόσο, τον περασμένο αιώνα, άρχισε να εξελίσσεται με την ανάπτυξη κρυπτογραφικών μηχανών, ιδίως το γερμανικής κατασκευής Enigma κατά τον Β' Παγκόσμιο Πόλεμο (Rijneveld, 2019). Μετά από αυτό, ο Alan Turing, αναγνωρισμένος ως ο πατέρας της επιστήμης των υπολογιστών, δημιούργησε τη μηχανή Bombe για να αποκρυπτογραφήσει τον κώδικα Enigma, ανοίγοντας το δρόμο για τον Colossus - την πρώτη προγραμματιζόμενη μηχανή ειδικά σχεδιασμένη για κρυπτανάλυση των κρυπτογραφικών συσκευών που χρησιμοποιήθηκαν σε αυτή τη σύγκρουση. Το 1949, ο Shannon καθιέρωσε τις θεμελιώδεις αρχές που μετέτρεψαν την κρυπτογραφία σε έναν αυστηρό επιστημονικό κλάδο εισάγοντας τις έννοιες του κρυπτοσυστήματος και της απόλυτης ασφάλειας, που προώθησαν σημαντικά την έρευνα στο πεδίο (Αριστείδης & Ζάχος, 2015).

Μετά από πολλά χρόνια, η ταχεία πρόοδος των ψηφιακών τεχνολογιών και η ευρεία εμβέλεια του Διαδικτύου έχουν μετατρέψει την κρυπτογραφία από ένα εργαλείο αποκλειστικά για στρατιωτική χρήση σε έναν πόρο διαθέσιμο σε όλους για ασφαλή επικοινωνία. Έχει εξελιχθεί από μια τέχνη που επικεντρώνεται στις δεξιότητες κωδικοποίησης σε μια επιστήμη που βασίζεται σε μαθηματικές μεθόδους, με ακριβείς

ορισμούς και αποδείξεις. Αυτός ο μετασχηματισμός σηματοδότησε μια σημαντική αλλαγή, ιδιαίτερα μετά το 1976, όταν οι Diffie και Hellman (1976) παρουσίασαν την επιδραστική εργασία τους «Νέες κατευθύνσεις στην κρυπτογραφία», εγκαινιάζοντας την εποχή της σύγχρονης κρυπτογραφίας.

Ο όρος απλό κείμενο περιγράφει το αρχικό μήνυμα, ενώ το κρυπτογραφημένο κείμενο υποδηλώνει την κωδικοποιημένη έκδοση. Η μετατροπή απλού κειμένου σε κρυπτογραφημένο κείμενο είναι γνωστή ως κρυπτογράφηση, ενώ η διαδικασία ανάκτησης απλού κειμένου από κρυπτογραφημένο κείμενο ονομάζεται αποκρυπτογράφηση. Οι μέθοδοι που χρησιμοποιούνται για την κρυπτογράφηση ονομάζονται κρυπτογραφικά συστήματα, κρυπτοσυστήματα ή κρυπτογράφηση. Οι κρυπτογραφικοί αλγόριθμοι αποτελούν τα στοιχεία αυτών των κρυπτογραφικών μηχανισμών. Τεχνικές που στοχεύουν στην αποκρυπτογράφηση μηνυμάτων χωρίς γνώση των ιδιοτήτων της κρυπτογράφησης εμπίπτουν στην κρυπτανάλυση, που συνήθως αναφέρεται ως «σπάσιμο του κώδικα». Στην κρυπτογραφία, το κλειδί υποδηλώνει το κοινό μυστικό που διέπει τις δυνατότητες τόσο για κρυπτογράφηση όσο και για αποκρυπτογράφηση, χρησιμεύοντας ως παράμετρος στον κρυπτογραφικό αλγόριθμο (Stallings, 2017).

Η ασφάλεια των επικοινωνιών εμπίπτει στην ευρύτερη κατηγορία της ασφάλειας πληροφοριών. Η ασφάλεια πληροφοριών ορίζεται ως «η προστασία των πληροφοριών και των πληροφοριακών συστημάτων από μη εξουσιοδοτημένη πρόσβαση, χρήση, αποκάλυψη, διακοπή, τροποποίηση ή καταστροφή με σκοπό την παροχή εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας» (National Institute of Standards and Technology, 2021).

Η εμπιστευτικότητα περιλαμβάνει τη διατήρηση του απορρήτου των πληροφοριών για να διασφαλιστεί ότι παραμένουν απρόσιτες σε μη εξουσιοδοτημένα άτομα. Η ακεραιότητα αφορά την προστασία των πληροφοριών από μη εξουσιοδοτημένες αλλοιώσεις, προστατεύοντάς τις από τη στιγμή της δημιουργίας τους, καθ' όλη τη διάρκεια της μεταφοράς τους και κατά την αποθήκευση. Η διαθεσιμότητα διασφαλίζει ότι οι εξουσιοδοτημένες οντότητες έχουν άμεση και αξιόπιστη πρόσβαση στις πληροφορίες.

Οι υπηρεσίες ασφαλείας παρέχουν τις απαραίτητες απαιτήσεις ασφάλειας, περιλαμβάνοντας διαδικασίες επεξεργασίας ή επικοινωνίας που έχουν σχεδιαστεί για να ενισχύσουν την προστασία του χειρισμού και της επεξεργασίας πληροφοριών. Αυτές οι

υπηρεσίες επικεντρώνονται στην άμυνα έναντι επιθέσεων από κακόβουλους χρήστες, με την κρυπτογραφία να χρησιμεύει ως κύρια τεχνική που χρησιμοποιείται για την προσφορά ή την ενίσχυση βασικών υπηρεσιών ασφαλείας, συμπεριλαμβανομένης της εμπιστευτικότητας, του ελέγχου ταυτότητας, του ελέγχου πρόσβασης και της μη άρνησης (Stallings, 2017).

Η διαδικασία που είναι γνωστή ως έλεγχος ταυτότητας διασφαλίζει τόσο την πηγή όσο και την ακεραιότητα των πληροφοριών κατά τη διάρκεια συνεδριών επικοινωνίας, μηνυμάτων, εγγράφων ή αποθηκευμένων δεδομένων, καθώς και την επιβεβαίωση της ταυτότητας οποιασδήποτε οντότητας που εμπλέκεται με ένα σύστημα. Αυτό οδηγεί στην εμφάνιση τριών κατηγοριών: πιστοποίηση πηγής, πιστοποίηση ταυτότητας και πιστοποίηση ακεραιότητας. Ο έλεγχος πρόσβασης περιλαμβάνει τον περιορισμό της πρόσβασης στους πόρους ενός συστήματος αποκλειστικά σε εξουσιοδοτημένες οντότητες. Εν τω μεταξύ, η εξουσιοδότηση αφορά την παροχή δικαιωμάτων πρόσβασης σε μια οντότητα, η οποία μεταφράζεται σε επίσημη έγκριση για την εκτέλεση μιας λειτουργίας ή μιας δραστηριότητας ασφαλείας.

Η προστασία έναντι της άρνησης ανάμειξης μιας οντότητας σε οποιαδήποτε ή όλες τις πτυχές της επικοινωνίας διασφαλίζεται με τη μη απόρριψη. Πρακτικά, τα πρωτόκολλα ασφαλείας χρησιμοποιούνται κατά την ψηφιακή επικοινωνία για την προστασία των πληροφοριών, χρησιμοποιώντας κρυπτογραφικούς μηχανισμούς που ενσωματώνουν κρυπτογραφικούς αλγόριθμους. Ένας κρυπτογραφικός αλγόριθμος είναι μια σαφώς καθορισμένη υπολογιστική διαδικασία που δέχεται πολλαπλές εισόδους, όπως το κρυπτογραφικό κλειδί, και δημιουργεί μια έξοδο (Stallings, 2017). Σε κάθε περίπτωση, ένας κρυπτογραφικός μηχανισμός παρέχει μια συγκεκριμένη υπηρεσία ασφαλείας.

Γενικά, οι κρυπτογραφικοί αλγόριθμοι και τα πρωτόκολλα μπορούν να ομαδοποιηθούν σε τέσσερις κύριες κατηγορίες (Stallings, 2017):

- Συμμετρική κρυπτογράφηση (Symmetric encryption): χρησιμοποιείται για την απόκρυψη των περιεχομένων τμημάτων (blocks) ή ροών (streams) δεδομένων οποιουδήποτε μεγέθους, συμπεριλαμβανομένων μηνυμάτων, αρχείων, κλειδιών κρυπτογράφησης και κωδικών πρόσβασης (passwords).
- Ασύμμετρη κρυπτογράφηση (Asymmetric encryption) ή Κρυπτογράφηση Δημόσιου Κλειδιού (Public Key Encryption – PKE): χρησιμοποιείται για την απόκρυψη μικρών τμημάτων δεδομένων, όπως η κρυπτογράφηση κλειδιών και

τιμές συναρτήσεων κατακερματισμού, οι οποίες χρησιμοποιούνται σε ψηφιακές υπογραφές.

- Αλγόριθμοι ακεραιότητας δεδομένων (Data integrity algorithms): Χρησιμοποιούνται για την προστασία τμημάτων δεδομένων από τροποποίηση.
- Πρωτόκολλα πιστοποίησης (Authentication protocols): Βασίζονται στη χρήση κρυπτογραφικών αλγορίθμων για την πιστοποίηση της ταυτότητας των οντοτήτων.

2.1 Βασικές έννοιες

Το πεδίο της θεωρίας υπολογισμών είναι ένα τμήμα των μαθηματικών που επικεντρώνεται στην αποτελεσματικότητα της επίλυσης προβλημάτων μέσω υπολογιστικών μοντέλων που χρησιμοποιούν αλγόριθμους. Γενικά, κατηγοριοποιείται σε δύο βασικούς τομείς: τη θεωρία υπολογισιμότητας, η οποία εξετάζει τις θεωρητικές δυνατότητες των υπολογιστών (δηλαδή, χωρίς περιορισμούς) και την υπολογιστική πολυπλοκότητα, η οποία διερευνά τους πρακτικούς περιορισμούς των υπολογιστών, όπως οι περιορισμοί χρόνου και χώρου (Yan, 2013).

Η θεωρία σκοπιμότητας, ένας κλάδος της θεωρίας πολυπλοκότητας, εστιάζει στις δυνατότητες και τους περιορισμούς των υπολογιστών που λειτουργούν εντός πολυωνυμικού χρόνου. Οι μηχανές Turing χρησιμεύουν ως θεωρητικό πλαίσιο για την προσομοίωση υπολογισμών. Αυτά τα μηχανήματα διαθέτουν μια κεφαλή που διασχίζει μια ταινία χωρισμένη σε δύο τετράγωνα. Ένας πεπερασμένος πίνακας περιγράφει την τρέχουσα κατάσταση του μηχανήματος και το τετράγωνο που σαρώνει, προσδιορίζοντας τις επόμενες ενέργειες του. Σε μια ντετερμινιστική μηχανή Turing, η μετάβαση από τη μια κατάσταση στην άλλη γίνεται με προβλέψιμο τρόπο, ακολουθώντας μια σαφώς καθορισμένη διαδρομή με βάση την τρέχουσα κατάστασή της, ενώ μια μη ντετερμινιστική μηχανή Turing έχει την ικανότητα να πλοηγείται σε πολλαπλά μονοπάτια (Barton, et al. ., 2019).

Όταν ένα πρόβλημα μπορεί να λυθεί σε πολυωνυμικό χρόνο, υποδηλώνει ότι η διάρκεια που απαιτείται για να βρεθεί μια λύση δεν υπερβαίνει μια πολυωνυμική συνάρτηση με βάση το μέγεθος της εισόδου του αλγορίθμου. Για παράδειγμα, ο χρόνος για μια σταθερή είσοδο είναι σταθερός. Η κατηγορία προβλημάτων που μπορούν να επιλυθούν σε πολυωνυμικό χρόνο από μια ντετερμινιστική μηχανή Turing αναφέρεται ως P (Πολύωνυμο). Τα προβλήματα σε αυτήν την κατηγορία θεωρούνται ως επιλύσιμα

(εφικτά) και σχετικά απλά στην επίλυση σε υπολογιστή (Barton, et al., 2019). Αντίθετα, η κατηγορία προβλημάτων που μια μη ντετερμινιστική μηχανή Turing μπορεί να λύσει σε πολυωνυμικό χρόνο είναι γνωστή ως NP (Non-deterministic Polynomial). Τα προβλήματα αυτής της κατηγορίας θεωρούνται δυσεπίλυτα και δύσκολα για να τα λύσει ένας υπολογιστής (Barton, et al., 2019).

Η κλάση NP περιλαμβάνει όλο το P, ωστόσο παραμένει αβέβαιο εάν αυτές οι δύο κατηγορίες μπορούν να συνυπάρχουν. Υπάρχει μια επικρατούσα πεποίθηση ότι το P δεν ισούται με το NP. Αυτό ισχύει ιδιαίτερα για προβλήματα που δεν μπορούν να επιλυθούν σε ντετερμινιστικό πολυωνυμικό χρόνο, που χρησιμεύουν ως βάση για την επιλογή τους σε κρυπτογραφικά σχήματα. Ωστόσο, είναι σημαντικό να αναγνωρίσουμε ότι η απουσία απόδειξης ότι ένα πρόβλημα είναι NP-σκληρό δεν σημαίνει ότι δεν είναι. Ως εκ τούτου, θα πρέπει να είναι κανείς προσεκτικός όταν κάνει τέτοιες υποθέσεις. Επιπλέον, ακόμα κι αν ένα πρόβλημα μπορεί να λυθεί σε πολυωνυμικό χρόνο, η πολυπλοκότητά του θα πρέπει να είναι τέτοια που θα απαιτεί ακόμα μια μη πρακτικά μεγάλη υπολογιστική διάρκεια (Barton, et al., 2019). Μεταξύ των NP-σκληρών προβλημάτων που χρησιμοποιούνται στη σύγχρονη κρυπτογραφία είναι το Πρόβλημα Παραγοντοποίησης Ακέραιου (IFP), το Πρόβλημα Διακριτού Λογαρίθμου (DLP) και το Πρόβλημα Διακριτού Ελλειπτικού Λογαρίθμου (ECDLP) (Stallings, 2017).

2.2 Κρυπτογραφικά Σχήματα και Βασικές Συναρτήσεις

Ένας βασικός στόχος της σύγχρονης κρυπτογραφίας είναι η διατήρηση της εμπιστευτικότητας των πληροφοριών κατά τις ψηφιακές ανταλλαγές. Όταν δύο μέρη επικοινωνούν μέσω ενός μη ασφαλούς καναλιού, είναι απαραίτητο να αποκρύψετε τα μηνύματα από ένα τρίτο μέρος—έναν μη εξουσιοδοτημένο, κακόβουλο χρήστη που μπορεί να έχει πρόσβαση στην επικοινωνία και να παρακολουθεί τα δεδομένα υποκλοπής του κρυπτογραφημένου κειμένου, το οποίο αναφέρεται σε έναν παθητικό υποκλοπή. Ο όρος "κανάλι επικοινωνίας" περιλαμβάνει σε γενικές γραμμές οποιαδήποτε ψηφιακή σύνδεση εντός δικτύων, συμπεριλαμβανομένου του Διαδικτύου, των τοπικών δικτύων και των δικτύων κινητής τηλεφωνίας. Στην ουσία, και τα δύο μέρη χρησιμοποιούν ένα κρυπτογραφικό σχήμα που βασίζεται σε ένα κλειδί—είτε δημόσιο μυστικό είτε ιδιωτικό κλειδί—για να διασφαλιστεί η εμπιστευτικότητά του.

Το κρυπτογραφικό κλειδί είναι μια μεταβλητή που είναι ξεχωριστή από το αρχικό μήνυμα και λειτουργεί παράλληλα με την κρυπτογραφική μέθοδο για να υπαγορεύσει

τον τρόπο λειτουργίας της. Αυτό επιτρέπει σε οποιονδήποτε έχει το κλειδί να το αναπαράγει, να το αντιστρέφει ή να το αλλάζει για να επιβεβαιώσει τη λειτουργία του αλγορίθμου, ενώ όσοι δεν διαθέτουν το κλειδί δεν μπορούν να εκτελέσουν αυτές τις ενέργειες.

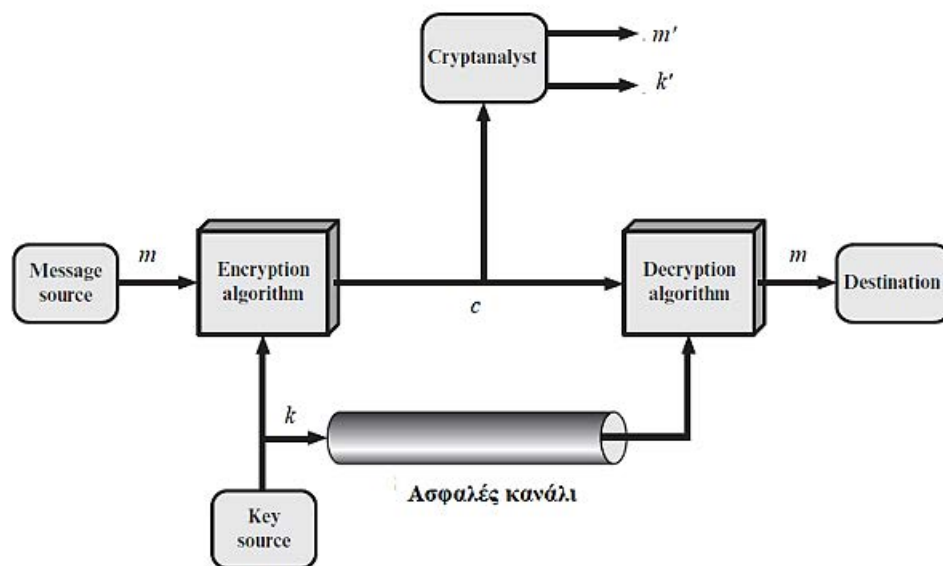
Τα κρυπτογραφικά συστήματα χαρακτηρίζονται από τρεις ανεξάρτητες διαστάσεις (Stallings, 2017):

1. Τον τύπο των λειτουργιών που χρησιμοποιούνται για την μετατροπή του αρχικού κειμένου σε κρυπτοκείμενο. Όλοι οι αλγόριθμοι κρυπτογράφησης βασίζονται σε δύο αρχές: την αντικατάσταση (substitution), όπου κάθε στοιχείο του αρχικού κειμένου αντιστοιχίζεται σε ένα άλλο στοιχείο και η μετάθεση ή μεταφορά (permutation ή transposition), όπου τα στοιχεία του αρχικού κειμένου αναδιατάσσονται. Τα περισσότερα σύγχρονα συστήματα χρησιμοποιούν διάφορα στάδια όπου εμπλέκονται και οι δύο τύποι και ονομάζονται κρυπτοσυστήματα γινομένου (product systems). Η βασική απαίτηση είναι να μη χαθεί οποιοδήποτε μέρος της πληροφορίας, δηλαδή όλες οι λειτουργίες να είναι αναστρέψιμες κατά την αποκρυπτογράφηση.
2. Τον αριθμό των κλειδιών που χρησιμοποιούνται. Στην περίπτωση της χρήσης ενός κλειδιού τα συστήματα χαρακτηρίζονται ως συμμετρικά, απλού κλειδιού, μυστικού κλειδιού ή συμβατικά συστήματα. Στην περίπτωση χρήσης δύο κλειδιών τα συστήματα χαρακτηρίζονται ως ασύμμετρα, δύο κλειδιών ή δημόσιου κλειδιού.
3. Τον τρόπο με τον οποίο γίνεται η επεξεργασία του αρχικού κειμένου. Ένα κρυπτοσύστημα τμήματος (block cipher) επεξεργάζεται την είσοδο ενός τμήματος της εισόδου παράγοντας ένα τμήμα εξόδου για κάθε τμήμα εισόδου. Ένα κρυπτοσύστημα ροής (stream cipher) επεξεργάζεται τα στοιχεία εισόδου συνεχόμενα, παράγοντας ως έξοδο ένα στοιχείο τη φορά.

Τα συστήματα της κλασσικής κρυπτογραφίας ήταν συμμετρικά και οι τρόποι για τη δημιουργία κώδικα βασιζόταν αποκλειστικά σε μεθόδους αντικατάστασης και μεταφοράς κυρίως των γραμμάτων του αλφάβητου σε κείμενα της φυσικής γλώσσας. Στην σύγχρονη κρυπτογραφία όλα τα σχήματα βασίζονται αυστηρά στη μαθηματική τεκμηρίωση με εργαλεία τη γραμμική άλγεβρα, τη θεωρία των πιθανοτήτων (και μάλιστα των διακριτών πιθανοτήτων), τη στατιστική, την αφηρημένη άλγεβρα (θεωρία των ομάδων), τη θεωρία των ακέραιων αριθμών, καθώς και στη θεωρία υπολογισμού, με

ιδιαίτερη έμφαση στην υπολογιστική πολυπλοκότητα. Κεντρικό ρόλο παίζει η (εκτιμώμενη) υπολογιστική δυσκολία αριθμοθεωρητικών και αλγεβρικών προβλημάτων και μάλιστα στην μέση περίπτωση. Οι λειτουργίες, τα κλειδιά και η επεξεργασία του αρχικού κειμένου βασίζονται σε μαθηματικές συναρτήσεις, υπολογισμούς και αλγόριθμους. Η σύγχρονη κρυπτογραφία χαρακτηρίζεται πλέον ως υπολογιστική κρυπτογραφία (Katz & Lindell, 2014).

Στη συμμετρική κρυπτογραφία τα δύο μέρη μοιράζονται το ίδιο κλειδί για την μυστική τους επικοινωνία. Το ένα μέρος στέλνει το μήνυμα στο άλλο χρησιμοποιώντας το μυστικό κλειδί για την κρυπτογράφηση και τη δημιουργία του κρυπτοκειμένου που μεταφέρεται στον παραλήπτη. Ο παραλήπτης αποκωδικοποιεί το κρυπτοκείμενο με το ίδιο κλειδί για να ανακτήσει το αρχικό μήνυμα, όπως φαίνεται στο παρακάτω σχήμα.



Εικόνα 1 Συμμετρικό κρυπτογραφικό σχήμα

Βασική απαίτηση για τη λειτουργία ενός συμμετρικού κρυπτοσυστήματος είναι ότι το κοινό κλειδί πρέπει να έχει προσυμφωνηθεί πριν την έναρξη της επικοινωνίας μεταξύ των δύο μερών, έτσι ώστε να δημιουργηθεί ένα ασφαλές κανάλι επικοινωνίας.

Τυπικά, ένα συμμετρικό κρυπτογραφικό σχήμα είναι μια τριάδα αλγορίθμων (KeyGen, Enc, Dec) που ορίζονται ως εξής (Katz & Lindell, 2014):

- Ο αλγόριθμος δημιουργίας κλειδιών KeyGen είναι ένας πιθανοτικός αλγόριθμος ο οποίος εξάγει ένα κλειδί k που επιλέγεται σύμφωνα με κάποια στατιστική κατανομή (distribution).

- Ο αλγόριθμος κρυπτογράφησης Enc δέχεται ως είσοδο ένα κλειδί k και ένα μήνυμα m και εξάγει ένα κρυπτοκείμενο c . Ως $\text{Enc}_k(m)$ δηλώνεται η κρυπτογράφηση του μηνύματος m χρησιμοποιώντας το κλειδί k .
- Ο αλγόριθμος αποκρυπτογράφησης Dec δέχεται ως είσοδο ένα κλειδί k και ένα κρυπτοκείμενο c και εξάγει το μήνυμα m . Ως $\text{Dec}_k(c)$ δηλώνεται η αποκρυπτογράφηση του κρυπτοκειμένου c χρησιμοποιώντας το κλειδί k .

Ένα σχήμα κρυπτογράφησης για να είναι ορθό, θα πρέπει για κάθε k που εξάγεται από τον KeyGen και για κάθε μήνυμα m θα πρέπει να ισχύει:

$$\text{Dec}_k(\text{Enc}_k(m)) = m.$$

Αυτό ουσιαστικά υποδηλώνει ότι όταν ένα μήνυμα κρυπτογραφείται και στη συνέχεια αποκρυπτογραφείται με το ίδιο κλειδί, πρέπει να παραχθεί το αρχικό μήνυμα. Η τέλεια ακρίβεια συνεπάγεται ότι το Dec λειτουργεί ντετερμινιστικά, διασφαλίζοντας ότι δεν υπάρχει απώλεια γενικότητας, καθώς παράγει με συνέπεια την ίδια έξοδο με κάθε εκτέλεση.

Ο χώρος μηνυμάτων αναφέρεται στη συλλογή μηνυμάτων που ορίζεται από το σχήμα, το οποίο είναι πεπερασμένο και τυπικά αντιπροσωπεύεται από το M , όπου $|M| > 1$, και κάθε μήνυμα συμβολίζεται ως $m \in M$. Ομοίως, ο χώρος των κλειδιών περιλαμβάνει όλες τις πιθανές εξόδους κλειδιών που παράγονται από τον αλγόριθμο KeyGen , επίσης πεπερασμένες, και συνήθως υποδεικνύονται με K , με κάθε κλειδί να αντιπροσωπεύεται ως $k \in K$. Συχνά, KeyGen απλά επιλέγει ένα ομοιόμορφο κλειδί από το K . Δεδομένου ότι ο αλγόριθμος KeyGen λειτουργεί πιθανολογικά, η έξοδος $\text{Enc}_k(m)$ ποικίλλει με κάθε εκτέλεση, με αποτέλεσμα ένα διαφορετικό κρυπτογραφημένο κείμενο c κάθε φορά που εκτελείται. Κατά συνέπεια, είναι συνήθης πρακτική να χρησιμοποιείται το σύμβολο $\leftarrow$ για να υποδηλώσει την έξοδο του αλγορίθμου. Επομένως, η έξοδος c του πιθανοτικού αλγορίθμου $\text{Enc}(m)$ εκφράζεται ως $c \leftarrow \text{Enc}(m)$. Αντίθετα, ένας ντετερμινιστικός αλγόριθμος αποδίδει την ίδια έξοδο κάθε φορά που εκτελείται. Σε τέτοιες περιπτώσεις, είναι σύνηθες να χρησιμοποιείται το σύμβολο $:=$ για να υποδείξει την έξοδο του αλγορίθμου.

Το σύνολο των τιμών που παράγονται ως εξοδοί από το $\text{Enc}_k(m)$ για κάθε πιθανή επιλογή του k από το K και του m από το M (μαζί με όλες τις τυχαίες επιλογές του Enc λόγω της πιθανολογικής του φύσης) ορίζει τον χώρο κρυπτογραφημένου κειμένου, ο οποίος είναι επίσης πεπερασμένος. Είναι προφανές από την προηγούμενη συζήτηση ότι εάν ένας υποκλοπής έχει γνώση του αλγορίθμου Dec και του μυστικού κλειδιού k που μοιράζονται

τα μέρη που επικοινωνούν, θα έχουν τη δυνατότητα να αποκρυπτογραφήσουν οποιοδήποτε κρυπτογραφημένο κείμενο. Κατά συνέπεια, είναι σημαντικό για τα μέρη να μοιράζονται με ασφάλεια το κλειδί, διασφαλίζοντας ότι παραμένει εμπιστευτικό από όλους τους άλλους. Τον 19ο αιώνα, ο Kerckhoffs καθιέρωσε μια αρχή που συνεχίζει να στηρίζει το σχεδιασμό των κρυπτογραφικών συστημάτων: «η ασφάλεια ενός συστήματος πρέπει να βρίσκεται μόνο στο απόρρητο του κλειδιού και να μην εξαρτάται από τη γνώση του αλγόριθμου κρυπτογράφησης» (Αριστείδης & Ζάχος, 2015).

Στην εφαρμογή, οι ακολουθίες byte αποτελούν κλειδιά, μηνύματα και κρυπτογραφημένα κείμενα. Συνήθως, τα πλήκτρα έχουν καθορισμένο μήκος, ενώ τα μηνύματα και τα κρυπτογραφημένα κείμενα μπορεί να διαφέρουν σε μήκος ή να είναι σταθερά. Επιπλέον, τα κλειδιά, τα μηνύματα και τα κρυπτογραφημένα κείμενα μπορούν να λάβουν άλλες μαθηματικές μορφές, συμπεριλαμβανομένων ακεραίων ή πιο περίπλοκων τύπων όπως πίνακες, πολυώνυμα ή στοιχεία ομάδας. Ανεξάρτητα από τον τύπο τους, τελικά αναπαρίστανται ως ακολουθίες byte.

Το κρυπτόςυστημα που συζητήθηκε προηγουμένως αποτυγχάνει να εξασφαλίσει την ακεραιότητα του μηνύματος. Εάν ένας εισβολέας μπορεί να αλλάξει τα bit του κρυπτογραφημένου κειμένου - υποδεικνύοντας ενεργή παρά παθητική συμμετοχή - ο παραλήπτης ενδέχεται να μην γνωρίζει ότι το ληφθέν μήνυμα διαφέρει από το αρχικό. Επιπλέον, οι ταυτότητες των μερών που επικοινωνούν δεν επαληθεύονται, γεγονός που καθιστά αναγκαία τη χρήση διαφορετικών κρυπτογραφικών μεθόδων, όπως Κωδικοί ελέγχου ταυτότητας μηνυμάτων (MAC) (Katz & Lindell, 2014), και στα δύο σενάρια.

Δεν θα εμβαθύνουμε σε συγκεκριμένες λεπτομέρειες σχετικά με τις άλλες δύο πτυχές του διαχωρισμού των συμμετρικών κρυπτογραφικών συστημάτων, δηλαδή τις λειτουργίες που χρησιμοποιούνται για τη μετατροπή του αρχικού κειμένου σε κρυπτογραφημένο κείμενο και τη μέθοδο επεξεργασίας για το αρχικό κείμενο, καθώς αυτές ξεφεύγουν από το σκοπό αυτής της εργασίας. Αξίζει να σημειωθεί ότι η συμμετρική κρυπτογραφία βασίζεται σε ψευδοτυχαίες συναρτήσεις και μεταθέσεις και μπορεί να εφαρμοστεί πρακτικά χρησιμοποιώντας κρυπτοσυστήματα θραυσμάτων με προκαθορισμένο κλειδί και μήκος θραύσματος.

Το Advanced Encryption Standard (AES) είναι το πιο αναγνωρισμένο συμμετρικό κρυπτογραφικό σχήμα που τυποποιείται από το NIST, το οποίο χρησιμοποιείται εκτενώς σε διάφορες εφαρμογές και πρωτόκολλα ασφαλείας παγκοσμίως. Αυτό το πρότυπο περιγράφει τον αλγόριθμο του Rijndael, μια μέθοδο κρυπτογράφησης τμημάτων ικανή

να επεξεργάζεται τμήματα δεδομένων 128 bit ενώ χρησιμοποιεί μήκη κλειδιών 128, 192 και 256 bit. Κατά συνέπεια, υπάρχουν τρεις παραλλαγές: AES-128, AES-192 και AES-256. Το AES λειτουργεί μέσω της επαναλαμβανόμενης εκτέλεσης απλών κύκλων που περιλαμβάνουν μεταθέσεις κλειδιών, μεταθέσεις και προσθήκες.

Ένα θεμελιώδες στοιχείο της σύγχρονης κρυπτογραφίας είναι η μονόδρομη λειτουργία. Ουσιαστικά, αυτή η συνάρτηση μπορεί να υπολογιστεί εύκολα. Ωστόσο, όταν παρέχεται με μια είσοδο, η οποία συχνά αναφέρεται ως εικόνα, η αναστροφή της αποδεικνύεται μια πρόκληση. Θα πρέπει να σημειωθεί ότι αυτό ισχύει γενικά και μπορεί να υπάρχει κάποιος αριθμός εικόνων που είναι εύκολο να αντιστραφούν. Ο ορισμός της μονόδρομης συνάρτησης τυπικά δίνεται ως εξής (Rijneveld, 2019):

Μια συνάρτηση $f: \{0, 1\}^* \rightarrow \{0, 1\}^*$ ονομάζεται μονόδρομη εάν ισχύει:

- Δοθέντος ενός $x \in \{0, 1\}^*$, υπάρχει ένας αλγόριθμος πολυωνυμικού χρόνου για τον υπολογισμό της $f(x)$.
- Για κάθε πιθανοτικό αλγόριθμο πολυωνυμικού χρόνου A , δοθείσης της $f(x)$ για μια τυχαία επιλογή του $x \in \{0, 1\}^{\text{poly}(k)}$, τρέχοντας τον A με είσοδο $f(x)$, η πιθανότητα εύρεσης οποιουδήποτε $x' \in \{0, 1\}^*$ έτσι ώστε $f(x) = f(x')$ είναι αμελητέα στο k .

Ένα άλλο σημαντικό δομικό στοιχείο της σύγχρονης κρυπτογραφίας που βασίζεται στην ιδέα της μονόδρομης συνάρτησης και με ευρεία χρήση σε πολλά κρυπτογραφικά σχήματα και πρωτόκολλα είναι οι συναρτήσεις κατακερματισμού (hash functions). Οι συναρτήσεις κατακερματισμού χρησιμοποιούνται σε περιπτώσεις που χρειάζεται να διασφαλιστεί η ακεραιότητα των δεδομένων. Οι κρυπτογραφικές συναρτήσεις κατακερματισμού χρησιμοποιούνται συνήθως ως συνιστώσες ενός άλλου κρυπτογραφικού σχήματος.

Οι κρυπτογραφικές συναρτήσεις κατακερματισμού που χρησιμοποιούνται στην πράξη, δέχονται ως είσοδο ένα μήνυμα και παράγουν μια συντμημένη μορφή στην έξοδο με καθορισμένο μήκος k που ονομάζεται τιμή κατακερματισμού (hash value) ή σύνοψη μηνύματος (message digest) ή απλά σύνοψη. Συνήθως δημιουργούνται χωρίς κλειδιά, και συμβολίζονται ως $H: \{0, 1\}^* \rightarrow \{0, 1\}_k$.

Υπάρχουν τρία υπολογιστικά προβλήματα που σχετίζονται τις κρυπτογραφικές συναρτήσεις κατακερματισμού.

1. Η σύγκρουση (collision): Να βρεθούν x, x' τέτοια ώστε εάν $x \neq x'$, $H(x) = H(x')$

2. Η προ-εικόνα (pre-image) – αναφέρεται και ως πρώτο όρισμα: Δοθείσης της $H(x)$ να βρεθεί το x .
3. Η δεύτερη προ-εικόνα (second pre-image) – αναφέρεται και ως δεύτερο όρισμα:

Δοθέντων των $H(x)$ και x , να βρεθούν $x \neq x'$ τέτοια ώστε $H(x) = H(x')$.

