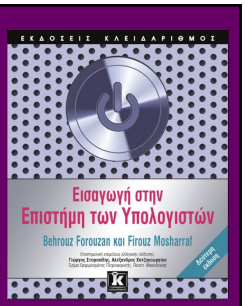
16 Ασφάλεια



Εισαγωγή στην Επιστήμη των Υπολογιστών © Εκδόσεις Κλειδάριθμος

16.1

Στόχοι

Μετά την ολοκλήρωση αυτού του κεφαλαίου, ο σπουδαστής θα είναι σε θέση:

- Να ορίζει τους τρεις στόχους ασφάλειας — την εμπιστευτικότητα, την ακεραιότητα, και τη διαθεσιμότητα — καθώς και τους τύπους επιθέσεων κατά αυτών των στόχων.
- Να ορίζει τις πέντε υπηρεσίες ασφάλειας — την εμπιστευτικότητα των δεδομένων, την ακεραιότητα των δεδομένων, την πιστοποίηση αυθεντικότητας, τη μη απάρνηση, και τον έλεγχο πρόσβασης — που αποτρέπουν τις επιθέσεις κατά της ασφάλειας.
- Να περιγράφει δύο τεχνικές για την παροχή υπηρεσιών ασφάλειας: την κρυπτογραφία και τη στεγανογραφία.
- Να κατανοεί τις διαφορές μεταξύ της κρυπτογραφίας συμμετρικού κλειδιού και της κρυπτογραφίας ασύμμετρου κλειδιού και να περιγράφει το πώς εξασφαλίζεται η εμπιστευτικότητα με τη χρήση κρυπτογραφικών αλγορίθμων συμμετρικού κλειδιού ή ασύμμετρου κλειδιού.
- Να περιγράφει τον τρόπο με τον οποίο διασφαλίζεται η ακεραιότητα με τη χρήση κρυπτογραφικών συναρτήσεων κατακερματισμού.
- Να κατανοεί την ιδέα των ψηφιακών υπογραφών και το πώς μπορούν να εξασφαλίζουν την ακεραιότητα και την πιστοποίηση αυθεντικότητας μηνυμάτων, και τη μη απάρνηση.
- Να περιγράφει συνοπτικά την πιστοποίηση αυθεντικότητας οντότητας και τις κατηγορίες πειστηρίων: κάτι που είναι γνωστό, κάτι που κατέχεται, και κάτι που ενυπάρχει.
- Να περιγράφει τις τέσσερις τεχνικές που χρησιμοποιούνται για την πιστοποίηση αυθεντικότητας οντότητας: την τεχνική που βασίζεται σε κωδικούς πρόσβασης, την τεχνική πρόκλησης-απόκρισης, την τεχνική μηδενικής γνώσης, και τη βιομετρία.
- Να περιγράφει τη διαχείριση κλειδιών.

16.2

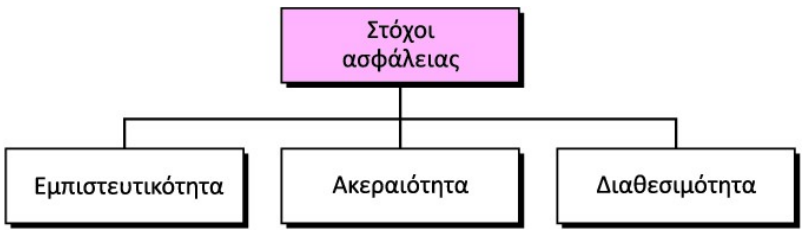
16-1 ΕΙΣΑΓΩΓΗ

Σε αυτή την ενότητα θα περιγράψουμε τη γενική ιδέα πίσω από την ασφάλεια των πληροφοριών.

16.3

Στόχοι ασφάλειας

Πρώτα θα εξετάσουμε τους τρεις στόχους ασφάλειας: την ***εμπιστευτικότητα***, την ***ακεραιότητα***, και τη **διαθεσιμότητα** (Εικόνα 16.1).



Εικόνα 16.1 **Κατηγοριοποίηση στόχων ασφάλειας**

16.4

Εμπιστευτικότητα

Η εμπιστευτικότητα (confidentiality), αφορά τη διατήρηση του απορρήτου των πληροφοριών από μη εξουσιοδοτημένη πρόσβαση, και είναι ίσως το δημοφιλέστερο ζήτημα στην ασφάλεια των πληροφοριών: οι εμπιστευτικές πληροφορίες πρέπει να προστατεύονται. Μια εταιρεία θα πρέπει να προφυλάσσεται από κακόβουλες ενέργειες που θέτουν σε κίνδυνο την εμπιστευτικότητα των πληροφοριών της.

Ακεραιότητα

Οι πληροφορίες πρέπει να αλλάζουν συνεχώς. Όταν ο πελάτης μιας τράπεζας καταθέτει ή παίρνει χρήματα, το υπόλοιπο του λογαριασμού του πρέπει να αλλάζει ανάλογα. Η ακεραιότητα (integrity) προϋποθέτει ότι οι αλλαγές πρέπει να γίνονται μόνο από εξουσιοδοτημένους χρήστες και μέσω εξουσιοδοτημένων μηχανισμών.

16.5

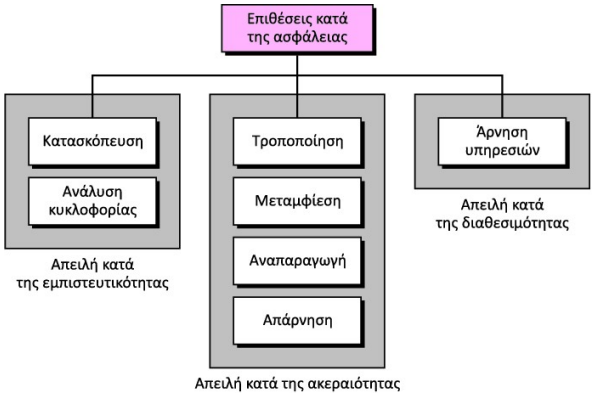
Διαθεσιμότητα

Το τρίτο συστατικό στοιχείο στην ασφάλεια των πληροφοριών είναι η διαθεσιμότητα (availability). Οι πληροφορίες που παράγονται και αποθηκεύονται από μια εταιρεία πρέπει να είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες και εφαρμογές. Αν οι πληροφορίες δεν είναι διαθέσιμες, είναι άχρηστες. Οι πληροφορίες χρειάζεται να αλλάζουν συνεχώς, πράγμα που σημαίνει ότι πρέπει να είναι προσπελάσιμες από αυτούς που έχουν εξουσιοδότηση να τις προσπελάζουν. Σε μια εταιρεία, η μη διαθεσιμότητα των πληροφοριών είναι εξίσου επιζήμια με την έλλειψη εμπιστευτικότητας ή ακεραιότητας. Φανταστείτε απλώς τι θα συμβεί σε μια τράπεζα αν οι πελάτες της δεν έχουν τη δυνατότητα να προσπελάζουν τον λογαριασμό τους για να εκτελούν συναλλαγές.

