1 ΕΙΣΑΓΩΓΗ

Προτού ξεκινήσουμε την περιήγησή μας στον κόσμο της κρυπτογραφίας, ας δούμε ορισμένα πρακτικά προβλήματα που κατά καιρούς έχουμε συναντήσει ή έχουμε φανταστεί.

- Το πρόβλημα του «μυστικού υπολογισμού». Πολλές φορές για λόγους διακριτικότητας είναι επιθυμητό να μην αποκαλύπτεται το εισόδημα κάποιου, αλλά απαιτούνται υπολογισμοί που περιλαμβάνουν ένα τέτοιο δεδομένο. Για παράδειγμα, μια ομάδα διευθυντών που παρευρίσκονται γύρω από ένα τραπέζι και θέλουν να υπολογίσουν το μέσο όρο των μισθών τους χωρίς όμως να αποκαλυφθούν αυτοί καθαυτοί οι μισθοί τους, θα πρέπει με κάποιον τρόπο να φανερώσουν το μισθό τους μόνον στο συνολικό άθροισμα έτσι ώστε όλοι οι μισθοί να «κρυφτούν» μεταξύ τους.
- Μια ειδική περίπτωση του προβλήματος του μυστικού υπολογισμού είναι το «πρόβλημα του ραντεβού». Ο Βύρων, από καιρό θέλει να ζητήσει την Αλίκη σε ραντεβού, αλλά φοβάται την απόρριψη. Έτσι επιθυμεί το ενδιαφέρον του για την Αλίκη να μην αποκαλυφθεί σε αυτήν παρά μόνον εάν υπάρχει αντίστοιχα ενδιαφέρον από τη μεριά της. Θα ήταν πολύ βολικό να υπάρχει κάποιος τρόπος έτσι ώστε ο Βύρων να ξέρει εκ των προτέρων αν η Αλίκη έχει σκοπό να δεχτεί την πρόταση για το ραντεβού. Σε αυτήν την περίπτωση ο Βύρων έχει την τύχη (ή καλύτερα, τα μαθηματικά) με το μέρος του. Η λύση του προβλήματος απαιτεί μια σειρά από υπολογισμούς και από τα δύο μέλη όπου η επιθυμία και των δύο για το ραντεβού είναι κρυμμένη και αποκαλύπτεται μόνον εάν είναι καταφατική. Εάν ο ένας από τους δύο ή και οι δύο δεν ενδιαφέρονται για το ραντεβού, τότε η διαδικασία των υπολογισμών θα παράγει ένα αποτέλεσμα όπου δεν θα είναι φανερή η επιθυμία κανενός από τους δύο. Φυσικά, εάν ο Βύρων που ενδιαφέρεται για την Αλίκη δει ότι το αποτέλεσμα δεν είναι καταφατικό, μπορεί να συμπεράνει ότι δεν ενδιαφέρεται η Αλίκη. Έχει όμως γλιτώσει από την αμηχανία που θα του επέφερε η άρνηση της Αλίκης εάν την ζητούσε σε ραντεβού.

- Το πρόβλημα της «μυστικής επικοινωνίας». Αυτό είναι και από τα πιο παραδοσιακά προβλήματα και αιτίες που εμφανίσθηκε η κρυπτογραφία. Πολλές φορές επιθυμούμε να επικοινωνήσουμε με κάποιον είτε άμεσα είτε έμμεσα (π.χ. αποστέλλοντας κάποιο γράμμα), χωρίς να γίνει αντιληπτό το περιεχόμενο σε τρίτους. Ορισμένες φορές μπορεί να επιθυμούμε να μη γίνει αντιληπτή και η ίδια η διαδικασία της επικοινωνίας.

Ίσως η σχέση του πρώτου και δεύτερου προβλήματος να μην είναι προφανής με την επιστήμη της κρυπτογραφίας. Εντούτοις προβλήματα μυστικού υπολογισμού είναι αντικείμενα της σύγχρονης κρυπτογραφίας με ποικίλες εφαρμογές όπως το ηλεκτρονικό χρήμα, οι ψηφιακές εκλογές, και η ηλεκτρονική δημοπρασία. Το τρίτο πρόβλημα αναφέρεται στην κλασσική κρυπτογραφία, τότε που η κρυπτογραφία δεν εθεωρείτο επιστήμη αλλά τέχνη. Σήμερα μπορούμε να υποστηρίξουμε ότι η κρυπτογραφία είναι περισσότερο επιστήμη παρά τέχνη, και το βιβλίο αυτό επιχειρεί να υποστηρίξει αυτήν τη θέση.

1.1. Ορισμοί και ορολογία

Στη διεθνή βιβλιογραφία προτείνονται διάφοροι ορισμοί της κρυπτογραφίας. Ο πιο διαδεδομένος αναφέρεται στο πρόβλημα της μυστικής επικοινωνίας:

ΟΡΙΣΜΟΣ 1.1 – Η κρυπτογραφία μελετά τρόπους με τους οποίους μπορούμε να μετασχηματίσουμε ένα μήνυμα σε φαινομενικά ακατάληπτη μορφή.

Μπορούμε να αντιληφθούμε από τα παραπάνω προβλήματα πως ο ορισμός αυτός αν και μπορεί να καλύψει στο μέγιστο βαθμό τη χρήση της κρυπτογραφίας από την εποχή της Αρχαίας Αιγύπτου μέχρι και τη Βιομηχανική Επανάσταση, στην εποχή της Πληροφορικής έχει βασικές ελλείψεις. Ο ορισμός που δόθηκε από τον Rivest (1990) εισάγει την έννοια του ***αντιπάλου*** και είναι ίσως ο πιο ακριβής και πλήρης ορισμός. Από το σημείο αυτό, με τον όρο κρυπτογραφία θα εννοούμε το εξής:

ΟΡΙΣΜΟΣ 1.2 – Η κρυπτογραφία ασχολείται με την επικοινωνία παρουσία αντιπάλων.

Όντως, η ύπαρξη αντιπάλου σε κάποια επικοινωνία είναι η βασική αιτία ύπαρξης και εφαρμογής της κρυπτογραφίας. Εκτός από την επιθυμία μας να κρύψουμε ένα μήνυμα από τα μάτια των αντιπάλων, που μπορεί να είναι ο ταχυδρόμος, ο δημοσιογράφος, ή ο κύριος της διπλανής πόρτας που πρόθυμα δέχεται να μας διευκολύνει ταχυδρομώντας το γράμμα μας, θα πρέπει με κάποιον τρόπο να μην αλλοιωθεί το μήνυμά μας, ή αν αλλοιωθεί να γίνει αντιληπτό από τον παραλήπτη, και επίσης να φτάσει στον πραγματικό του παραλήπτη και όχι σε κάποιον που τον υποδύεται. Οι τρόποι αντιμετώπισης αυτών των καταστάσεων περιγράφονται τυπικά με τις ***κρυπτογραφικές υπηρεσίες*** που αναφέρονται στην επόμενη παράγραφο.