Σε πολλές εφαρμογές, είναι προτιμότερο να μειωθούν οι συγκρούσεις για να διασφαλιστεί ότι κάθε είσοδος αντιστοιχίζεται σε μια μοναδική έξοδο. Ο σχεδιασμός της συνάρτησης κατακερματισμού ποικίλλει ανάλογα με την προβλεπόμενη χρήση της. Για παράδειγμα, εάν ο στόχος είναι να δημιουργηθεί ένα σχήμα που απλώς αντιστέκεται στις συγκρούσεις, μια συνάρτηση που πληροί την προϋπόθεση της αντίστασης του δεύτερου ορίσματος θα αρκεί (Rijneveld, 2019).

Τυποποιημένες από το NIST, οι συναρτήσεις κατακερματισμού έχουν γίνει διεθνή αποδοχή, με την τελευταία οικογένεια να είναι το SHA-3 (Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας, 2015). Οι τέσσερις συναρτήσεις κατακερματισμού εντός της οικογένειας SHA-3 ορίζονται ως SHA3-224, SHA3-256, SHA3-384 και SHA3-512, όπου το επίθημα υποδηλώνει το προεπιλεγμένο μήκος εξόδου. Η οικογένεια SHA-2, η οποία περιλαμβάνει SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 και SHA-512/256, παράγει ισοδύναμα μήκη εξόδου, επιτρέποντας την εναλλάξιμη χρήση του SHA-3 συναρτήσεις κατακερματισμού με αυτές του SHA-2 και αντίστροφα.

Η εισαγωγή του προτύπου φέρνει στο προσκήνιο την έννοια μιας επεκτάσιμης-εξόδου συνάρτησης (XOF), η οποία λειτουργεί σε συμβολοσειρές bit, γνωστές επίσης ως μηνύματα, επιτρέποντας στην έξοδο να επεκταθεί σε οποιοδήποτε μήκος επιθυμείτε. Τα δύο XOF εντός του SHA-3 χαρακτηρίζονται ως SHAKE128 και SHAKE256, με τους αριθμούς 128 και 256 να αντιπροσωπεύουν τις αντίστοιχες δυνάμεις ασφαλείας τους, ένα θέμα που θα επεξεργαστούμε στην επόμενη παράγραφο. Σύμφωνα με τον Rijneveld (2019), ο ορισμός μιας κλιμακούμενης συνάρτησης εξόδου (XOF) $H: \{0, 1\}^* \rightarrow \{0, 1\}^*$ είναι ότι πληροί τις προϋποθέσεις ως κλιμακούμενη συνάρτηση εξόδου εάν $H': \{0, 1\}^* \rightarrow \{0, 1\}^l$, που προκύπτει με περικοπή H , διατηρεί αντίσταση σύγκρουσης τόσο στο πρώτο όσο και στο δεύτερο όρισμα για κάθε έξοδο μήκους l .

Οι έξι αλγόριθμοι SHA-3 είναι κατασκευασμένοι για να διασφαλίζουν μοναδικά χαρακτηριστικά όπως αντίσταση σε συγκρούσεις, μαζί με αντίσταση πρώτου και δεύτερου ορίσματος.

2.3 Κρυπτογραφικά Συστήματα Δημόσιου Κλειδιού

Στις σύγχρονες επικοινωνίες που περιλαμβάνουν εκατομμύρια οντότητες, η εφαρμογή της συμμετρικής κρυπτογραφίας αντιμετωπίζει σημαντικές προκλήσεις που σχετίζονται με τη διανομή κλειδιών. Όταν χρησιμοποιείται ένα συμμετρικό σύστημα κρυπτογράφησης, είναι απαραίτητο για τα μέρη που επικοινωνούν είτε να έχουν προηγουμένως μοιραστεί ένα κοινό μυστικό κλειδί είτε να βασίζονται σε ένα κέντρο διανομής κλειδιών. Αυτή η κατάσταση υποδηλώνει έναν συμβιβασμό στην απόλυτη μυστικότητα που είναι θεμελιώδης για την κρυπτογραφία. Ένα συγκεκριμένο ζήτημα προκύπτει όταν υπάρχει ανάγκη δημιουργίας και ανταλλαγής εφήμερων κλειδιών που σχετίζονται με μια συνεδρία επικοινωνίας, ενώ ταυτόχρονα απαιτείται έλεγχος ταυτότητας της πηγής (Stallings, 2017).

Στην εργασία τους του 1976 "Πολλαπλοί Κρυπτογραφικές Τεχνικές", οι Diffie και Hellmann καθιέρωσαν τα κριτήρια για ένα σύστημα ανταλλαγής κρυπτογραφικών κλειδιών, το οποίο στη συνέχεια επηρέασε την κρυπτογράφηση δημόσιου κλειδιού (PKC), αν και δεν παρείχαν πρακτική εφαρμογή. Δύο χρόνια αργότερα, το 1978, ο Rivest και η ομάδα του εισήγαγαν την πρώτη βιώσιμη μέθοδο για την εκτέλεση κρυπτογραφικών συστημάτων δημόσιου κλειδιού στην εργασία τους με τίτλο "Μία μέθοδος για την απόκτηση ψηφιακών υπογραφών και κρυπτοσυστημάτων δημόσιου κλειδιού", η οποία βασίστηκε στις προκλήσεις που σχετίζονται με την επίλυση του Πρόβλημα παραγοντοποίησης ακεραίων (Integer Factorization Problem - IFP) (Rivest, et al., 1978). Ο Merkle, ο οποίος επίσης ανέπτυξε μια παρόμοια ιδέα, δημοσίευσε τα ευρήματά του αργότερα το 1979 (Merkle, 1979).

Το αρχικό σύστημα ψηφιακών υπογραφών που βασίστηκε σε υπογραφές με βάση το κατακερματισμό (HBS) εισήχθη από τη Lamport το 1979, σηματοδοτώντας την αρχή καινοτόμων τεχνικών. Μετά από αυτό, ο Elgamal πρότεινε κρυπτοσυστήματα που βασίζονται σε DLP σε πεπερασμένα πεδία το 1985, ενώ οι Miller και Koblitz προχώρησαν αργότερα στον τομέα προτείνοντας την εφαρμογή της κρυπτογραφίας ελλειπτικών καμπυλών (ECC) σε πεπερασμένα πεδία το 1985 και το 1987, αντίστοιχα. Αυτή η πρόοδος στην κρυπτογραφία δημόσιου κλειδιού (PKC) συνέβαλε σημαντικά στην ανάπτυξη της ασφάλειας του Διαδικτύου. Επιπλέον, είναι σημαντικό να αναφέρουμε ότι ο McEliece είχε ήδη παρουσιάσει ένα σύστημα PKC με τις ρίζες του στη θεωρία των αλγεβρικών κωδίκων (κρυπτογραφία με βάση τον κώδικα) το 1978, αν και δεν είδε ουσιαστική πρόοδο κατά τη διάρκεια αυτών των ετών.

Είναι σημαντικό να τονιστεί ότι η συμμετρική κρυπτογραφία δεν καταργείται από την PKC. Αντίθετα, αντιμετωπίζει τις προκλήσεις του. Από το 1988, οι Diffie και Hellmann υποστήριξαν ότι αν και η χρήση του PKC είναι απαραίτητη, η εφαρμογή του θα πρέπει να περιοριστεί σε σενάρια που περιλαμβάνουν ανταλλαγή κλειδιών και ψηφιακές υπογραφές, υποστηρίζοντας υβριδικά συστήματα που ενσωματώνουν μεθόδους και από τις δύο κατηγορίες.

Στο PKC, η ασφαλής επικοινωνία μεταξύ δύο μερών περιλαμβάνει τη δημιουργία ενός ζεύγους κλειδιών από κάθε οντότητα: ένα δημόσιο κλειδί, που δηλώνεται ως pk , το οποίο διανέμεται ευρέως, και ένα ιδιωτικό ή μυστικό κλειδί, που αναφέρεται ως sk , που παραμένει εμπιστευτικό. Η παρουσία αυτών των δύο κλειδιών εισάγει ασυμμετρία στο σχήμα, οδηγώντας στον εναλλακτικό χαρακτηρισμό του ως ασύμμετρη κρυπτογραφία, με τα αντίστοιχα συστήματα να ονομάζονται επίσης ασύμμετρα σχήματα. Ανάλογα με τη συγκεκριμένη περίπτωση χρήσης, μετά τη δημιουργία των κλειδιών, ο αποστολέας μπορεί να χρησιμοποιήσει το δικό του ιδιωτικό κλειδί, το δημόσιο κλειδί του παραλήπτη ή και τα δύο για να εκτελέσει μια κρυπτογραφική λειτουργία. Κατά συνέπεια, η κρυπτογραφία δημόσιου κλειδιού εξυπηρετεί διάφορους σκοπούς, συμπεριλαμβανομένης της κρυπτογράφησης/αποκρυπτογράφησης για υπηρεσίες ασφάλειας εμπιστευτικότητας, των ψηφιακών υπογραφών για τις υπηρεσίες ασφαλείας ελέγχου ταυτότητας και της ανταλλαγής κλειδιών (Stallings, 2017).

Αν και η συμμετρική κρυπτογραφία βασίζεται σε ψευδοτυχαίες συναρτήσεις και μεταθέσεις και μπορεί να εφαρμοστεί πρακτικά μέσω κοινόχρηστων κρυπτοσυστημάτων ή δομών που περιλαμβάνουν συναρτήσεις μονής κατεύθυνσης και κατακερματισμού, η κρυπτογραφία δημόσιου κλειδιού προσθέτει ένα νέο επίπεδο στην υπολογιστική κρυπτογραφία, ανάλογα αποκλειστικά με αριθμητικά προβλήματα που θεωρούνται υπολογιστικά μη πρακτικά (Katz & Lindell, 2014).

Οι Diffie και Hellmann (1976), έστω και εάν δεν παρουσίασαν ένα πρακτικό σύστημα, έθεσαν τις απαιτήσεις για τους αλγόριθμους της PKC:

- Είναι υπολογιστικά εύκολο για τον παραλήπτη B να δημιουργήσει το ζεύγος κλειδιών (pk , sk).
- Είναι υπολογιστικά εύκολο για τον αποστολέα, γνωρίζοντας το δημόσιο κλειδί pk και το μήνυμα m που πρέπει να κρυπτογραφηθεί να δημιουργήσει το σχετικό κρυπτοκείμενο c .

- Ο παραλήπτης μπορεί εύκολα να αποκρυπτογραφήσει το κρυπτογραφημένο κείμενο c με το ιδιωτικό κλειδί sk για να ανακτήσει το αρχικό μήνυμα m .
- Για έναν αντίπαλο που γνωρίζει το δημόσιο κλειδί pk , η ανάκτηση του ιδιωτικού κλειδιού sk είναι υπολογιστικά μη πρακτική.
- Ομοίως, είναι υπολογιστικά ανέφικτο για έναν αντίπαλο με πρόσβαση στο δημόσιο κλειδί pk και στο κρυπτογραφημένο κείμενο c να λάβει το αρχικό μήνυμα m .

Η βάση των κρυπτογραφικών σχημάτων δημόσιου κλειδιού βρίσκεται στις μονόδρομες συναρτήσεις *trapdoor*, οι οποίες είναι δύσκολο να αναστραφούν εκτός εάν είναι διαθέσιμο ένα συγκεκριμένο μυστικό, γνωστό ως *trapdoor* (Stallings, 2017). Ουσιαστικά, αυτό που απαιτείται είναι μια μαθηματική πράξη που επιτρέπει την απλή εκτέλεση προς μία κατεύθυνση -κρυπτογράφηση- ενώ καθιστά αδύνατη την εκτέλεση προς την αντίθετη κατεύθυνση -αποκρυπτογράφηση- χωρίς πρόσβαση σε μια εμπιστευτική πληροφορία, δηλαδή το ιδιωτικό κλειδί.

Υπάρχουν πολυάριθμες πιθανές μονόδρομες συναρτήσεις, συμπεριλαμβανομένης της παραγοντοποίησης ακεραίων και του υπολογισμού διακριτών λογαρίθμων. Ωστόσο, αυτές οι συναρτήσεις είναι υπολογιστικά μονόδρομες, πράγμα που σημαίνει ότι με επαρκή υπολογιστική ισχύ, ένα άτομο μπορεί να τις αντιστρέψει πιο γρήγορα από ό,τι μέσω της εξαντλητικής αναζήτησης (Αριστείδης & Ζάχος, 2015).

Στα κρυπτοσυστήματα δημόσιου κλειδιού, το κλειδί κρυπτογράφησης αντιπροσωπεύεται από ένα δημόσιο κλειδί που παράγεται από μια συγκεκριμένη οντότητα. Όποιος γνωρίζει το δημόσιο κλειδί του παραλήπτη μπορεί να το χρησιμοποιήσει για την κρυπτογράφηση μηνυμάτων, με αποτέλεσμα τη δημιουργία των αντίστοιχων κρυπτογραφημένων κειμένων. Το κλειδί αποκρυπτογράφησης αντιπροσωπεύεται από το ιδιωτικό κλειδί, το οποίο χρησιμοποιείται από την οντότητα που το κατέχει για την ανάκτηση του αρχικού μηνύματος από οποιοδήποτε κρυπτογραφημένο κείμενο που δημιουργείται με το συσχετισμένο δημόσιο κλειδί. Αυτή η μέθοδος διασφαλίζει ότι διατηρείται η εμπιστευτικότητα των κρυπτογραφημένων μηνυμάτων, ακόμη και με την παρουσία ενός αντιπάλου που γνωρίζει το κλειδί κρυπτογράφησης αλλά δεν έχει πρόσβαση στο κλειδί αποκρυπτογράφησης.

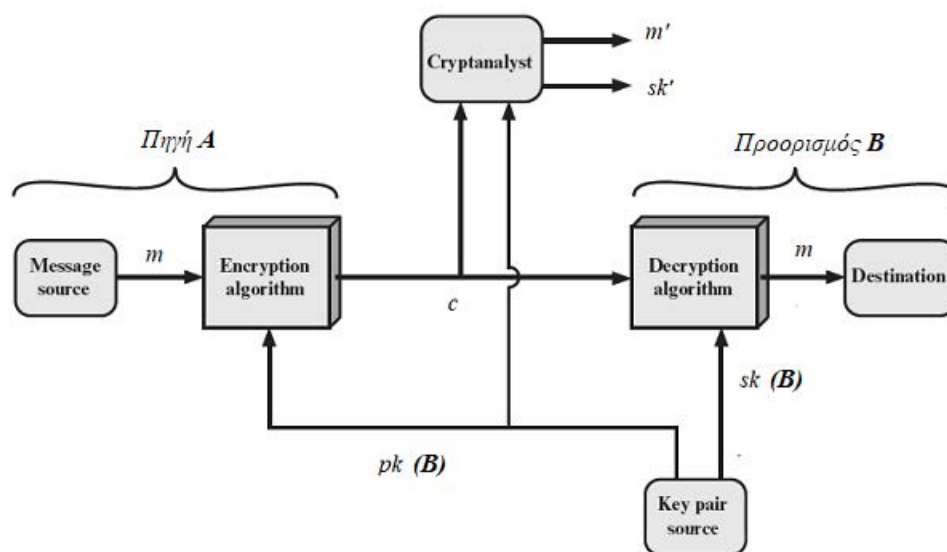
Ένα σχήμα κρυπτογράφησης δημόσιου κλειδιού (PKE), όπως ορίστηκε από τον Rijneveld το 2019, αποτελείται συνήθως από τρεις αλγόριθμους: KeyGen, Enc και Dec. Ο αλγόριθμος KeyGen, ο οποίος δημιουργεί κλειδιά, είναι πιθανολογικός και παράγει

ένα ζεύγος κλειδιών (pk, sk) , που περιλαμβάνει ένα δημόσιο κλειδί pk και ένα ιδιωτικό-μυστικό κλειδί sk . Ο αλγόριθμος κρυπτογράφησης, Enc , είναι επίσης πιθανολογικός και παίρνει το δημόσιο κλειδί pk και ένα μήνυμα m ως είσοδο, με αποτέλεσμα ένα κρυπτογραφημένο κείμενο c . Ο συμβολισμός $Enc_{pk}(m)$ αντιπροσωπεύει την κρυπτογράφηση του μηνύματος m με το δημόσιο κλειδί pk . Αντίθετα, ο αλγόριθμος Dec είναι ντετερμινιστικός. Δέχεται το ιδιωτικό κλειδί sk και ένα κρυπτογραφημένο κείμενο c ως είσοδο και εξάγει είτε το μήνυμα m είτε ένα ειδικό σύμβολο που υποδηλώνει αποτυχία αποκρυπτογράφησης. Ο συμβολισμός $Dec_{sk}(c)$ υποδεικνύει την αποκρυπτογράφηση του c χρησιμοποιώντας το ιδιωτικό κλειδί sk .

Το σχήμα κρυπτογράφησης για να είναι ορθό, θα πρέπει για κάθε (pk, sk) που εξάγεται από τον KeyGen και κάθε μήνυμα m θα πρέπει να ισχύει:

$$Dec_{sk}(Enc_{pk}(m)) = m.$$

Για τους χώρους των μηνυμάτων M , των κλειδιών K και των κρυπτοκειμένων ισχύει αντίστοιχα ότι ισχύει και στα συμμετρικά κρυπτοσυστήματα.



Εικόνα 2 Σχήμα κρυπτογράφησης δημόσιου κλειδιού

Στις περισσότερες κρυπτογραφικές εφαρμογές, χρησιμοποιείται ένας συνδυασμός συμμετρικών και ασύμμετρων αλγορίθμων, μαζί με συναρτήσεις κατακερματισμού, λόγω των μοναδικών πλεονεκτημάτων και αδυναμιών που είναι εγγενείς σε κάθε τύπο αλγορίθμου. Αυτές οι συνδυασμένες προσεγγίσεις είναι κοινώς γνωστές ως υβριδικά σχήματα. Ένα παράδειγμα τέτοιου σχήματος είναι ο Μηχανισμός Ενθυλάκωσης

Κλειδιού (KEM), ο οποίος επιτρέπει στα μέρη που συμμετέχουν στην επικοινωνία να μοιράζονται ένα προσωρινό κλειδί κατά τη διάρκεια της συνεδρίας τους.

Η θεμελιώδης ιδέα του KEM περιλαμβάνει τη χρήση κρυπτογράφησης δημόσιου κλειδιού για το μυστικό κλειδί, ακολουθούμενη από κρυπτογράφηση του μηνύματος χρησιμοποιώντας μια μέθοδο συμμετρικής κρυπτογράφησης μαζί με το μυστικό κλειδί. Ενώ η κρυπτογραφία ιδιωτικού κλειδιού χρησιμεύει ως μέρος αυτής της διαδικασίας, το KEM λειτουργεί ως ένα πλήρες κρυπτοσύστημα δημόσιου κλειδιού, βασιζόμενο στην αρχή ότι ο αποστολέας και ο παραλήπτης δεν διαθέτουν κανένα κοινό μυστικό κλειδί εκ των προτέρων. Οι αλγόριθμοι για τον αποστολέα και τον παραλήπτη αναφέρονται ως ενθυλάκωση και αποκαψύλωση, αντίστοιχα.

Γενικά, ένας μηχανισμός ενθυλάκωσης κλειδιού (KEM) αποτελείται από τρεις αλγόριθμους (KeyGen, Encaps, Decaps) όπως ορίζεται από τον Rijneveld (2019). Ο αλγόριθμος KeyGen, υπεύθυνος για τη δημιουργία κλειδιών, λειτουργεί πιθανολογικά για να παράγει ένα ζεύγος κλειδιών (pk , sk), το οποίο περιλαμβάνει ένα δημόσιο κλειδί pk και ένα ιδιωτικό-μυστικό κλειδί sk . Ο αλγόριθμος Encaps, επίσης πιθανολογικός, χρησιμοποιεί το δημόσιο κλειδί pk ως είσοδο για να δημιουργήσει ένα κοινό μυστικό ss μαζί με ένα κρυπτογραφημένο κείμενο c . Αντίθετα, ο αλγόριθμος Decaps είναι ντετερμινιστικός. Επεξεργάζεται το κρυπτογραφημένο κείμενο c και το ιδιωτικό κλειδί sk για να δώσει είτε το κοινό μυστικό ss' είτε το False εάν αντιμετωπίσει αποτυχία.

Τα KEM μπορεί να είναι δομημένα με τρόπο που δεν διασφαλίζει ότι ο παραλήπτης του ενθυλακωμένου μυστικού μπορεί να αποκρυπτογραφήσει με επιτυχία το κρυπτογραφημένο κείμενο. Αυτό μπορεί να οδηγήσει είτε σε εσφαλμένο κοινό μυστικό είτε σε ψευδές αποτέλεσμα, ανάλογα με το σχέδιο. Οι ορισμοί που αφορούν την αποκρυπτογράφηση και την αποτυχία αποκαψυλίωσης αντιμετωπίζουν αυτήν τη συμπεριφορά. Η αποτυχία αποκαψυλίωσης ορίζεται ως εξής (Rijneveld, 2019):

Ένα KEM θεωρείται ακριβές όταν, για κάθε ζεύγος (pk , sk) που δημιουργείται από το KeyGen() και κατά τη διάρκεια κάθε εκτέλεσης Encaps, αντιπροσωπεύεται ως (ss , c) που λαμβάνεται από το Encaps(pk) και (ss') που προέρχεται από το Decaps(c , pk), ισχύει η συνθήκη $ss = ss'$. Ένα σφάλμα αποκαψυλίωσης παρουσιάζεται όταν ο αλγόριθμος, δεδομένου ενός συγκεκριμένου c και sk , παράγει ένα αποτέλεσμα False κατά τη λειτουργία του.

Οι κρυπτογραφικές μέθοδοι γνωστές ως ψηφιακές υπογραφές προσφέρουν ένα μέσο για την εγγύηση τόσο της αυθεντικότητας όσο και της ακεραιότητας των μηνυμάτων. Όταν

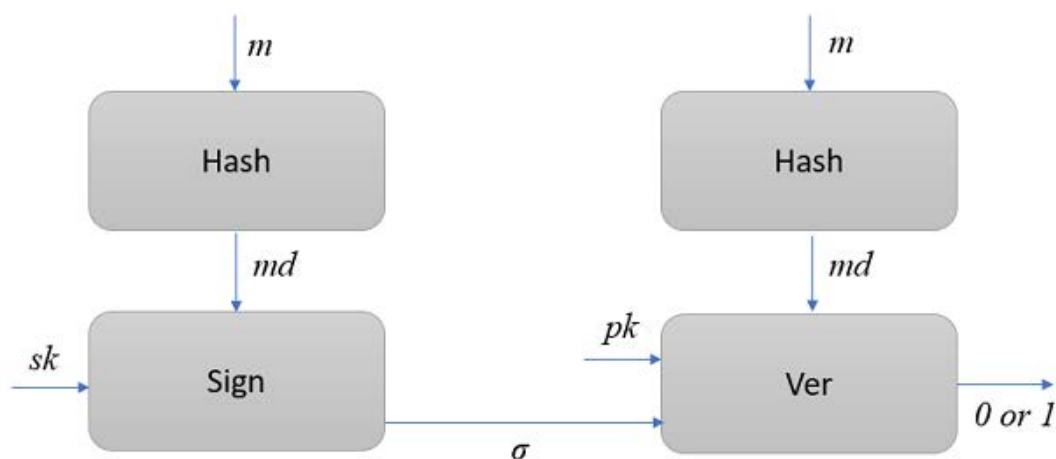
παρουσιάζεται με ένα μήνυμα m , ο υπογράφοντας χρησιμοποιεί το μυστικό κλειδί του sk για να δημιουργήσει μια υπογραφή σ που τον συνδέει με το μήνυμα. Οποιοσδήποτε έχει πρόσβαση στο δημόσιο κλειδί pk του υπογράφοντος μπορεί να επιβεβαιώσει τόσο την προέλευση όσο και την ακρίβεια του μηνύματος. Κατά συνέπεια, αυτή η διαδικασία ενισχύει την εμπιστευτικότητα του μηνύματος, η οποία επιτυγχάνεται μέσω της δημιουργίας ενός κοινόχρηστου κλειδιού μέσω ενός μηχανισμού ανταλλαγής κλειδιών, που ακολουθείται από την κρυπτογράφηση των μηνυμάτων χρησιμοποιώντας αυτό το κλειδί.

Ένα σχήμα ψηφιακής υπογραφής αποτελείται γενικά από ένα σύνολο τριών αλγορίθμων (KeyGen, Sign, Verify) όπως περιγράφεται από τον Rijneveld το 2019. Ο αλγόριθμος KeyGen, υπεύθυνος για τη δημιουργία κλειδιού, είναι πιθανολογικός και παράγει ένα δημόσιο κλειδί pk μαζί με ένα ιδιωτικό μυστικό κλειδί sk , σχηματίζοντας ένα ζεύγος κλειδιών (pk , sk). Ο αλγόριθμος υπογραφής, Sign, μπορεί επίσης να είναι πιθανολογικός, λαμβάνοντας το μυστικό κλειδί sk και ένα μήνυμα m ως εισόδους για τη δημιουργία μιας υπογραφής s . Ο συμβολισμός $Sign_{sk}(m)$ αντιπροσωπεύει την υπογραφή του μηνύματος m που δημιουργήθηκε με το κλειδί sk . Από την άλλη πλευρά, ο αλγόριθμος Verify είναι ντετερμινιστικός, και απαιτεί ένα δημόσιο κλειδί pk , μια υπογραφή σ και ένα μήνυμα m ως είσοδο. Παράγει μια έξοδο b bit, όπου $b=1$ υποδηλώνει ότι η υπογραφή είναι έγκυρη (αποδεκτή) και $b=0$ σημαίνει ότι η υπογραφή είναι άκυρη (απορρίπτεται). Η συνάρτηση $Verify_{pk}(m,s)$ χρησιμοποιείται για να επιβεβαιώσει την εγκυρότητα της υπογραφής σ για το μήνυμα m .

Το σχήμα ψηφιακής υπογραφής για να είναι ορθό θα πρέπει για κάθε (pk, sk) που εξάγεται από τον KeyGen για κάθε μήνυμα m να ισχύει:

$$Verify_{pk}(m, Sign_{sk}(m)) = 1$$

Στα περισσότερα κρυπτογραφικά σχήματα ψηφιακών υπογραφών ισχύει το μοντέλο κατακερματισμός-και-υπογραφή (hash-and-sign), όπως φαίνεται στο παρακάτω σχήμα. Σύμφωνα με αυτό το μοντέλο, το πρώτο βήμα του αλγόριθμου υπογραφής Sign και του αλγόριθμου επαλήθευσης Verify είναι ο κατακερματισμός του μηνύματος m και η δημιουργία του digest md ως είσοδο.



Εικόνα 3 Η διαδικασία της ψηφιακής υπογραφής

Όλοι οι αλγόριθμοι των κρυπτογραφικών σχημάτων της PKC βασίζονται αποκλειστικά σε αριθμοθεωρητικά προβλήματα που θεωρούνται υπολογιστικά ανέφικτα, και πιο συγκεκριμένα βασίζονται στα προβλήματα IFP και DPL. Αν και πρόκειται για δύο διαφορετικά προβλήματα, οι μαθηματικές λειτουργίες των αλγορίθμων τους βασίζονται στην ύψωση μεγάλων ακέραιων αριθμών σε δύναμη και στην αριθμητική modulo και το ζεύγος των κλειδιών δημιουργείται σε σχέση με ένα πεδίο παραμέτρων. Αυτό έχει ως αποτέλεσμα τα κλειδιά που δημιουργούνται από τους αλγόριθμους KeyGen είναι πολύ μεγαλύτερα σε τάξεις μεγέθους σε σχέση με τα συμμετρικά κλειδιά. Τα ασύμμετρα σχήματα απαιτούν πολύ περισσότερους υπολογιστικούς πόρους στο χρόνο και στο χώρο από ότι τα συμμετρικά, γι' αυτό άλλωστε κατά κανόνα στα πρωτόκολλα ασφάλειας χρησιμοποιούνται υβριδικά σχήματα (Katz & Lindell, 2014).

Αλγόριθμος	Δύσκολο Πρόβλημα	Κρυπτογράφηση / Αποκρυπτογράφηση	Ψηφιακές Υπογραφές	Ανταλλαγή Κλειδιών
RSA	IFP	Ναι	Ναι	Ναι
Ελλειπτικές καμπύλες	DLP	Ναι	Ναι	Ναι
Diffie-Hellmann	DLP IPF	Όχι	Όχι	Ναι
DSA	DLP	Όχι	Ναι	Όχι

Πίνακας 1 Εφαρμογές κρυπτογραφικών συστημάτων δημόσιου κλειδιού

2.4 Μοντέλα Απειλής

Τα συνηθισμένα μοντέλα απειλής- τα οποία ουσιαστικά είναι τα είδη των κρυπταναλυτικών επιθέσεων - με αύξουσα σειρά όσον αφορά την ισχύ του αντιπάλου είναι (Katz & Lindell, 2014):

- Επίθεση Μόνο Κρυπτοκειμένου - Ciphertext Only Attack (CO). Ο αντίπαλος παρακολουθεί παθητικά το κανάλι επικοινωνίας, συλλέγοντας κρυπτοκείμενα με στόχο να ανακτήσει το αρχικό μήνυμα ή/και το μυστικό κλειδί. Η επίθεση αυτή ισχύει για οποιοδήποτε κανάλι επικοινωνίας είναι δημόσιο.
- Επίθεση Γνωστού Μηνύματος - Known Plaintext Attack (KPA). Ο αντίπαλος όπως και πριν είναι απλά ωτακουστής. Γνωρίζει όμως και κάποια ζεύγη μηνυμάτων και αντίστοιχων κρυπτοκειμένων. Ο στόχος είναι η εύρεση του μυστικού κλειδιού έτσι ώστε να μπορεί να αποκρυπτογραφήσει κρυπτοκείμενα στα οποία χρησιμοποιείται το ίδιο κλειδί για την κρυπτογράφηση.
- Επίθεση Επιλεγμένου Μηνύματος - Chosen Plaintext Attack (CPA). Στην κατηγορία αυτή των επιθέσεων ο αντίπαλος μπορεί να ενεργήσει επιθετικά έχοντας πρόσβαση στον μηχανισμό κρυπτογράφησης, έτσι ώστε να μπορεί να διαλέξει ένα μέρος του μηνύματος και να δημιουργήσει το αντίστοιχο κρυπτοκείμενο. Ο στόχος του αντιπάλου είναι να βρει το μυστικό κλειδί.
- Επίθεση Επιλεγμένου Κρυπτοκειμένου - Chosen Ciphertext Attack (CCA). Ο αντίπαλος έχει πρόσβαση στον μηχανισμό κρυπτογράφησης, έτσι ώστε να μπορεί να διαλέξει ένα μέρος του κρυπτοκειμένου και να δημιουργήσει το αντίστοιχο μήνυμα. Ο στόχος του αντιπάλου είναι να βρει το μυστικό κλειδί.

Μια επίθεση ωμής βίας μπορεί να χρησιμοποιηθεί για την ανάκτηση του μυστικού κλειδιού, όπου ο εισβολέας επιχειρεί συστηματικά κάθε πιθανό κλειδί εντός του χώρου κλειδιού. Αυτό σημαίνει ότι οι συμβατικοί αλγόριθμοι αναζήτησης απαιτούν 2^n προσπάθειες για την αποκάλυψη ενός μυστικού κλειδιού που έχει μήκος n bit. Για παράδειγμα, για να βρει κανείς το κλειδί για το AES-128, θα χρειαστεί να κάνει 2^{128} προσπάθειες, έναν αστρονομικό αριθμό ακόμη και για τους πιο προηγμένους υπερυπολογιστές που διατίθενται σήμερα. Λαμβάνοντας υπόψη τα σημαντικά μεγαλύτερα μήκη κλειδιών στα σύγχρονα σχήματα δημόσιου κλειδιού, μια επίθεση ωμής βίας είναι παράλογη.

Τα παιχνίδια ασφαλείας που περιγράφουν τα μοντέλα απειλών ορίζουν και περιγράφουν τη σημασιολογική ασφάλεια των κρυπτογραφικών σχημάτων. Αυτά τα παιχνίδια ασφαλείας περιλαμβάνουν δύο συμμετέχοντες: τον αμφισβητία και τον αντίπαλο. Ο αμφισβητίας δημιουργεί την πρόκληση που πρέπει να αντιμετωπίσει ο αντίπαλος. Και οι δύο συμμετέχοντες είναι πιθανοτικές οντότητες πολυωνυμικού χρόνου (PPT). Σε ορισμένους ορισμούς, ο αμφισβητίας αναλαμβάνει επίσης το ρόλο ενός «μαντείου» κρυπτογράφησης ή αποκρυπτογράφησης όταν αναμένεται ότι ο αντίπαλος θα έχει πρόσβαση σε έναν τέτοιο χρησμό (Katz & Lindell, 2014). Η βάση των παιχνιδιών ασφαλείας βρίσκεται στην αρχή της δυσδιάκρισης, η οποία υποστηρίζει ότι ένας αντίπαλος που παρουσιάζεται με ένα κρυπτογραφημένο κείμενο c δεν μπορεί να συναγάγει τίποτα σχετικά με το αρχικό μήνυμα m από το οποίο προήλθε το c . Επιπρόσθετα, βασίζονται στην αρχή της μη προσαρμοστικότητας (ή μη ελατότητας), που σημαίνει ότι ένας αντίπαλος στον οποίο δίνεται ένα κρυπτογραφημένο κείμενο c δεν μπορεί να αντλήσει διαφορετικό κρυπτογραφημένο κείμενο c' έτσι ώστε τα σχετικά μηνύματα m και m' να συσχετίζονται σημαντικά (Bellare, et. al., 1998).

Γενικά, δύο έννοιες σημασιολογικής ασφαλείας που προέρχονται από παιχνίδια ασφαλείας σκιαγραφούν την ασφάλεια των μηχανισμών ενθυλάκωσης κλειδιών (KEM) και των σχημάτων δημόσιου κλειδιού (PKEs): Indistinguishability under the Chosen Message Attack (IND-CPA) και Indistinguishability under the Chosen Ciphertext Attack (IND-CCA2) (Rijneveld, 2019). Στο πλαίσιο του IND-CPA για PKE, η υποκείμενη ιδέα είναι ότι ένας αντίπαλος, ακόμη και όταν παρουσιάζεται με δύο πιθανά απλά κείμενα, δεν μπορεί να συνδέσει με συνέπεια ένα από αυτά τα απλά κείμενα με ένα συγκεκριμένο κρυπτογραφημένο κείμενο. Το παιχνίδι IND-CPA χρησιμεύει ως πλαίσιο για παθητικές επιθέσεις.