16.6

Επιθέσεις

Οι τρεις στόχοι της ασφάλειας — η εμπιστευτικότητα, η ακεραιότητα, και η διαθεσιμότητα — μπορεί να υπονομευθούν από επιθέσεις κατά της ασφάλειας. Στην Εικόνα 16.2 παρουσιάζεται μια συσχέτιση των κατηγοριών επιθέσεων με τους στόχους ασφάλειας.



Εικόνα 16.2 **Κατηγορίες επιθέσεων σε σχέση με τους στόχους ασφάλειας**

16.7

Επιθέσεις που απειλούν την εμπιστευτικότητα

Γενικά υπάρχουν δύο τύποι επιθέσεων που απειλούν την εμπιστευτικότητα των πληροφοριών: η κατασκόπευση, και η ανάλυση κυκλοφορίας. Η κατασκόπευση (snooping) αναφέρεται στη μη εξουσιοδοτημένη πρόσβαση ή την υποκλοπή δεδομένων. Η ανάλυση κυκλοφορίας αναφέρεται σε άλλα είδη πληροφοριών που συλλέγονται από τους εισβολείς με παρακολούθηση της κυκλοφορίας.

Επιθέσεις που απειλούν την ακεραιότητα

Η ακεραιότητα των δεδομένων μπορεί να υπονομευθεί με διάφορα είδη επιθέσεων: τροποποίηση, μεταμφίεση, αναπαραγωγή, και απάρνηση.

16.8

Επιθέσεις που απειλούν τη διαθεσιμότητα

Οι επιθέσεις άρνησης υπηρεσιών (denial of service, DoS) μπορεί να επιβραδύνουν ή να διακόψουν τελείως την παροχή υπηρεσιών από ένα σύστημα. Αυτό επιτυγχάνεται με την εφαρμογή διάφορων στρατηγικών από τους επιτιθέμενους. Για παράδειγμα, μπορεί να απασχολούν ένα σύστημα σε τέτοιο βαθμό ώστε τελικά να καταρρεύσει, ή να υποκλέψουν μηνύματα που στέλνονται προς μία κατεύθυνση και να εξαπατήσουν το σύστημα αποστολής ότι κάποιο από τα μέρη που εμπλέκονται στην επικοινωνία έχει χάσει το μήνυμα και πρέπει να το ξαναστείλει.

16.9

Υπηρεσίες ασφάλειας

Έχουν οριστεί διάφορα πρότυπα υπηρεσιών ασφάλειας για την επίτευξη των στόχων ασφάλειας και την αποτροπή επιθέσεων κατά της ασφάλειας. Στην Εικόνα 16.3 παρουσιάζεται η κατηγοριοποίηση πέντε συνηθισμένων υπηρεσιών.

Εικόνα 16.3 Υπηρεσίες ασφάλειας

16.10

Τεχνικές

Η πραγματική υλοποίηση των στόχων ασφάλειας απαιτεί τη χρήση μαθηματικών. Οι επικρατέστερες τεχνικές σήμερα είναι δύο: η μία είναι πολύ γενική και ονομάζεται *κρυπτογραφία* (cryptography), και η άλλη είναι πιο συγκεκριμένη και ονομάζεται *στεγανογραφία* (steganography).

Κρυπτογραφία

Ορισμένες υπηρεσίες ασφάλειας μπορούν να υλοποιηθούν με χρήση κρυπτογραφίας. Η λέξη *κρυπτογραφία* προέρχεται από τις λέξεις "κρυπτός" και "γράφω".

Στεγανογραφία

Η λέξη *στεγανογραφία* προέρχεται από τις λέξεις "στεγανός" και "γράφω" και σημαίνει "συγκαλυμμένη γραφή", σε αντίθεση με τη λέξη "κρυπτογραφία" που σημαίνει "κρυφή γραφή".

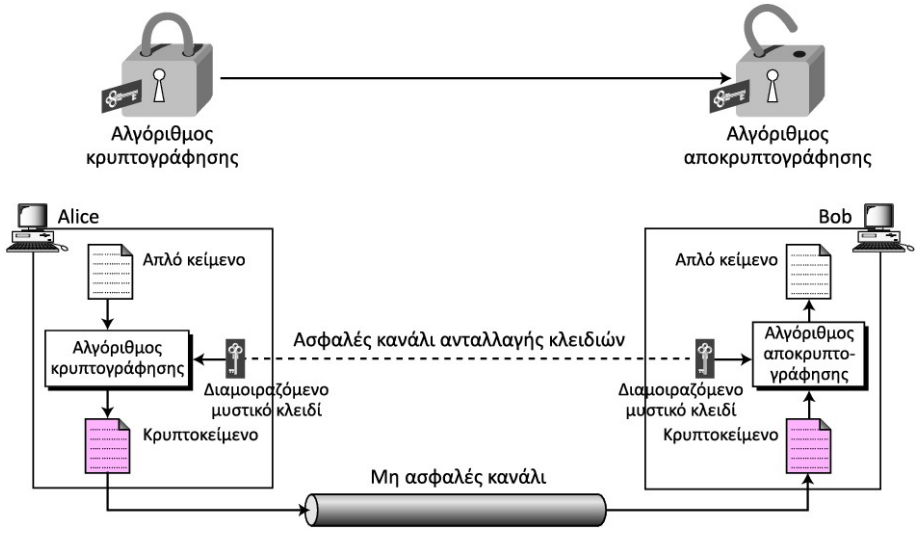
16.11

16-2 ΚΡΥΠΤΟΓΡΑΦΙΑ ΣΥΜΜΕΤΡΙΚΟΥ ΚΛΕΙΔΙΟΥ

Στην Εικόνα 16.4 παρουσιάζεται η γενική ιδέα της κρυπτογραφίας συμμετρικού κλειδιού. Η Alice μπορεί να στείλει ένα μήνυμα στον Bob μέσω ενός μη ασφαλούς καναλιού με την πεποίθηση ότι κάποιος άλλος χρήστης, όπως η Eve, δεν θα μπορέσει να κατανοήσει το περιεχόμενο του μηνύματος "κρυφακούγοντας" στο κανάλι.

Το αρχικό μήνυμα από την Alice προς τον Bob αναφέρεται ως απλό κείμενο (plaintext), ενώ το μήνυμα που στέλνεται μέσω του καναλιού αναφέρεται ως κρυπτοκείμενο (ciphertext). Η Alice χρησιμοποιεί έναν αλγόριθμο κρυπτογράφησης και ένα κοινό μυστικό κλειδί, ενώ ο Bob χρησιμοποιεί έναν αλγόριθμο αποκρυπτογράφησης και το ίδιο μυστικό κλειδί.

16.12



Εικόνα 16.4 **Η γενική ιδέα της κρυπτογραφίας συμμετρικού κλειδιού**

16.13

Κλασικοί κρυπταλγόριθμοι

Οι κλασικοί κρυπταλγόριθμοι χρησιμοποιούσαν δύο τεχνικές για την απόκρυψη πληροφοριών από εισβολείς: την *αντικατάσταση* και την *αναδιάταξη*.