Η αρχική μορφή του μηνύματος, αποτελεί το ***απλό κείμενο*** (plaintext), ενώ το κρυπτογραφημένο κείμενο αποτελεί το ***κρυπτοκείμενο*** (ciphertext). Ο μετασχηματισμός του απλού κειμένου σε κρυπτοκείμενο ονομάζεται ***κρυπτογράφηση*** (encryption) ενώ ο μετασχηματισμός του κρυπτοκειμένου σε απλό κείμενο ονομάζεται ***αποκρυπτογράφηση*** (decryption). Οι διαδικασίες της κρυπτογράφησης και της αποκρυπτογράφησης υλοποιούνται με ***αλγόριθμο κρυπτογράφησης*** και ***αποκρυπτογράφησης*** αντίστοιχα. Οι δύο αυτοί αλγόριθμοι συνιστούν τον ***κρυπταλγόριθμο*** (cipher). Η διαδικασία κρυπτογράφησης (και αποκρυπτογράφησης) απαιτεί μια επιπλέον ποσότητα πληροφορίας που την ονομάζουμε ***κλειδί*** (key). Η ύπαρξη του κλειδιού είναι και η ειδοποιός διαφορά της κρυπτογράφησης με την ***κωδικοποίηση*** (encoding). Αναλυτικότερα, η κρυπτογράφηση και αποκρυπτογράφηση ενός κειμένου μπορεί να πραγματοποιηθεί με επιτυχία μόνον από τον κάτοχο του σωστού κλειδιού. Ο όρος «κλειδί» είναι πολύ εύστοχος καθότι το κλειδί παραπέμπει σε κάτι μυστικό, που έχει συγκεκριμένους κατόχους, και είναι αναγκαίο για να κλειδώνει και ξεκλειδώνει κλειδαριές. Έτσι λοιπόν ένας αλγόριθμος κρυπτογράφησης μπορεί να παρομοιαστεί με μια κλειδαριά, η οποία χρησιμοποιείται για να φυλάξει ένα μήνυμα. Όποιος έχει το κλειδί μπορεί χωρίς μεγάλη προσπάθεια να ανοίξει την κλειδαριά και να διαβάσει το μήνυμα.

ΟΡΙΣΜΟΣ 1.3 – Η περιγραφή των διαδικασιών κρυπτογράφησης και αποκρυπτογράφησης αποτελούν το ***κρυπτοσύστημα.***

Επιστρέφοντας πάλι στον Ορισμό 1.2, ο αντίπαλος ενός κρυπτοσυστήματος θα επικεντρωθεί στο να ανακαλύψει το σωστό κλειδί, δηλαδή το κλειδί εκείνο με το οποίο θα μπορέσει να ανοίξει την κλειδαριά και να διαβάσει το μήνυμα.

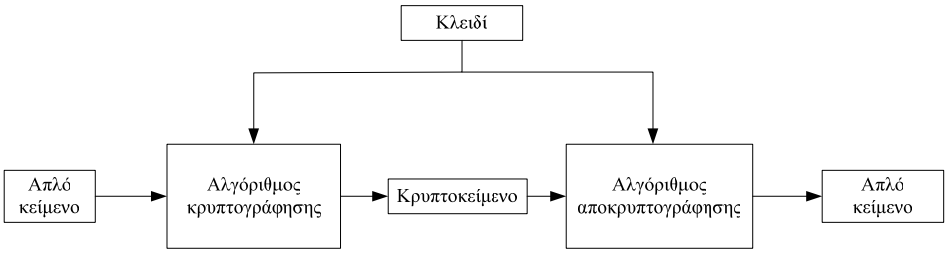
ΟΡΙΣΜΟΣ 1.4 – ***Κρυπτανάλυση*** είναι η επιστήμη που ασχολείται με την αποκρυπτογράφηση του κρυπτοκειμένου χωρίς την κατοχή του κλειδιού.

Εναλλακτικά, ο αντίπαλος μπορεί να ενδιαφέρεται περισσότερο στο να ανακαλύψει το κλειδί, για να μπορεί να αποκρυπτογραφήσει όλα τα μηνύματα που ενδεχομένως στάλθηκαν με τη χρήση του κλειδιού αυτού. Ο στόχος όμως παραμένει στο να ανακτήσει την πληροφορία που βρίσκεται κρυμμένη στο κρυπτοκείμενο. Σε αυτό το σημείο εύλογα γεννιέται η απορία του πώς είναι δυνατό να μπορούμε να ανακτήσουμε απευθείας το απλό κείμενο από το κρυπτοκείμενο, χωρίς να ανακαλύψουμε πρώτα το κλειδί. Αυτό το θέμα είναι γνωστό ως ***αποτυχία πρωτοκόλλου*** (protocol failure) όπου ο αντίπαλος «ξεγελάει» ένα κρυπτοσύστημα στο να εκτελέσει την αποκρυπτογράφηση σε ένα κρυπτοκείμενο το οποίο δεν του ανήκει. Ο αντίπαλος μπορεί να μη γνωρίζει το κλειδί, το οποίο μπορεί να είναι πολύ καλά θαμμένο μέσα στο σύστημα, αλλά μπορεί να εκμεταλλευτεί την πρόσβασή του σε αυτό και να επιτύχει την αποκρυπτογράφηση.

1.1.1. Συμμετρικά και ασύμμετρα κρυπτοσυστήματα

ΟΡΙΣΜΟΣ 1.5 – Ένα κρυπτοσύστημα ονομάζεται ***συμμετρικό***, όταν το κλειδί της κρυπτογράφησης είναι το ίδιο με αυτό της αποκρυπτογράφησης.