Δοθέντος ενός κρυπτογραφικού σχήματος δημόσιου κλειδιού (KeyGen, Enc, Dec), θεωρείται το παρακάτω παιχνίδι μεταξύ του προκαλούντος (challenger) και ενός αντίπαλου (adversary) A (Rijneveld, 2019):

1. Ο C τρέχει $(pk, sk) \leftarrow \text{KeyGen}()$ και στέλνει το pk στον A .
2. Ο A μπορεί να εκτελέσει ένα πολυωνυμικό αριθμό κλήσεων στον Enc και σε άλλες λειτουργίες.
3. Ο A στέλνει ελεύθερα επιλεγμένα μηνύματα m_0 και m_1 στον C .
4. Ο C επιλέγει τυχαία ένα $b \in \{0, 1\}$, και απαντά με $c \leftarrow \text{Enc}(pk, m_b)$.

5. Ο Α μπορεί να εκτελέσει έναν πολυωνυμικό αριθμό κλήσεων στον Enc και σε άλλες λειτουργίες.
6. Ο Α εξάγει μια εικασία (μαντεία) b' . Η επίθεση είναι επιτυχής εάν $b = b'$.

Το σχήμα PKE λέγεται ότι είναι IND-CPA ασφαλές όταν ένας αντίπαλος Α που διαθέτει πολυωνυμικό χρόνο ως προς την παράμετρο ασφάλειας n , έχει αμελητέο πλεονέκτημα σε σχέση με την τυχαία εικασία. Να σημειώσουμε εδώ, ότι δεν υπάρχει περιορισμός στα μήκη των μηνυμάτων και, καθώς είναι ίδιου μήκους και εφόσον ο αντίπαλος τρέχει σε πολυωνυμικό χρόνο, τότε τα μηνύματα έχουν μήκος πολυωνυμικό στο n , όπου n η παράμετρος ασφάλειας.

Στο IND-CCA2 παιχνίδι ασφάλειας ο αντίπαλος έχει πρόσβαση σε ένα μαντείο (oracle) που του επιτρέπει να αποκρυπτογραφήσει τα πάντα εκτός από το κρυπτοκείμενο της πρόκλησης. Επίσης, ο αντίπαλος δεν θα πρέπει να μπορεί να διαχωρίσει τα δύο κρυπτοκείμενα. Η διαφορά ανάμεσα στο IND-CCA2 και στο IND-CPA έγκειται στο πότε επιτρέπεται στον αντίπαλο να ζητήσει κρυπτογραφήσεις αφότου έχει λάβει το κρυπτοκείμενο της πρόκλησης. Έτσι, Στην περίπτωση του KEM, το παιχνίδι είναι διαφορετικό από αυτό του PKE. Αντί ο αντίπαλος να επιλέξει δύο μηνύματα προς κρυπτογράφηση για τον προκαλούντα, ο προκαλών παράγει ένα κατάλληλα ενθυλακωμένο κοινό μυστικό και διαλέγει ένα τυχαίο στοιχείο στο ίδιο πεδίο. Ο αντίπαλος δεν θα πρέπει να μπορεί να διαχωρίσει το κοινό μυστικό από το τυχαίο στοιχείο (Rijneveld, 2019). Το παιχνίδι IND-CCA2 εκφράζει ένα μοντέλο για παθητική επίθεση.

Δοθέντος ενός μηχανισμού ενθυλάκωσης κλειδιού (KeyGen, Encaps, Decaps), θεωρείται το παρακάτω παιχνίδι μεταξύ του προκαλούντος C και ενός αντίπαλου A (Rijneveld, 2019):

1. Ο C τρέχει $(pk, sk) \leftarrow \text{KeyGen}()$.
2. Ο C τρέχει $(K, c) \leftarrow \text{Encaps}(pk)$.
3. Ο C διαλέγει K' στο πεδίο του $\text{Encaps}()$, καθώς και το $b \in \{0, 1\}$.
4. Ο C στέλνει τα pk , K_b και c στον A .
5. Ο A μπορεί να εκτελέσει έναν πολυωνυμικό αριθμό λειτουργιών, καθώς και ερωτήματα προς ένα μαντείο για να υπολογίσει $\text{Decaps}(sk, c')$ για κρυπτοκείμενα $c' \neq c$.
6. Ο A εξάγει μια εικασία b' . Η επίθεση είναι επιτυχημένη εάν $b = b'$.

Ο μηχανισμός ενθυλάκωσης κλειδιού λέγεται ότι είναι IND-CCA2 ασφαλής εάν οποιοσδήποτε αντίπαλος A , που διαθέτει πολωνυμικό χρόνο ως προς την παράμετρο ασφάλειας n , έχει αμελητέο πλεονέκτημα σε σχέση με την τυχαία εικασία. Στις ψηφιακές υπογραφές εισέρχεται η έννοια της πλαστογραφίας (forgery). Θεωρούμε ότι ο αντίπαλος με δεδομένο το δημόσιο κλειδί επαλήθευσης και ένα μήνυμα παράγει μια έγκυρη υπογραφή χωρίς τη συμμετοχή του αποστολέα-υπογράφοντα. Ορίζονται τρία είδη πλαστογράφησης (Barton, et al., 2019):

- Καθολική πλαστογράφηση: Ο αντίπαλος μπορεί να υπογράψει οποιοδήποτε μήνυμα με μια υπογραφή που φαίνεται να είναι έγκυρη
- Επιλεκτική πλαστογράφηση: Ο αντίπαλος μπορεί να παράγει μία έγκυρη υπογραφή σε ένα τυχαίο μήνυμα της επιλογής του
- Υπαρξιακή πλαστογράφηση: Ο αντίπαλος μπορεί να παράγει μία έγκυρη υπογραφή για τουλάχιστον ένα τυχαίο μήνυμα

Η πρότυπη έννοια σημασιολογικής ασφάλειας για τις ψηφιακές υπογραφές είναι η υπαρξιακή μη-πλαστογράφηση στην επίθεση επιλεγμένων μηνυμάτων (Existential Unforgery Chosen Message Attack - EU-CMA ή ισοδύναμα EUF-CMA). Διαισθητικά, αυτή η έννοια συλλαμβάνει την ιδέα ότι, ένας αντίπαλος δεν θα πρέπει να είναι ικανός να παράγει έγκυρες ψηφιακές υπογραφές για κάθε μήνυμα m , ακόμα και εάν κατέχει υπογραφές σε διάφορα μηνύματα της επιλογής του.

Για ένα σχήμα ψηφιακής υπογραφής (KeyGen, Sign, Verify), θεωρείται το παρακάτω παιχνίδι μεταξύ του προκαλούντος και ενός αντιπάλου A (Rijneveld, 2019):

1. Ο C τρέχει $(pk, sk) \leftarrow \text{KeyGen}()$ και στέλνει το pk στον A .
2. Ο A στέλνει ένα ελεύθερα επιλεγμένο μήνυμα m_i στον C .
3. Ο C αποκρίνεται με $\sigma_i \leftarrow \text{Sign}(m_i, sk)$.
4. Ο A επαναλαμβάνει τα βήματα 2. και 3. για q επαναλήψεις, με q πολωνυμικό ως προς την παράμετρο ασφάλειας n .
5. Ο A εξάγει ένα ζεύγος (m', σ') . Αυτή είναι μια έγκυρη πλαστογράφηση εφόσον $\text{Verify}(m', \sigma', pk) = \text{True}$ για $m' \neq m_i$ για όλα τα $i \in \{1, \dots, q\}$.

Το σχήμα της ψηφιακής υπογραφής λέγεται ότι είναι EU-CMA ασφαλές εάν οποιοσδήποτε αντίπαλος A , που διαθέτει πολωνυμικό χρόνο ως προς την παράμετρο ασφάλειας n , έχει αμελητέα πιθανότητα επιτυχίας.

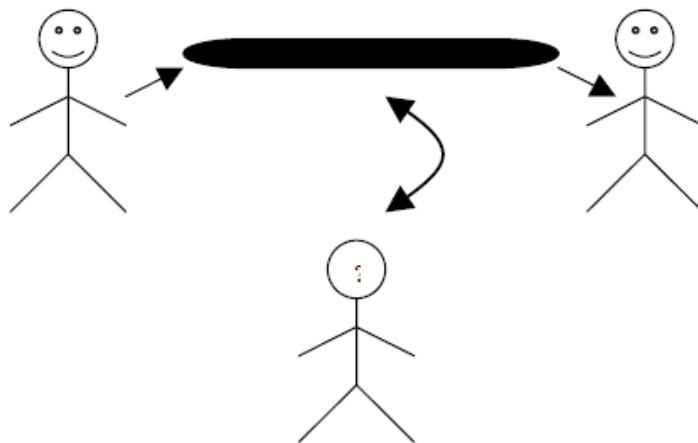
3 Εργαλεία Κρυπτογράφησης και Κρυπτανάλυσης

3.1 Ιστορική Αναδρομή

Η αναζήτηση της μυστικότητας έχει τις ρίζες της στις απαρχές της ανθρωπότητας. Σχεδόν ταυτόχρονα με την εμφάνιση της γραφής, η κρυπτογραφία προέκυψε τόσο ως ιδεολογική έννοια όσο και ως πρακτική. Αυτή η τέχνη της διατήρησης του απορρήτου δημιούργησε το πεδίο της κρυπτογραφίας. Η ανάλυση της ετυμολογίας του όρου (κρυπτογραφία + γραφή) αποκαλύπτει την εγγενή σημασία του.

Η εξέλιξη της κρυπτογραφίας μπορεί να κατηγοριοποιηθεί ευρέως σε τρεις διακριτές φάσεις (Bellare, 2004). Η αρχική φάση επικεντρώθηκε σε μεθόδους κρυπτογράφησης που σχετίζονται με έντυπες μορφές, χρησιμοποιώντας μελάνι και χαρτί, που περιελάμβανε την αντικατάσταση και την αναδιάταξη των γραμμάτων του αλφαβήτου, όπως αποδεικνύεται από τον κρυπτογραφικό αλγόριθμο του Καίσαρα. Η δεύτερη φάση αφορά την εποχή των κρυπτογραφικών μηχανών, ιδιαίτερα αξιοσημείωτη κατά τον Β' Παγκόσμιο Πόλεμο, που τονίστηκε από τη γερμανική μηχανή Enigma. Η τελική φάση αναγνωρίζεται ως το σύγχρονο κρυπτογραφικό πλαίσιο, που προκύπτει από τη συνεργατική αλληλεπίδραση μαθηματικών και υπολογιστών, όπου οι υπολογιστές διευκόλυναν την εφαρμογή πιο περίπλοκων αλγορίθμων κρυπτογράφησης, ενώ τα μαθηματικά συνέβαλαν στο σχεδιασμό τους.

Παρόλα αυτά, αυτό που ξεκίνησε ως μορφή τέχνης —πιθανώς ακόμη και παιχνίδι— έχει μετατραπεί σε έναν επιστημονικό κλάδο γνωστό ως σύγχρονη κρυπτογραφία, επικεντρωμένος στη διαφύλαξη των συστημάτων υπολογιστών, των δικτύων πληροφοριών και επικοινωνίας. Η έρευνά της περιλαμβάνει τα μαθηματικά, συμπεριλαμβανομένης της θεωρίας αριθμών και των αλγεβρικών δομών, καθώς και τη θεωρία της υπολογιστικής πολυπλοκότητας (Bell, et al., 2003). Ακόμη και με τις εξελίξεις στην κρυπτογραφία, ο πρωταρχικός της στόχος εξακολουθεί να είναι η διασφάλιση της ασφαλούς επικοινωνίας σε μη ασφαλή κανάλια.

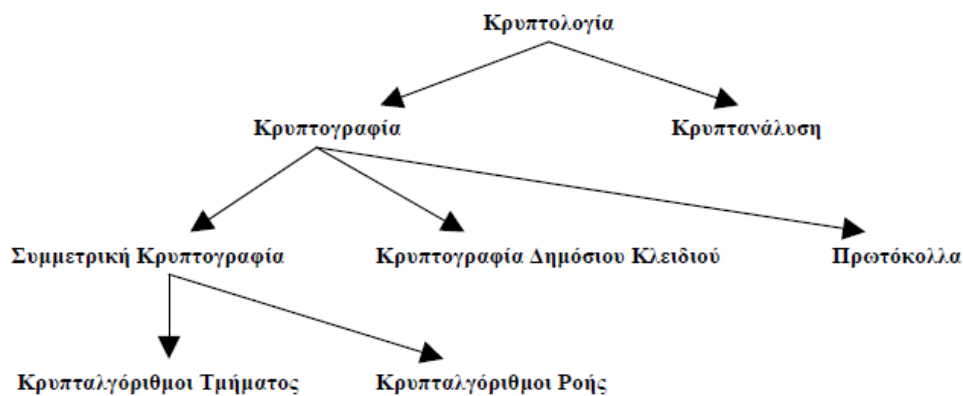


Εικόνα 4 Απομίμηση ορισμένων πτυχών ενός ιδεατού καναλιού επικοινωνίας που συνδέει τον αποστολέα S (sender) σε ένα αποδέκτη R (receiver)

Δυστυχώς, δεν υπάρχουν ιδανικοί δίαυλοι επικοινωνίας στον πραγματικό κόσμο για ζευγάρια ατόμων που ανταλλάσσουν πληροφορίες. Συνήθως, αυτά τα άτομα χρησιμοποιούν ανοιχτά δίκτυα, όπως το Διαδίκτυο, για την επικοινωνία τους. Για την επίτευξη στόχων ασφάλειας, όπως η εμπιστευτικότητα ή η αυθεντικότητα, ένα κρυπτοσυστήματος προσφέρει ένα πρωτόκολλο τόσο στον αποστολέα όσο και στον παραλήπτη. Ένα πρωτόκολλο είναι ουσιαστικά ένα σύνολο προγραμμάτων—που περιλαμβάνει αλγόριθμους και λογισμικό—σχεδιασμένα για κάθε συμμετέχοντα. Τα αποτελεσματικά πρωτόκολλα είναι κρίσιμα στοιχεία για ασφαλή υπολογιστικά συστήματα. Η ασφάλεια περιλαμβάνει διάφορες πτυχές. Πολλά στοιχεία πρέπει να ευθυγραμμιστούν για να θεωρηθεί ένα σύστημα ασφαλές. Το κρυπτογραφικό πρωτόκολλο αντιπροσωπεύει μόνο ένα στοιχείο αυτού του περίπλοκου παζλ και, αν δεν έχει σχεδιαστεί επαρκώς, οι επιτιθέμενοι θα εκμεταλλευτούν τις αδυναμίες του.

Η κρυπτογραφία επικεντρώνεται στη δημιουργία και αξιολόγηση πρωτοκόλλων ασφαλείας (Goldreich, 2001). Αυτά τα πρωτόκολλα καθορίζουν τους κανόνες λειτουργίας και συμπεριφοράς για όλα τα μέρη που συμμετέχουν στη συμφωνία. Στην ουσία λειτουργούν ως κατανεμημένο πρόγραμμα και είναι κοινώς γνωστά ως σχήματα. Μια κρίσιμη έρευνα που προκύπτει είναι ο τρόπος ανάλυσης αυτών των πρωτοκόλλων. Το πρώτο βήμα για την εύρεση μιας λύσης πρωτοκόλλου για ένα συγκεκριμένο πρόβλημα ασφαλείας είναι η κατανόηση των σχετικών απειλών και στόχων.

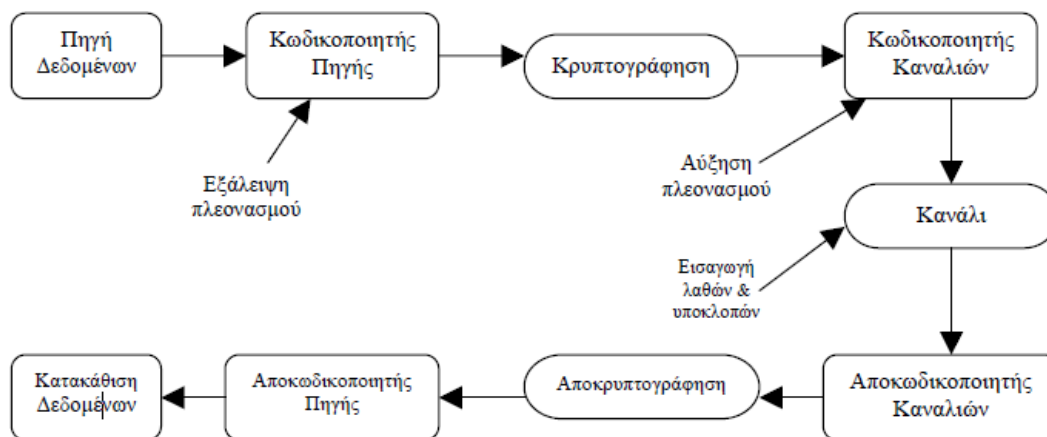
Στον τομέα της κρυπτογραφίας, υπάρχουν καθιερωμένες οδηγίες. Η κύρια οδηγία δηλώνει ότι η ήττα ενός αντιπάλου μπορεί να επιτευχθεί μόνο με τη χρήση πρωτοκόλλων. Οι τακτικές που κρίνονται άδικες, όπως ο εκφοβισμός ή η σύλληψη, απαγορεύονται για την υπέρβαση ενός αντιπάλου. Αν και αυτές οι στρατηγικές μπορεί να παράγουν αποτελέσματα, δεν πληρούν τις προϋποθέσεις ως νόμιμες κρυπτογραφικές πρακτικές. Η δευτερεύουσα κατευθυντήρια γραμμή υπογραμμίζει την αναγκαιότητα δημόσιας πρόσβασης στα πρωτόκολλα, ενώ τα μυστικά πρέπει να προστατεύονται μέσα σε κλειδιά. Είναι σημαντικό να κατανοήσουμε ότι διαδικασίες όπως η κρυπτογράφηση, η αποκρυπτογράφηση ή η κρυπτανάλυση ενός μηνύματος εμπίπτουν στην ευρύτερη κατηγορία της Κρυπτολογίας (Barr, 2002). Η Κρυπτολογία περιλαμβάνει το συνολικό επιστημονικό κλάδο που περιλαμβάνει τόσο την Κρυπτογραφία όσο και την Κρυπτανάλυση.



Εικόνα 5 Ο επιστημονικός κλάδος της κρυπτολογίας

3.2 Κρυπτογραφία και Κωδικοποίηση

Υπάρχουν τρεις βασικές μορφές κωδικοποίησης στα σύγχρονα συστήματα επικοινωνιών: κωδικοποιητής της πηγής (source coding), κωδικοποιητής λάθους (error coding - επίσης αποκαλούμενος κωδικοποιητής καναλιών (channel coding)) και κρυπτογράφηση (encryption).



Εικόνα 6 Η κωδικοποίηση στα ψηφιακά συστήματα επικοινωνίας

Ο πλεονασμός υπάρχει στους περισσότερους τύπους δεδομένων, συμπεριλαμβανομένου του κειμένου. Αυτό υποδηλώνει ότι οι τυπικές αναπαραστάσεις μηνυμάτων, όπως το αγγλικό κείμενο, χρησιμοποιούν περισσότερα bits από όσα είναι απαραίτητα για τη μετάδοση του πραγματικού περιεχομένου. Οι τεχνικές στην κωδικοποίηση πηγής εξαλείφουν αυτόν τον πλεονασμό, μειώνοντας έτσι το μήκος του μηνύματος. Ο στόχος της κρυπτογράφησης είναι να μετατρέψει το περιεχόμενο ενός μηνύματος σε μια μορφή που δεν είναι κατανοητή. Μόνο άτομα που διαθέτουν τα κρυπτογραφικά κλειδιά θα πρέπει να έχουν τη δυνατότητα να ανακτήσουν το αρχικό περιεχόμενο. Μπορεί κανείς να θεωρήσει την κρυπτογράφηση ως μια παραλλαγή κωδικοποίησης (Stallings, 2003). Εν τω μεταξύ, ο ρόλος των κωδικών καναλιών είναι να ενισχύσουν την ανθεκτικότητα των δεδομένων έναντι σφαλμάτων που μπορεί να προκύψουν κατά τη μετάδοση μέσω του καναλιού.

Η κατανόηση της κρυπτογραφίας είναι ζωτικής σημασίας για τη διαφοροποίηση μεταξύ αυτών των τριών τύπων κωδικοποίησης. Συγκεκριμένα, είναι σημαντικό να μην συγχέουμε τους κωδικούς σφάλματος με την κρυπτογράφηση. Σε γενικές γραμμές, οι κωδικοί σφάλματος προστατεύουν από ακούσιες δυσλειτουργίες, όπως σφάλματα μετάδοσης που προκαλούνται από θόρυβο, ενώ η κρυπτογράφηση προστατεύει από διακοπές που προέρχονται από ανθρώπινες επιθέσεις, όπως προσπάθειες ανάγνωσης ή τροποποίησης ενός μηνύματος. Σαφώς, οι επιθέσεις που προκύπτουν από φυσικά αίτια (θόρυβος) διαφέρουν σημαντικά από εκείνες που πραγματοποιούνται από έναν ενημερωμένο και με καλά πόρους υποκλοπή.

3.3 Ψηφιακές Πληροφορίες και Κρυπτογραφία

Σε ένα υπολογιστικό πλαίσιο, αναλύουμε μοτίβα bit ή δυαδικές ακολουθίες που επικοινωνούν μηνύματα κειμένου ή διάφορες μορφές πολυμέσων, συμπεριλαμβανομένων εικόνων και ήχων. Μια δυαδική ακολουθία που είτε μεταδίδεται είτε αποθηκεύεται με ασφάλεια σε ένα μέσο αναφέρεται ως απλό κείμενο. Αντιπροσωπεύουμε το απλό κείμενο ως:

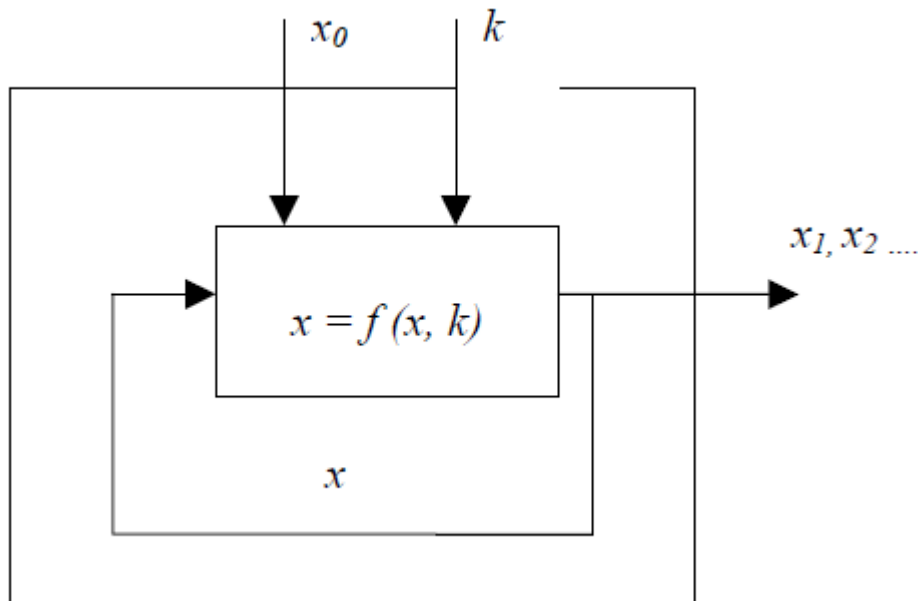
$P = \{p_1, p_2, \dots, p_i, \dots, p_n \mid p_i \in P\}$, με το P να αντιπροσωπεύει ένα πεπερασμένο σύνολο συμβόλων απλού κειμένου. Στη σφαίρα των ψηφιακών κρυπτοσυστημάτων, αυτό το αλφάβητο είναι δυαδικό, που σημαίνει $P = Z_2 = \{0, 1\}$. Επιπλέον, μπορούμε να εξερευνήσουμε το αλφάβητο των byte ($P = Z_{256} = \{0, 1\}^8$) ή ακόμη πιο εκτεταμένα μοτίβα δεδομένων.

Έστω $c = \{c_1, c_2, \dots, c_i, \dots, c_n \mid c_i \in C\}$ υποδηλώνει το κρυπτογραφημένο μήνυμα ή κρυπτογραφημένο κείμενο. Συνήθως, το αλφάβητο C μπορεί να διαφέρει από το P , αν και σε πολλές περιπτώσεις, $P = C = \{0, 1\}^m$.

Σε γενικές γραμμές, ένα κρυπτογραφικό σύστημα περιλαμβάνει το συνεκτικό υπολογιστικό πλαίσιο που διασφαλίζει την ασφάλεια των πληροφοριών μέσω ενός αρμονικού συνδυασμού λύσεων λογισμικού και υλικού, ενώ εκτελεί κρυπτογραφικούς αλγόριθμους όπως κρυπτογράφηση, αποκρυπτογράφηση, επικύρωση και διαχείριση κλειδιών. Σε πρακτικές εφαρμογές, η αποτελεσματικότητα ενός κρυπτογραφικού συστήματος βασίζεται σε μεγάλο βαθμό στην ανθρώπινη συμμετοχή.

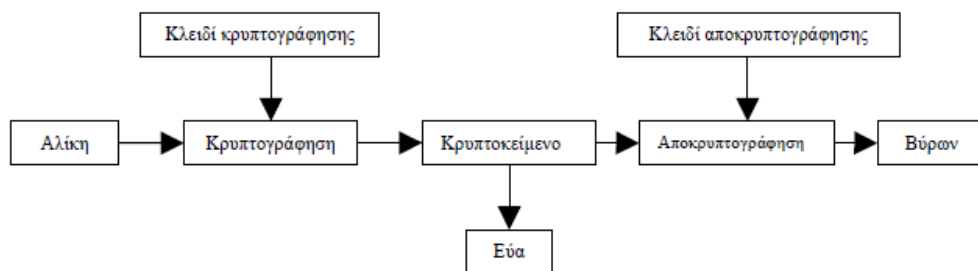
Ένα κρυπτογραφικό σύστημα, σε έναν πιο συγκεκριμένο ορισμό, χρησιμεύει ως ένα μαθηματικό πλαίσιο που μεταβάλλει τις πληροφορίες για να τις καταστήσει απρόσιτες για έναν αντίπαλο. Μπορεί επίσης να θεωρηθεί ως ένα δυναμικό σύστημα.

$$S = \langle X, f: X \times K \rightarrow X \rangle,$$



Σε αυτό το πλαίσιο, το σύνολο X αντιπροσωπεύει ένα διάστημα, ενώ η συνάρτηση f υποδηλώνει έναν κρυπτογραφικό μετασχηματισμό που βασίζεται στο κλειδί K . Η κατάσταση του συστήματος, $x \in X$, κωδικοποιεί συγκεκριμένες πληροφορίες, όπως ένα απλό κείμενο ή μια υπογραφή (στους περισσότερους κρυπτογραφικούς αλγόριθμους, έχουμε $X = P = C$). Το σύστημα δημιουργεί μια ακολουθία καταστάσεων $x_0, x_1, \dots, x_n, \dots$, όπου το x_n ορίζεται ως $f(x_{n-1}, k) = f_n(x_0, k)$, με το x_0 να ανήκει στο X και το k να ανήκει στο K . Η αρχική συνθήκη x_0 χρησιμεύει ως κείμενο εισόδου και η τελική κατάσταση x_n αντιπροσωπεύει το κείμενο εξόδου.

Οι ορισμοί είναι οι εξής: το x αντιπροσωπεύει απλό κείμενο $P = \{x_1, x_2, \dots, x_p\}$, το οποίο είναι ένα πεπερασμένο εύρος απλού κειμένου. Το y υποδηλώνει κρυπτογραφημένο κείμενο $C = \{y_1, y_2, \dots, y_c\}$, που αντιπροσωπεύει ένα πεπερασμένο εύρος κρυπτογραφημένου κειμένου. Το k σημαίνει το κλειδί $K = \{k_1, k_2, \dots, k_l\}$, το οποίο είναι το πεπερασμένο εύρος των πλήκτρων. Υπάρχουν l κρυπτογραφικές συναρτήσεις ek_i : $P \rightarrow C$ ή $ek_i(x) = y$, μαζί με l συναρτήσεις αποκρυπτογράφησης dk_i : $C \rightarrow P$ ή $dk_i(y) = x$. Οι συναρτήσεις ek_1 και dk_2 χρησιμεύουν ως αντίστροφες συναρτήσεις όταν $k_1 = k_2$, έτσι ώστε $dk_i(y) = dk_i(ek_i(x)) = x$ για κάθε $k_1 \in K$.



Εικόνα 7 Κλασσικό κρυπτοσύστημα

Το ανωτέρω σύστημα (σχήμα 5.4) αποδίδεται μαθηματικά ως:

$$A \longrightarrow f \quad B \longrightarrow f^{-1} \quad A$$

Όπου f καλείται ο κρυπτογραφικός μετασχηματισμός και f^{-1} ο μετασχηματισμός αποκρυπτογράφησης. Μια τέτοια παράσταση καλείται κρυπτογραφικό σύστημα ή απλά κρυπτοσύστημα.

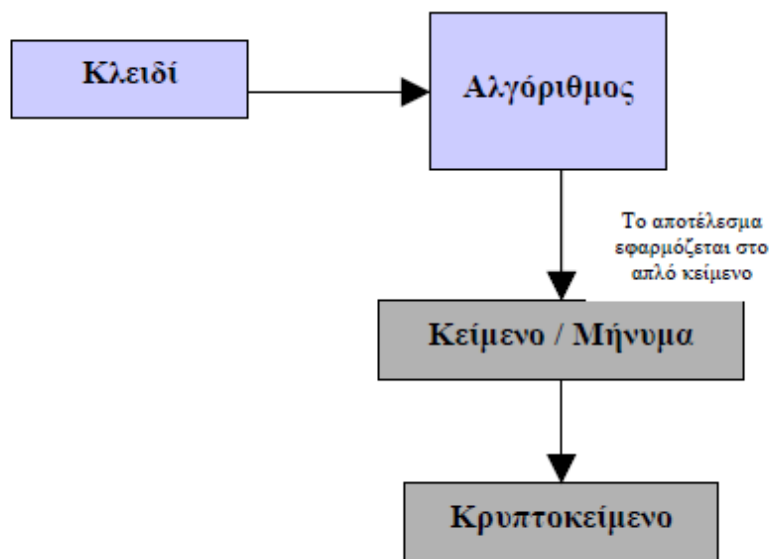
3.4 Ορισμοί του Κρυπτογραφικού Συστήματος

Κατά συνέπεια, η κρυπτογραφία διερευνά τεχνικές για να μετατρέψει ένα μήνυμα σε μια εντελώς ακατανόητη μορφή. Αφορά τις ανταλλαγές μεταξύ αντιπάλων. Πράγματι, η ύπαρξη ενός αντιπάλου σε ορισμένες επικοινωνίες είναι το πρωταρχικό κίνητρο πίσω από τη δημιουργία και την εφαρμογή της κρυπτογραφίας (Mao, 2004).

Η κρυπτογράφηση είναι μια μέθοδος που μετατρέπει τα αρχικά δεδομένα, γνωστά ως απλό κείμενο ή καθαρό κείμενο, σε μια μορφή που εμφανίζεται τυχαία και μη αναγνώσιμη, που αναφέρεται ως κρυπτογραφημένο κείμενο [Stallings, 2003]. Η πράξη της επαναφοράς κρυπτογραφημένου κειμένου σε απλό κείμενο ονομάζεται αποκρυπτογράφηση. Το απλό κείμενο μπορεί να υπάρχει σε μορφές κατανοητές από τον άνθρωπο, όπως έγγραφα ή υπολογιστές, όπως εκτελέσιμος κώδικας. Από τη στιγμή που τα δεδομένα έχουν αλλάξει σε κρυπτογραφημένο κείμενο, δεν μπορούν να χρησιμοποιηθούν αποτελεσματικά ούτε από ανθρώπους ούτε από μηχανές μέχρι να πραγματοποιηθεί η διαδικασία αποκρυπτογράφησης. Αυτός ο μηχανισμός επιτρέπει την ασφαλή μετάδοση εμπιστευτικών πληροφοριών σε μη ασφαλή κανάλια χωρίς τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης. Ενώ οι λογικοί και φυσικοί έλεγχοι πρόσβασης προστατεύουν συνήθως τα δεδομένα που είναι αποθηκευμένα σε έναν υπολογιστή, μια τέτοια ισχυρή ασφάλεια δεν μπορεί να διατηρηθεί όταν αποστέλλονται

ευαίσθητες πληροφορίες μέσω ενός δικτύου, αφήνοντάς το εκτεθειμένο σε πιθανές απειλές (Trappe & Washington, 2002).

Οι διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης χρησιμοποιούν τους συγκεκριμένους αλγόριθμους τους, οι οποίοι δημιουργούν συλλογικά την κρυπτογράφηση. Ένα κρυπτογραφικό σύστημα, ή κρυπτοσύστημα, ορίζεται ως ένα πλαίσιο που επιτρέπει τόσο την κρυπτογράφηση όσο και την αποκρυπτογράφηση. Σε αυτό το πλαίσιο, ο αλγόριθμος κρυπτογράφησης καθορίζει την ευκολία ή τη δυσκολία των σχετικών λειτουργιών. Γενικά, αυτοί οι αλγόριθμοι αποτελούνται από περίπλοκους μαθηματικούς τύπους που εκτελούνται με συγκεκριμένη σειρά στο απλό κείμενο. Οι περισσότερες μέθοδοι κρυπτογράφησης εξαρτώνται από μια μυστική τιμή που αναφέρεται ως κλειδί, η οποία συνεργάζεται με τον αλγόριθμο για να εκτελέσει τις λειτουργίες τόσο της κρυπτογράφησης όσο και της αποκρυπτογράφησης του κειμένου. Είναι η ύπαρξη του κλειδιού που διαφοροποιεί θεμελιωδώς την κρυπτογράφηση από την αποκρυπτογράφηση.