Κρυπταλγόριθμοι αντικατάστασης

Ένας κρυπταλγόριθμος αντικατάστασης (substitution cipher) αντικαθιστά ένα σύμβολο με κάποιο άλλο. Αν τα σύμβολα στο απλό κείμενο είναι αλφαβητικοί χαρακτήρες, τότε οι χαρακτήρες αντικαθίστανται από άλλους.

Ένας κρυπταλγόριθμος αντικατάστασης αντικαθιστά ένα σύμβολο με κάποιο άλλο.

Ο απλούστερος κρυπταλγόριθμος αντικατάστασης είναι ο κρυπταλγόριθμος μετατόπισης (shift cipher).

16.14

Παράδειγμα 16.1

Χρησιμοποιήστε τον (προσθετικό) κρυπταλγόριθμο μετατόπισης με κλειδί = 15 για να κρυπτογραφήσετε το μήνυμα "hello".

Λύση

Εφαρμόζουμε τον αλγόριθμο κρυπτογράφησης στο απλό κείμενο, από χαρακτήρα σε χαρακτήρα:

Απλό κείμενο: h	→	Μετατόπιση 15 χαρακτήρες προς τα κάτω	→	Κρυπτοκείμενο: w
Απλό κείμενο: e	→	Μετατόπιση 15 χαρακτήρες προς τα κάτω	→	Κρυπτοκείμενο: t
Απλό κείμενο: l	→	Μετατόπιση 15 χαρακτήρες προς τα κάτω	→	Κρυπτοκείμενο: a
Απλό κείμενο: l	→	Μετατόπιση 15 χαρακτήρες προς τα κάτω	→	Κρυπτοκείμενο: a
Απλό κείμενο: o	→	Μετατόπιση 15 χαρακτήρες προς τα κάτω	→	Κρυπτοκείμενο: d

Επομένως το κρυπτοκείμενο που προκύπτει είναι "wtaad".

16.15

Κρυπταλγόριθμοι αναδιάταξης

Ένας κρυπταλγόριθμος αναδιάταξης (transposition cipher) δεν αντικαθιστά σύμβολα με άλλα, παρά αλλάζει τη θέση των υπαρχόντων συμβόλων. Για παράδειγμα, ένα σύμβολο στην πρώτη θέση του απλού κειμένου μπορεί να τοποθετηθεί στη δέκατη θέση του κρυπτοκειμένου, ενώ ένα σύμβολο στην όγδοη θέση του απλού κειμένου μπορεί να τοποθετηθεί στην πρώτη θέση του κρυπτοκειμένου. Με άλλα λόγια, ένας κρυπταλγόριθμος αναδιάταξης αναδιατάσσει (μεταθέτει) τα σύμβολα.

Ένας κρυπταλγόριθμος αναδιάταξης αναδιατάσσει τα σύμβολα.

16.16

Παράδειγμα 16.2

Η Alice πρέπει να στείλει στον Bob το μήνυμα "**Enemy attacks tonight**" (Ο εχθρός θα επιτεθεί απόψε). Η Alice και ο Bob έχουν συμφωνήσει να χωρίσουν το κείμενο σε ομάδες των πέντε χαρακτήρων και μετά να μεταθέσουν τους χαρακτήρες σε κάθε ομάδα. Στη συνέχεια βλέπετε τον τρόπο ομαδοποίησης των χαρακτήρων μετά την προσθήκη ενός ψευδοχαρακτήρα (z) στο τέλος ώστε η τελευταία ομάδα να έχει το ίδιο μέγεθος με τις υπόλοιπες.

e n e m y a t t a c k s t o n i g h t z

Το κλειδί που χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση είναι ένα κλειδί μετάθεσης, με βάση το οποίο μετατίθενται οι χαρακτήρες. Για αυτό το μήνυμα, ας υποθέσουμε ότι η Alice και ο Bob χρησιμοποιούν το ακόλουθο κλειδί:

Κρυπτογράφηση ↓	3	1	4	5	2	↑ Αποκρυπτογράφηση
	1	2	3	4	5	

16.17

Παράδειγμα 16.2 Συνέχεια

Ο τρίτος χαρακτήρας σε κάθε τμήμα του απλού κειμένου γίνεται ο πρώτος χαρακτήρας στο αντίστοιχο τμήμα του κρυπτοκειμένου, ο πρώτος χαρακτήρας σε κάθε τμήμα του απλού κειμένου γίνεται ο δεύτερος χαρακτήρας στο τμήμα του κρυπτοκειμένου, και ούτω καθεξής. Η μετάθεση δίνει το εξής αποτέλεσμα:

e e m y n t a a c t t k o n s h i t z g

Έτσι η Alice στέλνει στον Bob το κρυπτοκείμενο "eemyntaacttkonshitzg". Ο Bob χωρίζει το κρυπτοκείμενο σε ομάδες των πέντε χαρακτήρων και, χρησιμοποιώντας το κλειδί με αντίστροφη σειρά, δημιουργεί το απλό κείμενο.

16.18

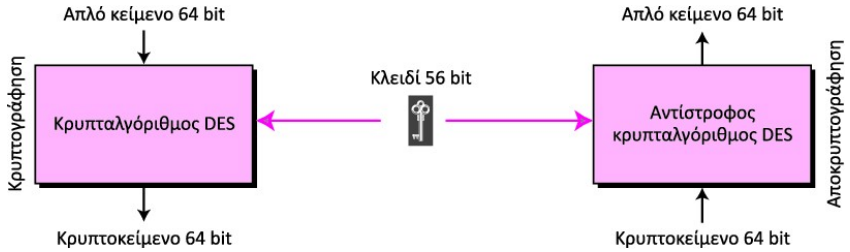
Σύγχρονοι κρυπταλγόριθμοι συμμετρικού κλειδιού

Από τη στιγμή που οι κλασικοί κρυπταλγόριθμοι δεν είναι πλέον ασφαλείς, τις τελευταίες δεκαετίες έχουν αναπτυχθεί σύγχρονοι κρυπταλγόριθμοι συμμετρικού κλειδιού. Σε έναν σύγχρονο κρυπταλγόριθμο συνήθως χρησιμοποιείται ένας συνδυασμός αντικατάστασης, αναδιάταξης, και μερικών άλλων σύνθετων μετασχηματισμών για τη δημιουργία ενός κρυπτοκειμένου από απλό κείμενο. Οι σύγχρονοι κρυπταλγόριθμοι βασίζονται σε bit (αντί σε χαρακτήρες). Το απλό κείμενο, το κρυπτοκείμενο, και το κλειδί είναι όλα συμβολοσειρές από bit. Σε αυτή την ενότητα θα εξετάσουμε εν συντομία δύο παραδείγματα σύγχρονων κρυπταλγορίθμων συμμετρικού κλειδιού: DES και AES. Θα περιγράψουμε αρκετά συνοπτικά αυτούς τους δύο κρυπταλγορίθμους, γι' αυτό οι αναγνώστες που θέλουν περισσότερες λεπτομέρειες θα πρέπει να συμβουλευθούν τις αναφορές στο τέλος του κεφαλαίου.