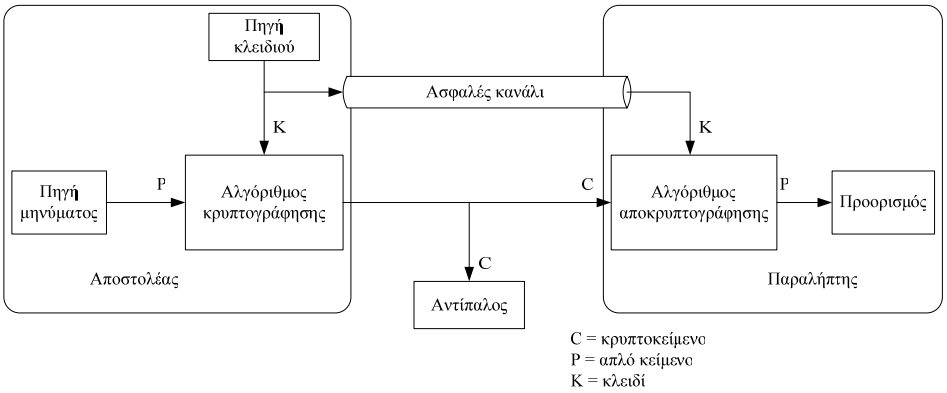
Τα συμμετρικά κρυπτοσυστήματα είναι και τα πιο διαδεδομένα χρονικά, καθότι τα ασύμμετρα κρυπτοσυστήματα εμφανίστηκαν επίσημα το 1976. Ένα συμμετρικό κρυπτοσύστημα αποτελείται από πέντε μέρη, όπως φαίνεται στο Σχήμα 1.1.



Σχήμα 1.1 Ένα συμμετρικό κρυπτοσύστημα

Το απλό κείμενο εισάγεται μαζί με το κλειδί στον αλγόριθμο κρυπτογράφησης. Όπως είναι φανερό στο παραπάνω σχήμα, το κλειδί είναι ανεξάρτητο του απλού κειμένου. Το αποτέλεσμα του αλγόριθμου κρυπτογράφησης είναι το κρυπτοκείμενο. Για δεδομένο απλό κείμενο, δύο διαφορετικά κλειδιά παράγουν δύο διαφορετικά κρυπτοκείμενα. Ο αλγόριθμος αποκρυπτογράφησης δέχεται ως είσοδο το κρυπτοκείμενο και το κλειδί το οποίο είναι το ίδιο με αυτό του αλγόριθμου κρυπτογράφησης. Ο αλγόριθμος αποκρυπτογράφησης εφαρμόζει τους αντίστροφους μετασχηματισμούς από αυτούς του αλγόριθμου κρυπτογράφησης και επαναφέρει το κείμενο στην αρχική του μορφή, αυτήν του απλού κειμένου.

Η αδυναμία του συμμετρικού συστήματος φαίνεται στο μοντέλο επικοινωνίας, που παρουσιάζεται στο Σχήμα 1.2.

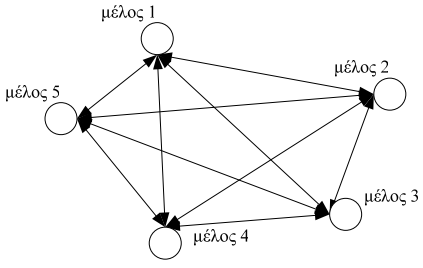


Σχήμα 1.2 Μοντέλο επικοινωνίας συμμετρικού κρυπτοσυστήματος

Η απαίτηση του κρυπτοσυστήματος να χρησιμοποιείται το ίδιο κλειδί στην κρυπτογράφηση και αποκρυπτογράφηση, προϋποθέτει ότι ο αποστολέας και ο παραλήπτης έχουν κάποιον ασφαλή τρόπο να μοιραστούν αυτήν την πληροφορία. Η υπόθεση που κάναμε ότι το κλειδί δημιουργείται και βρίσκεται αρχικά στον αποστολέα είναι έγκυρη, καθώς η κρυπτογράφηση προηγείται της αποκρυπτογράφησης. Επομένως, ο αποστολέας θα πρέπει να στείλει το κλειδί στον παραλήπτη, χωρίς να πέσει στα χέρια του αντιπάλου. Γιατί όμως να μπούμε στη διαδικασία κρυπτογραφίας εφόσον μπορούμε να έχουμε ασφαλές κανάλι; Θα μπορούσαμε να στέλναμε απ' ευθείας το κείμενο και δεν θα ήταν αναγκαία η κρυπτογράφησή του. Όπως θα διαπιστώσουμε, η κρυπτογραφία στην πραγματικότητα δεν λύνει τα προβλήματα, αλλά απλώς τα μετασχηματίζει σε μορφές τις οποίες μπορούμε πιο εύκολα να ελέγξουμε. Τα ασφαλή κανάλια δεν είναι πάντοτε διαθέσιμα, απαιτούν σχετικά μεγάλη προσπάθεια για να δημιουργηθούν και η μορφή τους είναι ανάλογα με την περίσταση. Για παράδειγμα ο αποστολέας και ο παραλήπτης μπορεί να είχαν συναντηθεί κάποια στιγμή στο παρελθόν και να είχαν μοιραστεί το κλειδί με την προοπτική να το χρησιμοποιήσουν σε μελλοντική επικοινωνία. Το ασφαλές κανάλι ήταν η επαφή τους χωρίς τη μεσολάβηση κάποιου τρίτου (μιας τηλεφωνικής εταιρείας για παράδειγμα). Ένας άλλος τρόπος για τη δημιουργία ασφαλούς καναλιού, είναι να τεμαχιστεί το κλειδί και τα τεμάχια να διαβιβασθούν μέσω διαφορετικών καναλιών, όπως τηλεφωνικά, ταχυδρομικά, ή με κούριερ, έτσι ώστε ο αντίπαλος να μην είναι σε θέση να μπορεί να τα παρακολουθεί όλα και να συλλέξει όλα τα τεμάχια για να χτίσει το κλειδί. Επίσης το κλειδί είναι πολύ μικρότερο σε μέγεθος από το απλό κείμενο και επιπλέον μπορεί να επαναχρησιμοποιηθεί για την κρυπτογράφηση πολλών κειμένων. Αυτό βέβαια είναι και μια πολύ σημαντική κρυπτογραφική αδυναμία που μπορεί να εκμεταλλευτεί ο αντίπαλος και να σπάσει το κρυπτοσύστημα όπως θα αναλύσουμε σε επόμενη ενότητα.

Το πρόβλημα του τετραγώνου

Η συμμετρική κρυπτογραφία έχει και μια άλλη πολύ σημαντική αδυναμία, που καθιστά τη χρήση της σε δίκτυα επικοινωνιών με πολλά μέλη πρακτικά αδύνατη. Η αδυναμία αναφέρεται ως το «πρόβλημα του τετραγώνου», το οποίο παρουσιάζεται στο Σχήμα 1.3.