Εικόνα 8 Λειτουργία του κλειδιού

Ένας αλγόριθμος, ο οποίος είναι ένα σύνολο μαθηματικών κανόνων, διέπει τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης. Αν και πολλοί αλγόριθμοι είναι δημοσίως γνωστοί και δεν ταξινομούνται στη σφαίρα της κρυπτογράφησης, οι ιδιαίτερες λειτουργίες αυτών των αλγορίθμων κρυπτογράφησης ενδέχεται να παραμείνουν άγνωστες στο ευρύ κοινό. Όταν οι ιδιαιτερότητες ενός αλγορίθμου δεν είναι οργανωμένες, υποδηλώνει ότι αφορά διαφορετικό θέμα. Η εμπιστευτικότητα του κλειδιού είναι ζωτικής σημασίας όταν χρησιμοποιείται ένας αναγνωρισμένος αλγόριθμος

κρυπτογράφησης. Αυτό το κλειδί μπορεί να είναι οποιαδήποτε τιμή που προκύπτει από μια μακρά ακολουθία τυχαίων bits. Κάθε αλγόριθμος διαθέτει ένα keyspace, το οποίο είναι ένα εύρος τιμών που μπορούν να χρησιμοποιηθούν για τη δημιουργία ενός κλειδιού. Το ίδιο το κλειδί περιλαμβάνει τυχαίες τιμές που υπάρχουν εντός των καθορισμένων ορίων του χώρου κλειδιών. Ένας πιο εκτεταμένος χώρος κλειδιών έχει ως αποτέλεσμα μεγαλύτερο αριθμό πιθανών τιμών για διάφορα κλειδιά, οδηγώντας σε αυξημένη τυχειότητα και καθιστώντας πιο δύσκολο για έναν εισβολέα να τα υπολογίσει. Αντίθετα, ένας μικρότερος χώρος πλήκτρων περιορίζει τον αριθμό των πιθανών κλειδιών. Για να βελτιωθεί η τυχειότητα, ο αλγόριθμος κρυπτογράφησης πρέπει να χρησιμοποιεί ολόκληρο τον χώρο κλειδιών και να επιλέξει τις τιμές ανάλογα.

3.5 Η δύναμη του κρυπτογραφικού συστήματος

Ένα θεμελιώδες κριτήριο στην αντικειμενική μέτρηση της δύναμης ενός κρυπτοσυστήματος είναι η αρχή του Kerchoff:

«Η ασφάλεια ενός κρυπτοσυστήματος δεν εξαρτάται από τη μυστικότητα του αλγόριθμου κρυπτογράφησης. Η ασφάλεια του κρυπτοσυστήματος εξαρτάται μόνον από το να διατηρείται μυστικό το κλειδί»

Ο Shannon, ο θεμελιωτής της θεωρίας της πληροφορίας διατύπωσε το 1949 ένα σύνολο από μέτρα τα οποία χαρακτηρίζουν έναν ορθά σχεδιασμένο αλγόριθμο κρυπτογράφησης:

1. Βαθμός απαιτούμενης κρυπτογραφικής ασφάλειας. Το μέτρο αυτό αφορά το κέρδος του αντιπάλου σε πληροφορία, όταν παρατηρεί το κρυπτοκείμενο.
2. Μήκος του κλειδιού. Η ευκολία χειρισμού του κλειδιού εξαρτάται από το μήκος του.
3. Πρακτική εκτέλεση της κρυπτογράφησης και της αποκρυπτογράφησης. Η προσπάθεια που απαιτείται για την κρυπτογράφηση και την αποκρυπτογράφηση, σε χρόνο ή λειτουργίες.
4. Διόγκωση του κρυπτοκειμένου. Είναι επιθυμητό το κρυπτοκείμενο να έχει το ίδιο μήκος (ή συγκρίσιμου μεγέθους) με το απλό κείμενο.
5. Διάδοση των σφαλμάτων κρυπτογράφησης. Είναι επιθυμητό ένα σφάλμα κατά την κρυπτογράφηση να επηρεάζει σε όσον το δυνατόν λιγότερο βαθμό την αποκρυπτογράφηση.

Η παρουσία μέτρων μέσα σε ένα κρυπτοσύστημα είναι ουσιαστική αλλά παράδοξη, οδηγώντας στο συμπέρασμα ότι κανένα κρυπτοσύστημα δεν μπορεί να ανταποκριθεί πλήρως σε όλα τα μέτρα στον υψηλότερο βαθμό. Η σύγχυση και η διάχυση είναι δύο βασικές ιδιότητες που χρησιμοποιούνται για την αξιολόγηση της ευρωστίας της κρυπτογραφίας (Diffie & Hellman, 2022).

Η ικανότητα ενός αλγορίθμου κρυπτογράφησης που είναι γνωστός ως σύγχυση εμποδίζει έναν αντίπαλο να προβλέψει πώς οι αλλαγές στο απλό κείμενο θα επηρεάσουν το κρυπτογραφημένο κείμενο. Από την άλλη πλευρά, η διάχυση αναφέρεται στην ικανότητα του αλγορίθμου κρυπτογράφησης να διασφαλίζει ότι ένα τμήμα του απλού κειμένου επηρεάζει όσα τμήματα του κρυπτογραφημένου κειμένου είναι εφικτό (Boneh & Shoup, 2020).

Η μέθοδος κρυπτογράφησης αντλεί τη δύναμή της από διάφορους παράγοντες: τον αλγόριθμο που χρησιμοποιείται, την εμπιστευτικότητα του κλειδιού, το μήκος του κλειδιού και την αλληλεπίδραση αυτών των στοιχείων. Στον τομέα της κρυπτογραφίας, όταν αναφερόμαστε στη δύναμη, μιλάμε για το πόσο δύσκολο είναι να υπολογίσουμε είτε τον αλγόριθμο είτε το κλειδί, τα οποία παραμένουν άγνωστα. Η διαδικασία διάσπασης ενός κλειδιού περιλαμβάνει την αξιολόγηση μιας εξαιρετικά μεγάλης σειράς πιθανών τιμών με την ελπίδα να εντοπιστεί κάποια που μπορεί να αποκρυπτογραφήσει με επιτυχία ένα συγκεκριμένο μήνυμα. Η ισχύς σχετίζεται με την ουσιαστική ποσότητα προσπάθειας και χρόνου επεξεργασίας που απαιτείται είτε για να σπάσετε το κλειδί είτε για να καθορίσετε την αξία του. Ανάλογα με τον αλγόριθμο που χρησιμοποιείται και το μήκος του κλειδιού, η προσπάθεια να σπάσει το κλειδί μπορεί να κυμαίνεται από μια απλή εργασία έως μια ανέφικτη φιλοδοξία.

Ο στόχος της δημιουργίας μιας μεθόδου κρυπτογράφησης είναι η ελαχιστοποίηση του κινδύνου που σχετίζεται με την αποκάλυψη ευαίσθητων πληροφοριών καθιστώντας τις παραβιάσεις συμμόρφωσης και ασφάλειας οικονομικά ανέφικτες ή χρονοβόρες (Bernstein & Lange, 2017). Ο όρος "συντελεστής εργασίας" είναι ένας άλλος τρόπος αναφοράς στο φάσμα της ισχύος του κρυπτογραφικού συστήματος, που αντιπροσωπεύει μια εκτίμηση της προσπάθειας που πρέπει να καταβάλει ένας εισβολέας για να διεισδύσει στην κρυπτογράφηση. Είναι σημαντικό να ληφθεί υπόψη η ισχύς του προστατευτικού μηχανισμού σε σχέση με την ευαισθησία των δεδομένων που κρυπτογραφούνται.

Η ανθεκτικότητα ενός κρυπτοσυστήματος έναντι επιθέσεων από αντιπάλους είναι ένα θέμα που μπορεί να διερευνηθεί από πολλές οπτικές γωνίες. Αυτή η αναγκαιότητα

καθορισμού αντικειμενικών κριτηρίων για την αξιολόγηση της κρυπτογραφικής ισχύος οδήγησε στην ανάπτυξη αρκετών μαθηματικών μοντέλων.

Ένα κρυπτόςυστημα θεωρείται ότι έχει άνευ όρων ασφάλεια όταν το κρυπτογραφημένο κείμενο δεν αποκαλύπτει πληροφορίες σχετικά με το απλό κείμενο σε έναν αντίπαλο. Αυτή η υπόθεση λειτουργεί με την παραδοχή ότι ο αντίπαλος διαθέτει άπειρους υπολογιστικούς πόρους. Αντίθετα, ένα κρυπτόςυστημα χαρακτηρίζεται ως υπολογιστικά ασφαλές όταν η απαιτούμενη υπολογιστική ισχύς του αντιπάλου ξεπερνά τις δικές του δυνατότητες (Bernstein & Lange, 2017). Θεωρείται ότι ο αντίπαλος μπορεί να εκτελέσει μια επίθεση στο κρυπτόςυστημα που απαιτεί πολωνυμική υπολογιστική ισχύ, υποδεικνύοντας ότι οι παράμετροι ασφαλείας του συστήματος μπορούν να εκφραστούν πολωνυμικά τόσο σε χώρο όσο και σε χρόνο. Όταν μπορεί να αποδειχθεί ότι η ασφάλεια ενός κρυπτοσυστήματος ευθυγραμμίζεται με ένα γνωστό και διεξοδικά εξετασμένο πρόβλημα που ταξινομείται ως "σκληρό", θεωρείται αποδεδειγμένα ασφαλές.

3.6 Κρυπτανάλυση

Η επιστήμη της ανάκτησης του απλού κειμένου X από το κρυπτογραφημένο κείμενο Y είναι γνωστή ως κρυπτοανάλυση. Ενώ συχνά γίνεται αντιληπτό ως μια μαθηματική προσέγγιση για την ανάκτηση απλού κειμένου, υπάρχουν και άλλες τεχνικές, όπως η κρυπτανάλυση πλευρικού καναλιού, η οποία μπορεί να αποκαλύψει ένα μυστικό κλειδί, για παράδειγμα, αναλύοντας την κατανάλωση ενέργειας μιας έξυπνης κάρτας.

Τα κρυπτογραφικά συστήματα πρέπει να ακολουθούν την αρχή Kerckhoff, ένα αξίωμα που εισήχθη από τον Auguste Kerckhoffs το 1883, το οποίο δηλώνει ότι ένα κρυπτογραφικό σύστημα πρέπει να παραμένει ασφαλές ακόμα κι αν ο εισβολέας γνωρίζει όλα τα στοιχεία του, εκτός από το μυστικό κλειδί. Είναι σημαντικό να κατανοήσουμε ότι η αρχή Kerckhoffs θεωρείται «αντιδιαισθητική» (Dobraunig, et al., 2015). Η γοητεία της δημιουργίας ενός συστήματος που φαίνεται πιο ασφαλές με την απόκρυψη των λεπτομερειών του είναι ισχυρή. αυτή η προσέγγιση είναι γνωστή ως "ασφάλεια από την αφάνεια". Ωστόσο, τα ιστορικά στοιχεία καταδεικνύουν σταθερά ότι τέτοια συστήματα τείνουν να είναι θεμελιωδώς αδύναμα και μπορούν εύκολα να παραβιαστούν μόλις αποκαλυφθεί ο «μυστικός» σχεδιασμός τους ή αποκαλυφθεί μέσω εναλλακτικών καναλιών. Ένα αξιοσημείωτο παράδειγμα αυτού είναι το Content Scrambling System (CSS) που χρησιμοποιείται για την προστασία του περιεχομένου DVD, το οποίο καταργήθηκε εύκολα μόλις αναλυθεί η κατασκευή του.

4 Αλγόριθμοι και Εργαλεία Κρυπτογράφησης και Κρυπτανάλυσης

4.1 Επιθέσεις ενάντια στους αλγορίθμους κρυπτογράφησης

Κατά την εξέταση της μαθηματικής κρυπτανάλυσης, μπορούμε να εντοπίσουμε τέσσερα διαφορετικά σενάρια με βάση τις πληροφορίες που διαθέτει ο εισβολέας τόσο για το απλό κείμενο όσο και για το κρυπτογραφημένο κείμενο. • Επίθεση χρησιμοποιώντας μόνο κρυπτογραφημένο κείμενο

Η κατανόηση του ζητήματος περιλαμβάνει τις εξισώσεις: $y_1 = ek(x_1)$, $y_2 = ek(x_2)$ και ούτω καθεξής.

Ο στόχος του schemer είναι να αποκτήσει x_1 , x_2 , ... ή να ασφαλίσει το κλειδί k .

Η κατανόηση της υπόθεσης: συγκεκριμένα ζεύγη $(x_1, y_1 = ek(x_1))$, $(x_2, y_2 = ek(x_2))$. Στόχος του συνωμότη: να αποκτήσει το κλειδί k . Επιλεγμένη επίθεση απλού κειμένου Η κατανόηση της υπόθεσης: συγκεκριμένα ζεύγη $(x_1, y_1 = ek(x_1))$, $(x_2, y_2 = ek(x_2))$, από τα οποία έχει τη δυνατότητα να επιλέξει x_1 και x_2 .

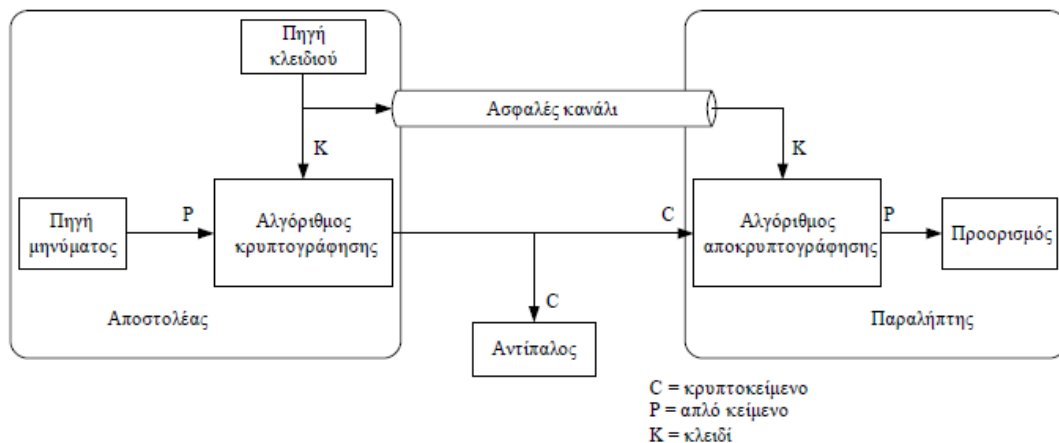
Ο στόχος του συνωμότη είναι να αποκτήσει το κλειδί k μέσω μιας επιλεγμένης επίθεσης κρυπτογραφημένου κειμένου. Αυτό περιλαμβάνει την κατανόηση της εικασίας: συγκεκριμένα ζεύγη $(x_1, y_1 = ek(x_1))$, $(x_2, y_2 = ek(x_2))$, από τα οποία μπορούν να επιλεγούν τα y_1 και y_2 .

Ο στόχος του σχεδιογράφου είναι να αποκτήσει το κρίσιμο κλειδί k .

4.2 Κατηγοριοποίηση κρυπτογραφικών συστημάτων

Τα κρυπτογραφικά συστήματα μπορούν να ταξινομηθούν σε δύο βασικούς τύπους: συμμετρικά και ασύμμετρα. Συχνά αναφέρονται ως συστήματα συμμετρικού κλειδιού, ενός κλειδιού ή μυστικού κλειδιού, τα συμμετρικά κρυπτογραφικά συστήματα χρησιμοποιούν το ίδιο κλειδί τόσο για κρυπτογράφηση όσο και για αποκρυπτογράφηση (Buchanan, et al., 2017). Σε αυτή τη διαδικασία, το απλό κείμενο συνδυάζεται με το

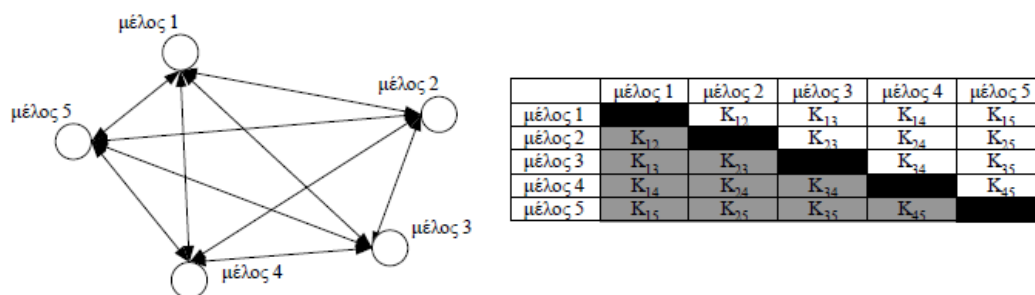
κλειδί και τροφοδοτείται στον αλγόριθμο κρυπτογράφησης, παράγοντας κρυπτογραφημένο κείμενο ως έξοδο. Για την αποκρυπτογράφηση, το κρυπτογραφημένο κείμενο και το ίδιο κλειδί που χρησιμοποιείται κατά την κρυπτογράφηση εισάγονται στον αλγόριθμο αποκρυπτογράφησης. Αυτός ο αλγόριθμος εκτελεί στη συνέχεια τους αντίστροφους μετασχηματισμούς της διαδικασίας κρυπτογράφησης, επαναφέροντας το κείμενο στην αρχική του κατάσταση απλού κειμένου.



Εικόνα 9 Μοντέλο επικοινωνίας συμμετρικού κρυπτοσυστήματος

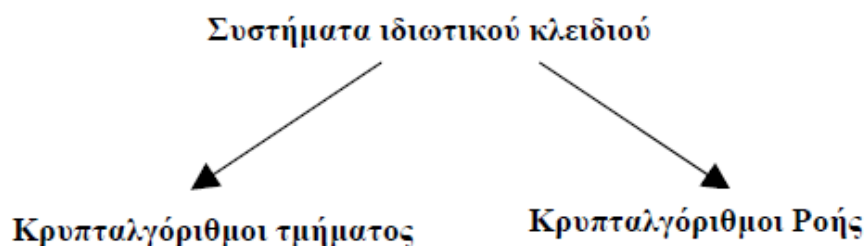
Η αναγκαιότητα χρήσης του ίδιου κλειδιού τόσο για κρυπτογράφηση όσο και για αποκρυπτογράφηση στο κρυπτοσύστημα βασίζεται στην υπόθεση ότι υπάρχει μια ασφαλής μέθοδος για τον αποστολέα και τον παραλήπτη να ανταλλάξουν αυτό το κλειδί. Αυτό εγείρει το ερώτημα: γιατί να ασχοληθούμε καθόλου με την κρυπτογράφηση εάν είναι διαθέσιμο ένα ασφαλές κανάλι; Θα μπορούσαμε απλώς να μεταδώσουμε το κείμενο απευθείας, καθιστώντας την κρυπτογράφηση περιττή.

Μια άλλη σημαντική ευπάθεια υπάρχει στη συμμετρική κρυπτογραφία, καθιστώντας την εφαρμογή της σε ανοιχτά δίκτυα επικοινωνίας με πολλούς συμμετέχοντες σχεδόν ανέφικτη. Αυτή η ευπάθεια είναι γνωστή ως «πρόβλημα της πλατείας».



Εικόνα 10 Πλήθος κλειδιών για $n=5$ μέλη

Έστω ότι n μέλη επικοινωνούν μεταξύ τους χρησιμοποιώντας συμμετρική κρυπτογραφία. Τότε, ανά δύο θα πρέπει να μοιράζονται κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση. Το κάθε μέλος θα πρέπει να αποθηκεύσει $n-1$ διαφορετικά κλειδιά, προκειμένου να μπορεί να επικοινωνήσει με οποιοδήποτε από τα άλλα μέλη. Η συμμετρική κρυπτογραφία κατηγοριοποιείται στους κρυπταλγόριθμους τμήματος και ροής.



Εικόνα 11 Κατηγοριοποίηση συμμετρικής κρυπτογραφίας

4.3 Κρυπταλγόριθμοι τμήματος (block ciphers)

Η ιδέα περιλαμβάνει το διαχωρισμό της σειράς των μηνυμάτων σε τμήματα ομοιόμορφου μήκους, τα οποία στη συνέχεια υποβάλλονται σε κρυπτογράφηση και στη συνέχεια αποκρυπτογράφηση. Το μήνυμα χωρίζεται σε μπλοκ, με κάθε μπλοκ να κρυπτογραφείται ξεχωριστά. Αντί να κρυπτογραφείται κομμάτι προς κομμάτι, η διαδικασία λαμβάνει χώρα σε τμήματα του μηνύματος. Οι διάφοροι τρόποι λειτουργίας, που είναι ουσιαστικά τεχνικές κρυπτογράφησης, χρησιμεύουν ως μέθοδοι για τη σύνδεση τμηματικών κρυπτογραφικών αλγορίθμων. Ο σκοπός τους είναι να ενισχύσουν την κρυπτογραφική

ισχύ και να αποκρύψουν πιο αποτελεσματικά τυχόν ίχνη πληροφοριών απλού κειμένου που μπορεί να υπάρχουν μέσα στο κρυπτογραφημένο κείμενο. Υπάρχουν τέσσερις τυπικοί τρόποι λειτουργίας:

Η πιο απλή μέθοδος κρυπτογράφησης μπλοκ είναι η Λειτουργία Ηλεκτρονικού Βιβλίου Κωδικών (ECB), όπου κάθε μπλοκ απλού κειμένου δημιουργεί με συνέπεια ένα πανομοιότυπο μπλοκ κρυπτογραφημένου κειμένου. Αυτή η τεχνική αντλεί το όνομά της από την αναλογία ενός μεγάλου βιβλίου που περιέχει όλα τα ζεύγη απλού κειμένου και κρυπτογραφημένου κειμένου που αντιστοιχούν σε κάθε κλειδί μέσα στο κρυπτόςυστημα.

Η κρυπτογράφηση ενός τμήματος του απλού κειμένου βασίζεται επίσης στο προηγούμενο μέρος. Πριν από την κρυπτογράφηση, το αρχικό μήνυμα υποβάλλεται σε λειτουργία XOR με το προηγούμενο κρυπτογραφημένο κείμενο. Ένα βασικό χαρακτηριστικό αυτής της μεθόδου είναι ο μηχανισμός αλυσίδας της, ο οποίος διασφαλίζει ότι η αποκρυπτογράφηση οποιουδήποτε δεδομένου μπλοκ κρυπτογραφημένου κειμένου επηρεάζεται από όλα τα προηγούμενα μπλοκ κρυπτογραφημένου κειμένου (Menezes, et al., 2018). Η λειτουργία ανάδρασης κρυπτογράφησης (CFB) λειτουργεί με τρόπο παρόμοιο με το CBC. Σε αυτήν τη λειτουργία, το κρυπτογραφημένο κείμενο δημιουργείται μέσω της εκ νέου κρυπτογράφησης του προηγούμενου κρυπτογραφημένου κειμένου, σε συνδυασμό με μια αποκλειστική συνένωση με το απλό κείμενο. Η διάκριση μεταξύ CBC και CFB έγκειται στο γεγονός ότι το CFB κρυπτογραφεί δεδομένα ένα byte τη φορά, όπου κάθε byte κρυπτογραφείται σε συνδυασμό με τα προηγούμενα επτά byte του κρυπτογραφημένου κειμένου.

Η λειτουργία ανάδρασης εξόδου (OFB) χρησιμεύει ως μέθοδος για τη μετατροπή ενός αλγόριθμου μπλοκ σε αλγόριθμο ροής. Ενώ λειτουργεί παρόμοια με το CFB, ενσωματώνει έναν μηχανισμό σχεδιασμένο να ελαχιστοποιεί τα σφάλματα (Menezes, et al., 2018). Στους κρυπτογράφησης ροής, η διαδικασία κρυπτογράφησης λαμβάνει χώρα κομμάτι προς bit (ή byte προς byte). Μέσα σε ένα ψηφιακό κρυπτόςυστημα, τα αλφάβητα που περιλαμβάνουν απλό κείμενο, κρυπτογραφημένο κείμενο και ροή κλειδιών αποτελούνται από bit. Ένα κρίσιμο στοιχείο ενός κρυπτογραφικού αλγορίθμου ροής είναι η γεννήτρια ροής κλειδιών, η οποία παράγει μια περιοδική ακολουθία κλειδιών. Το αρχικό σημείο αυτής της περιόδου ορίζεται από το κλειδί έναρξης K , το οποίο λειτουργεί επίσης ως το μυστικό κλειδί για το κρυπτόςυστημα. Ουσιαστικά, αυτή η γεννήτρια δημιουργεί μια ψευδοτυχαία ακολουθία δυαδικών ψηφίων που σχηματίζουν το κλειδί,

και αυτά τα μπιτ κλειδιών XORed με τα bit μηνύματος για τη δημιουργία του κρυπτογραφημένου κειμένου και η διαδικασία μπορεί να αντιστραφεί. Η αποκλειστική λειτουργία διαχωρισμού λειτουργεί παρόμοια με το modulo προσθήκης 2.

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

Πίνακας 2 Πίνακας αληθείας για την αποκλειστική διάζευξη

Αρκετοί συμμετρικοί κρυπτογραφικοί αλγόριθμοι βρίσκονται σε εμπορική χρήση τη παρούσα χρονική στιγμή. Οι κυριότεροι είναι (Menezes, et al., 2018):

Αλγόριθμοι	Μήκος Κλειδιού	Ισχύς	Παρατηρήσεις
DES	64	Αδύναμος	Ιδρύθηκε το 1981, έγινε το αμερικανικό πρότυπο για την ασύμμετρη κρυπτογράφηση δεδομένων. Αυτός ο αλγόριθμος μπλοκ, που χρησιμοποιείται από το 1976, είναι ο πιο συχνά χρησιμοποιούμενος, κρυπτογραφώντας δεδομένα σε τμήματα 64 bit με μέγεθος κλειδιού 56 bit (ή 64 bit όταν

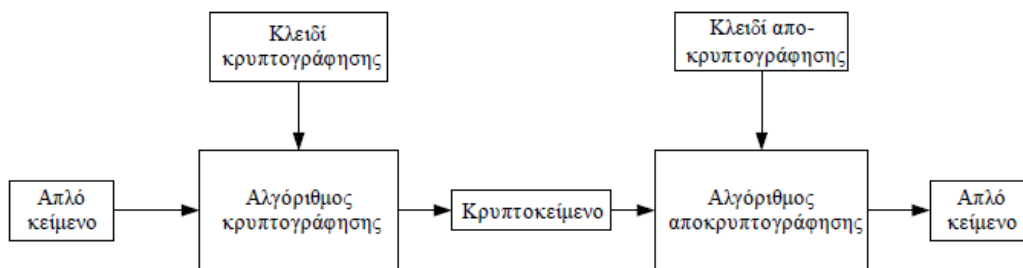
			περιλαμβάνονται 8 bit για ισοτιμία).
3DES	161, 112, 168	Ισχυρός	Κρυπτογραφεί το κείμενο τρεις φορές, χρησιμοποιώντας διαφορετικό κλειδί κάθε φορά
AES	28, 192, 256	Ισχυρός	Πρόκειται για επέκταση του αλγορίθμου DES. Έχει κλειδί 128, 192 ή 256 bit.
IDEA	64, 128	Ισχυρός	Θεωρείται ως μία από τις πιο ασφαλείς επιλογές, δημιουργήθηκε το 1990 από τους Lai και Massey. Αυτή η μέθοδος κρυπτογράφησης έχει σχεδιαστεί παρόμοια με το DES, επεξεργάζεται τμήματα 64-bit και χρησιμοποιεί ένα κλειδί 128-bit.
BLOWFISH	32, 448	Αδύναμος	Δημιουργήθηκε από τη Schneier, αυτή η μέθοδος κρυπτογράφησης επεξεργάζεται τμήματα 64 bit και προσφέρει ένα

			μεταβλητό μήκος κλειδιού, που φτάνει το μέγιστο τα 448 bit. Επιπλέον, λειτουργεί με μεγαλύτερη ταχύτητα από το DES.
RCS	32, 64, 128	Αδύναμος	Μια παραλλαγή του RCS, γνωστή ως RC6, αναπτύχθηκε από τον Ron Rivest για την RSA. Αυτός ο κρυπτογράφος διαθέτει μεταβλητό μήκος κλειδιού, λειτουργεί σε επίπεδο byte και θεωρείται ταυτόχρονα εξαιρετικά ασφαλής και γρήγορος, καθιστώντας τον ευρέως χρησιμοποιούμενο.

Πίνακας 3 Συμμετρικοί κρυπτογραφικοί αλγόριθμοι

Σε αντίθεση με τη συμμετρική κρυπτογραφία, σε ένα ασύμμετρο κρυπτοσύστημα ο αλγόριθμος κρυπτογράφησης είναι ίδιος με τον αλγόριθμο αποκρυπτογράφησης, με τη μόνη διαφορά ότι κατά την αποκρυπτογράφηση χρησιμοποιείται το αντίστοιχο κλειδί. Η ασύμμετρη κρυπτογραφία βασίζεται αποκλειστικά σε μαθηματικές υποθέσεις για τον

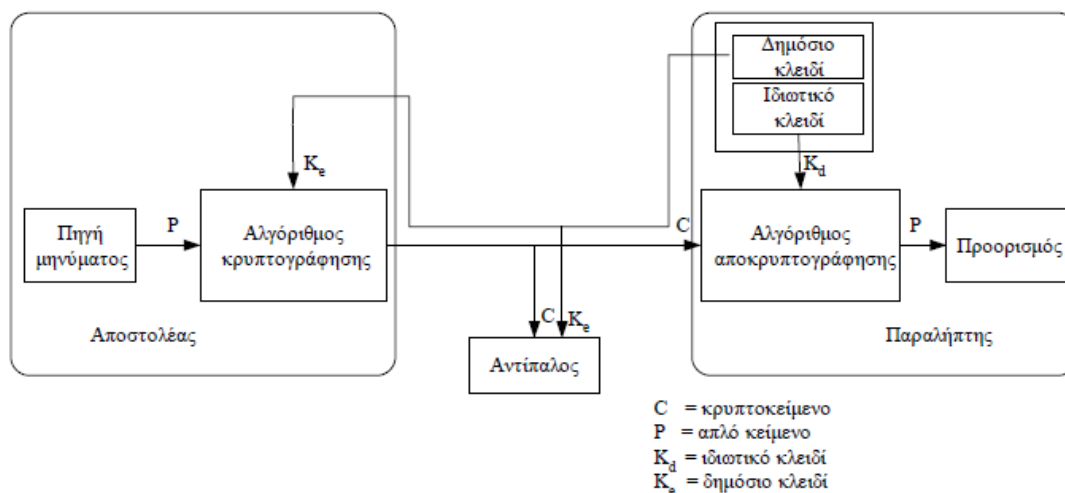
λόγο ότι υπάρχει μαθηματική εξάρτηση μεταξύ του δημόσιου και του ιδιωτικού κλειδιού (Moller, 2003).



Εικόνα 12 Ασύμμετρο κρυπτόςστημα

Σύμφωνα με την ασύμμετρη κρυπτογραφία, το κλειδί κρυπτογράφησης δεν μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση, ή ακόμη καλύτερα, εάν χρησιμοποιηθεί το κλειδί κρυπτογράφησης για αποκρυπτογράφηση, το αποτέλεσμα δεν θα είναι το αρχικό απλό κείμενο. Το κλειδί αποκρυπτογράφησης είναι γνωστό μόνον στον παραλήπτη του μηνύματος. Έτσι σε αντίθεση με τα συμμετρικά κρυπτοσυστήματα, τα κλειδιά δημιουργούνται στον παραλήπτη, ο οποίος είναι ο μόνος που μπορεί να παράγει και να συσχετίσει ένα ζευγάρι ασύμμετρων κλειδιών (Barthe, et al., 2014). Το κλειδί για την κρυπτογράφηση ονομάζεται δημόσιο κλειδί γιατί μπορεί να διατεθεί ελεύθερα χωρίς να απαιτείται ασφαλές κανάλι για τη μετάδοσή του. Το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση είναι το ιδιωτικό κλειδί και παραμένει υπό την κατοχή του παραλήπτη. Έτσι το μοντέλο επικοινωνίας ενός ασύμμετρου κρυπτοσυστήματος δεν περιλαμβάνει ασφαλές κανάλι, αλλά η μετάδοση του μηνύματος περιλαμβάνει τα ακόλουθα στάδια:

1. Ο αποστολέας ζητάει από τον παραλήπτη το δημόσιο κλειδί K_e .
2. Ο παραλήπτης στέλνει το δημόσιο κλειδί μέσω του μη ασφαλούς καναλιού επικοινωνίας.
3. Ο αποστολέας κρυπτογραφεί το μήνυμα P με το δημόσιο κλειδί του παραλήπτη και στέλνει το κρυπτοκείμενο στον παραλήπτη C .
4. Ο παραλήπτης αποκρυπτογραφεί το κρυπτοκείμενο χρησιμοποιώντας το ιδιωτικό κλειδί K_d .

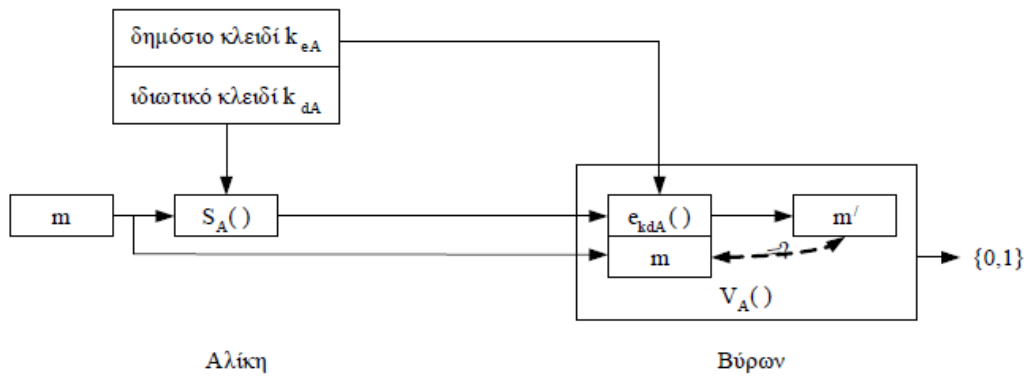


Εικόνα 13 Μοντέλο επικοινωνίας ασύμμετρου κρυπτοσυστήματος

Η βάση της ασύμμετρης κρυπτογραφίας βασίζεται στην ιδέα ότι η εξαγωγή ή η απόκτηση του ιδιωτικού κλειδιού θα πρέπει να είναι υπολογιστικά μη πρακτική. Συγκεκριμένα, περιλαμβάνει μια μονόδρομη συνάρτηση που επιτρέπει τον εύκολο υπολογισμό της εξόδου της, αλλά θέτει σημαντικές προκλήσεις για την αντιστροφή (που σημαίνει ότι για κάθε δεδομένο y_i , είναι αδύνατο να προσδιοριστεί ένα x_i έτσι ώστε: $f(x_i) = y_i$). Οι πρόσθετες πληροφορίες που απαιτούνται για την αντιστροφή αυτής της λειτουργίας αναφέρονται ως trapdoor. Αυτές οι λειτουργίες είναι απαραίτητες για το πλαίσιο των συστημάτων Δημοσίου Κλειδιού (Van Tilborg & Jajodia, 2014).