16.19

DES

Το πρότυπο DES (Data Encryption Standard, Πρότυπο Κρυπτογράφησης Δεδομένων) είναι ένας κρυπταλγόριθμος τμήματος συμμετρικού κλειδιού που δημοσιεύτηκε το 1977 από το Εθνικό Ίδρυμα Προτύπων και Τεχνολογίας των Η.Π.Α (National Institute of Standards and Technology, NIST). Ο DES παραμένει ο πιο διαδεδομένος κρυπταλγόριθμος τμήματος συμμετρικού κλειδιού από τότε που δημοσιεύτηκε (Εικόνα 16.5).



Εικόνα 16.5 **Κρυπτογράφηση και αποκρυπτογράφηση με τον DES**

16.20

AES

Ο AES (Advanced Encryption Standard, Προηγμένο Πρότυπο Κρυπτογράφησης) είναι ένας κρυπταλγόριθμος τμήματος συμμετρικού κλειδιού ο οποίος δημοσιεύτηκε το 2001 από το Εθνικό Ίδρυμα Προτύπων και Τεχνολογίας των Η.Π.Α (NIST) ως απάντηση στα μειονεκτήματα του DES (όπως το μικρό μέγεθος κλειδιού). Δείτε την Εικόνα 16.6.

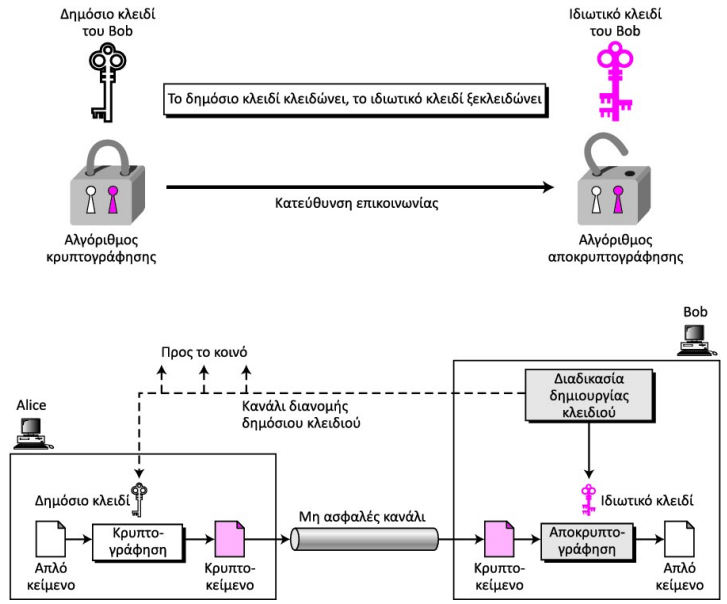
Εικόνα 16.6 **Η γενική σχεδίαση του κρυπταλγορίθμου κρυπτογράφησης AES**

16.21

16-3 ΚΡΥΠΤΟΓΡΑΦΙΑ ΑΣΥΜΜΕΤΡΟΥ ΚΛΕΙΔΙΟΥ

Στην Εικόνα 16.7 παρουσιάζεται η γενική ιδέα της κρυπτογραφίας ασύμμετρου κλειδιού όταν χρησιμοποιείται για τη διασφάλιση της εμπιστευτικότητας. Σε αντίθεση με την κρυπτογραφία συμμετρικού κλειδιού, στην κρυπτογραφία ασύμμετρου κλειδιού χρησιμοποιούνται ξεχωριστά κλειδιά, όπως βλέπετε στην εικόνα: ένα ιδιωτικό κλειδί και ένα δημόσιο κλειδί. Αν παρομοιάσουμε την κρυπτογράφηση και την αποκρυπτογράφηση με το κλείδωμα και το ξεκλείδωμα λουκέτων με κλειδιά, τότε το λουκέτο που κλειδώνεται με ένα δημόσιο κλειδί μπορεί να ξεκλειδωθεί μόνο με το αντίστοιχο ιδιωτικό κλειδί. Έτσι, δεν θα πρέπει να επιτρέπεται σε κάποιον τρίτο, π.χ στην Eve, να διαφημίζει το δημόσιο κλειδί της στην κοινότητα προσποιούμενη ότι πρόκειται για το δημόσιο κλειδί του Bob.

16.22



Εικόνα 16.7 **Η γενική ιδέα της κρυπτογραφίας ασύμμετρου κλειδιού**

16.23

Παράδειγμα 16.3

Ο Bob επιλέγει $p = 7$ και $q = 11$ και υπολογίζει $n = 7 \times 11 = 77$. Τώρα επιλέγει δύο εκθέτες, το 13 και το 37, χρησιμοποιώντας τη σύνθετη διαδικασία που αναφέραμε προηγουμένως. Το δημόσιο κλειδί είναι ($n = 77$ και $e = 13$) και το ιδιωτικό κλειδί είναι ($d = 37$). Τώρα ας υποθέσουμε ότι η Alice θέλει να στείλει στον Bob το απλό κείμενο 5. Η κρυπτογράφηση και η αποκρυπτογράφηση γίνονται ως εξής.

Κρυπτογράφηση στην πλευρά της Alice	Αποκρυπτογράφηση στην πλευρά του Bob
P: 5 $\rightarrow$ $C = 5^{13} = 26 \bmod 77$	C: 26 $\rightarrow$ $P = 26^{37} = 5 \bmod 77$

16.24

16-4 ΣΥΓΚΡΙΣΗ ΜΕΘΟΔΩΝ

Τόσο η κρυπτογραφία συμμετρικού κλειδιού όσο και η κρυπτογραφία ασύμμετρου κλειδιού θα εξακολουθήσουν να συνυπάρχουν. Πιστεύουμε ότι αλληλοσυμπληρώνονται, αφού τα πλεονεκτήματα της μίας αντισταθμίζουν τα μειονεκτήματα της άλλης.

16.25

Το πλήθος των μυστικών

Οι νοητικές διαφορές μεταξύ των δύο συστημάτων βασίζονται στον τρόπο με τον οποίο αυτά τα συστήματα κρατούν ένα μυστικό. Στην κρυπτογραφία συμμετρικού κλειδιού, ο μυστικός όρος (token) πρέπει να διαμοιράζεται μεταξύ των δύο μελών. Στην κρυπτογραφία ασύμμετρου κλειδιού ο μυστικός όρος δεν διαμοιράζεται, αλλά κάθε μέλος δημιουργεί τον δικό του.

Η κρυπτογραφία συμμετρικού κλειδιού βασίζεται στη διαμοιραζόμενη μυστικότητα ενώ η κρυπτογραφία ασύμμετρου κλειδιού βασίζεται στην "προσωπική" μυστικότητα.