	μέλος 1	μέλος 2	μέλος 3	μέλος 4	μέλος 5
μέλος 1		K_{12}	K_{13}	K_{14}	K_{15}
μέλος 2	K_{12}		K_{23}	K_{24}	K_{25}
μέλος 3	K_{13}	K_{23}		K_{34}	K_{35}
μέλος 4	K_{14}	K_{24}	K_{34}		K_{45}
μέλος 5	K_{15}	K_{25}	K_{35}	K_{45}	

Σχήμα 1.3 Πλήθος κλειδιών για n=5 μέλη

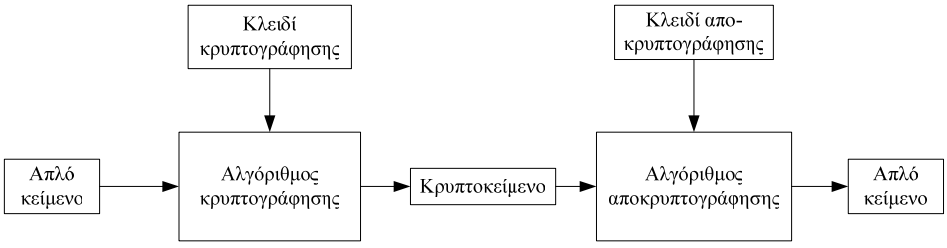
Έστω ότι *n* μέλη επικοινωνούν μεταξύ τους χρησιμοποιώντας συμμετρική κρυπτογραφία. Τότε, ανά δύο θα πρέπει να μοιράζονται κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση. Το κάθε μέλος θα πρέπει να αποθηκεύσει *n*-1 διαφορετικά κλειδιά, προκειμένου να μπορεί να επικοινωνήσει με οποιοδήποτε από τα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

$$\frac{n(n-1)}{2} = \frac{n^2 - n}{2}$$

κλειδιά. Το τετράγωνο στον αριθμητή υποδηλώνει το ρυθμό αύξησης των κλειδιών με την αύξηση των μελών. Στο Σχήμα 1.3 ο αριθμός των κλειδιών που θα πρέπει να μοιρασθούν αντιπροσωπεύεται από τα ευθύγραμμα τμήματα που συνδέουν τα μέλη. Για *n*=5, ο αριθμός των κλειδιών ανέρχεται σε 10. Εάν εμφανισθεί ένα ακόμη μέλος, ο αριθμός των κλειδιών θα είναι 15. Για αυτόν το σχετικά μικρό αριθμό μελών, το πρόβλημα δεν είναι εμφανές. Ας μην ξεχνάμε όμως ότι για κάθε ένα από τα κλειδιά αυτά θα πρέπει με κάποιον τρόπο να υπάρχει και κάποιο ασφαλές κανάλι επικοινωνίας. Για μια μικρή λίστα αποδεκτών στο Internet με 1000 μέλη, ο αριθμός των κλειδιών είναι 499.500. Εκτός από το γεγονός ότι μισό εκατομμύριο ασφαλή κανάλια επικοινωνίας είναι οικονομικώς ασύμφορο (αν όχι αδύνατο), τίθεται και το θέμα της αποθήκευσης των κλειδιών. Επίσης, όπως θα δούμε σε επόμενο κεφάλαιο, ένα κλειδί έχει μια πεπερασμένη περίοδο ζωής και θα πρέπει να ανανεώνεται περιοδικά.

Η αδυναμία των συμμετρικών κρυπτοσυστημάτων να εξαρτώνται από ένα ασφαλές κανάλι επικοινωνίας, καθώς και το πρόβλημα του τετραγώνου, ήταν οι δύο κύριοι λόγοι που συνέβαλλαν στην ανακάλυψη της ασύμμετρης κρυπτογραφίας.

ΟΡΙΣΜΟΣ 1.6 – Ένα κρυπτοσύστημα ονομάζεται ***ασύμμετρο***, όταν χρησιμοποιούνται δύο διαφορετικά κλειδιά, το ένα για την κρυπτογράφηση και το άλλο για την αποκρυπτογράφηση.



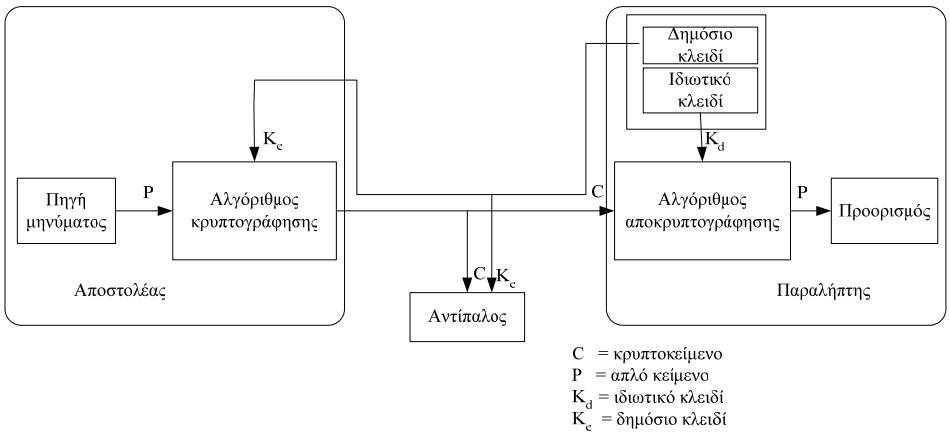
Σχήμα 1.4 Ένα ασύμμετρο κρυπτοσύστημα

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. 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 C στον παραλήπτη.
4. Ο παραλήπτης αποκρυπτογραφεί το κρυπτοκείμενο χρησιμοποιώντας το ιδιωτικό κλειδί K_d.

Το μοντέλο επικοινωνίας του ασύμμετρου κρυπτοσυστήματος φαίνεται στο Σχήμα 1.5.