Ένα συναρπαστικό και πρακτικό χαρακτηριστικό ενός ασύμμετρου κρυπτοσυστήματος είναι η ικανότητα χρήσης ενός ζεύγους ιδιωτικού/δημόσιου κλειδιού αντίστροφα. Συγκεκριμένα, το ιδιωτικό κλειδί μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση απλού κειμένου, ενώ το δημόσιο κλειδί μπορεί να αποκρυπτογραφήσει το κρυπτογραφημένο κείμενο που προκύπτει. Αυτή η λειτουργία αποτελεί τη βάση της λειτουργίας των ψηφιακών υπογραφών. Μόνο ο κάτοχος του ιδιωτικού κλειδιού έχει τη δυνατότητα να κρυπτογραφήσει ένα μήνυμα χρησιμοποιώντας το ιδιωτικό του κλειδί, ενώ ο καθένας μπορεί να εκτελέσει την αποκρυπτογράφηση. Όταν το κρυπτογραφημένο κείμενο συνδυάζεται με το απλό κείμενο, ο παραλήπτης μπορεί να επαληθεύσει την αυθεντικότητα του μηνύματος συγκρίνοντας το αποκρυπτογραφημένο αποτέλεσμα με το αρχικό κείμενο, επιβεβαιώνοντας ότι προέρχεται από τον κάτοχο του ιδιωτικού κλειδιού. Παρακάτω είναι ένα απλό σύστημα ψηφιακής υπογραφής που χρησιμοποιεί ασύμμετρη κρυπτογραφία. Η Αλίκη κρυπτογραφεί το μήνυμα χρησιμοποιώντας το ιδιωτικό της κλειδί και το κρυπτογραφημένο κείμενο που προκύπτει χρησιμεύει ως η ψηφιακή της

υπογραφή για το μήνυμα m . Στη συνέχεια μεταδίδει το μήνυμα μαζί με την ψηφιακή υπογραφή στον Βύρων. Με πρόσβαση στο δημόσιο κλειδί της Αλίκης, ο Βύρων μπορεί να επαληθεύσει την ψηφιακή υπογραφή αποκρυπτογραφώντας το κρυπτογραφημένο κείμενο με αυτό το κλειδί και επιβεβαιώνοντας εάν τα δύο μηνύματα είναι πανομοιότυπα.



Εικόνα 14 Απλό σύστημα ψηφιακής υπογραφής

5 Cryptool

5.1 Το πρόγραμμα Cryptool

Το Cryptool χρησιμεύει ως μια εφαρμογή ανοιχτού κώδικα που έχει σχεδιαστεί για να διδάσκει και να αποσαφηνίζει έννοιες που σχετίζονται με την κρυπτογραφία. Ξεκίνησε το 1998 από γερμανικά πανεπιστήμια και εταιρείες, συμπεριλαμβανομένης της Deutsche Bank, και σκοπός του ήταν να ενισχύσει την ευαισθητοποίηση σε θέματα ασφάλειας. Τελικά, μεταφέρθηκε στην κοινότητα προγραμματισμού ως πρωτοβουλία ανοιχτού κώδικα. Επί του παρόντος, περισσότεροι από 50 συνεισφέροντες από όλο τον κόσμο συμμετέχουν στην ανάπτυξη και τις βελτιώσεις του (Στάθης, 2019).

Το Cryptool δημιουργήθηκε αρχικά στα αγγλικά και έκτοτε έχει μεταφραστεί σε πολλές γλώσσες, όπως γερμανικά, πολωνικά, ισπανικά, γαλλικά και σερβικά. Επιπλέον, η ελληνική κοινότητα έχει ξεκινήσει τη διαδικασία μετάφρασής του στα ελληνικά. Αυτό το λογισμικό λειτουργεί σε σύστημα Windows και υπάρχει επίσης διαθέσιμη έκδοση JCryptool, η οποία απαιτεί την εγκατάσταση της γλώσσας Java. Χρησιμοποιεί βιβλιοθήκες όπως Secude, Cryptovision και OpenSSL (Στάθης, 2019).

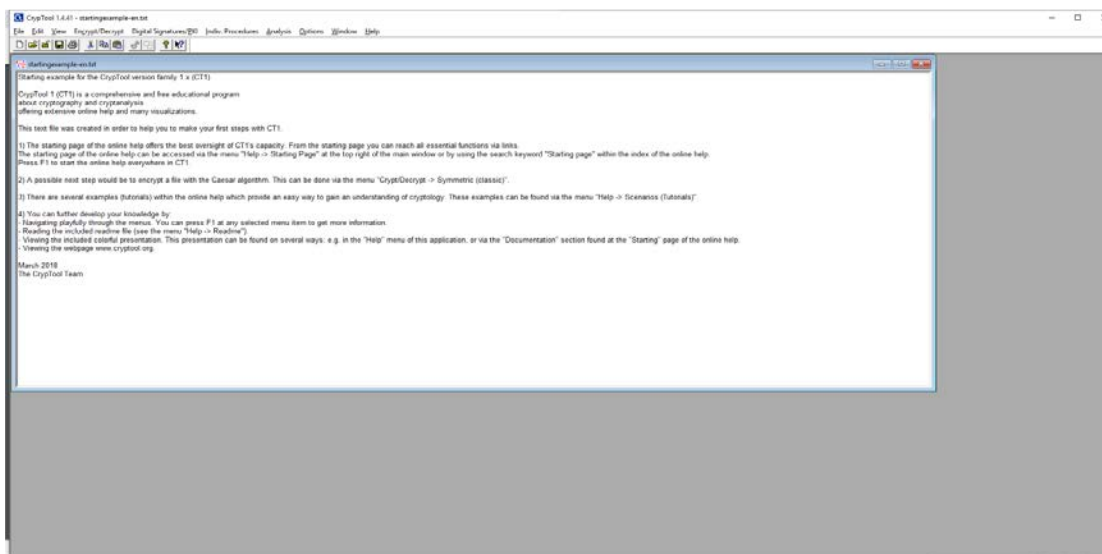
Προορισμένο κυρίως για εκπαιδευτική χρήση, το συγκεκριμένο πρόγραμμα διαθέτει μια διεπαφή χρήστη που είναι εύκολα πλοηγήσιμη, ακόμη και για αρχάριους που θέλουν να μάθουν «κάτι περισσότερο για την κρυπτογραφία». Κατά την εκκίνηση του προγράμματος, οι χρήστες καλωσορίζονται με εκπαιδευτικές οδηγίες που παρουσιάζονται σε μορφή HTML (Στάθης, 2019). Επιπλέον, η επίσημη σελίδα του προγράμματος παρέχει πρόσθετους πόρους, συμπεριλαμβανομένων συνδέσμων λήψης για το Cryptool και ολοκληρωμένη τεκμηρίωση. Αυτό το πρόγραμμα περιλαμβάνει μια ποικιλία κλασικών και ασύμμετρων μεθόδων κρυπτογράφησης (όπως RSA, ψηφιακές υπογραφές, DES κ.λπ.), πολλές από τις οποίες απεικονίζονται μέσω κινούμενων γραφικών για τη βελτίωση της κατανόησης του χρήστη.

Από το 2007, η αρχική έκδοση Cryptool 2.0, που αναπτύχθηκε σε γλώσσα C#/NET/WPF, έχει δει την προσθήκη δύο νέων έργων που χρησιμεύουν ως βελτιώσεις. Αυτά τα έργα παρέχουν οπτικοποίηση αλγορίθμων και διαδραστικά χαρακτηριστικά που διευκολύνουν την εκμάθηση και την κατανόηση τεχνικών κρυπτογράφησης (Στάθης, 2019). Επιπλέον, το Jcryptotool 1.0, που δημιουργήθηκε με χρήση JAVA/Eclipse/RCP/SWT, είναι

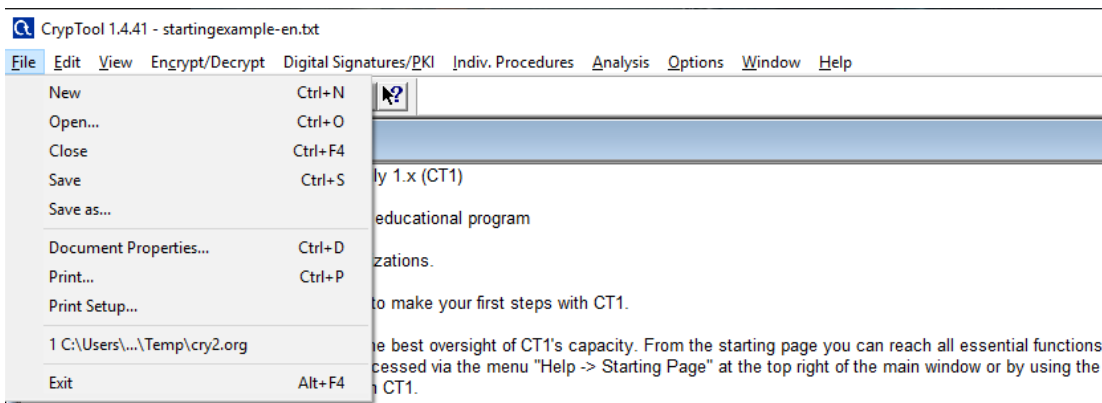
ανεξάρτητο από την πλατφόρμα και προσφέρει μια προσέγγιση με επίκεντρο το έγγραφο και τη λειτουργία.

5.2 Περιήγηση στο περιβάλλον του Cryptool

Το πρόγραμμα Cryptool μπορεί να διαβάσει μόνο αρχεία τύπου *.txt, τα οποία είτε τα έχετε δημιουργήσει ήδη από πιο πριν στον υπολογιστή σας και θέλετε να τα επεξεργαστείτε μέσω του προγράμματος, είτε τα δημιουργείτε απ' ευθείας μέσω του Cryptool. Για να δημιουργήσετε ένα νέο μήνυμα, μέσω του ίδιου του προγράμματος επιλέγετε από το βασικό μενού File → New ή Ctrl+N.

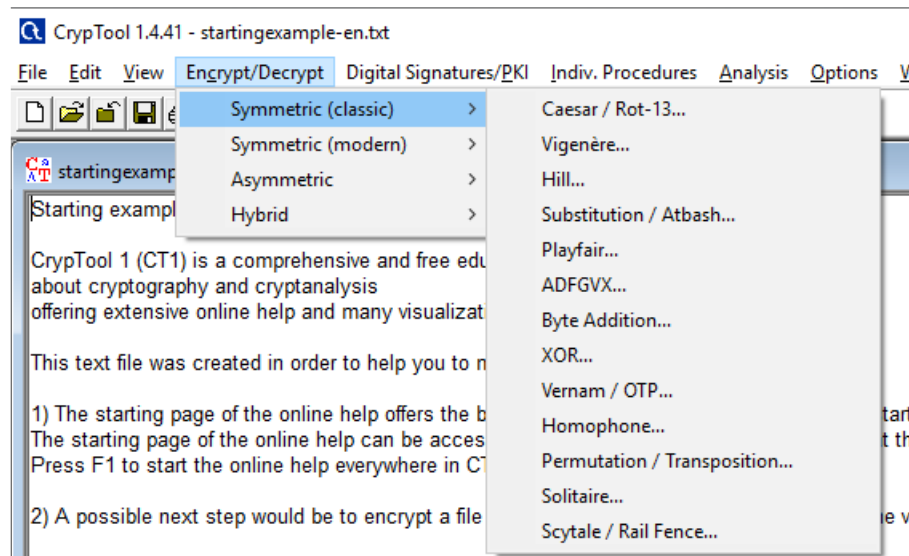


Από το μενού → File μπορείτε διαχειριστείτε το αρχείο το οποίο θα χρησιμοποιήσετε όπως δημιουργήσετε ή να ανοίξετε ένα ήδη υπάρχων αρχείο, να το αποθηκεύσετε και να το εκτυπώσετε.

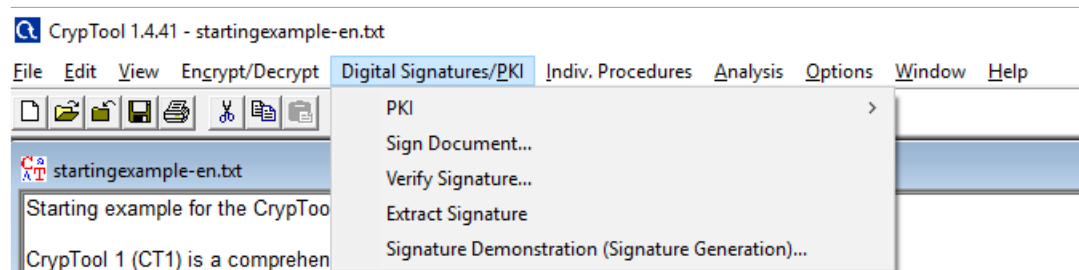


Η καρτέλα Edit αφορά επιλογές επεξεργασίας του κειμένου το οποίο έχετε επιλέξει ενώ η καρτέλα View παρέχει δυνατότητες με τις οποίες μπορείτε εσείς να ορίσετε την εργαλειοθήκη με την οποία θα δουλεύεται .

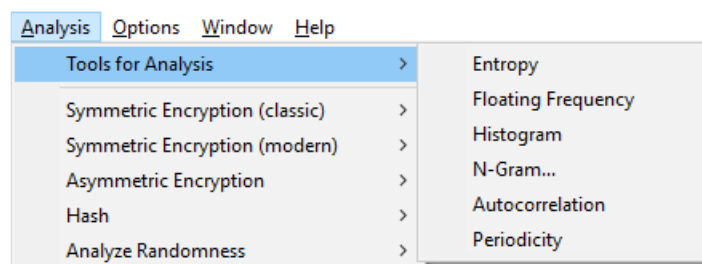
Από το μενού → Encrypt/Decrypt είναι ίσως η πιο βασική λειτουργία του προγράμματος καθώς μέσω αυτού επιλέγεται ποιον αλγόριθμο επιθυμείτε να χρησιμοποιήσετε για κρυπτογράφηση ή αποκρυπτογράφηση του αρχείου. Ο κάθε αλγόριθμος κατατάσσεται σε μια από τις τέσσερις κατηγορίες (Συμμετρική (μοντέρνα ή κλασσική) , ασύμμετρη και υβριδική) κρυπτογράφηση - αποκρυπτογράφηση.



Από το μενού η καρτέλα Digital Signatures/PKI αφορά επιλογές για να ορίσουμε ψηφιακή υπογραφή στο κείμενο μας.



Από το μενού η επιλογή Analysis μας επιτρέπει με την χρήση κατάλληλων εργαλείων να αναλύσουμε το κρυπτογραφημένο ή το αρχικό κείμενο και να εξάγουμε πολύ χρήσιμα συμπεράσματα για την εύρεση τρωτών σημείων των αλγορίθμων που χρησιμοποιήθηκαν.



Τέλος από το μενού η καρτέλα Option αφορά ρυθμίσεις που μπορούμε να κάνουμε στο πρόγραμμα και να επιλέξουμε διάφορες επιλογές του προγράμματος πχ επιλογή font

γραμματοσειράς, εύρος τιμών στα οποία θα εμφανίζονται τα αποτελέσματα (ιστογράμματα) κ.α.

Η επιλογή window αφορά ρυθμίσεις σχετικά με την εμφάνιση παραθύρου του προγράμματος Cryptool και στην καρτέλα Help μπορούμε να βρούμε χρήσιμες πληροφορίες σχετικά με το πρόγραμμα , διάφορα tutorial σχετικά με τους αλγορίθμους που χρησιμοποιεί και γενικά για τις λειτουργίες που προσφέρει το πρόγραμμα.

Το Cryptool ομαδοποιεί τις λειτουργίες του σε Κρυπτογράφηση/Αποκρυπτογράφηση ενώ για κάθε επιμέρους κατηγορία την χωρίζει σε υποκατηγορίες.

5.3 Ψηφιακή Υπογραφή με το Cryptool 1

Η ψηφιακή υπογραφή αποτελεί την σημαντικότερη εξέλιξη όσον αφορά την εργασία που έχει γίνει πάνω στην κρυπτογραφία δημόσιου κλειδιού. Παρέχει ένα σύνολο χαρακτηριστικών ασφαλείας που θα ήταν δύσκολο να υλοποιηθούν διαφορετικά. Στην ουσία αποτελεί ένα κομμάτι κώδικα που περιέχει πληροφορίες οι οποίες εξασφαλίζουν την εγκυρότητα του εγγράφου.

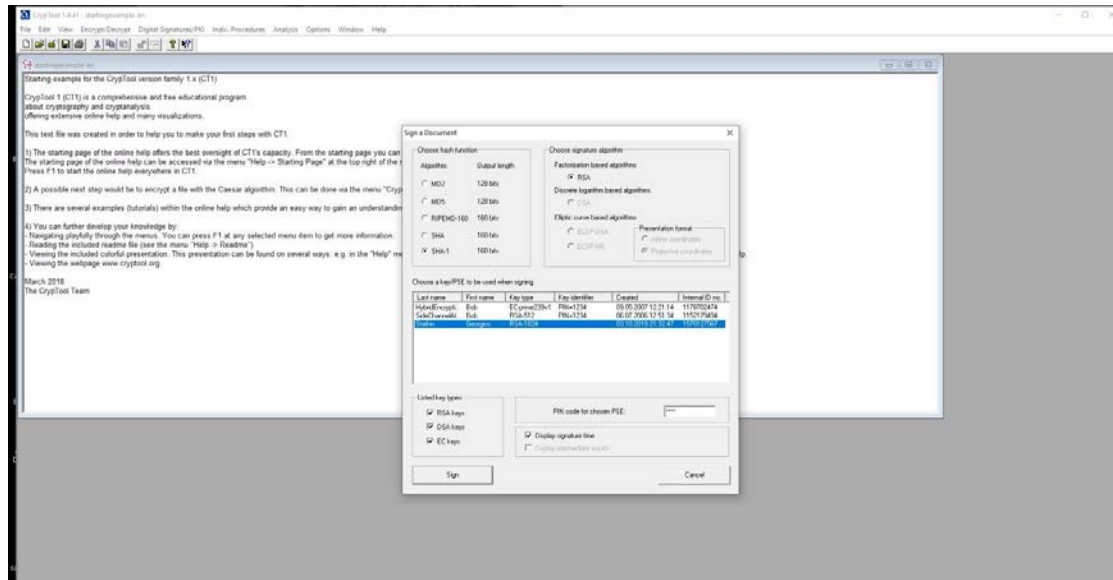
Έστω ότι επιλέγουμε ένα δικό μας κείμενο, και με χρήση του Cryptool εφαρμόζουμε ψηφιακή υπογραφή στο κείμενο σας

Έστω ότι θέλω να εφαρμόσω ψηφιακή υπογραφή στο παρακάτω κείμενο

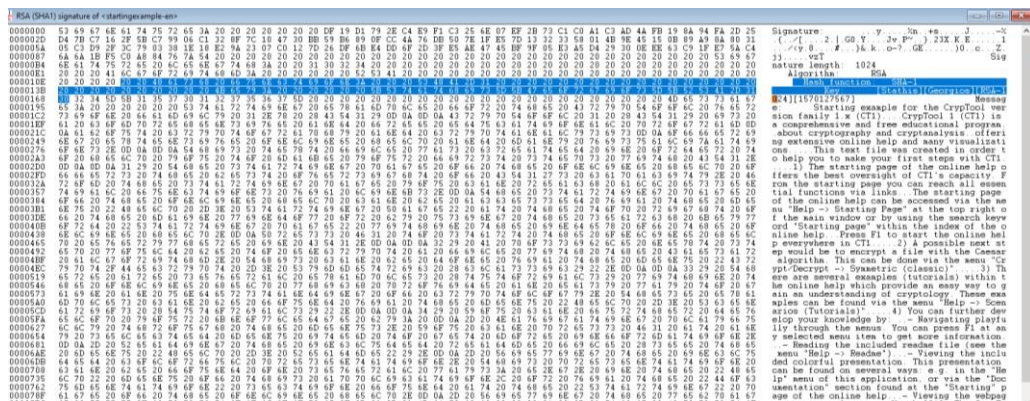


Επιλέγω Digital Signatures/PKI → Sign Document→ και εμφανίζεται το παρακάτω παράθυρο

Στο συγκεκριμένο παράθυρο μπορούμε να επιλέξουμε τον αλγόριθμο Hash Function που χρησιμοποιούμε, τον αλγόριθμο κρυπτογραφίας δημοσίου κλειδιού και το πιστοποιημένο ζεύγος κλειδίων. Για ψηφιακή υπογραφή βάζουμε στο αντίστοιχο κελί το PIN που έχουμε καθορίσει για το πιστοποιημένο ζεύγος κλειδίων και πατάμε το κουμπί Sign

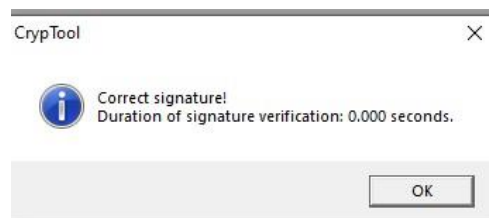
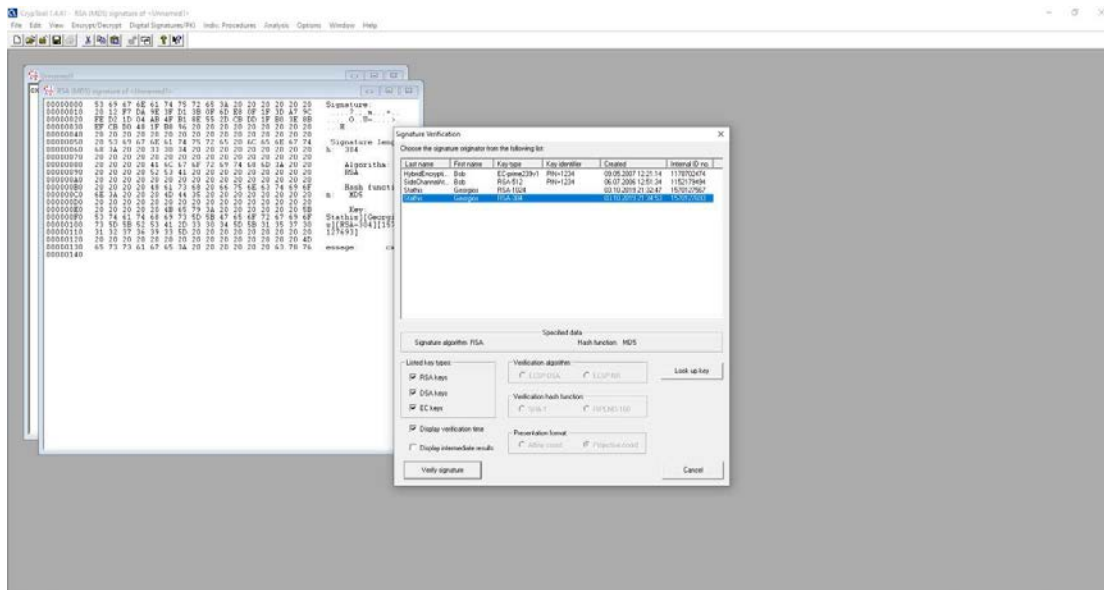


Στο συγκεκριμένο παράδειγμα υπογράφηκε ψηφιακά το αρχείο startingexample.txt με την συνάρτηση κατακερματισμού SHA1.



Στο κείμενο που προέκυψε εντοπίστηκε η ψηφιακή υπογραφή και η συνάρτηση κατακερματισμού που χρησιμοποιήθηκε.

Με την βοήθεια του Cryptool μπορούμε να διασφαλίσουμε την αξιοπιστία της ψηφιακής υπογραφής. Από το μενού επιλέγουμε το κατάλληλο ζεύγος κλειδίων. Στη συνέχεια πατάμε Verify Signature ώστε να ολοκληρωθεί η διαδικασία της επικύρωσης της ψηφιακής υπογραφής και θα εμφανιστεί το αντίστοιχο μήνυμα εάν ήταν επιτυχής η επικύρωση ή όχι.



5.4 Cryptool 2.0 και Κρυπτογράφημα ΚΑΙΣΑΡΑ

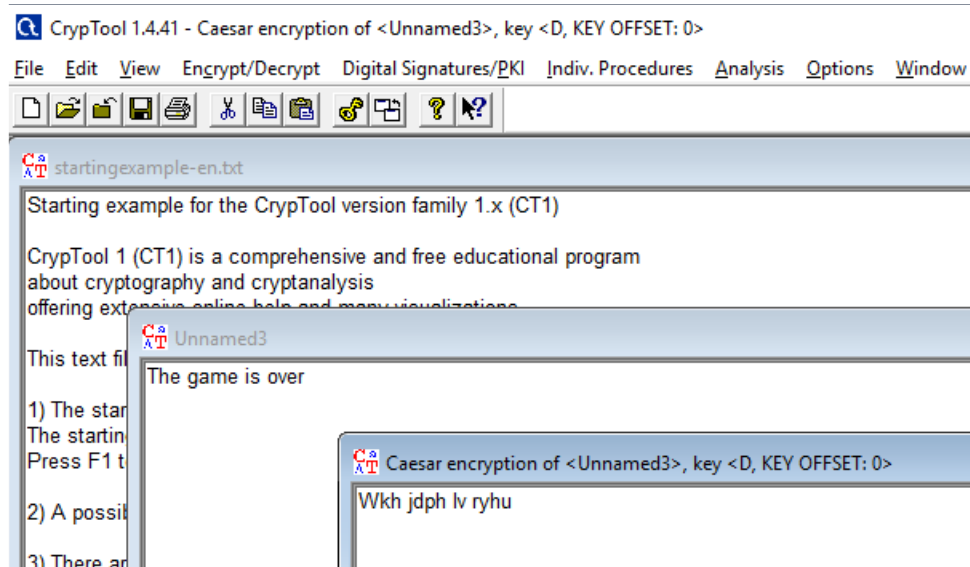
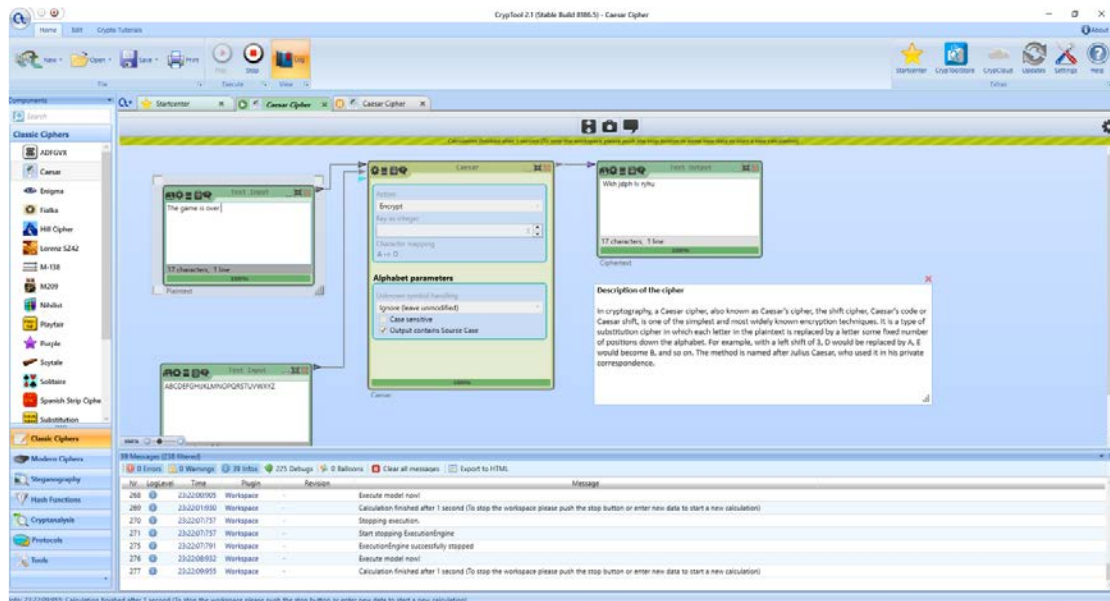
Ο αλγόριθμος του Καίσαρα είναι από τα πρώτα κρυπτογραφικά σχήματα που χρησιμοποιήθηκαν και ανήκει στην κατηγορία των μεταθετικών κρυπτογραφημάτων. Ο Ιούλιος Καίσαρας στα γράμματα του, αντικαθιστούσε το πρώτο γράμμα του αλφάβητου με το τέταρτο (ή τρεις θέσεις αριστερά...δηλαδή όπου Δ στο κρυπτογράφημα = Α στο κανονικό κείμενο):

κανονικό: Α Β Γ Δ Ε Ζ Η Θ Ι Κ Λ Μ Ν Ξ Ο Π Ρ Σ Τ Υ Φ Χ Ψ Ω καίσαρας: Δ Ε Ζ Η Θ Ι Κ Λ Μ Ν Ξ Ο Π Ρ Σ Τ Υ Φ Χ Ψ Ω Α Β Γ Ιστορικές πηγές αναφέρουν ότι ο Καίσαρας είχε κάνει την παρακάτω δήλωση μια μέρα πριν δολοφονηθεί[12]: Για να σπάσουμε ένα τέτοιο μήνυμα, και εφόσον δεν ξέρουμε ότι η μετάθεση είναι κατά 3 γράμματα αριστερά, ο πιο ευθύς τρόπος προσέγγισης είναι να πάρουμε ένα τμήμα του και να γράψουμε όλες τις πιθανές μεταθέσεις των γραμμάτων έως ότου κάποια λέξη αποκτήσει νόημα.

Ο συγκεκριμένος αλγόριθμος θεωρεί το αλφάβητο κυκλικό, δηλαδή το γράμμα μετά το Ζ είναι το Α. Γενικά, ο αλγόριθμος μπορεί να κάνει μετατόπιση κατά k θέσεις, επομένως μπορεί να γραφεί ως εξής: $C = E(k,p) = (p+k) \bmod 26$, δηλαδή κάθε γράμμα p του αρχικού μηνύματος αντικαθίσταται με το γράμμα k του κρυπτογραφημένου αλφάβητου.

Έτσι, συμπεραίνουμε ότι ο συγκεκριμένος αλγόριθμος δεν είναι ιδιαίτερα ασφαλής και μπορεί να σπάσει πολύ εύκολα εξαιτίας του πολύ μικρού κλειδιού που χρησιμοποιεί και διότι μπορεί να πάρει πολύ λίγες διαφορετικές τιμές (πχ 26 για το αγγλικό αλφάβητο).

Χρησιμοποιώντας την έκδοση Cryptool 2.1 κρυπτογραφήθηκε με ολίσθηση 3 γραμμάτων η έκφραση 'The game is over' η οποία αντιστοιχεί στην κρυπτογραφημένη έκφραση Wkh jdph lv ryhu



Επιλέγουμε το αλφάβητο να ξεκινάει από το 0 (value of the first alphabet character) και Number value = 3 (δηλαδή ολίσθηση κατά 3 χαρακτήρες). Πράγματι παρατηρείται ότι το αποτέλεσμα είναι το ίδιο.

5.5 Υβριδική κρυπτογράφηση και αποκρυπτογράφηση

Η συγκεκριμένη κρυπτογράφηση αποτελεί έναν συνδυασμό συμμετρικών και ασύμμετρων μεθόδων κρυπτογράφησης. Με αυτόν τον τρόπο συνδυάζονται τα πλεονεκτήματα και των δυο μεθόδων ώστε να έχουμε τα βέλτιστα αποτελέσματα. Συγκεκριμένα τα δεδομένα κρυπτογραφούνται συμμετρικά όμως τα κλειδιά παραδίδονται με ασύμμετρη κρυπτογράφηση. Η συγκεκριμένη κρυπτογραφία μπορεί να χρησιμοποιηθεί για πολλούς παραλήπτες ταυτόχρονα.

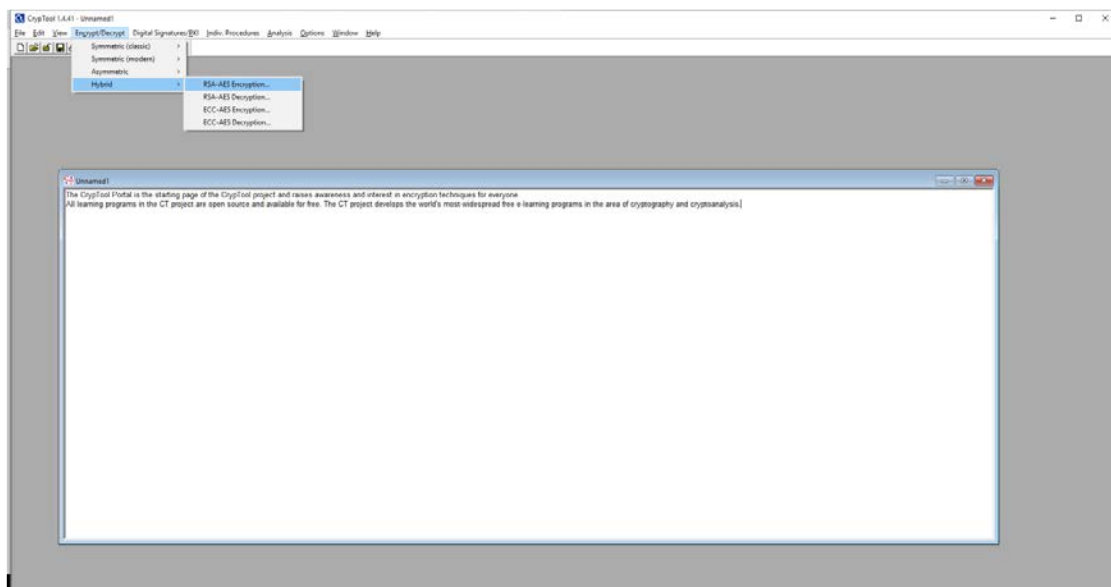
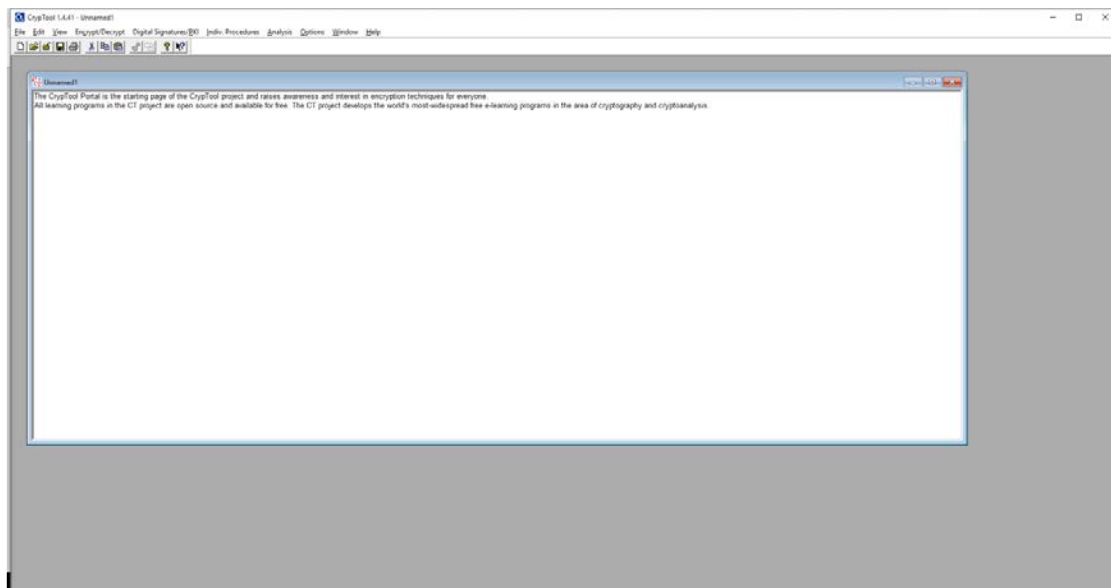
Τα βήματα για την υβριδική κρυπτογραφία είναι τα εξής:

1. Δημιουργείται ένα συμμετρικό κλειδί κρυπτογραφίας με χρήση ενός αλγορίθμου συμμετρικής κρυπτογραφίας (πχ του DES ή AES)
2. Η αρχική πληροφορία κρυπτογραφείται με το συμμετρικό κλειδί που έχει δημιουργηθεί.
3. Το συμμετρικό κλειδί κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη.
4. Τα δυο κρυπτογραφημένα κείμενα αποτελούν τον ψηφιακό φάκελο του παραλήπτη.