16.26

Η ανάγκη και για τα δύο συστήματα

Εκτός από την εμπιστευτικότητα υπάρχουν και άλλα θέματα ασφάλειας που χρειάζονται την κρυπτογραφία ασύμμετρου κλειδιού. Σε αυτά περιλαμβάνεται η πιστοποίηση αυθεντικότητας και οι ψηφιακές υπογραφές (περιγράφονται αργότερα). Ενώ η κρυπτογραφία συμμετρικού κλειδιού βασίζεται στην αντικατάσταση και τη μετάθεση συμβόλων, η κρυπτογραφία ασύμμετρου κλειδιού βασίζεται στην εφαρμογή μαθηματικών συναρτήσεων σε αριθμούς.

Στην κρυπτογραφία συμμετρικού κλειδιού πραγματοποιείται μετάθεση ή αντικατάσταση συμβόλων, ενώ στην κρυπτογραφία ασύμμετρου κλειδιού πραγματοποιείται επεξεργασία αριθμών.

16.27

16-5 ΑΛΛΕΣ ΥΠΗΡΕΣΙΕΣ ΑΣΦΑΛΕΙΑΣ

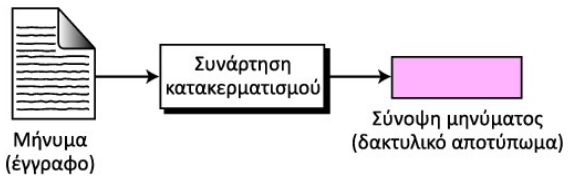
Τα κρυπτογραφικά συστήματα που έχουμε μελετήσει μέχρι τώρα παρέχουν μυστικότητα, ή εμπιστευτικότητα, όμως καμία από τις άλλες υπηρεσίες που αναφέραμε στην αρχή του κεφαλαίου. Σε αυτή την ενότητα θα δείτε πώς εξασφαλίζεται η παροχή άλλων υπηρεσιών.

16.28

Ακεραιότητα μηνύματος

Υπάρχουν περιπτώσεις όπου ίσως να μην χρειάζεται η μυστικότητα αλλά να απαιτείται η ακεραιότητα. Ένας τρόπος διατήρησης της ακεραιότητας ενός εγγράφου ήταν ανέκαθεν η χρήση ενός ***δακτυλικού αποτυπώματος***. Το ηλεκτρονικό ισοδύναμο του ζεύγους εγγράφου και δακτυλικού αποτυπώματος είναι το ζεύγος ***μηνύματος*** και ***σύνοψης***. Για να διατηρείται η ακεραιότητα ενός μηνύματος, το μήνυμα περνά μέσω ενός αλγορίθμου που ονομάζεται ***κρυπτογραφική συνάρτηση κατακερματισμού*** (cryptographic hash function). Η συνάρτηση αυτή δημιουργεί μια συμπιεσμένη εικόνα του μηνύματος η οποία μπορεί να χρησιμοποιηθεί ως δακτυλικό αποτύπωμα. Στην Εικόνα 16.8 παρουσιάζεται το μήνυμα, η κρυπτογραφική συνάρτηση κατακερματισμού, και η σύνοψη του μηνύματος.

16.29



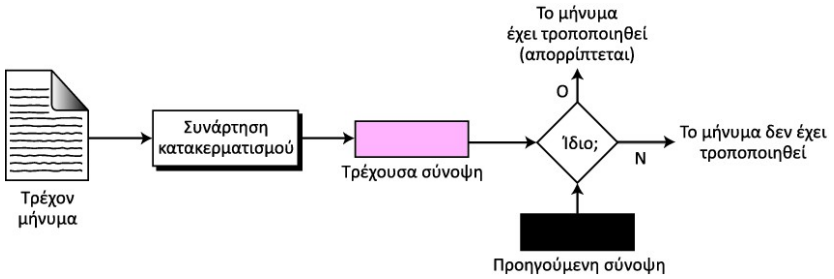
Εικόνα 16.8 **Μήνυμα και σύνοψη**

Η σύνοψη μηνύματος πρέπει να προστατεύεται από αλλαγές.

16.30

Έλεγχος ακεραιότητας

Για να ελέγξουμε την ακεραιότητα ενός μηνύματος ή εγγράφου, μπορούμε να εκτελέσουμε πάλι την κρυπτογραφική συνάρτηση κατακερματισμού και να συγκρίνουμε τη νέα σύνοψη μηνύματος με την προηγούμενη. Αν και οι δύο είναι ίδιες, τότε είμαστε σίγουροι ότι το αρχικό μήνυμα δεν έχει τροποποιηθεί. Η ιδέα παρουσιάζεται στην Εικόνα 16.9.



Εικόνα 16.9 Έλεγχος ακεραιότητας

16.31

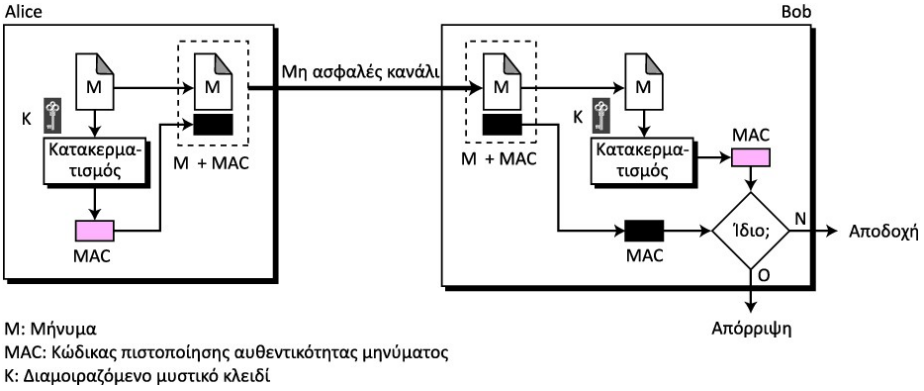
Πιστοποίηση αυθεντικότητας μηνύματος

Η σύνοψη εγγυάται την ακεραιότητα ενός μηνύματος, δηλαδή διασφαλίζει ότι το μήνυμα δεν έχει τροποποιηθεί. Η σύνοψη μηνύματος, όμως, δεν πιστοποιεί την ταυτότητα του αποστολέα του μηνύματος. Όταν η Alice στέλνει ένα μήνυμα στον Bob, αυτός πρέπει να επιβεβαιώνει ότι το μήνυμα προέρχεται πράγματι από την Alice. Για να επιτρέπει την πιστοποίηση της αυθεντικότητας των μηνυμάτων, η Alice πρέπει να παρέχει αποδείξεις ότι τα μηνύματα προέρχονται από αυτήν και όχι από κάποιον απατεώνα. Η σύνοψη μηνύματος από μόνη της δεν παρέχει αυτήν την απόδειξη. Η σύνοψη που δημιουργείται από μια κρυπτογραφική συνάρτηση κατακερματισμού συνήθως ονομάζεται **κωδικός ανίχνευσης τροποποίησης** (modification detection code, MDC). Αυτό που χρειαζόμαστε για την πιστοποίηση αυθεντικότητας του μηνύματος (πιστοποίηση αυθεντικότητας προέλευσης δεδομένων) είναι ένας **κωδικός πιστοποίησης αυθεντικότητας μηνύματος** (message authentication code, MAC).