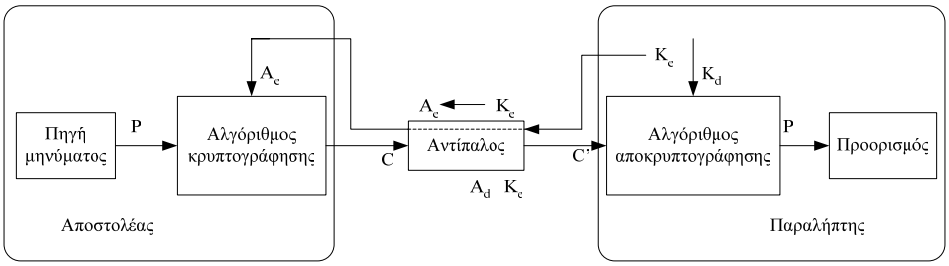


Σχήμα 1.5 Μοντέλο επικοινωνίας ασύμμετρου κρυπτοσυστήματος

Μια ενδιαφέρουσα και χρήσιμη ιδιότητα του ασύμμετρου κρυπτοσυστήματος είναι ότι ένα ζευγάρι ιδιωτικού/δημόσιου κλειδιού μπορεί να χρησιμοποιηθεί αντίστροφα, δηλαδή το ιδιωτικό κλειδί μπορεί να κρυπτογραφήσει ένα απλό κείμενο, και το δημόσιο κλειδί να αποκρυπτογραφήσει το αντίστοιχο κρυπτοκείμενο. Αυτή η ιδιότητα είναι η αρχή λειτουργίας της ***ψηφιακής υπογραφής***. Ο κάτοχος του ιδιωτικού κλειδιού είναι ο μόνος που μπορεί να κρυπτογραφήσει ένα κείμενο με το ιδιωτικό του κλειδί, ενώ οποιοσδήποτε μπορεί να το αποκρυπτογραφήσει. Εάν το κρυπτογραφημένο κείμενο συνοδεύεται από το απλό κείμενο, τότε ο παραλήπτης

μπορεί να συγκρίνει το απλό κείμενο με το αποτέλεσμα της αποκρυπτογράφησης και να επαληθεύσει ότι το κείμενο προέρχεται από τον κάτοχο του ιδιωτικού κλειδιού.

Για μια ακόμη φορά η κρυπτογραφία δεν έχει λύσει το πρόβλημα, αλλά το έχει μετασχηματίσει. Πλέον, δεν τίθεται πρόβλημα της διανομής του κλειδιού, αλλά υπάρχει το πρόβλημα του «ενδιάμεσου ατόμου» (man in the middle). Εφόσον ο αποστολέας και ο παραλήπτης επικοινωνούν με ψηφιακά μέσα στέλνοντας μόνο μηνύματα, ο αντίπαλος έχει τη δυνατότητα στο μοντέλο του ασύμμετρου κρυπτοσυστήματος να συμμετέχει ενεργά, προκειμένου να αποκρυπτογραφήσει το μήνυμα. Η επίθεση του ενδιάμεσου ατόμου παρουσιάζεται στο Σχήμα 1.6. Ο αντίπαλος παρεμβάλλεται μεταξύ του αποστολέα και του αποδέκτη και αναλαμβάνει να δρομολογεί τα μηνύματα που ανταλλάσσονται μεταξύ του αποστολέα και του αποδέκτη. Έτσι, κατά την περίοδο της αποστολής του δημόσιου κλειδιού, ο αντίπαλος αντικαθιστά το δημόσιο κλειδί του παραλήπτη K_e με το δικό του δημόσιο κλειδί A_e, εφόσον γνωρίζει και το ιδιωτικό του κλειδί A_d. Ο αποστολέας πιστεύει ότι το δημόσιο κλειδί που έλαβε είναι του παραλήπτη του μηνύματος, ενώ το κλειδί αυτό στην πραγματικότητα είναι του αντιπάλου. Συνεπώς, το μήνυμα κρυπτογραφείται (C) με το δημόσιο κλειδί του αντιπάλου. Στη συνέχεια, ο αντίπαλος αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί, το κρυπτογραφεί με το δημόσιο κλειδί του παραλήπτη και μεταβιβάζει το νέο κρυπτοκείμενο (C′) στον παραλήπτη, με αποτέλεσμα η παρεμβολή του να μη γίνει αντιληπτή από κανέναν από τους δύο συμμετάσχοντες.



Σχήμα 1.6 Η επίθεση του «ενδιάμεσου ατόμου».

Στη συνέχεια του βιβλίου, για πρακτικούς λόγους θα χρησιμοποιούμε ονόματα για τα μέλη που συμμετέχουν σε ένα σύστημα επικοινωνίας. Ο αποστολέας θα είναι η Αλίκη, ενώ ο παραλήπτης θα είναι ο Βύρων. Όπως θα δούμε πολλές φορές ο ρόλος του παραλήπτη και του αποστολέα αντιστρέφεται, οπότε η χρήση ονομάτων παρέχει το πλεονέκτημα αυτής της εναλλαγής. Εξάλλου είναι αναμενόμενο σε μια επικοινωνία τα μέλη που επικοινωνούν να εναλλάσσονται στους ρόλους του αποστολέα και του παραλήπτη. Έτσι θα συναντήσουμε δηλώσεις όπως «Η Αλίκη στέλνει το κρυπτοκείμενο στον Βύρωνα», «Ο Βύρων υπογράφει το απλό κείμενο», κ.ο.κ.

1.1.2. Κρυπτογραφικές υπηρεσίες και πρωτόκολλα

Παραπέμποντας στον Ορισμό 1.2, η κρυπτογραφία ασχολείται με την επικοινωνία παρουσία αντιπάλων. Ο λόγος που αποδεχόμαστε έναν τόσο γενικό ορισμό είναι γιατί και οι απειλές στις επικοινωνίες είναι ποικίλες, και η κρυπτογραφία παρέχει τη δυνατότητα αντιμετώπισής των. Οι κρυπτογραφικές υπηρεσίες είναι υπηρεσίες που χρησιμοποιώντας κρυπτογραφία, στοχεύουν στην αντιμετώπιση συγκεκριμένων απειλών. Οι κρυπτογραφικές υπηρεσίες είναι οι ακόλουθες:

- ***Εμπιστευτικότητα*** (Confidentiality)**.** Είναι η προστασία από τη μη εξουσιοδοτημένη αποκάλυψη της πληροφορίας. Η εμπιστευτικότητα θα πρέπει να προσφέρεται με τέτοιον τρόπο ώστε να είναι αδύνατη η αποκάλυψη και πολλές φορές η ίδια η ύπαρξη της πληροφορίας σε μη εξουσιοδοτημένα άτομα. Για παράδειγμα, κατά την κρίση στον Περσικό Κόλπο, η πληροφορία ότι η στρατιωτική ηγεσία των Ηνωμένων Πολιτειών προετοίμαζε επιχειρήσεις διέρρεε λόγω του αυξημένου αριθμού παραγγελιών σε πιτσαρία γειτονική του Πενταγώνου κατά τις νυκτερινές ώρες.
- ***Ακεραιότητα*** (Integrity). Είναι η προστασία από τη μη εξουσιοδοτημένη τροποποίηση των δεδομένων. Η ακεραιότητα θα πρέπει να παρέχει στον παραλήπτη και γενικότερα στον κάτοχο ενός μηνύματος τη δυνατότητα να μπορεί να ανιχνεύσει πιθανές αλλαγές στο μήνυμα από μη εξουσιοδοτημένα άτομα. Στον χώρο των τηλεπικοινωνιών και της θεωρίας της πληροφορίας, η ακεραιότητα είναι γνωστή ως ανίχνευση σφαλμάτων, όπου ένα μήνυμα μπορεί να υποστεί τροποποίηση λόγω του θορύβου του καναλιού επικοινωνίας.
- ***Αυθεντικοποίηση*** (Authentication). Είναι η εξασφάλιση του ότι γνωρίζουμε το χρήστη ή γενικότερα την οντότητα που επικοινωνούμε (user/ entity authentication). Αυθεντικοποίηση δεδομένων (data authentication) είναι η εξασφάλιση ότι ένα μήνυμα προέρχεται πράγματι από τον αποστολέα που πιστεύουμε ότι το έστειλε.
- ***Μη-απάρνηση*** (Non-repudiation). Είναι η υπηρεσία κατά την οποία ο παραλήπτης δεν μπορεί να απαρνηθεί ότι έλαβε το μήνυμα (μη-απάρνηση προορισμού (non-repudiation of destination)), ή η υπηρεσία κατά την οποία ο αποστολέας δεν μπορεί να απαρνηθεί ότι έστειλε το μήνυμα (μη-απάρνηση προέλευσης (non-repudiation of origin)).