Αρχικά, ο αποστολέας κρυπτογραφεί τα δεδομένα με ένα τυχαίο κλειδί που έχει προηγουμένως δημιουργήσει. Τα δεδομένα μπορούν να αποκρυπτογραφούνται από τον παραλήπτη με το ίδιο κλειδί (συμμετρική κρυπτογράφηση). Τώρα, ο αποστολέας πρέπει να κρυπτογραφήσει το κλειδί (που έχει προηγουμένως δημιουργήσει) ασύμμετρα. Στη συνέχεια, το κλειδί και τα δεδομένα μπορούν να σταλούν στον παραλήπτη. Τέλος, ο παραλήπτης μπορεί να αποκρυπτογραφήσει το κλειδί με το ιδιωτικό του κλειδί και με το κοινό πλέον κλειδί μπορεί να αποκρυπτογραφήσει τα δεδομένα.

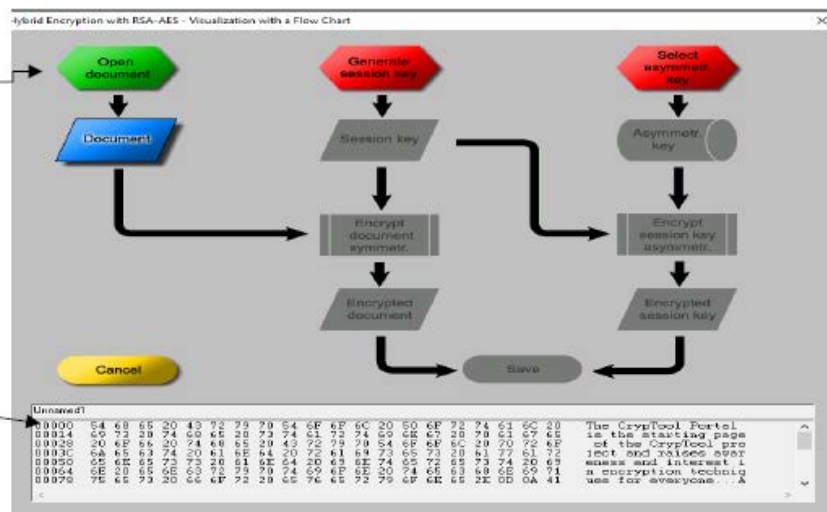
Με την χρήση του Cryptool, χρησιμοποιώντας υβριδική κρυπτογραφία, κρυπτογραφούμε το εξής κείμενο: The CrypTool Portal is the starting page of the CrypTool project and raises awareness and interest in encryption techniques for everyone.

All learning programs in the CT project are open source and available for free. The CT project develops the world's most-widespread free e-learning programs in the area of cryptography and cryptanalysis.



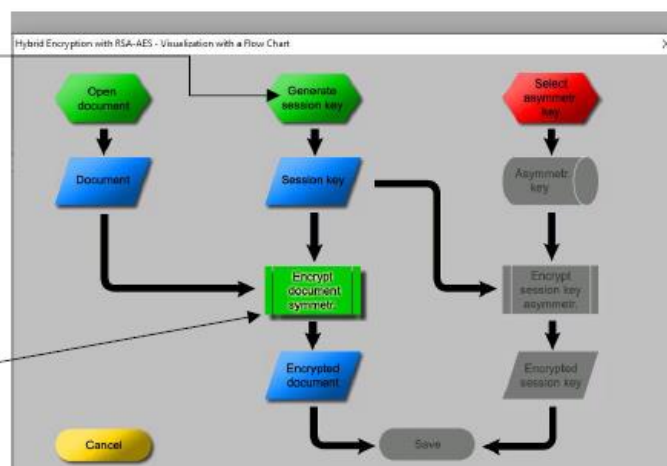
Άνοιγμα του εγγράφου

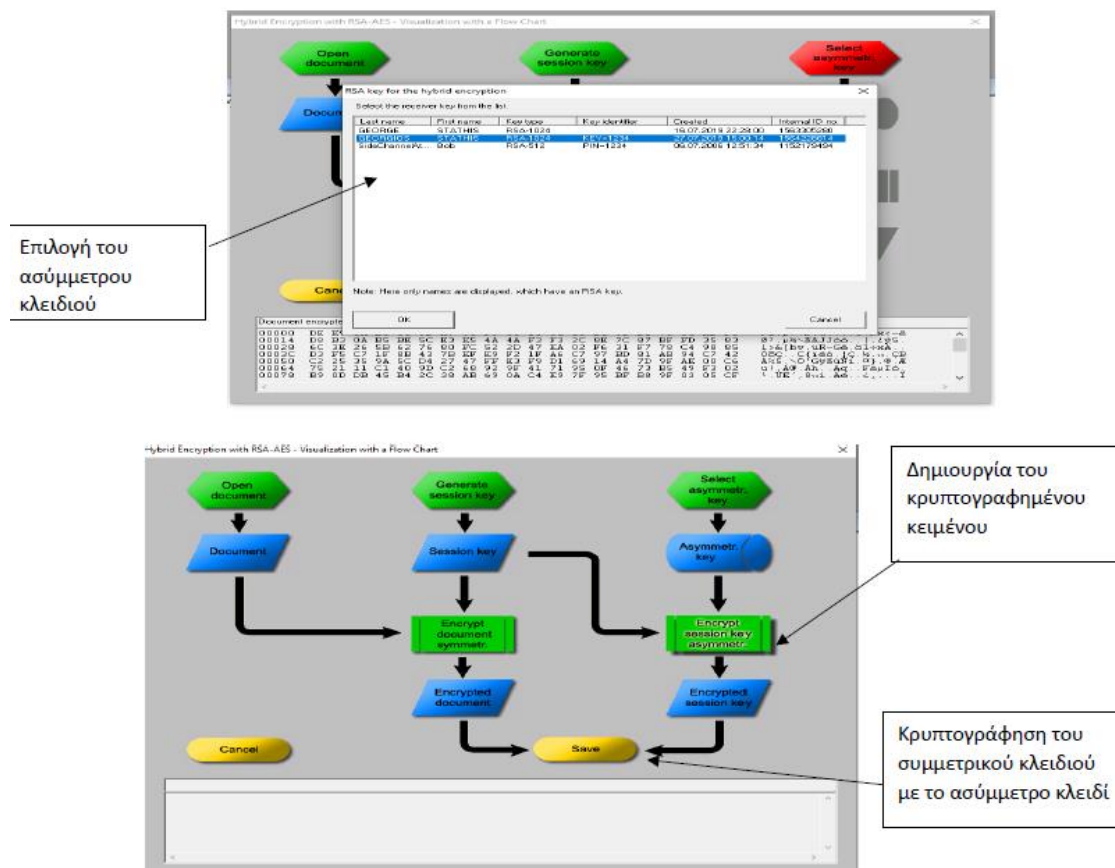
Προβολή του εγγράφου



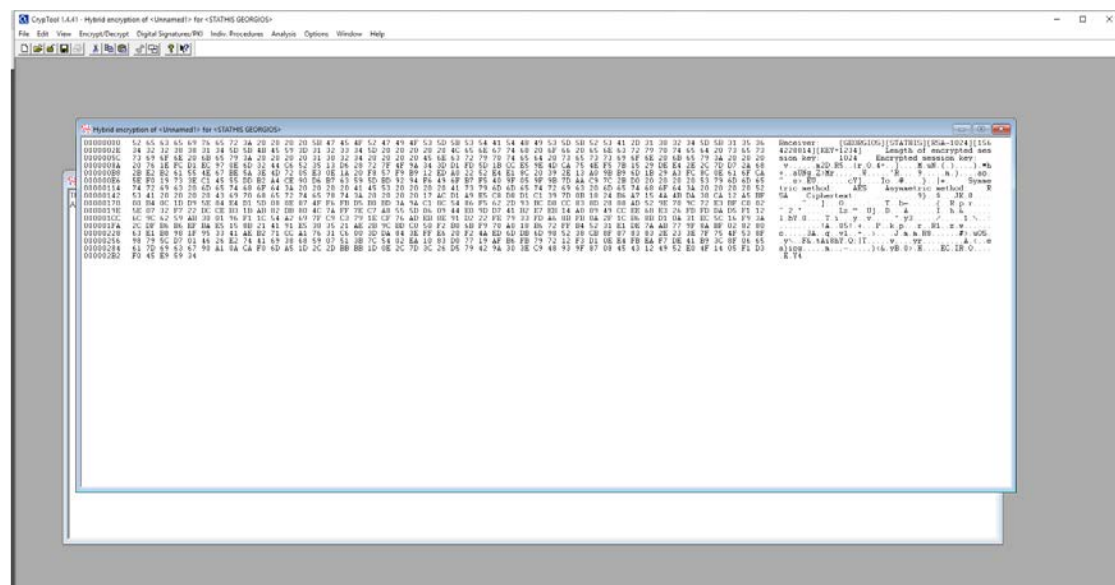
Δημιουργία συμμετρικού κλειδιού

Κρυπτογράφηση του αρχικού κειμένου





Παρακάτω εμφανίζεται το κρυπτογραφημένο κείμενο:



6 Ψηφιακές Υπογραφές

Ο όρος "υπογραφή" παραδοσιακά προκαλεί την εικόνα ενός χειρόγραφου σήματος σε έντυπα έγγραφα, υποδηλώνοντας την ταυτότητα, την πρόθεση, τη συγκατάθεση και τη διαβεβαίωση του υπογράφοντος ότι είναι νομικά υποχρεωμένος από το περιεχόμενο του εν λόγω εγγράφου, διασφαλίζοντας ότι η υπογραφή δεν μπορεί να αρνηθεί σε οποιοσδήποτε μελλοντικές συνθήκες. Όταν συζητάμε για ηλεκτρονικές υπογραφές, αναφερόμαστε σε ψηφιακές υπογραφές που παράγονται μέσω κρυπτογραφικών μεθόδων, παρά σε χειρόγραφες υπογραφές που παράγονται μέσω μεθόδων ηλεκτρονικής μεταφοράς όπως η σάρωση (Gayathri, et al., 2020).

Η φράση ψηφιακή ή ηλεκτρονική υπογραφή αναφέρεται στη συλλογή των bit που είτε προστίθενται από τον αποστολέα σε ένα έγγραφο είτε συνδέονται λογικά με αυτό. Αυτές οι υπογραφές εξυπηρετούν βασικές λειτουργίες: επαληθεύουν ότι τα μεταδιδόμενα δεδομένα παραμένουν αναλλοίωτα, παρέχουν μη απόρριψη για το μήνυμα και επαληθεύουν την ταυτότητα του αποστολέα των πληροφοριών. Σύμφωνα με σχετική οδηγία (1999/93/EK) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, η Ελλάδα θέσπισε το προεδρικό διάταγμα 150/2001, το οποίο θεσπίζει ίσο καθεστώς για τις ψηφιακές και τις χειρόγραφες υπογραφές, ενσωματώνοντάς τις πλήρως.

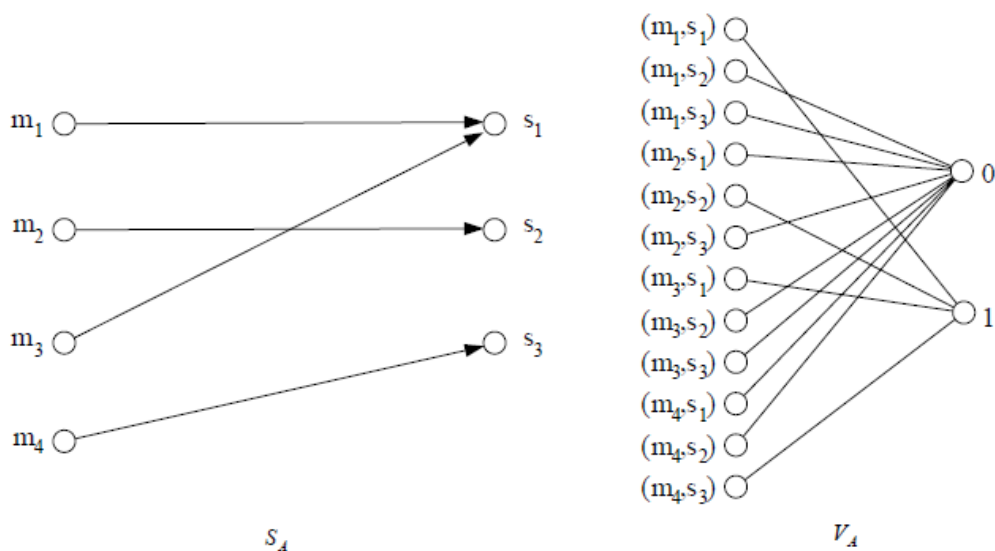
Μια ψηφιακή υπογραφή προέρχεται από ασύμμετρη κρυπτογραφία. Είναι σημαντικό να τονιστεί ότι κατά τη δημιουργία μιας ψηφιακής υπογραφής, οι πληροφορίες που υπογράφονται παραμένουν μη κρυπτογραφημένες. Αντίθετα, παράγεται μια σύντομη μαθηματική περίληψη (πέψη). Το έχουμε εξετάσει λεπτομερέστερα:

Έστω ότι το M αντιπροσωπεύει μια συλλογή μηνυμάτων, το S υποδηλώνει ένα σύνολο τιμών και το SA σημαίνει μια συνάρτηση μετασχηματισμού $SA: M \rightarrow S$ που σχετίζεται με μια οντότητα που προσδιορίζεται ως A . Το σύνολο S αποτελείται από υπογραφές, όπου μόνο η οντότητα A μπορεί να υπολογίσει "εύκολα". Η τιμή $SA(m) = s \in S$ για οποιοδήποτε $m \in M$. Αυτή η διαδικασία αναφέρεται ως πράξη υπογραφής.

Στους ορισμούς που παρέχονται παραπάνω, η λέξη "ευκολία" αναφέρεται στις προκλήσεις που αντιμετωπίζει η οντότητα που προσπαθεί να υπολογίσει την αντίστοιχη συνάρτηση. Μεταξύ των μηνυμάτων και των υπογραφών, μόνο η οντότητα A μπορεί να

προσδιορίσει το s έτσι ώστε για ένα συγκεκριμένο $m \in M$, να ισχύει ότι $SA(m) = s$, ενώ για οποιονδήποτε αντίπαλο, η εκτέλεση αυτού του υπολογισμού είναι υπολογιστικά ανέφικτη. Όταν η οντότητα A αποκαλύπτει ένα ζεύγος (s, m) όπου $SA(m)$ ισούται με s , πρέπει να είναι υπολογιστικά εφικτό να επιβεβαιωθεί ότι πράγματι $SA(m) = s$ για να θεωρηθεί έγκυρη η υπογραφή. Αυτή η διαδικασία επαλήθευσης διευκολύνεται από τη λειτουργία επαλήθευσης VA .

Οι λειτουργίες SA για ψηφιακή υπογραφή και VA για επαλήθευση σχηματίζουν ένα σύστημα ψηφιακής υπογραφής για την οντότητα A . Θεωρήστε το σύνολο μηνυμάτων $M = \{m_1, m_2, m_3, m_4, m_5\}$ και το σύνολο υπογραφών $S = \{s_1, s_2, s_3\}$. Οι διαδικασίες υπογραφής και επαλήθευσης απεικονίζονται στο παρακάτω σχήμα.



Εικόνα 15 Σύστημα ψηφιακής υπογραφής

Στην πραγματικότητα, ο συνολικός αριθμός των μηνυμάτων υπερβαίνει τον συνολικό αριθμό των υπογραφών. Στην πραγματικότητα, υπάρχουν σημαντικά περισσότερα μηνύματα από ό,τι πιθανές υπογραφές. Αυτό οδηγεί σε προκλήσεις σε δίκτυα που ανταλλάσσουν πολυάριθμα και ουσιαστικά μηνύματα, όπου η κίνηση μπορεί να αυξηθεί σε μη διαχειρίσιμα επίπεδα και η παραγωγικότητα μπορεί να μειωθεί. Ενώ το σύστημα ψηφιακής υπογραφής καθιερώνει μια λειτουργία υπογραφής που είναι ένα προς ένα, στερείται διασφαλίσεων έναντι επιθέσεων πλαστογραφίας, σημειώνοντας αυτό ως το δεύτερο μειονέκτημα του συστήματος.

6.1 Συναρτήσεις κατακερματισμού ή κατατεμαχισμού ή κατάτμησης (hash functions)

Οι συναρτήσεις κατακερματισμού είναι υπολογιστικά εφικτές συναρτήσεις που αντιστοιχίζουν σειρές bits μεταβλητού μεγέθους σε σειρές bits σταθερού μήκους. Οι κυριότερες χρήσεις των συναρτήσεων κατακερματισμού στην κρυπτογραφία είναι στις ψηφιακές υπογραφές και στα πρωτόκολλα αναγνώρισης.

Οι hash συναρτήσεις αποτελούν δομικές κρυπτογραφικές πράξεις σε πολλά κρυπτοσυστήματα αλλά κατεξοχήν αποτελούν βασικούς μηχανισμούς για την υλοποίηση της ακεραιότητας και αυθεντικοποίησης των δεδομένων. Ορίζουμε μια συνάρτηση hash (Σχήμα 5.12) $h:F^* \rightarrow G_n$ αντιστοιχίζει ένα στοιχείο $x \in F^*$ αυθαίρετου μήκους, στο στοιχείο $y \in G_n$ με συγκεκριμένο μήκος n : $y=h(x)$.

Μια κρυπτογραφική συνάρτηση hash είναι μια συνάρτηση hash με τις ακόλουθες ιδιότητες:

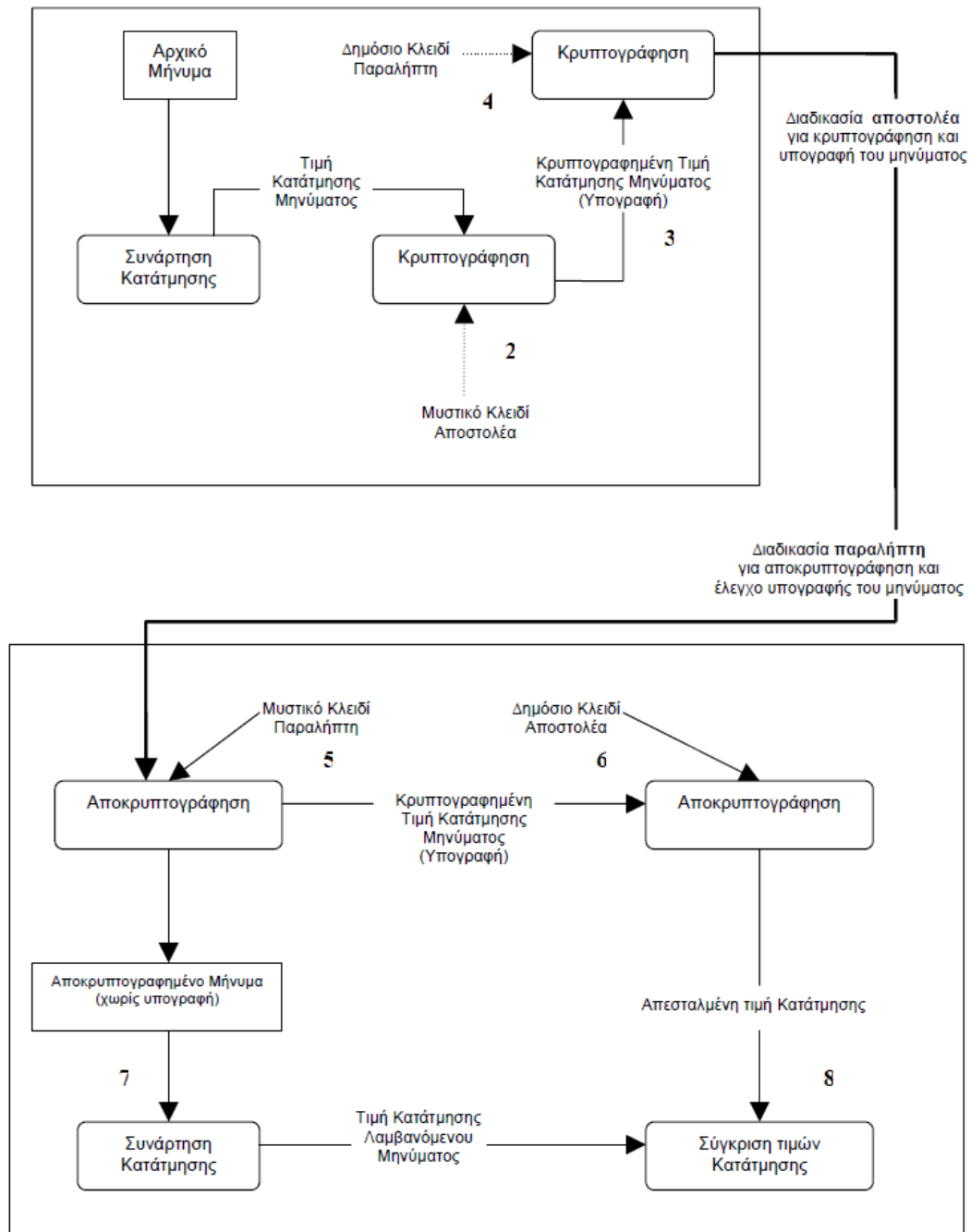
1. δοθέντος y , είναι υπολογιστικά αδύνατο να βρεθεί x τέτοιο ώστε $h(x) = y$
2. δοθέντων $x, h(x)$, είναι υπολογιστικά αδύνατο να βρεθεί x' τέτοιο ώστε $h(x') = h(x)$
3. είναι υπολογιστικά αδύνατο να βρεθούν $x_1, x_2 \in F^*$, τέτοια ώστε, $h(x_1) = h(x_2)$.

Σε πρακτικές εφαρμογές, είναι δυνατή η παράκαμψη μόνο ορισμένων ιδιοτήτων κρυπτογραφικών συναρτήσεων κατακερματισμού, ανάλογα με τη συγκεκριμένη περίπτωση χρήσης. Κατά συνέπεια, οι οικογένειες αυτών των συναρτήσεων κατακερματισμού κατηγοριοποιούνται με βάση κοινά χαρακτηριστικά. Συγκεκριμένα, αυτές οι συναρτήσεις που διατηρούν τις ιδιότητες (1) και (2) αναφέρονται ως μονόδρομες συναρτήσεις κατακερματισμού, ενώ αυτές που υποστηρίζουν τις ιδιότητες (2) και (3) είναι γνωστές ως συναρτήσεις κατακερματισμού ανθεκτικές σε σύγκρουση (συναρτήσεις κατακερματισμού αντίστασης σύγκρουσης). (Berman, et al., 2018).

Οι κατηγορίες κρυπτογραφικών συναρτήσεων κατακερματισμού που χρησιμοποιούνται για τον έλεγχο ταυτότητας και την ακεραιότητα ταξινομούνται σε κωδικούς ελέγχου ταυτότητας μηνυμάτων και κωδικούς ανίχνευσης τροποποιήσεων (Berman, et al., 2018). Ένας Κωδικός ελέγχου ταυτότητας μηνυμάτων (MAC) χρησιμεύει ως μια μονόδρομη συνάρτηση κατακερματισμού κρυπτογράφησης που παρέχει περιορισμένη αντίσταση έναντι συγκρούσεων. Είναι υπολογιστικά ανέφικτο να προσδιοριστεί το x' έτσι ώστε το $hk(x')$ να ισούται με $hk(x)$ όταν δίνονται τα x και $hk(x)$.

Ο Κώδικας Ανίχνευσης Τροποποίησης (MDC) λειτουργεί ως μονόδρομη, χωρίς κλειδί κρυπτογραφική συνάρτηση κατακερματισμού που παρέχει περιορισμένη αντίσταση σε συγκρούσεις: είναι υπολογιστικά ανέφικτο να προσδιοριστεί το x' έτσι ώστε το $h(x')$ να ισούται με $h(x)$ όταν δίνονται x και $h(x)$ (Berman, et al., 2018). Η απόφαση για χρήση είτε του MAC είτε του MDC εξαρτάται από τις ιδιαίτερες συνθήκες της εφαρμογής και την εικαζόμενη φύση της επίθεσης του αντιπάλου.

Υπάρχουν πολυάριθμες αναγνωρισμένες συναρτήσεις κατακερματισμού, που διαθέτουν μεγέθη κατακερματισμού 128 bit (RSA, MD2, MD4) και 160 bit (SHA-1, MD5). Η δημιουργία των RSA, MD2, MD4 και MD5 αποδίδεται στον Ron Rivest, ενώ το SHA-1 αναπτύχθηκε από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST). Παρακάτω, ένα παράδειγμα δείχνει τη χρήση συναρτήσεων διαμερισμάτων για την αντιμετώπιση ζητημάτων που σχετίζονται με τις ψηφιακές υπογραφές.



Εικόνα 16 Παράδειγμα χρήσης συναρτήσεων κατάτμησης

1. Ο αποστολέας καθορίζει την τιμή στην οποία θα χωριστεί το μήνυμα.
2. Η τιμή του διαμερίσματος κρυπτογραφείται στη συνέχεια χρησιμοποιώντας το μυστικό κλειδί του, το οποίο χρησιμεύει ως ψηφιακή υπογραφή του μηνύματος.
3. Η κρυπτογραφημένη τιμή κατακερματισμού επισυνάπτεται στο κείμενο από τον αποστολέα.

4. Το υπογεγραμμένο κείμενο, το οποίο περιλαμβάνει τόσο το κείμενο όσο και την υπογραφή, κρυπτογραφείται από τον αποστολέα χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη.
5. Το υπογεγραμμένο κείμενο λαμβάνεται από τον παραλήπτη, ο οποίος στη συνέχεια χρησιμοποιεί το ιδιωτικό μυστικό κλειδί του για να το αποκρυπτογραφήσει.
6. Στη συνέχεια, η τιμή κατακερματισμού εξάγεται από την υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα.
7. Η ίδια η συνάρτηση κατάτμησης εξακολουθεί να χρησιμοποιείται από τον δέκτη για τον προσδιορισμό της τιμής διαμερίσματος του κειμένου που παραλείφθηκε.
8. Τελικά, ο παραλήπτης αξιολογεί τις δύο τιμές διαίρεσης. Εάν προκύψει ασυμφωνία, υποδηλώνει ότι είτε το κείμενο έχει παραβιαστεί κατά τη μετάδοση είτε ότι η ταυτότητα του αποστολέα δεν είναι όπως αναπαρίσταται.

6.2 Διαχείριση κλειδιών: παραγωγή και διανομή

Θα μπορούσε να υποστηριχθεί ότι ένας σημαντικός αριθμός ατόμων πιστεύει ότι η σύγχρονη τεχνολογία έχει την ικανότητα να επιλύσει το διαρκές ζήτημα της ασφαλούς κοινής χρήσης μυστικών κλειδιών μεταξύ των μερών που επικοινωνούν. Ωστόσο, αυτή η άποψη αποτυγχάνει να αναγνωρίσει ότι οι άνθρωποι, οι οποίοι διαδραματίζουν κρίσιμο ρόλο στην τεχνολογική διαδικασία, είναι στην πραγματικότητα ο πιο αδύναμος κρίκος αυτής της αλυσίδας. Οι επιλογές και οι συμπεριφορές τους μπορεί συχνά να είναι ασταθείς. Τελικά, αντιμετωπίζουμε την πρόκληση της ανταλλαγής κλειδιών.

Η διαχείριση των κλειδιών περιλαμβάνει πολλές βασικές διαδικασίες, συμπεριλαμβανομένης της δημιουργίας, διανομής, εγκατάστασης, χρήσης, ανανέωσης, ανάκλησης, αποθήκευσης και καταστροφής τους. Ενώ όλες οι δραστηριότητες διαχείρισης -εκτός από την καταστροφή κλειδιών- μπορούν να χρησιμοποιούν κρυπτογραφικές μεθόδους, ο όρος κρυπτοπερίοδος υποδηλώνει το χρόνο που απαιτείται για τη δημιουργία, τη διανομή και τη χρήση ενός κλειδιού. Διάφοροι παράγοντες επηρεάζουν την κρυπτοπερίοδο ενός κλειδιού: α) το μήκος του κλειδιού, β) η ευαισθησία εμπιστευτικότητας του απλού κειμένου, γ) ο τύπος του κλειδιού και δ) το κρυπτόςυστημα που χρησιμοποιείται (Mishra, et al., 2021). Επιπλέον, τα κλειδιά μπορούν να ταξινομηθούν με βάση τον τύπο κρυπτογραφικού αλγορίθμου - τρεις κατηγορίες περιλαμβάνουν μυστικά κλειδιά που χρησιμοποιούνται σε συμμετρικά

κρυπτοσυστήματα, μαζί με δημόσια και ιδιωτικά κλειδιά σε ασύμμετρα κρυπτοσυστήματα - και με βάση τις συγκεκριμένες εφαρμογές τους, όπως κλειδιά συνόδου, τερματικά κλειδιά και κύρια κλειδιά. Η σχέση μεταξύ των εννοιών του αντιπάλου και του κλειδιού είναι σημαντική, καθώς οι στόχοι του αντιπάλου συχνά περιλαμβάνουν την αποκάλυψη του κύριου κλειδιού, του κλειδιού περιόδου λειτουργίας ή ακόμα και παλαιότερων κλειδιών.

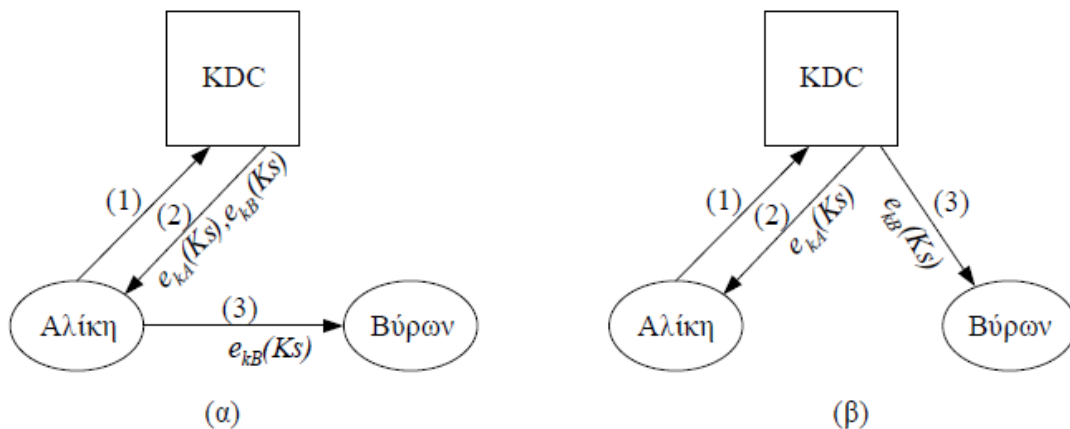
Ο όρος "εγκατάσταση κλειδιού" υποδηλώνει το σύνολο των διαδικασιών που επιτρέπουν στις επικοινωνούσες οντότητες να αποκτήσουν τα βασικά κλειδιά για ασφαλείς κρυπτογραφικές ανταλλαγές. Συχνά αναφέρονται ως κλειδιά περιόδου λειτουργίας, αυτοί οι μηχανισμοί για τη δημιουργία κλειδιών γενικά περιλαμβάνουν τα βήματα δημιουργίας, μεταφοράς και εγκατάστασης κλειδιών. Οι κρυπτογραφικές μέθοδοι που σχετίζονται με την εγκατάσταση κλειδιού ονομάζονται πρωτόκολλα δημιουργίας κλειδιών.

Μια σημαντική πρόκληση που αντιμετωπίζει η συμμετρική κρυπτογραφία είναι η ασφαλής και διακριτική μετάδοση του κλειδιού από τον αποστολέα στον δέκτη. Αυτό το ζήτημα αποτελεί τη βάση του προβλήματος ανταλλαγής κλειδιών. Αυτό εμπεριέχει (Barman, et al., 2014):

- διασφάλιση ότι τα κλειδιά ανταλλάσσονται, ώστε ο αποστολέας και ο παραλήπτης μπορούν να πραγματοποιήσουν την κρυπτογράφηση και την αποκρυπτογράφηση.
- διασφάλιση ότι ο οποιοσδήποτε επίβουλος δεν μπορεί να σπάσει τον κώδικα και
- διασφάλιση του παραλήπτη ότι το μήνυμα κρυπτογραφήθηκε από τον αποστολέα

Όπως σημειώθηκε προηγουμένως, η ισχύς ενός κρυπτογραφικού αλγορίθμου βασίζεται σε μεγάλο βαθμό στις τεχνικές που χρησιμοποιούνται για τη διανομή κλειδιών. Οι αναποτελεσματικές μέθοδοι διανομής κλειδιών ευνοούν τις ιδανικές συνθήκες για κρυπτοαναλυτικές επιθέσεις. Ενώ η πρόκληση διανομής κλειδιού επηρεάζει πρωτίστως τη συμμετρική κρυπτογραφία και αντιμετωπίζεται μέσω προσεγγίσεων κρυπτογραφίας δημόσιου κλειδιού, ορισμένα ζητήματα διανομής κλειδιών εξακολουθούν να υφίστανται ακόμη και στις τεχνικές κρυπτογράφησης δημόσιου κλειδιού. Και οι δύο τύποι κρυπτογραφίας μπορούν να αντιμετωπίσουν αυτές τις προκλήσεις χρησιμοποιώντας αξιόπιστα τρίτα μέρη (TTP) ή διαμεσολαβητές. Στη συμμετρική κρυπτογραφία, αυτός ο αξιόπιστος διαμεσολαβητής αναφέρεται ως Κέντρο Διανομής Κλειδιών (KDC), ενώ, στην ασύμμετρη κρυπτογραφία, είναι γνωστός ως Αρχή Πιστοποίησης (CA) (Alderman, et al., 2014).