16.32

Κωδικός πιστοποίησης αυθεντικότητας μηνύματος

Για να βεβαιωθούμε για την ακεραιότητα του μηνύματος και να πιστοποιήσουμε την αυθεντικότητα της προέλευσής του πρέπει να αλλάξουμε τον κωδικό ανίχνευσης τροποποίησης (MDC) σε κωδικό πιστοποίησης αυθεντικότητας (MAC). Η διαφορά τους είναι ότι ο δεύτερος κωδικός περιλαμβάνει ένα μυστικό στοιχείο μεταξύ της Alice και του Bob.



M: Μήνυμα
MAC: Κώδικας πιστοποίησης αυθεντικότητας μηνύματος
K: Διαμοιραζόμενο μυστικό κλειδί

Εικόνα 16.10 **Κωδικός πιστοποίησης αυθεντικότητας μηνύματος**

16.33

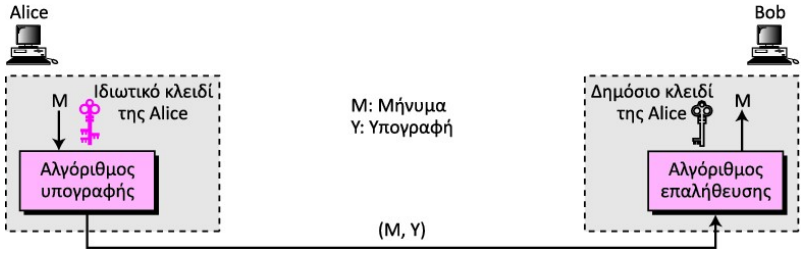
Ψηφιακές υπογραφές

Η έννοια της υπογραφής είναι γνωστή σε όλους. Οι άνθρωποι υπογράφουν έγγραφα για να δείχνουν ότι προέρχονται ή έχουν εγκριθεί από αυτούς. Η υπογραφή αποτελεί απόδειξη προς τον παραλήπτη ότι το έγγραφο προέρχεται από το σωστό άτομο. Με άλλα λόγια, η υπογραφή σε ένα έγγραφο, μετά την επαλήθευσή της, αποτελεί ένδειξη της αυθεντικότητας του εγγράφου. Όταν η Alice στέλνει ένα μήνυμα στον Bob, αυτός πρέπει να ελέγχει την αυθεντικότητα του αποστολέα: δηλαδή πρέπει να διασφαλίζει ότι το μήνυμα προέρχεται από την Alice και όχι από την Eve. Για τον σκοπό αυτό, ο Bob μπορεί να ζητήσει από την Alice να υπογράφει ηλεκτρονικά τα μηνύματα. Με άλλα λόγια, η ηλεκτρονική υπογραφή μπορεί να αποδεικνύει την αυθεντικότητα της Alice ως αποστολέα του μηνύματος. Αυτού του είδους η υπογραφή αναφέρεται ως **ψηφιακή υπογραφή** (digital signature).

16.34

Διαδικασία ψηφιακής υπογραφής

Στην Εικόνα 16.11 παρουσιάζεται η διαδικασία ψηφιακής υπογραφής. Ο αποστολέας χρησιμοποιεί έναν **αλγόριθμο υπογραφής** για να υπογράψει το μήνυμα. Έπειτα το μήνυμα και η υπογραφή στέλνονται στον παραλήπτη. Αυτός λαμβάνει το μήνυμα και την υπογραφή και εφαρμόζει τον **αλγόριθμο επαλήθευσης** στον συνδυασμό μηνύματος και υπογραφής. Αν το αποτέλεσμα επαληθευτεί το μήνυμα γίνεται αποδεκτό, διαφορετικά απορρίπτεται.



Εικόνα 16.11 **Η διαδικασία ψηφιακής υπογραφής**

16.35

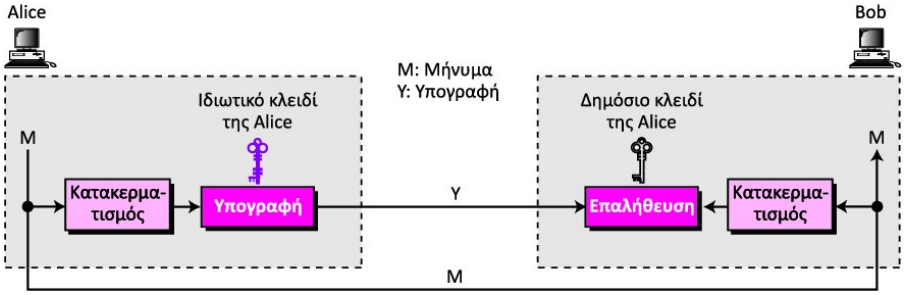
Η ψηφιακή υπογραφή απαιτεί ένα σύστημα δημόσιου κλειδιού. Ο υπογράφων υπογράφει έγγραφα με το ιδιωτικό κλειδί του, και αυτός που επαληθεύει (ο ελεγκτής) τα επαληθεύει με το δημόσιο κλειδί του υπογράφοντος.

Σε ένα κρυπτοσύστημα χρησιμοποιείται το ιδιωτικό και το δημόσιο κλειδί του παραλήπτη, ενώ σε μια ψηφιακή υπογραφή χρησιμοποιείται το ιδιωτικό και το δημόσιο κλειδί του αποστολέα.

16.36

Υπογραφή της σύνοψης

Τα κρυπτοσυστήματα ασύμμετρου κλειδιού δεν είναι καθόλου αποδοτικά όταν πρέπει να χειριστούν μεγάλα μηνύματα. Παρόλο που σε ένα σύστημα ψηφιακών υπογραφών τα μηνύματα συνήθως είναι μεγάλα, πρέπει να χρησιμοποιούμε τεχνολογία ασύμμετρου κλειδιού. Η λύση είναι η υπογραφή μιας σύνοψης του μηνύματος, η οποία είναι πολύ μικρότερη από το ίδιο το μήνυμα.

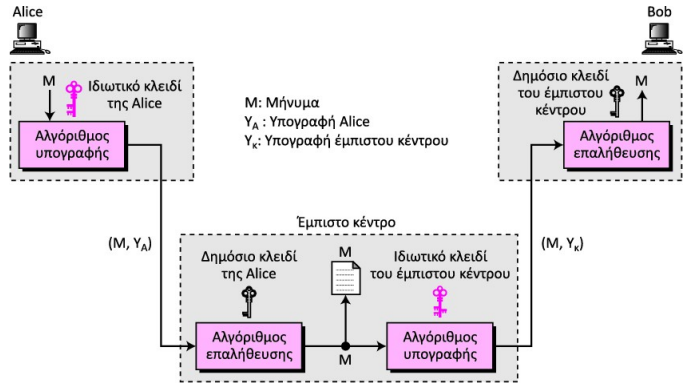


Εικόνα 16.12 Υπογραφή της σύνοψης

16.37

Υπηρεσίες

Μια ψηφιακή υπογραφή παρέχει τρεις από τις πέντε υπηρεσίες ασφάλειας που αναφέραμε στην αρχή: **πιστοποίηση αυθεντικότητας μηνύματος**, **ακεραιότητα μηνύματος**, και **μη απάρνηση**. Έχουμε ήδη ασχοληθεί με τις δύο πρώτες, ενώ η τρίτη μπορεί να περιγραφεί με την επόμενη εικόνα.