Θα πρέπει να σημειωθεί ότι υπάρχει αλληλεξάρτηση της ακεραιότητας και της αυθεντικοποίησης ενός μηνύματος. Δεν είναι δυνατό να προσφέρεται με επιτυχία μόνον ακεραιότητα χωρίς να προσφέρεται αυθεντικοποίηση και αντίστροφα. Σε περίπτωση που προσφέρεται αυθεντικοποίηση χωρίς ακεραιότητα, ο αντίπαλος μπορεί να τροποποιήσει την πληροφορία αυθεντικοποίησης, προσδίδοντας διαφορετικό κάτοχο στο μήνυμα. Σε περίπτωση που προσφέρεται ακεραιότητα χωρίς αυθεντικοποίηση, ο αντίπαλος μπορεί ανεξέλεγκτα να τροποποιήσει το μήνυμα

και να επανυπολογίσει το κρυπτογραφικό άθροισμα ελέγχου που προσδιορίζει την ακεραιότητα του μηνύματος

ΟΡΙΣΜΟΣ 1.7 – *Κρυπτογραφικό πρωτόκολλο* είναι η πλήρως αποσαφηνισμένη διαδικασία που πρέπει να ακολουθήσουν τα επικοινωνούντα μέλη, προκειμένου να επιτύχουν μια συγκεκριμένη κρυπτογραφική υπηρεσία.

Το βασικό χαρακτηριστικό του κρυπτογραφικού πρωτοκόλλου είναι ότι πρέπει το κάθε μέλος να γνωρίζει σε κάθε χρονική στιγμή (κατά τη διάρκεια εκτέλεσης του πρωτοκόλλου) πιο βήμα πρέπει να εκτελεστεί και πως πρέπει να εκτελεστεί. Οποιαδήποτε παρέκκλιση από τη διαδικασία που απαιτεί το κρυπτογραφικό πρωτόκολλο έχει ως αποτέλεσμα την κατάρρευση της επικοινωνίας ή της υποκείμενης κρυπτογραφικής υπηρεσίας.

ΠΑΡΑΔΕΙΓΜΑ 1.1 – Απλό πρωτόκολλο ανταλλαγής κλειδιών. Η Αλίκη και ο Βύρων αποφασίζουν να χρησιμοποιήσουν ένα συμμετρικό κρυπτοσύστημα για να ανταλλάξουν εμπιστευτικά μηνύματα. Η διανομή του κλειδιού γίνεται μέσω ασύμμετρου κρυπτοσυστήματος με το ακόλουθο πρωτόκολλο:

1. Η Αλίκη δημιουργεί ένα συμμετρικό κλειδί.
2. Η Αλίκη ζητά το δημόσιο κλειδί του Βύρωνα.
3. Ο Βύρων στέλνει το δημόσιό του κλειδί στην Αλίκη.
4. Η Αλίκη κρυπτογραφεί το συμμετρικό κλειδί με το κλειδί του Βύρωνα.
5. Η Αλίκη στέλνει το κρυπτογραφημένο κλειδί στον Βύρωνα σε μορφή κρυπτογραφημένου μηνύματος.
6. Ο Βύρων αποκρυπτογραφεί το κρυπτογραφημένο μήνυμα και ανακτά το συμμετρικό κλειδί.

Με την ολοκλήρωση του πρωτοκόλλου η Αλίκη και ο Βύρων έχουν ένα κοινό συμμετρικό κλειδί το οποίο το μοιράστηκαν με εμπιστευτικότητα.

1.1.3. Αρχές μέτρησης κρυπτογραφικής δύναμης

Το πρώτο στάδιο στην ανάλυση της δύναμης ενός κρυπτοσυστήματος είναι η υπόθεση της ικανότητας του αντιπάλου. Η ικανότητα του αντιπάλου κρίνεται με βάση τους πόρους που διαθέτει, καθώς και με την πρόσβαση που έχει στο κρυπτοκείμενο, στο απλό κείμενο και στο κρυπτοσύστημα. Οι δυνατότητες επίθεσης ενός αντιπάλου σε ένα κρυπτοσύστημα χωρίζονται στις ακόλουθες κατηγορίες:

- Επίθεση στο κρυπτοκείμενο (ciphertext-only). Ο αντίπαλος έχει πρόσβαση μόνο σε ορισμένα κομμάτια του κρυπτοκειμένου και ο αντικειμενικός του σκοπός είναι να αποκρυπτογραφήσει το κρυπτοκείμενο αυτό, ή να ανακαλύψει το αντίστοιχο κλειδί. Ένα κρυπτοσύστημα το οποίο είναι ευάλωτο σε μια τέτοια επίθεση θεωρείται ανασφαλές.
- Επίθεση με γνωστό απλό κείμενο (known-plaintext). Ο αντίπαλος γνωρίζει αντιστοιχίες κρυπτοκειμένου με απλό κείμενο, και ο αντικειμενικός του

σκοπός είναι η ανακάλυψη του αντίστοιχου κλειδιού. Πολλές φορές συναντάμε μηνύματα όπως γράμματα, όπου η αρχή και το τέλος τους είναι τυποποιημένα, όπως «αγαπητέ κ….» και «με εκτίμηση….». Στον κόσμο των δικτύων των υπολογιστών τα πρωτόκολλα επικοινωνίας εμφανίζουν συστηματικά τυποποιημένα μηνύματα. Ένα κρυπτοσύστημα το οποίο υποπίπτει σε επίθεση γνωστού απλού κειμένου θεωρείται ανασφαλές.