Ένα Κέντρο Διανομής Κλειδιών (KDC) είναι ένα ξεχωριστό και αξιόπιστο δίκτυο οντοτήτων όπου κάθε στοιχείο επικοινωνίας πρέπει να δημιουργεί και να μοιράζεται ένα κοινό μυστικό κλειδί. Για να διασφαλιστεί η εμπιστευτική επικοινωνία με το KDC, όλα τα στοιχεία δικτύου είναι υποχρεωμένα να μοιράζονται αυτό το μυστικό κλειδί. Ωστόσο, αυτή η αναγκαιότητα θέτει μια πρόκληση στον τομέα της διανομής δημόσιου κλειδιού (Graff, 2001). Στο πλαίσιο του KDC, είναι υπεύθυνο για τη δημιουργία του κλειδιού συνεδρίας. Τα δύο σενάρια που αφορούν το KDC απεικονίζονται στο παρακάτω σχήμα.



Εικόνα 17 KDC με (α) ενδιάμεση και (β) άμεση επικοινωνία

Στην πρώτη εναλλακτική, η Αλίκη απευθύνεται στο KDC (1) για να ζητήσει ένα κλειδί συνεδρίας για την επικοινωνία της με τον Βύρων. Το KDC δημιουργεί το κλειδί συνόδου ks και το κρυπτογραφεί χρησιμοποιώντας το κλειδί kA , το οποίο μοιράζεται με την Αλίκη, καθώς και το κλειδί kB , το οποίο μοιράζεται με τον Βύρων, με αποτέλεσμα δύο κρυπτογραφημένα κείμενα: $ekA(ks)$ και $ekB(ks)$. Στη συνέχεια, το KDC μεταδίδει και τα δύο κρυπτογραφημένα κείμενα στην Αλίκη (2). Στη συνέχεια, η Αλίκη προωθεί το κρυπτογραφημένο κείμενο $ekB(ks)$ στον Βύρων. Τελικά, τόσο η Αλίκη όσο και ο Βύρων αποκρυπτογραφούν τα αντίστοιχα κρυπτογραφημένα κείμενά τους για να ανακτήσουν το κλειδί συνόδου ks .

Στη δεύτερη εναλλακτική, η επικοινωνία επανεκκινείται από την Αλίκη, η οποία στέλνει ένα αίτημα κλειδιού συνεδρίας στο KDC για να δημιουργήσει επαφή με τον Βύρων (1). Το KDC δημιουργεί ένα κλειδί περιόδου λειτουργίας, κρυπτογραφώντας το μεμονωμένα με τα κλειδιά της Αλίκης και του Βύρων, παρόμοια με το προηγούμενο σενάριο. Στη συνέχεια, τα κρυπτογραφημένα κλειδιά αποστέλλονται ξεχωριστά στην Αλίκη (2) και στον Βύωνα (3). Τελικά, τόσο η Αλίκη όσο και ο Βύρων αποκρυπτογραφούν το κρυπτογραφημένο κείμενο που έλαβαν για να αποκτήσουν το κλειδί συνεδρίας.

Σε εκτεταμένα δίκτυα που χαρακτηρίζονται από ποικίλες και εξελισσόμενες τοπολογίες επικοινωνίας, το ζήτημα της διανομής κλειδιών προκύπτει όταν τα στοιχεία δικτύου που πρέπει να επικοινωνήσουν δεν μπορούν να ανήκουν στο ίδιο KDC. Οι μηχανισμοί διαχείρισης δημόσιου κλειδιού, ιδιαίτερα η υποδομή δημόσιου κλειδιού (PKI), αντιμετωπίζουν αποτελεσματικά αυτές τις προκλήσεις.

Απαιτείται λύση λόγω ζητημάτων που αφορούν τόσο την αυθεντικότητα όσο και την ακεραιότητα στη διανομή των δημόσιων κλειδιών. Ο Stallings (2003) εντοπίζει δύο κύρια προβλήματα: τη διανομή των δημόσιων κλειδιών και την εφαρμογή κρυπτογραφίας δημόσιου κλειδιού για τη διανομή ιδιωτικών κλειδιών. Υπάρχουν αρκετές προτεινόμενες λύσεις για τη διανομή των δημόσιων κλειδιών. Ενδεικτικά:

- Δημόσιες καταχωρήσεις όπου ο κάθε χρήστης μπορεί να γνωστοποιεί ευρέως τα δημόσια κλειδιά του ή να τα αποστέλλει σε επιλεγμένους χρήστες.
- Δημόσιος κατάλογος, ο οποίος υποστηρίζεται από μία Έμπιστη Τρίτη Οντότητα. Ο κατάλογος είναι συνήθως δυναμικός καθώς πρέπει να διευθετεί τις προσθήκες ή τις διαγραφές.
- Αρχή Πιστοποίησης (Certification Authority - CA) για τη διανομή πιστοποιητικών σε κάθε επικοινωνούντα στοιχείο.

Η υποδομή δημόσιου κλειδιού περιλαμβάνει όλα αυτά τα στοιχεία. Όπως αναφέρθηκε προηγουμένως, το YDK λειτουργεί σε συνδυασμό με το KDK για να εξασφαλίσει αξιόπιστη και αποτελεσματική διαχείριση κλειδιών και πιστοποιητικών. Αυτό μας οδηγεί να διερευνήσουμε τι πραγματικά συνεπάγεται το YDK. Ένα PKI περιλαμβάνει το απαραίτητο υλικό, λογισμικό, προσωπικό, πολιτικές και διαδικασίες που απαιτούνται για τη δημιουργία, τη διαχείριση, την αποθήκευση, τη διανομή και την ανάκληση πιστοποιητικών που χρησιμοποιούν κρυπτογραφία δημόσιου κλειδιού. Σε αυτό το πλαίσιο, το PKI εκσυγχρονίζει όλες αυτές τις λειτουργίες, αποδεικνύοντας πιο αποτελεσματικό όταν εξυπηρετεί μια μεγάλη βάση χρηστών και διευκολύνει την ευρεία δημιουργία και διανομή ψηφιακών πιστοποιητικών με αξιόπιστο τρόπο. Αποτελείται βασικά από τέσσερα κύρια συστατικά:

Ο μηχανισμός ελέγχου ταυτότητας αντιπροσωπεύεται από το πιστοποιητικό, το οποίο χρησιμεύει ως κρυπτογραφική απόδειξη ότι το εν λόγω δημόσιο κλειδί ανήκει πραγματικά στον χρήστη που ισχυρίζεται την ιδιοκτησία.

Η αρχή που είναι αρμόδια για τη λήψη της τελικής απόφασης για την πιστοποίηση του αντικειμένου πιστοποίησης είναι η Αρχή Πιστοποίησης. Η Αρχή Καταχώρισης χειρίζεται και επεξεργάζεται αιτήματα πιστοποίησης που υποβάλλονται από τελικούς χρήστες.

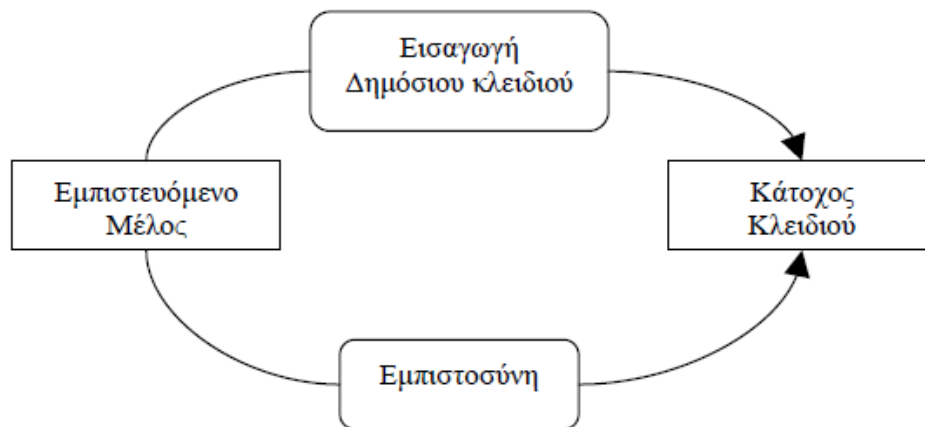
Το Lightweight Directory Access Protocol (LDAP) χρησιμεύει ως αποθετήριο που αποθηκεύουν και παρέχουν πρόσβαση σε πιστοποιητικά και καταλόγους για ανάκληση πιστοποιητικού. Ουσιαστικά, το LDAP λειτουργεί ως πρωτόκολλο πελάτη-διακομιστή, επιτρέποντας πρόσβαση σε διάφορες πληροφορίες που περιέχονται σε μια βάση δεδομένων ή έναν κατάλογο που προσφέρει διάφορες υπηρεσίες.

6.3 Η Υποδομή Δημόσιου Κλειδιού – Public Key Infrastructure

Στον τομέα των επιχειρήσεων και των επικοινωνιών που διέπονται από συμβάσεις, ορισμένες βασικές παραδοχές προκύπτουν όταν μια συναλλαγή εκτελείται μέσω του παραδοσιακού υπογεγραμμένου εγγράφου, το οποίο παραδίδεται προσωπικά και φυσικά, σε σφραγισμένη συσκευασία, στα εμπλεκόμενα συμβαλλόμενα μέρη. Οι οργανισμοί που εμπλέκονται σε επιχειρηματικές επικοινωνίες μέσω ανοιχτών δικτύων πρέπει γενικά να διασφαλίζουν ότι γνωρίζουν τους ομολόγους τους, ότι το περιεχόμενο της επικοινωνίας παραμένει αμετάβλητο από την υπογραφή, ότι κανένα μη εξουσιοδοτημένο άτομο δεν έχει πρόσβαση στις πληροφορίες και ότι ο υπογράφων δεν έχει αρνηθεί να στείλει το έγγραφο (Adams & Lloyd, 2002). Αυτές οι βασικές εγγυήσεις επιτρέπουν τις εξ αποστάσεως συναλλαγές μεταξύ των συμβαλλομένων μερών. Ο πρωταρχικός στόχος μιας Υποδομής Δημοσίου Κλειδιού είναι να προσφέρει παρόμοιες διαβεβαιώσεις σχετικά με το περιεχόμενο και τα μέρη που εμπλέκονται σε συναλλαγές που πραγματοποιούνται μέσω ανοιχτών δικτύων, συχνά μεταξύ μερών που μπορεί να μην είναι εξοικειωμένοι μεταξύ τους. Επιτρέποντας τη χρήση ψηφιακών υπογραφών και κρυπτογράφησης, το PDS μπορεί να παρέχει τις ίδιες θεμελιώδεις υπηρεσίες ασφάλειας με τις παραδοσιακές ανταλλαγές δεδομένων και πληροφοριών (Adams & Lloyd, 2002).

Στο πλαίσιο της λογικής PSC, μια κρίσιμη ενέργεια για τη δημιουργία μιας σχέσης εμπιστοσύνης περιλαμβάνει την αρχική οντότητα εισαγωγής ενός δημόσιου κλειδιού από τη δεύτερη οντότητα και διασφάλιση της ακεραιότητάς του για ασφαλή αποθήκευση ή επικοινωνία με άλλα μέρη. Η οντότητα που πραγματοποιεί την εισαγωγή του δημόσιου κλειδιού αναφέρεται ως το εξαρτημένο μέρος, καθώς στοχεύει να εξαρτάται από αυτό το δημόσιο κλειδί για να διαφυλάξει μελλοντικές αλληλεπιδράσεις με τον κάτοχο του

κλειδιού, ο οποίος είναι η οντότητα που παρείχε το κλειδί. Αυτή η σχέση μεταξύ των οντοτήτων απεικονίζεται παρακάτω.



Εικόνα 18 Σχέση οντοτήτων

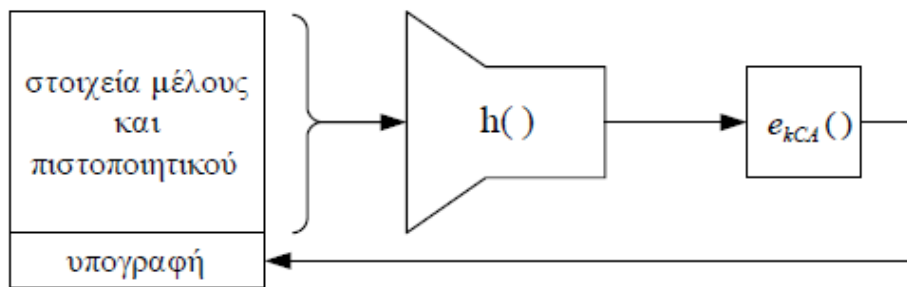
Κάθε οργανισμός έχει την ικανότητα να λειτουργεί ταυτόχρονα ως έμπιστος συμμετέχων και ως κάτοχος κλειδιού. Ωστόσο, για λόγους σαφήνειας, αυτές οι λειτουργίες κατηγοριοποιούνται σε δύο διακριτούς ρόλους. Για να αποφευχθεί οποιαδήποτε παρεξήγηση μεταξύ των εμπλεκόμενων μερών, η θεμελιώδης λειτουργία δημόσιου κλειδιού πρέπει να εκτελείται με τρόπο που να διατηρεί την αυθεντικότητα και την ακεραιότητα του κλειδιού, διασφαλίζοντας ότι λαμβάνεται αναλλοίωτο από τον νόμιμο κάτοχο (Fernandes, 2001).

Επί του παρόντος, η ευρέως αναγνωρισμένη μέθοδος για την επικύρωση ενός νέου συνεργάτη ή οντότητας επικοινωνίας περιλαμβάνει έγκριση από ένα έμπιστο τρίτο μέρος ή αρχή. Αυτή η στρατηγική δίνει τη δυνατότητα σε δύο άτομα να εμπιστεύονται σιωπηρά το ένα το άλλο, παρά την έλλειψη προηγούμενης προσωπικής σχέσης. Σε αυτό το πλαίσιο, ένα τρίτο μέρος προσφέρει τη διασφάλιση της ακριβούς ταυτότητας, επιβεβαιώνοντας σε κάθε συνεργάτη επικοινωνίας ότι ο άλλος είναι γνήσιος ή νόμιμος (Jøsang, et al., 1999).

Ένα αξιόπιστο τρίτο μέρος, κοινώς γνωστό ως TTP, είναι μια αναθέτουσα οντότητα στην οποία πρέπει να βασίζονται όλοι οι άλλοι συμμετέχοντες στην ανταλλαγή πληροφοριών. Συχνά αναφέρεται ως Αρχή Πιστοποίησης (CA) λόγω του ρόλου της στην έκδοση πιστοποιητικών, η ΕΤΟ εκπληρώνει αυτή τη λειτουργία (Fratto, 2001). Ένα

πιστοποιητικό περιλαμβάνει δύο στοιχεία: τα δεδομένα και την ψηφιακή υπογραφή. Τα δεδομένα περιλαμβάνουν πληροφορίες σχετικά με το κύριο, τις ιδιαιτερότητες του πιστοποιητικού και λεπτομέρειες σχετικά με τις κρυπτογραφικές μεθόδους που χρησιμοποιούνται για τη δημιουργία της ψηφιακής υπογραφής.

Παρακάτω εμφανίζεται η διαδικασία για τη δημιουργία ψηφιακού πιστοποιητικού. Χρησιμοποιώντας ένα μονόδρομο κατακερματισμό, η Αρχή Πιστοποίησης συντάσσει μια σύνοψη των πληροφοριών που περιέχονται στην αρχική ενότητα του πιστοποιητικού, την οποία στη συνέχεια κρυπτογραφεί χρησιμοποιώντας το ιδιωτικό κλειδί kd_{CA} .



Εικόνα 19 Διαδικασία δημιουργίας ψηφιακού πιστοποιητικού

Το πρότυπο που διέπει πρωτίστως τα PKI που χρησιμοποιούν τεχνολογίες Διαδικτύου είναι το πιστοποιητικό X.509. Όπως ορίζεται από την ITU, το X.509 χρησιμεύει ως πρότυπο ελέγχου ταυτότητας που βασίζεται στην ασύμμετρη κρυπτογραφία (Mitchell, 2000). Ουσιαστικά, το πιστοποιητικό X.509 διασφαλίζει τη σύνδεση μεταξύ της ταυτότητας μιας οντότητας και του δημόσιου κλειδιού της. Οι ακόλουθες πληροφορίες περιλαμβάνονται συνήθως σε ένα πιστοποιητικό X.509:

- Στοιχεία έκδοσης πιστοποιητικού
- Σειριακός αριθμός του πιστοποιητικού
- Εκδότης του πιστοποιητικού
- Διάρκεια ισχύος του πιστοποιητικού
- Όνομα της επαληθευμένης οντότητας
- Δημόσιο κλειδί που έχει επικυρωθεί
- Προαιρετικές επεκτάσεις
- Αναγνωριστικά για τους αλγόριθμους που χρησιμοποιούνται κατά την υπογραφή
- Η ίδια η υπογραφή.

Ένα ψηφιακό πιστοποιητικό χρησιμεύει ως το έγγραφο που συνδέει ένα άτομο (ή οντότητα) με το ζεύγος κλειδιών που χρησιμοποιείται για την ψηφιακή υπογραφή ηλεκτρονικών επικοινωνιών. Περιλαμβάνει λεπτομέρειες όπως το όνομα του συνδρομητή, το δημόσιο κλειδί του συνδρομητή, το δημόσιο κλειδί της αρχής έκδοσης πιστοποιητικών και ενδεχομένως πρόσθετες σχετικές πληροφορίες σχετικά με τον συνδρομητή. Υπογεγραμμένο από την αρχή πιστοποίησης, το ψηφιακό πιστοποιητικό διασφαλίζει ότι οι πληροφορίες μέσα σε αυτό παραμένουν αναλλοίωτες (Cheng, et al., 2018). Η ανάκληση του πιστοποιητικού είναι δυνατή σε περιπτώσεις όπου το ιδιωτικό κλειδί εκτίθεται στο κοινό ή εάν υπάρχουν αλλαγές που επηρεάζουν την ακρίβεια των στοιχείων ταυτότητας, όπως η αναχώρηση από έναν οργανισμό.

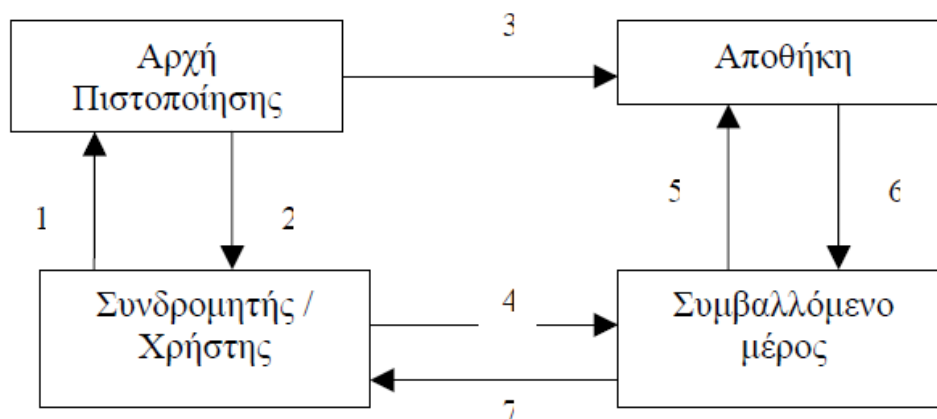
Η Υποδομή Δημοσίου Κλειδιού (PKI) χρησιμεύει ως ένα ολοκληρωμένο πλαίσιο ασφαλείας που προσφέρει υπηρεσίες ασφαλείας σε διάφορες ανεξάρτητες εφαρμογές και υπηρεσίες (Bruschi, et al., 2003). Η έννοια του PKI περιλαμβάνει μια συνδεδεμένη σειρά υλικού, λογισμικού και συγκεκριμένων κρυπτογραφικών στοιχείων που συνεργάζονται για να συμμορφωθούν με τις πολιτικές και τις διαδικασίες που είναι απαραίτητες για την ασφαλή λειτουργία των επιχειρηματικών εφαρμογών. Τα κρυπτογραφικά στοιχεία που χρησιμοποιούνται βασίζονται σε δημόσιο κλειδί ή ασύμμετρη κρυπτογραφία, επιτρέποντας σε δύο μέρη να διεξάγουν μια αξιόπιστη ανταλλαγή πληροφοριών, ακόμη και απουσία προηγούμενης επικοινωνίας (Bruschi, et al., 2003).

Μια υλοποίηση PKI προσφέρει το πλεονέκτημα των ασφαλών συνδέσεων χρήστη. Κατά τη στιγμή της σύνδεσης, ο χρήστης υποβάλλεται σε έλεγχο ταυτότητας έναντι της υποδομής, επιτρέποντας την πρόσβαση σε εφαρμογές εντός αυτού του πλαισίου. Αυτή η ασφαλής και «έμπιστη» υποδομή επικοινωνιών προκύπτει από ένα μείγμα τεχνολογίας, πολιτικής και διαδικασιών διαχείρισης (Carayannis & Turner, 2005). Μια τέτοια αξιόπιστη υποδομή είναι απαραίτητη για την κάλυψη των αναγκών ασφαλείας που επιθυμείτε στο διαδικτυακό χώρο. Ο όρος "υποδομή" υποδηλώνει μια κοινόχρηστη αρχιτεκτονική που επιτρέπει την ασφαλή υλοποίηση και χρήση τόσο γενικών εφαρμογών, όπως καταλόγων, όσο και επιχειρηματικών εφαρμογών, όπως ιστοτόπων. Τα δομικά συστατικά είναι (Carayannis & Turner, 2005):

- Αρχή Πιστοποίησης (CA): Λειτουργώντας ως το βασικό στοιχείο ενός PKI, ενεργεί ως ο αξιόπιστος διαμεσολαβητής επιφορτισμένος με την επικύρωση των δημόσιων κλειδιών των μελών του. Η Αρχή Πιστοποίησης είναι όπου συγκεντρώνεται η ακεραιότητα ολόκληρης της υποδομής.

- Αρχή Καταχώρησης (RA): Είναι ο αξιόπιστος οργανισμός που είναι υπεύθυνος για την έκδοση και την ανάκληση πιστοποιητικών δημόσιου κλειδιού καθώς και λιστών ανάκλησης πιστοποιητικών.
- Λίστα ανάκλησης πιστοποιητικών (CRL): Αναφέρεται στη συλλογή ανακληθέντων πιστοποιητικών, που συνήθως υπογράφονται από την οντότητα έκδοσης. Υπάρχουν διάφοροι λόγοι για τους οποίους μπορεί να ανακληθούν τα πιστοποιητικά. Για παράδειγμα, ένα πιστοποιητικό μπορεί να ακυρωθεί εάν χαθεί το ιδιωτικό κλειδί που ανήκει στον ιδιοκτήτη ή εάν υπάρξει αλλαγή στο όνομα του κατόχου.
- Αποθετήριο: ένας ψηφιακός χώρος που προορίζεται για την αποθήκευση πιστοποιητικών και τη λίστα ανάκλησης πιστοποιητικών. Τα πιστοποιητικά και οι λίστες ανάκλησης πιστοποιητικών τοποθετούνται σε αυτά τα αποθετήρια από την ΑΠ. Αυτή η περιοχή διατηρεί με ασφάλεια δεδομένα σχετικά με όλα τα πιστοποιητικά που εκδίδονται από την ΑΠ και επιβάλλει κανονισμούς που απαγορεύουν τη δημιουργία διπλότυπων ταυτοτήτων.
- Τελικός χρήστης: ένα μέρος που χρησιμοποιεί τα πιστοποιητικά για να εξακριβώσει με σιγουριά το δημόσιο κλειδί μιας άλλης οντότητας.

Παρακάτω παρουσιάζεται η διαδικασία ροής του PKI.



Εικόνα 20 Γραφική αναπαράσταση της ροής του PKI

- Βήμα 1: Ο συνδρομητής/χρήστης απευθύνεται στην αρχή εγγραφής για την απόκτηση ψηφιακού πιστοποιητικού.
- Βήμα 2: Η ταυτότητα του συνδρομητή επαληθεύεται και επιβεβαιώνεται από την ΑΠ, η οποία στη συνέχεια εκδίδει το ψηφιακό πιστοποιητικό.

- Βήμα 3: Το πιστοποιητικό δημοσιεύεται από την ΑΠ στο χώρο αποθήκευσης.
- Βήμα 4: Για να διασφαλιστεί η αυθεντικότητα της μετάδοσης, να διατηρηθεί η ακεραιότητα του μηνύματος και να διασφαλιστεί η μη απόρριψη, ο συνδρομητής υπογράφει ψηφιακά το ηλεκτρονικό μήνυμα χρησιμοποιώντας το ιδιωτικό του κλειδί πριν το στείλει στον αντισυμβαλλόμενο.
- Βήμα 5: Με τη λήψη του μηνύματος, ο αντισυμβαλλόμενος επαληθεύει την ψηφιακή υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του συνδρομητή και στη συνέχεια προχωρά στο κατάστημα για να επιβεβαιώσει την ταυτότητα, την κατάσταση και την εγκυρότητα του πιστοποιητικού του συνδρομητή.
- Βήμα 6: Τα αποτελέσματα του υγειονομικού ελέγχου πιστοποιητικού συνδρομητή επιστρέφονται στον αντισυμβαλλόμενο από το αποθετήριο.
- Βήμα 7: Ο αντισυμβαλλόμενος μπορεί να κάνει μια τεκμηριωμένη επιλογή σχετικά με την εμπιστοσύνη του στο μήνυμα του χρήστη.

Οι λειτουργίες της ΥΔΚ θα μπορούσαν να συνοψισθούν στον ακόλουθο πίνακα (Hunt, 2001):

Υπηρεσίες	Περιγραφή	Υλοποίηση – Εφαρμογή
Εγγραφή χρηστών	Συλλογή πληροφοριών χρήστη, επιβεβαίωση ταυτότητας	Υπηρεσίες CA ή αυτόνομες RA
Έκδοση πιστοποιητικών	Δημιουργία πιστοποιητικών σε απόκριση αιτήματος χρήστη ή διαχειριστή	Λειτουργίες CA
Ανάκληση πιστοποιητικών	Δημιουργία και δημοσίευση Λίστας Ανάκλησης Πιστοποιητικών (Certificate Revocation Lists – CRLs)	Διαχειριστικό λογισμικό που συνδέεται με τη CA
Αποθήκευση και ανάκτηση πιστοποιητικών & CRLs	Τα πιστοποιητικά και οι CRLs καθίστανται διαθέσιμα στους	Αποθήκες για τα CRLs και πιστοποιητικά σε ασφαλή πιστά αντίγραφα τα οποία

	εξουσιοδοτημένους χρήστες	είναι προσβάσιμα μέσω του πρωτοκόλλου LDAP
Επικύρωση του βασισμένου στην πολιτική πιστοποιητικού	Επιβολή περιορισμών βασισμένων στην πολιτική για την αλυσίδα πιστοποίησης και επιβεβαίωση ότι οι περιορισμοί ισχύουν	Λειτουργίες CA
Χρονοσφραγίδα (timestamp)	Χρονοσφραγίδα για κάθε κλειδί	Λειτουργίες CA
Διαχείριση κύκλου ζωής κλειδιού	Ενημέρωση, αρχειοθέτηση και ανανέωση κλειδίων	Αυτοματοποιημένο λογισμικό ή χειροκίνητες ενέργειες

Η πολιτική πιστοποιητικών χρησιμεύει ως το κεντρικό στοιχείο ενός PKI, περιγράφοντας την κοινότητα που χρησιμοποιεί το PKI, τις προβλεπόμενες εφαρμογές που υποστηρίζει και τους κανόνες δέσμευσης που απαιτείται να τηρούν όλα τα εμπλεκόμενα μέρη. Σε αυτό το πλαίσιο, μπορούμε να εντοπίσουμε τρία κύρια μοντέλα YDK που αξίζει να αναφερθούν, το καθένα ποικίλλει ως προς τα χαρακτηριστικά των κοινοτήτων που εξυπηρετεί, γεγονός που με τη σειρά του επηρεάζει τον τύπο της αρχής πολιτικής που πρέπει να ιδρύσουν και να επιβλέψουν (η πολιτική πιστοποιητικών). Αυτά τα μοντέλα περιλαμβάνουν: το κλειστό ή επιχειρηματικό μοντέλο, το μοντέλο Κοινότητας ενδιαφέροντος ή δικτύου και το ανοιχτό μοντέλο (Raavi, et al., 2021).

Ορισμένες κοινότητες διαθέτουν μια εγγενή ανεξαρτησία, που χαρακτηρίζεται από τις σαφώς καθορισμένες πολιτικές τους. Στο «κλειστό» μοντέλο, οι πολιτικές, οι πρακτικές και οι διαδικασίες του PKI αφορούν αποκλειστικά την τοπική κοινωνία που εξυπηρετεί. Μέσα σε αυτό το κλειστό πλαίσιο, η διοίκηση επιχειρήσεων του οργανισμού λειτουργεί ως πολιτική αρχή, θεσπίζοντας πολιτικές που σχετίζονται με την αναγνώριση και επικύρωση εργαζομένων, την αποθήκευση ιδιωτικού κλειδιού και τη διαχείριση ΑΠ, μεταξύ άλλων πτυχών (Raavi, et al., 2021). Επιπλέον, ορισμένες κοινότητες μπορούν να γίνουν καλύτερα κατανοητές ως μια ένωση ή συλλογή από διάφορες διακριτές ομάδες, όπως βιομηχανικές ενώσεις ή δίκτυα πανεπιστημιακών βιβλιοθηκών. Στο μοντέλο δικτύου, οι οργανισμοί συνεργάζονται για να καθορίσουν από κοινού τις πολιτικές, τις

διαδικασίες, τις υπηρεσίες ασφαλείας και τις εφαρμογές που θα υποστηρίξει το CSI τους. Ένα CSI που διευκολύνει τις αλληλεπιδράσεις μεταξύ των μελών αυτών των ευρύτερων κοινοτήτων αναφέρεται ως μοντέλο «δικτύου».

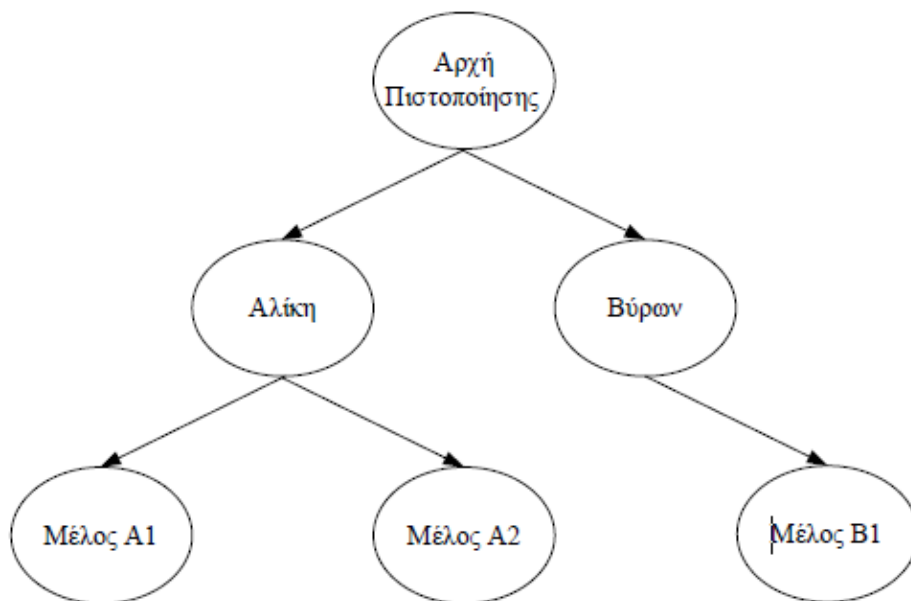
Ορισμένες κοινότητες έχουν ευρεία φύση και μπορούν να συνδεθούν είτε με άτυπες πολιτικές είτε με εκείνες που διαμορφώνονται κυρίως από κανονισμούς και νομοθεσία. Ένα παράδειγμα αυτού είναι η κοινότητα των καταναλωτών λιανικής. Ένα πρότυπο PKI που εξυπηρετεί τέτοιες επεκτατικές κοινότητες είναι γνωστό ως "ανοιχτό". Επί του παρόντος, τα ανοικτά PKI παραμένουν κυρίως στην εννοιολογική φάση. Η διάκριση μεταξύ ενός ανοιχτού δικτύου PKI και ενός δικτύου PKI μπορεί να γίνει κατανοητή ως διαφορά στο βαθμό.

Ο τρόπος με τον οποίο οργανώνονται οι σχέσεις μεταξύ των ΑΠ είναι κρίσιμος παράγοντας για τη δημιουργία ενός PKI. Ουσιαστικά, η δομή της ΑΠ υποδεικνύει πώς εκδίδει πιστοποιητικά. Έχουν προταθεί διάφορα γενικά δομικά μοντέλα, κοινώς γνωστά ως μοντέλα PKI. Χρησιμοποιείται επίσης η φράση μοντέλα εμπιστοσύνης, καθώς το πρότυπο PKI περιγράφει τη σχέση εμπιστοσύνης εντός του PKI (Gómez, et al., 2003).

Τα πιστοποιητικά χρησιμεύουν για την εδραίωση της εμπιστοσύνης ενός δικτύου στα δημόσια κλειδιά του μέσω μιας κατευθυνόμενης αναπαράστασης γραφήματος. Αυτό το γράφημα ευθυγραμμίζει τους κόμβους με οντότητες δικτύου, όπως χρήστες ή αρχές πιστοποίησης, ενώ οι άκρες αντιπροσωπεύουν τα πιστοποιητικά (Adams, et al., 2000). Είναι σημαντικό να διαφοροποιηθεί το γράφημα εμπιστοσύνης από το δίκτυο επικοινωνίας, καθώς οι άκρες στο γράφημα εμπιστοσύνης αντικατοπτρίζουν σχέσεις εμπιστοσύνης και όχι τρόπους επικοινωνίας. Επιπλέον, οι κόμβοι μέσα στο γράφημα αξιοπιστίας ενδέχεται να μην αντιστοιχούν σε κόμβους επικοινωνίας.