Εικόνα 16.13 Μη απάρνηση με χρήση ψηφιακών υπογραφών

16.38

Ψηφιακή Υπογραφή

- Η Alice θέλει να στείλει ένα υπογεγραμμένο μήνυμα στον Bob. Αρχικά θα περάσει το μήνυμα από τον αλγόριθμο κατατεμαχισμού και θα παράγει την σύνοψη του μηνύματος
- Η Alice θα κρυπτογραφήσει την σύνοψη με το ιδιωτικό κλειδί της και θα προσθέσει την κρυπτογραφημένη εκδοχή της στο τέλος του εγγράφου

16.39

Έλεγχος ψηφιακής υπογραφής

- Ο Bob θα ξεχωρίσει την κρυπτογραφημένη σύνοψη από το τέλος του εγγράφου και θα το αποκρυπτογραφήσει χρησιμοποιώντας το δημόσιο κλειδί της. Εφόσον η αποκρυπτογράφηση γίνει με επιτυχία γνωρίζει ότι η σύνοψη δεν έχει αλλοιωθεί και ότι ανήκει στην Alice.
- Κατόπιν θα πάρει το μήνυμα και θα το περάσει από τον αλγόριθμο κατατεμαχισμού και θα συγκρίνει την σύνοψη που υπολόγισε ο ίδιος με την σύνοψη που αποκρυπτογράφησε από την ψηφιακή υπογραφή. Αν οι συνόψεις είναι ίδιες, ο Bob γνωρίζει ότι το αρχικό μήνυμα δεν έχει αλλοιωθεί.

16.40

Πιστοποίηση αυθεντικότητας

- Η Alice μπορεί επίσης να προσθέσει και ένα πιστοποιητικό που πιστοποιεί ότι το δημόσιο κλειδί που θα χρησιμοποιηθεί αργότερα για την αποκρυπτογράφηση της υπογραφής της ανήκει πράγματι στην Alice.
- Το πιστοποιητικό θα πρέπει να έχει εκδοθεί από ένα έμπιστο πάροχο υπηρεσιών πιστοποίησης.

16.41

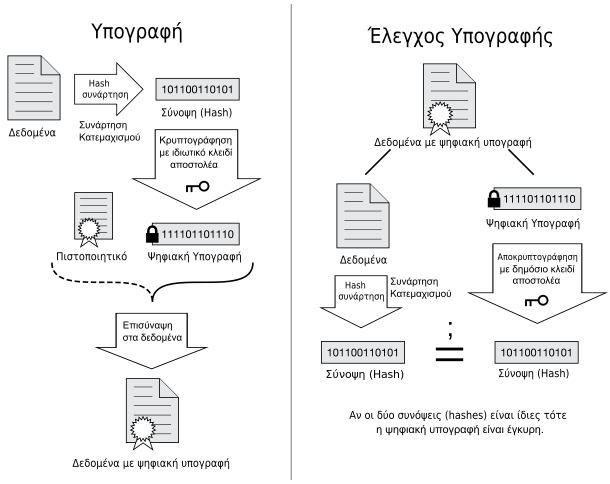
Πιστοποίηση αυθεντικότητας

- Εφόσον η αποκρυπτογράφηση γίνει με επιτυχία, ο Bob γνωρίζει ότι η σύνοψη δεν έχει αλλοιωθεί και ότι ανήκει στην Alice
- Αν θέλει να βεβαιωθεί ότι το δημόσιο κλειδί που χρησιμοποίησε ανήκει πραγματικά στην Alice θα διαβάσει το ψηφιακό πιστοποιητικό της Alice.

16.42

Ψηφιακή Υπογραφή

https://el.wikipedia.org/wiki:Digital_Signature_diagram_el.svg



16.43

Πιστοποίηση αυθεντικότητας οντότητας

Η πιστοποίηση αυθεντικότητας οντότητας είναι μια τεχνική που επιτρέπει σε ένα μέρος να αποδεικνύει την ταυτότητα ενός άλλου μέρους. Ως οντότητα μπορεί οριστεί ένα άτομο, μια διεργασία, ένα σύστημα-πελάτης, ή ένας διακομιστής. Η οντότητα της οποίας πρέπει να αποδειχθεί η ταυτότητα ονομάζεται **ενάγων**, ενώ το μέρος που θέλει να αποδείξει την ταυτότητα του ενάγοντος ονομάζεται **ελεγκτής**.

16.39

Πιστοποίηση αυθεντικότητας προέλευσης δεδομένων και οντότητας

Ανάμεσα στην πιστοποίηση αυθεντικότητας μηνύματος (πιστοποίηση αυθεντικότητας προέλευσης δεδομένων) που περιγράφηκε προηγουμένως, και την πιστοποίηση αυθεντικότητας οντότητας η οποία περιγράφεται σε αυτή την ενότητα υπάρχουν δύο διαφορές.

- Η πιστοποίηση αυθεντικότητας μηνύματος (ή πιστοποίηση αυθεντικότητας προέλευσης δεδομένων) μπορεί να μην γίνεται σε πραγματικό χρόνο, σε αντίθεση με την πιστοποίηση αυθεντικότητας οντότητας που γίνεται πάντα σε πραγματικό χρόνο.
- Με την πιστοποίηση αυθεντικότητας μηνύματος απλώς πιστοποιείται ένα μήνυμα: η διαδικασία πρέπει να επαναλαμβάνεται για κάθε νέο μήνυμα. Με την πιστοποίηση αυθεντικότητας οντότητας ο ενάγων πιστοποιείται για ολόκληρη τη διάρκεια μιας συνεδρίας.

16.40

Κατηγορίες επαλήθευσης

Στην πιστοποίηση αυθεντικότητας οντότητας, ο ενάγων πρέπει να πιστοποιεί την ταυτότητά του στον ελεγκτή. Αυτό μπορεί να γίνει με έναν από τους εξής τρεις τύπους πειστηρίων:

- **Κάτι που είναι γνωστό**. Αυτό είναι ένα μυστικό γνωστό μόνο στον ενάγοντα το οποίο μπορεί να εξακριβωθεί από τον ελεγκτή. Ορισμένα παραδείγματα αποτελούν οι κωδικοί πρόσβασης, οι αριθμοί PIN, μυστικά κλειδιά, και ιδιωτικά κλειδιά.
- **Κάτι που κατέχεται**. Αυτό είναι κάτι που μπορεί να αποδείξει την ταυτότητα του ενάγοντος. Παραδείγματα αποτελούν τα διαβατήρια, οι άδειες οδήγησης, οι κάρτες ταυτοτήτων, και οι πιστωτικές κάρτες.
- **Κάτι που ενυπάρχει**. Πρόκειται για ενυπάρχοντα χαρακτηριστικά του ενάγοντος. Ορισμένα παραδείγματα είναι οι συμβατικές υπογραφές, τα δακτυλικά αποτυπώματα, η φωνή, χαρακτηριστικά του προσώπου, η διάταξη του αμφιβληστροειδούς χιτώνα του ματιού, και ο τρόπος γραφής.