- Επίθεση με επιλεγμένο απλό κείμενο (chosen-plaintext). Ο αντίπαλος έχει τη δυνατότητα πρόσβασης στο κρυπτοσύστημα όπου δεν γνωρίζει το κλειδί και μπορεί να ζητά την κρυπτογράφηση μηνυμάτων. Με αυτόν τον τρόπο μπορεί να ανακαλύψει την αντιστοιχία του απλού κειμένου με το άγνωστο κρυπτοκείμενο
- Επίθεση προσαρμόσιμου επιλεγμένου απλού κειμένου (adaptive chosen-plaintext). Ο αντίπαλος είναι σε θέση να πραγματοποιήσει επίθεση με επιλεγμένο απλό κείμενο, αλλά επιπλέον μπορεί να εφαρμόσει μεθοδολογία σύμφωνα με την οποία η επόμενη επιλογή του απλού κειμένου εξαρτάται από τις προηγούμενες, προκειμένου να ανακαλύψει γρηγορότερα το κλειδί, από μια εξαντλητική αναζήτηση (exhaustive search).
- Επίθεση με επιλεγμένο κρυπτοκείμενο (chosen-ciphertext). Υποθέτοντας ότι ο αντίπαλος έχει πρόσβαση στον αλγόριθμο αποκρυπτογράφησης, ο αντικειμενικός σκοπός του είναι να ανακαλύψει το κλειδί αποκρυπτογράφησης προκειμένου να μπορεί στο μέλλον να αποκρυπτογραφεί τα νέα κρυπτοκείμενα, όταν δεν θα έχει πρόσβαση στον αλγόριθμο αποκρυπτογράφησης. Στα περισσότερα συμμετρικά κρυπτοσυστήματα η επίθεση αυτή έχει την ίδια ισχύ με την επίθεση του επιλεγμένου απλού κειμένου. Η επίθεση με επιλεγμένο κρυπτοκείμενο θεωρείται ως η πιο αυστηρή επίθεση.
- Επίθεση προσαρμόσιμου επιλεγμένου κρυπτοκειμένου (adaptive chosen-ciphertext). Η επίθεση αυτή είναι αντίστοιχη του προσαρμόσιμου επιλεγμένου απλού κειμένου, με τη διαφορά ότι ο αντίπαλος έχει πρόσβαση στον αλγόριθμο αποκρυπτογράφησης.

Η αρχή του Kerchoff

Στις παραπάνω δυνατότητες επίθεσης είναι προφανές ότι ο αντίπαλος γνωρίζει πλήρως τον αλγόριθμο κρυπτογράφησης. Αυτό εκτός από απαίτηση είναι και ένα θεμελιώδες κριτήριο στην αντικειμενική μέτρηση της δύναμης ενός κρυπτοσυστήματος το οποίο είναι γνωστό ως 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»

Η απαίτηση να είναι ο αλγόριθμος κρυπτογράφησης μυστικός υποθάλπει τόσο κινδύνους όσο και προβλήματα. Πρώτον, η αντικειμενική αξιολόγηση του αλγό-

ριθμου δεν θα είναι εφικτή, με αποτέλεσμα να είναι αδύνατον να υπολογισθεί η πραγματική του κρυπτογραφική δύναμη. Δεύτερον, η αντίστροφη ανάλυση (reverse engineering) επέτρεπε στον αντίπαλο να ανακαλύπτει τη δομή και λεπτομέρειες του αλγόριθμου κρυπτογράφησης. Η ιστορία μας έχει διδάξει ότι όποτε η κρυπτογραφία βασιζόταν στη μυστικότητα του αλγόριθμου κρυπτογράφησης, η κατάρρευση του κρυπτοσυστήματος ήταν σχεδόν βέβαιη. Τρίτον, εάν ένα κλειδί γίνει γνωστό είναι σχετικά εύκολη η αντικατάστασή του, ενώ εάν ο αλγόριθμος κρυπτογράφησης γίνει γνωστός, τότε υπάρχει σοβαρό πρόβλημα στην αποτελεσματικότητα της μυστικής επικοινωνίας.

Τα μέτρα του Shannon

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 ύπαρξη των μέτρων σε ένα κρυπτοσύστημα είναι υποχρεωτική, αλλά συγχρόνως και αντιφατική, με αποτέλεσμα να μην υπάρχει στην πραγματικότητα κρυπτοσύστημα το οποίο να ικανοποιεί όλα τα μέτρα στο μέγιστό τους. Για παράδειγμα, πλήρης έλλειψη του μέτρου 1 σημαίνει ότι ο αντίπαλος μπορεί να ανακτήσει πλήρως το απλό κείμενο, ή ακόμη καλύτερα, το απλό κείμενο είναι ένα αποδεκτό κρυπτοκείμενο. Η πλήρης έλλειψη των μέτρων 3 και 4 επιτρέπει κρυπτοσυστήματα που μπορούν να μεγιστοποιούν όλα τα άλλα μέτρα. Η πλήρης έλλειψη του μέτρου 5 δέχεται ύπαρξη κρυπτοσυστήματος που μεγιστοποιεί όλα τα άλλα μέτρα, αλλά σε περίπτωση σφάλματος κατά την κρυπτογράφηση, η ανάκτηση του απλού κειμένου θα ήταν αδύνατη, ακόμη και για κάποιο τμήμα αυτού.

Σύγχυση και Διάχυση

Δύο ιδιότητες που χρησιμοποιούνται στην αξιολόγηση της κρυπτογραφικής δύναμης είναι η σύγχυση (confusion) και η διάχυση (diffusion).

Έστω ένα απλό κείμενο το οποίο αντιστοιχεί σε ένα κρυπτοκείμενο μέσω ενός κρυπταλγόριθμου. Εάν αντικαταστήσουμε ένα σύμβολο του απλού κειμένου και κρυπτογραφήσουμε το νέο απλό κείμενο, τότε για έναν κρυπταλγόριθμο με υψηλή διάχυση, ο αντίπαλος δεν θα μπορεί να προβλέψει ποια σύμβολα του κρυπτοκειμένου θα μεταβληθούν ή γενικότερα θα επηρεαστούν.

ΟΡΙΣΜΟΣ 1.8 – *Σύγχυση* είναι η ικανότητα του αλγόριθμου κρυπτογράφησης όπου ο αντίπαλος δεν είναι σε θέση να προβλέψει ποιες μεταβολές θα συμβούν στο κρυπτοκείμενο, δεδομένης μιας μεταβολής στο απλό κείμενο.