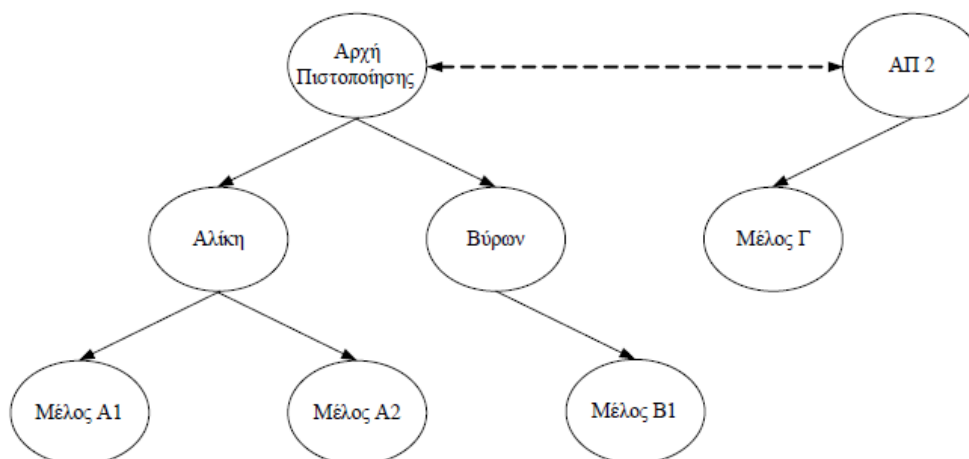
Τα μοντέλα εμπιστοσύνης περιγράφουν τον τρόπο με τον οποίο οι οντότητες συνεργάζονται μεταξύ τους για την επικύρωση ενός πιστοποιητικού. Το Αξιόπιστο Τρίτο Μέρος εκπροσωπείται από την Αρχή Πιστοποίησης. Ωστόσο, αυτό δεν εμποδίζει ορισμένα μέλη να αναλάβουν το ρόλο της Αρχής Πιστοποίησης για την πιστοποίηση άλλων. Κατά συνέπεια, ενώ μια Αρχή Πιστοποίησης μπορεί να εκδώσει ένα πιστοποιητικό για ένα μέλος, αυτό το μέλος μπορεί επίσης να εγκρίνει ένα άλλο μέλος δημιουργώντας ένα πιστοποιητικό. Ένα παράδειγμα που απεικονίζεται στο ακόλουθο δέντρο απεικονίζει την Αλίκη να πιστοποιεί τα Μέλη A1 και A2. Ως Έμπιστο Τρίτο Μέρος, η Αρχή Πιστοποίησης διασφαλίζει ότι όλα τα πιστοποιητικά που εκδίδει αναγνωρίζονται από κάθε μέλος που εμπλέκεται στο PKI. Για τον Βύρων, η επικοινωνία

με την Αλίκη απαιτεί μόνο εμπιστοσύνη στην Αρχή Πιστοποίησης, η οποία είναι έγκυρη αφού το δικό του πιστοποιητικό εκδόθηκε επίσης από την ίδια Αρχή Πιστοποίησης.



Εικόνα 21 Δέντρο πιστοποίησης - Μοντέλο εμπιστοσύνης

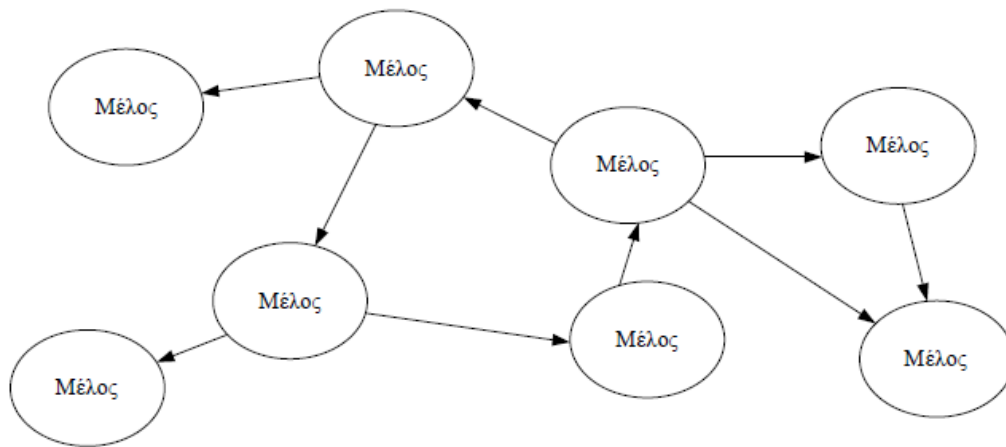
Εάν το μέλος Β1 επιθυμεί να επικοινωνήσει είτε με το μέλος Α1 είτε με το Α2, πρέπει να εμπιστευτεί τον Βύρων, την Αρχή Πιστοποίησης, καθώς και την Αλίκη. Ουσιαστικά, η εμπιστοσύνη δημιουργείται όταν υπάρχει μια διαδρομή στο δέντρο που οδηγεί από το Μέλος Β1 είτε στο Μέλος Α1 είτε στο Α2. Στην παρακάτω εικόνα, το μέλος C έχει εισαχθεί και επιδιώκει να επικοινωνήσει με τον Βύρων, αλλά διαθέτει πιστοποιητικό που έχει εκδοθεί από διαφορετική Αρχή Πιστοποίησης, CA2. Σε αυτό το σενάριο, είναι απαραίτητο για τον Βύρων να επαληθεύσει εάν η δική του Αρχή Πιστοποίησης αναγνωρίζει το AP2 και αντίστροφα, διασφαλίζοντας τη σύνδεση μεταξύ των δύο δέντρων πιστοποίησης. Αυτή η σύνδεση απεικονίζεται στο σχήμα με μια διακεκομμένη γραμμή, η οποία αναφέρεται ως διασταυρούμενη πιστοποίηση.



Εικόνα 22 Διαπιστοποίηση

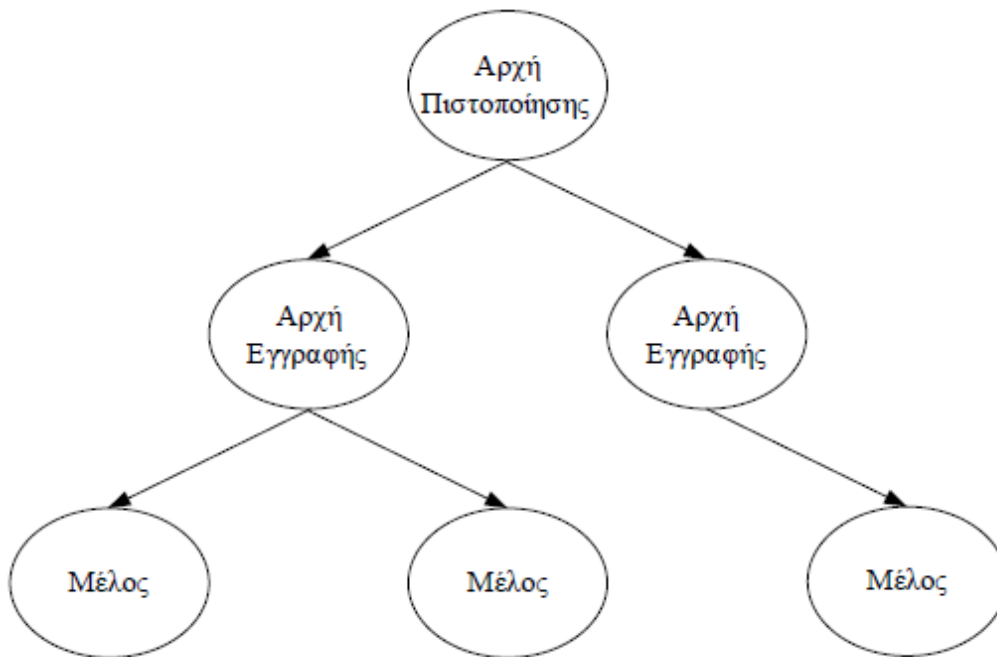
Η ικανότητα της Αλίκης, του Βύρων και των γενικών μελών να εκδίδουν πιστοποιητικά αποτελεί σημαντικό ζήτημα. Καθώς το δέντρο επεκτείνεται σε βάθος, αυξάνεται επίσης ο αριθμός των οντοτήτων μεταξύ ενός μέλους και της Αρχής Πιστοποίησης. Κατά συνέπεια, η διαδρομή πιστοποίησης που συνδέει δύο μέλη μπορεί να γίνει υπερβολικά μακρά. Όπως αναμενόταν, με την αύξηση του βάθους των δέντρων, η ασφάλεια ενός PKI μειώνεται. Όσο μεγαλύτερη είναι η απόσταση μεταξύ δύο μελών, τόσο λιγότερη εμπιστοσύνη υπάρχει για τη γνησιότητα του πιστοποιητικού, καθώς αυξάνονται οι πιθανότητες να παρέμβει ένας αντίπαλος. Επιπλέον, η ύπαρξη πολλών μελών στο ενδιαμέσο παρέχει περισσότερες ευκαιρίες σε έναν εισβολέα να εκμεταλλευτεί τα τρωτά σημεία. Ένας αντίπαλος είναι πιθανό να στοχεύσει το μέλος με την πιο εύθραυστη ασφάλεια. Έτσι, η συνολική ασφάλεια της υποδομής εξαρτάται από τον πιο αδύναμο κρίκο της. Για το λόγο αυτό, καθιερώνονται μοντέλα που εμποδίζουν τα μέλη να εκδίδουν πιστοποιητικά και να λειτουργούν ως Αρχές Πιστοποίησης. Ως αποτέλεσμα, τα μοντέλα εμπιστοσύνης κατηγοριοποιούνται σε δύο τύπους: επίπεδα και ιεραρχικά.

Παρακάτω εμφανίζεται το μοντέλο επιπέδου εμπιστοσύνης. Αυτό το μοντέλο μοιάζει με αυτό που περιγράφηκε προηγουμένως, το οποίο διαφέρει στο ότι καμία μεμονωμένη οντότητα δεν λειτουργεί αποκλειστικά ως Αρχή Πιστοποίησης. Κατά συνέπεια, κάθε οντότητα επιτρέπεται να εκδίδει πιστοποιητικό για άλλον. Αυτή η προσέγγιση δημιουργεί έναν «ιστό εμπιστοσύνης», επιτρέποντας σε ένα νέο μέλος να ενταχθεί στο δίκτυο μέσω της εισαγωγής ενός υπάρχοντος μέλους.



Εικόνα 23 Επίπεδο μοντέλο εμπιστοσύνης

Το ιεραρχικό μοντέλο εμπιστοσύνης απαιτεί μια Έμπιστη Τρίτη Οντότητα η οποία λειτουργεί ως Αρχή Πιστοποίησης και προαιρετικά μία ή περισσότερες Αρχές Εγγραφής, όπως φαίνεται παρακάτω.



Εικόνα 24 Ιεραρχικό μοντέλο εμπιστοσύνης

Η αρχική επαλήθευση των στοιχείων ενός Μέλους εμπίπτει στην αρμοδιότητα της Αρχής Εγγραφής. Αυτός ο αρχικός έλεγχος ταυτότητας πραγματοποιείται εκτός του πλαισίου PKI και αναφέρεται ως αναγνώριση εκτός ζώνης, κατά την οποία το Μέλος παρέχει ένα έγγραφο ελέγχου ταυτότητας, όπως αστυνομική ταυτότητα ή διαβατήριό. Η βασική αρχή ότι "μια λειτουργία με το ιδιωτικό κλειδί ενός ατόμου εκτελείται μόνο όταν έχει

εξουσιοδοτηθεί από αυτό το άτομο" είναι κρίσιμη για την αποτελεσματικότητα του PKI. Για την επιτυχή εφαρμογή ενός PSC, απαιτείται σχολαστικός σχεδιασμός για την αντιμετώπιση διαφόρων ανησυχιών (Mansfield, 1999):

- Πολυπλοκότητα. Ένα ΥDK πλήρους κλίμακας αποτελείται από μια εκτεταμένη σειρά εξαρτημάτων, συμπεριλαμβανομένων εργατικού δυναμικού, λογισμικού και συστημάτων υλικού. Αυτά τα στοιχεία πρέπει να ενσωματωθούν ως σύνολο και όχι μεμονωμένα.
- Έξοδα. Ο προϋπολογισμός για την επέκταση ενός PKI καθορίζεται από την προβλεπόμενη χρήση του PKI εντός της επιχείρησης ή του οργανισμού.
- Η αποδοχή του χρήστη είναι απαραίτητη. Ένα πλεονέκτημα του PKI είναι ότι επιτρέπει τη χρήση πανομοιότυπων τύπων πιστοποιητικών για τον έλεγχο ταυτότητας τόσο συσκευών όσο και ατόμων. Η αποτελεσματικότητα του PKI εξαρτάται από την αποδοχή του χρήστη. Ανεξάρτητα από την ποιότητα της τεχνολογίας ασφαλείας που υπάρχει, εάν οι χρήστες δεν τηρούν τις πολιτικές ή δεν εφαρμόζουν απρόσεκτες πρακτικές ασφάλειας, τα συστήματα γίνονται ευάλωτα σε σημαντικούς κινδύνους επίθεσης τόσο από εσωτερικές όσο και από εξωτερικές πηγές.
- Κλιμάκωση. Το PKI πρέπει να είναι ικανό να φιλοξενεί έναν αυξανόμενο αριθμό χρηστών, ξεκινώντας από μια μικρή βάση.
- Εφαρμογές. Μια κύρια πρόκληση έγκειται στην ανάπτυξη εφαρμογών που είναι αρκετά συναρπαστικές ώστε να ενθαρρύνουν τα άτομα να ασχοληθούν με το PKI και να αφιερώσουν τον απαραίτητο χρόνο και πόρους για την εφαρμογή και τη διατήρησή του. Αυτή η πρόκληση αντιπροσωπεύει ένα ευρέως διαδεδομένο εμπόδιο. Με άλλα λόγια, ενώ οι εφαρμογές απαιτούν PKI, το PKI εξαρτάται εξίσου από την ύπαρξη εφαρμογών.
- Ποικιλομορφία. Μια επιτυχημένη υλοποίηση PKI χρειάζεται να φιλοξενεί διάφορα λειτουργικά συστήματα, ξεχωριστά μηχανήματα και λογισμικό πολλαπλών πελατών.
- Διαβεβαίωση. Ο στόχος του PKI είναι να επιτρέψει αξιολογήσεις εμπιστοσύνης που είναι εφικτές και αποτελεσματικές.

6.4 Πλεονεκτήματα και Μειονεκτήματα ΥΔΚ

Όπως κάθε αναδυόμενη τεχνολογία, η PKI έχει το δικό της σύνολο πλεονεκτημάτων, προκλήσεων και εξόδων. Ενώ χρησιμεύει ως εξαιρετική λύση για πολλά ζητήματα ασφάλειας, είναι σημαντικό να προσδιορίσετε πρώτα τις συγκεκριμένες πληροφορίες που απαιτούν προστασία. Διάφοροι προμηθευτές PKI προσφέρουν διαφορετικές επαναλήψεις της τεχνολογίας PKI και αυτές οι λύσεις διαφέρουν τόσο σε ποιότητα όσο και σε κόστος. Επιπλέον, είναι σημαντικό να αξιολογηθούν οι ίδιοι οι προμηθευτές για την ικανότητά τους να παρέχουν συνεχή υποστήριξη για υπάρχουσες πωλήσεις παράλληλα με τη μελλοντική εξυπηρέτηση πελατών. Αυτή η αξιολόγηση είναι ένα κρίσιμο στοιχείο στη διαδικασία λήψης αποφάσεων (Evans & Yen, 2005). Εάν ένας προμηθευτής αντιμετωπίσει πτώχευση, η πρόσβαση σε μελλοντικές υπηρεσίες μπορεί να γίνει προβληματική. Συνοπτικά, τα πλεονεκτήματα ενός ΥΔΚ περιλαμβάνουν την απλότητα του να έχει ο χρήστης απλώς να κάνει «κλικ» στη σχετική εικόνα, επιτρέποντας στο λογισμικό να χειριστεί τα υπόλοιπα. Αυτή η φιλική προς τον χρήστη προσέγγιση είναι πιθανό να ενισχύσει την αποδοχή των καταναλωτών. Με την πάροδο του χρόνου, το PKI αναμένεται να μειώσει το κόστος μειώνοντας την εξάρτηση από συναλλαγές που βασίζονται στην εμπιστοσύνη και η υψηλή ταχύτητα και συχνότητα αυτών των συναλλαγών θα μειώσει το κόστος ανά μονάδα αλληλεπιδράσεων PKI. Αυτό θα μπορούσε να ενισχύσει την αντιληπτή αξία για τους πελάτες και ενδεχομένως να οδηγήσει σε μεγαλύτερο μερίδιο αγοράς. Τελικά, το PKI αντιπροσωπεύει την πιο ασφαλή μέθοδο για την αντιμετώπιση ζητημάτων συναλλαγών στο Διαδίκτυο, συμπεριλαμβανομένων απειλών από χάκερ, κλοπής πληροφοριών, μη εξουσιοδοτημένης παρεμβολής, σκόπιμης εισαγωγής ιών, κλοπής ταυτότητας και διαφόρων άλλων εγκληματικών δραστηριοτήτων (Evans & Yen, 2005).

Το άγχος των καταναλωτών σχετικά με την πιθανότητα κυβερνητικής παρείσφρησης στις ιδιωτικές τους συναλλαγές έρχεται σε πλήρη αντίθεση με το αίσθημα κατά του PKI. Ορισμένες υπηρεσίες επιβολής του νόμου συνηγορούν υπέρ της ενσωμάτωσης της τεχνολογίας backdoor στις λύσεις PKI για να επιτραπεί ο έλεγχος των συναλλαγών σε αναζήτηση πιθανής εγκληματικής συμπεριφοράς. Ένα άλλο ζήτημα που σχετίζεται με την υιοθέτηση της τεχνολογίας PKI είναι ο κίνδυνος οι αρχές πιστοποίησης (CA), οι οποίες είναι υπεύθυνες για την έκδοση πιστοποιητικών, να γίνουν αμελείς ή διεφθαρμένες (Evans & Yen, 2005). Το σημαντικό κόστος που συνδέεται με την εφαρμογή αυτής της νέας τεχνολογίας παρέχει ένα σημαντικό πλεονέκτημα στις μεγάλες

επιχειρήσεις που μπορούν να αξιοποιήσουν οικονομίες κλίμακας, αφήνοντας τις μικρότερες εταιρείες ανίκανες να επενδύσουν παρόμοια και επομένως σε ανταγωνιστικό μειονέκτημα. Επιπλέον, είναι σημαντικό για το PKI να λειτουργεί σε ευθυγράμμιση τόσο με τα εθνικά όσο και με τα διεθνή πρότυπα και η ανάπτυξη τεχνικών απαιτήσεων θα πρέπει να διασφαλίζει ότι αυτά δεν χρησιμεύουν ως τιμολόγια ούτε δημιουργούν τεχνητά εμπόδια εισόδου στη σφαίρα του ηλεκτρονικού εμπορίου.

Για να κατανοήσουμε αποτελεσματικά το PSC, είναι σημαντικό να διερευνήσουμε τα εσωτερικά στοιχεία που εμπλέκονται (Lancaster, et al., 2003). Αυτά τα στοιχεία περιλαμβάνουν το απαραίτητο υλικό και λογισμικό (η εφαρμογή ενός συστήματος PKI απαιτεί συγκεκριμένο υλικό), το συνολικό σύστημα (ενώ το PKI αντιπροσωπεύει σημαντική πρόοδο στην ψηφιακή ασφάλεια, πρέπει να ενσωματωθεί στην ολοκληρωμένη πολιτική ασφάλειας του οργανισμού για σωστή εφαρμογή), οι ενδιαφερόμενοι το PKI (αυτό περιλαμβάνει την επιχείρηση που κυρώνει τα πρωτόκολλα ασφαλείας, την αρχή έκδοσης πιστοποιητικών και τους κατόχους ψηφιακών ταυτοτήτων), καθώς και τις σχετικές τεχνολογίες (μια επιχείρηση πρέπει να λάβει υπόψη την προϋπάρχουσα τεχνολογία κατά την υιοθέτηση PKI) (Lancaster, et al., 2003). Επιπλέον, η κατανόηση ενός PSC απαιτεί την εξέταση των εξωτερικών παραγόντων που έχουν επηρεάσει το σύστημα και συνέβαλαν στην υιοθέτησή του.

7 Συμπεράσματα

Ως τομέας που επικεντρώνεται στην ασφάλεια των επικοινωνιών, η κρυπτολογία μπορεί να υπερηφανεύεται για μια πλούσια ιστορία που εκτείνεται σε χιλιάδες χρόνια, παράλληλα με την εξέλιξη των διαφόρων μεθόδων επικοινωνίας. Όλα ξεκίνησαν με την εμφάνιση πρώιμων τεχνικών κρυπτογράφησης, οι οποίες βασίζονταν σε απλές αντικαταστάσεις συμβόλων μηνυμάτων, και έχουν προχωρήσει μέχρι σήμερα, όπου έχουν δημιουργηθεί πολυάριθμοι περίπλοκοι αλγόριθμοι κρυπτογράφησης και εξελιγμένα πρωτόκολλα για την απόκρυψη πληροφοριών. Ιδιαίτερα τις τελευταίες δεκαετίες, η εκρηκτική επέκταση των τηλεπικοινωνιών -κυρίως που αντιπροσωπεύεται από το Διαδίκτυο- έχει καταστήσει τη διαφύλαξη του απορρήτου της επικοινωνίας μια βασική απαίτηση, τοποθετώντας την κρυπτολογία στην πρώτη γραμμή των τεχνολογικών εξελίξεων. Σήμερα, η κρυπτολογία είναι το επίκεντρο έντονων ερευνητικών προσπαθειών, που εξελίσσεται από τέχνη σε επιστήμη που χαρακτηρίζεται από ακριβείς ορισμούς και αυστηρές αποδείξεις.

Στον 21ο αιώνα, η σύγχρονη τεχνολογία βασίζεται σε μεγάλο βαθμό σε κρυπτογραφικές εφαρμογές, πρωτόκολλα και τεχνικές, που είναι ζωτικής σημασίας για ασφαλή επικοινωνία, ασφαλή πρόσβαση, ηλεκτρονική ψηφοφορία, διαχείριση και ανάκτηση ευαίσθητων δεδομένων, καθώς και ηλεκτρονικές συναλλαγές. Μια αξιοσημείωτη πρόοδος σε αυτόν τον τομέα είναι η εμφάνιση του Bitcoin και των διαφόρων διαδόχων του, που χαρακτηρίζεται κυρίως από έλλειψη κεντρικού ελέγχου. Οι προαναφερθείσες εφαρμογές, μαζί με πολλές άλλες που δεν αναφέρονται, οφείλουν την ύπαρξή τους σε πρωτοποριακές ιδέες και αλγόριθμους, όπως τέλεια μυστικότητα, κρυπτογραφία δημόσιου κλειδιού, ασφαλή απομακρυσμένη ανταλλαγή κλειδιών, ψηφιακές υπογραφές, διαδραστικά συστήματα απόδειξης, αποδείξεις μηδενικής γνώσης, γεννήτριες ψευδοτυχαίων, σύνθεση πρωτοκόλλου, συναρτήσεις σύννοψης χωρίς σύγκρουση, υπολογιστική πολυπλοκότητα και πολλά άλλα. Ένα κοινό χαρακτηριστικό μεταξύ αυτών των μεθόδων είναι ότι η ασφάλειά τους βασίζεται όλο και περισσότερο σε αυστηρές μαθηματικές αποδείξεις.

Για παράδειγμα, μπορούμε πλέον να συμμετέχουμε σε ηλεκτρονική ψηφοφορία που διασφαλίζει την απόδειξη της ακρίβειας για διαφορετικά στάδια εφαρμογής της ή να

εκτελούμε συναλλαγές μέσω Bitcoin και άλλων κρυπτονομισμάτων χωρίς να χρειαζόμαστε κεντρική αρχή, με κάθε συναλλαγή να επικυρώνεται συλλογικά. Η εμφάνιση των κρυπτονομισμάτων σηματοδοτεί μια συνεχιζόμενη επανάσταση, διευκολύνοντας την αποκεντρωμένη και επαληθεύσιμα ασφαλή ψηφιακή εκτέλεση λειτουργιών που προηγουμένως απαιτούσαν μια έγκυρη παρουσία, όπως η οριστικοποίηση συμβολαίων και η ηλεκτρονική ψηφοφορία. Για άλλη μια φορά, τα μαθηματικά διαδραματίζουν κρίσιμο ρόλο, ενισχύοντας την εμπιστοσύνη σε βασικές λειτουργίες και καθιστώντας την κρυπτογραφία προσβάσιμη στο κοινό. Τα περισσότερα κρυπτογραφικά συστήματα είναι πλέον εντελώς διαφανή (η λειτουργία τους γίνεται κατανοητή) και η ασφάλειά τους βασίζεται αποκλειστικά σε αριθμητικούς αλγόριθμους που επιτρέπουν αποτελεσματικές λειτουργίες με αριθμούς που περιέχουν χιλιάδες ψηφία, με αποτέλεσμα τεράστια υπολογιστική δυσκολία (πολυπλοκότητα) για αντίστροφες πράξεις. Η κρυπτογραφία έχει τελικά ξεπεράσει τα παραδοσιακά της όρια των μυστικών υπηρεσιών και των στρατιωτικών εφαρμογών, έτοιμη να επεκτείνει τα οφέλη της σε όλη την ανθρωπότητα, προάγοντας έτσι τη δημοκρατία, προστατεύοντας την ιδιωτική ζωή και εν τέλει ενθαρρύνοντας την ενεργό και ισότιμη συμμετοχή στο οικονομικό, πολιτικό και κοινωνικό τοπίο.

Βιβλιογραφία

- Adams, C., & Lloyd, S. (2002). *Understanding PKI: Concepts, Standards and Deployment Considerations*. Addison Wesley.
- Adams, C., Burmester, M., & Desmedt, Y. (2000). Which PKI (Public Key Infrastructure) is the Right One? *7th ACM conference on Computer and communications security*, (σσ. 98-101).
- Alderman, J., Cid, C., Crampton, J., & Janson, C. (2014). *Publicly verifiable outsourced computation with a key distribution centre*. arXiv preprint arXiv:1406.5720.
- Barman, S., Chattopadhyay, S., & Samanta, D. (2014). An approach to cryptographic key distribution through fingerprint based key distribution center. *International Conference on Advances in Computing, Communications and Informatics* (σσ. 1629-1635). IEEE.
- Barr, T. (2002). *Invitation to Cryptology*. Prentice Hall.
- Barthe, G., Betarte, G., Campo, J., Luna, C., & Pichardie, D. (2014). System-level non-interference for constant-time cryptography. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, (σσ. 1267-1279).
- Barton, J., Buchanan, W. J., Abramson, W., & Pitropakis, N. (2019). Performance Analysis of TLS for Quantum Robust Cryptography on a Constrained Device. *CoRR*.
- Bell, T., Thimbleby, H., Fellows, M., Witten, I., Koblitz, N., & Powel, M. (2003). Explaining cryptographic systems. *Computers & Education*, 40, σσ. 199-215.
- Bellare, M. (2004). *Introduction to Modern Cryptography*. Ανάκτηση από <http://www.cse.ucsd.edu/users/mihir/>
- Bellare, M., Desai, A., Pointcheval, D., & Rogaway, P. (1998). Relations among notions of security for public-key encryption schemes. *Annual International Cryptology Conference*, (σσ. 26-45).

- Berman, I., Degwekar, A., Rothblum, R. D., & Vasudevan, P. N. (2018). Multi-collision resistant hash functions and their applications. *Advances in Cryptology—EUROCRYPT 2018: 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques* (σσ. 133-161). Tel Aviv: Springer International Publishing.
- Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, 549(7671), σσ. 188-194.
- Boneh, D., & Shoup, V. (2020). *A graduate course in applied cryptography*. Draft 0.5.
- Bruschi, D., Curti, A., & Rosti, E. (2003). A quantitative study of Public Key Infrastructures. *Computers & Security*, 22(1), σσ. 56-67.
- Buchanan, W. J., Li, S., & Asif, R. (2017). Lightweight cryptography methods. *Journal of Cyber Security Technology*, 1(3-4), σσ. 187-201.
- Carayannis, E., & Turner, E. (2005). Innovation diffusion and technology acceptance: The case of PKI technology. *Technovation*, σσ. 1-9.
- Cheng, J. C., Lee, N. Y., Chi, C., & Chen, Y. H. (2018). Blockchain and smart contract for digital certificate. *IEEE international conference on applied system invention (ICASI)* (σσ. 1046-1051). IEEE.
- Daemen, J., & Rijmen, V. (2020). *The Design of Rijndael: The Advanced Encryption Standard (AES)*. Springer.
- Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Trans. Inf. Theory*, 22(6), σσ. 644-654.
- Diffie, W., & Hellman, M. E. (1976). Multiuser cryptographic techniques. *June 7-10, 1976, national computer conference and exposition*, (σσ. 109-112).
- Diffie, W., & Hellman, M. E. (1988). The first ten years of public-key cryptography. *Proc. IEEE*, 76(5), σσ. 560-577.
- Diffie, W., & Hellman, M. E. (2022). New directions in cryptography. Στο *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*. 365-390.
- Dobraunig, C., Eichlseder, M., Mendel, F., & Schl  ffer, M. (2015). Cryptanalysis of ascon. *Topics in Cryptology—CT-RSA 2015: The Cryptographer's Track at the*

- RSA Conference 2015* (σσ. 371-387). San Francisco, CA, USA: Springer International Publishing.
- Elgamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theory*, 31(4), σσ. 469-472.
- Ellision, C., & Schneier, B. (2000). Risks of PKI: E-commerce. *Communication of the ACM*, 43(2), σ. 152.
- Evans, D., & Yen, D. (2005). Private key infrastructure: balancing computer transmission privacy with changing technology and security demands. *Computer Standards & Interfaces*, 27, σσ. 423-437.
- Fernandes, A. (2001). Risking A trust B in a public key infrastructure: old techniques of managing risk applied to new technology. *Decision Support Systems*, 31, σσ. 303-322.
- Fratto, M. (2001). In PKI we trust. *Network Computing*.
- Gayathri, N., Sakhtivel, R. K., Rizwan, P., Gandomi, A. H., Muthuramalingam, S., & Balamurugan, B. (2020). Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. *Neural Computing & Applications*, 32(3), σσ. 639-647.
- Goldreich, O. (2001). *Foundations of Cryptography, basic tools*. Cambridge University Press.
- Gómez, A., Martínez, G., & Cánovas, Ó. (2003). New security services based on PKI. *Future Generation Computer Systems*, 19, σσ. 251-262.
- Graff, J. (2001). *Cryptography and E-Commerce, A Wiley Tech Brief*.
- Hunt, R. (2001). Technological infrastructure for PKI and digital certification. *Computer Communications*, 24, σσ. 1460-1471.
- Jøsang, A., Meling, H., & Lu, M. (1999). The development of public key infrastructures; Are we on the right path? *Norwegian Informatics Conference (NIK'99)*. Trondheim, Norway.
- Katz, J., & Lindell, Y. (2014). *Introduction to Modern Cryptography*. Chapman and Hall/CRC.

- Koblitz, N. (1987). Elliptic curve cryptosystems. *Math. Comput.*, 48(177), σσ. 203-209.
- Lamport, L. (1979). *Constructing digital signatures from a one-way function*.
- Lancaster, S., Yen, D., & Huang, S. (2003). Public key infrastructure: a micro and macro analysis. *Computer Standards & Interfaces*, 25, σσ. 437-446.
- Mansfield, N. (1999). Designing a Practical Public Key Infrastructure (PKI). *Information Security Technical Report*, 4(4), σσ. 18-27.
- Mao, W. (2004). *Modern Cryptography – Theory and Practice*. Prentice Hall.
- McEliece, R. J. (1978). A public-key cryptosystem based on algebraic coding theory. *Coding Thv*, 4244, σσ. 114-116.
- Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). *Handbook of applied cryptography*. CRC press.
- Merkle, R. C. (1979). *Secrecy, Authentication and Public Key Systems*. Stanford.
- Miller, V. S. (1985). Use of elliptic curves in cryptography. *Conference on the theory and application of cryptographic techniques*, (σσ. 417-426).
- Mishra, N., Islam, S. H., & Zeadally, S. (2021). A comprehensive review on collision-resistant hash functions on lattices. *Journal of Information Security and Applications*, 58.
- Mitchell, C. (2000). PKI standards. *Information Security Technical Report*, 5(4), σσ. 17-32.
- Moller, B. (2003). *Public-Key Cryptography Theory and Practice*. Technischen Universitat Darmstadt.
- National Institute of Standards and Technology. (2001). *Advanced Encryption Standard (AES)*. Ανάκτηση από <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf>.
- National Institute of Standards and Technology. (2015). *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*. Ανάκτηση από <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf>
- National Institute of Standards and Technology. (2021). *Glossary*. Ανάκτηση από <https://csrc.nist.gov/glossary>

- Raavi, M., Chandramouli, P., Wuthier, S., Zhou, X., & Chang, S. Y. (2021). Performance characterization of post-quantum digital certificates. *International Conference on Computer Communications and Networks (ICCCN)* (σσ. 1-9). IEEE.
- Rijneveld, J. (2019). *Practical post-quantum cryptography*. Radboud Universiteit Nijmegen.
- Rivest, R. L., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM*, 21(2), σσ. 120-126.
- Stallings, W. (2003). *Cryptography and Network Security*. Prentice Hall.
- Stallings, W. (2017). *Cryptography and Network Security*. Pearson Education Limited.
- Trappe, W., & Washington, L. (2002). *Introduction to Cryptography with Coding Theory*. Prentice Hall.
- Van Tilborg, H. C., & Jajodia, S. (2014). *Encyclopedia of cryptography and security*. Springer Science & Business Media.
- Yan, S. Y. (2013). *Computational Number Theory and Modern Cryptography*. John Wiley & Sons.
- Αριστείδης, Π., & Ζάχος, Ε. (2015). *Υπολογιστική Κρυπτογραφία*. Ανάκτηση από <https://repository.kallipos.gr/handle/11419/5439>