Δηλαδή, ένας αλγόριθμος έχει υψηλή σύγχυση όταν οι σχέσεις μεταξύ του απλού κειμένου και του κρυπτοκειμένου είναι αρκετά πολύπλοκες, ώστε να χρειάζεται ο αντίπαλος να ξοδέψει σημαντικό χρόνο προκειμένου να τις προσδιορίσει.

ΟΡΙΣΜΟΣ 1.9 – *Διάχυση* είναι η ικανότητα του αλγόριθμου κρυπτογράφησης όπου ένα τμήμα του απλού κειμένου να έχει την ευκαιρία να επηρεάζει όσο το δυνατόν περισσότερα τμήματα του κρυπτοκειμένου.

Ένας αλγόριθμος έχει υψηλή διάχυση όταν ένα στοιχειώδες τμήμα του απλού κειμένου έχει την δυνατότητα να επηρεάσει όλα τα τμήματα του κρυπτοκειμένου, ανεξάρτητα της τοποθεσίας του τμήματος αυτού στο απλό κείμενο.

Μοντέλα αξιολόγησης ασφάλειας

Η δύναμη ενός κρυπτοσυστήματος να αντιστέκεται στις επιθέσεις του αντιπάλου είναι ένα αντικείμενο το οποίο μπορεί να εξεταστεί από πολλές πλευρές. Η ανάγκη καθορισμού αντικειμενικών μέτρων για τη μέτρηση της κρυπτογραφικής δύναμης είχε ως αποτέλεσμα τη δημιουργία διαφόρων μαθηματικών μοντέλων.

- Ασφάλεια άνευ όρων (unconditionally secure). Ένα κρυπτοσύστημα είναι άνευ όρων ασφαλές όταν το κρυπτοκείμενο δεν δίνει καμία πληροφορία στον αντίπαλο σχετικά με το απλό κείμενο. Η υπόθεση απαιτεί ότι ο αντίπαλος έχει άπειρη υπολογιστική ισχύ στη διάθεσή του. Το μοντέλο αυτό διατυπώθηκε από τον Shannon, όπου η ασφάλεια εξετάζεται κάτω από το πρίσμα της θεωρίας της πληροφορίας. Σύμφωνα με τη θεωρία της πληροφορίας, ένα κρυπτοσύστημα είναι άνευ όρων ασφαλές όταν η πιθανότητα που έχει ο αντίπαλος για να σπάσει το κρυπτοκείμενο είναι ίδια με την πιθανότητα που θα έχει εάν του δοθεί λύση για ένα τμήμα του κρυπτοκειμένου.
- Υπολογιστική ασφάλεια (computationally secure). Σε αυτό το μοντέλο εισάγεται πλέον η παράμετρος της δυνατότητας χρήσης υπολογιστικής ισχύος του αντιπάλου. Ένα κρυπτοσύστημα είναι υπολογιστικά ασφαλές, όταν προκειμένου να το σπάσει ο αντίπαλος απαιτείται υπολογιστική ισχύς πέραν των δυνατοτήτων του. Ο υπολογισμός γίνεται με βάση τον καλύτερο αλγόριθμο που γνωρίζει ο αντίπαλος προκειμένου να σπάσει το κρυπτοσύστημα. Ο προφανής αλγόριθμος που έχει για να σπάσει ένα κρυ-

πτοσύστημα είναι αυτός της ***εξαντλητικής αναζήτησης*** (exhaustive search) όπου ο αντίπαλος δοκιμάζει ένα ένα τα κλειδιά έως ότου ανακαλύψει το σωστό. Ο αναμενόμενος χρόνος ανακάλυψης του σωστού κλειδιού είναι ανάλογος του μισού του συνολικού αριθμού των κλειδιών. Σε ορισμένα κρυπτοσυστήματα έχουν ανακαλυφθεί και πιο «έξυπνοι» αλγόριθμοι αναζήτησης κλειδιών, που φτάνουν στο επιθυμητό αποτέλεσμα πιο γρήγορα από την εξαντλητική αναζήτηση. Συνεπώς, η υπολογιστική ασφάλεια δεν εγγυάται την ασφάλεια ενός κρυπτοσυστήματος, επειδή στο μέλλον μπορεί να ανακαλυφθεί αλγόριθμος κρυπτανάλυσης ο οποίος να μπορεί να εκτελεσθεί εντός των υπολογιστικών δυνατοτήτων του αντιπάλου.

- Ασφάλεια θεωρητικής πολυπλοκότητας (complexity theoretic). Θεωρείται ότι ο αντίπαλος μπορεί να πραγματοποιήσει επίθεση στο κρυπτοσύστημα η οποία απαιτεί πολυωνυμική υπολογιστική ισχύ. Δηλαδή, οι παράμετροι ασφάλειας του κρυπτοσυστήματος μπορούν να εκφραστούν πολυωνυμικά ως προς το χώρο και το χρόνο. Η ανάλυση με βάση το μοντέλο ασφάλειας θεωρητικής πολυπλοκότητας εξετάζει ασυμπτωτικά την αντοχή του κρυπτοσυστήματος σε κρυπταναλυτικές επιθέσεις και δεν έχει πρακτική αξία. Ωστόσο μια τέτοια ανάλυση μπορεί να οδηγήσει στη διαπίστωση θεμελιωδών εννοιών και αρχών ασφάλειας των κρυπτοσυστημάτων.
- Αποδείξιμη ασφάλεια (provable security). Ένα κρυπτοσύστημα είναι αποδείξιμα ασφαλές όταν μπορούμε να αποδείξουμε ότι η ασφάλειά του είναι ισοδύναμη κάποιου γνωστού και καλά μελετημένου προβλήματος που θεωρείται «δύσκολο». Παραδείγματα τέτοιων προβλημάτων βρίσκουμε στη θεωρία αριθμών, όπως η παραγοντοποίηση ενός μεγάλου σύνθετου αριθμού στους πρώτους παράγοντές του, και ο υπολογισμός του διακριτού λογάριθμου ενός αριθμού. Τα κρυπτοσυστήματα που είναι αποδείξιμα ασφαλή ανήκουν σε υποσύνολο των συστημάτων που είναι υπολογιστικά ασφαλή, αλλά ένα κρυπτοσύστημα αποδείξιμης ασφάλειας έχει πολύ καλές προοπτικές να είναι ασφαλές, αφού το υποκείμενο «δύσκολο» πρόβλημα έχει υποστεί εκτενείς μελέτες και είναι γενικώς αποδεκτό ως «δύσκολο».