16.41

16-6 ΔΙΑΧΕΙΡΙΣΗ ΚΛΕΙΔΙΩΝ

Για τη χρήση κρυπτογραφίας συμμετρικού κλειδιού πρέπει να δημιουργηθεί ένα μυστικό κλειδί μεταξύ των δύο μελών. Για τη χρήση ασύμμετρης κρυπτογραφίας, κάθε οντότητα πρέπει να δημιουργήσει ένα ζεύγος κλειδιών και να διανείμει με ασφάλεια το δημόσιο κλειδί στην ομάδα. Η διαχείριση κλειδιών ορίζει ορισμένες διαδικασίες για την ασφαλή δημιουργία και διανομή κλειδιών.

16.42

Διανομή συμμετρικών κλειδιών

Για την επίτευξη επικοινωνίας με συμμετρικά κλειδιά σε μια κοινότητα με n οντότητες, απαιτούνται $n\ (n - 1)/2$ κλειδιά. Το πλήθος των κλειδιών δεν είναι το μοναδικό πρόβλημα, αφού υπάρχει και το θέμα της διανομής των κλειδιών. Αν η Alice και ο Bob θέλουν να επικοινωνούν, πρέπει να βρουν έναν τρόπο να ανταλλάσσουν ένα μυστικό κλειδί. Αν η Alice θέλει να επικοινωνεί με ένα εκατομμύριο άτομα, πώς μπορεί να ανταλλάσσει με αυτά ένα εκατομμύριο κλειδιά; Η χρήση του Internet σίγουρα δεν είναι μια ασφαλής μέθοδος. Είναι προφανές ότι χρειαζόμαστε έναν αποδοτικό τρόπο να διατηρούμε και να διανέμουμε μυστικά κλειδιά.

16.43

Κέντρο διανομής κλειδιών: ΚΔΚ

Μια πρακτική λύση είναι η χρήση ενός έμπιστου τρίτου μέλους, το οποίο αναφέρεται ως **κέντρο διανομής κλειδιών (ΚΔΚ)**. Κάθε άτομο εδραιώνει ένα διαμοιραζόμενο μυστικό κλειδί με το ΚΔΚ. Μεταξύ του ΚΔΚ και κάθε μέλους εδραιώνεται ένα μυστικό κλειδί. Η διαδικασία έχει ως εξής:

1. Η Alice στείλει μια αίτηση στο ΚΔΚ με την οποία δηλώνει ότι χρειάζεται ένα (προσωρινό) μυστικό κλειδί συνεδρίας μεταξύ της ίδιας και του Bob.
2. Το ΚΔΚ ενημερώνει τον Bob για την αίτηση της Alice.
3. Αν ο Bob συμφωνήσει, δημιουργείται μια συνεδρία μεταξύ τους.

Ένα συμμετρικό κλειδί συνεδρίας μεταξύ δύο μελών χρησιμοποιείται μόνο μία φορά.

16.44

Διανομή δημόσιων κλειδιών

Στην κρυπτογραφία ασύμμετρου κλειδιού, οι χρήστες δεν χρειάζονται κάποιο διαμοιραζόμενο συμμετρικό κλειδί. Αν η Alice θέλει να στείλει ένα μήνυμα στον Bob, πρέπει μόνο να γνωρίζει το δημόσιο κλειδί του, το οποίο είναι γνωστό στο κοινό και διαθέσιμο σε όλους. Παρόμοια, αν ο Bob χρειάζεται να στείλει ένα μήνυμα στην Alice, πρέπει μόνο να γνωρίζει το δημόσιο κλειδί της, το οποίο επίσης είναι γνωστό σε όλους. Στην κρυπτογραφία δημόσιου κλειδιού, ο καθένας κρύβει το ιδιωτικό κλειδί του και κοινοποιεί το δημόσιο κλειδί του.

Στην κρυπτογραφία δημόσιου κλειδιού, όλοι έχουν πρόσβαση στο δημόσιο κλειδί των υπολοίπων αφού τα δημόσια κλειδιά είναι διαθέσιμα στο κοινό.

16.45

Δημοσιοποίηση στο κοινό

Η απλούστερη προσέγγιση είναι η ανακοίνωση των δημόσιων κλειδιών στο κοινό. Έτσι, ο Bob μπορεί να τοποθετήσει το δημόσιο κλειδί του στην ιστοσελίδα του ή να το δημοσιεύσει σε διάφορα έντυπα. Όταν η Alice θελήσει να στείλει ένα μήνυμα στον Bob, μπορεί να βρει το δημόσιο κλειδί του από την ιστοσελίδα του ή από κάποιο έντυπο, ή ακόμα και να του το ζητήσει με κάποιο μήνυμα. Με αυτή την προσέγγιση, όμως, δεν παρέχεται ασφάλεια, αφού υπάρχει η δυνατότητα πλαστογράφησης.

16.46

Έμπιστο κέντρο

Μια πιο ασφαλής προσέγγιση είναι η μεσολάβηση ενός έμπιστου κέντρου το οποίο διατηρεί έναν κατάλογο με δημόσια κλειδιά. Ο κατάλογος αυτός, όπως και ένας τηλεφωνικός, ενημερώνεται δυναμικά. Κάθε χρήστης μπορεί να επιλέξει ένα ιδιωτικό και ένα δημόσιο κλειδί, να κρατήσει μυστικό το ιδιωτικό κλειδί, και να στείλει το δημόσιο κλειδί για να συμπεριληφθεί στον κατάλογο. Ένα τέτοιο κέντρο απαιτεί από κάθε χρήστη να εγγράφεται σε αυτό και να αποδεικνύει την ταυτότητά του. Ο κατάλογος μπορεί να δημοσιοποιείται από το έμπιστο κέντρο. Επίσης, το κέντρο μπορεί να εξυπηρετεί αιτήσεις που αφορούν πληροφορίες σχετικά με ένα δημόσιο κλειδί.

16.47

Αρχή πιστοποίησης

Με την προηγούμενη προσέγγιση, ένα κέντρο θα μπορούσε να επιφορτιστεί σημαντικά αν το πλήθος των αιτήσεων είναι μεγάλο. Μια εναλλακτική λύση είναι η δημιουργία **πιστοποιητικών δημόσιων κλειδιών**. Ο Bob έχει τις εξής δύο απαιτήσεις: θέλει ο κόσμος να γνωρίζει το δημόσιο κλειδί του και δεν θέλει κανένας να μπορεί να δεχθεί ένα πλαστογραφημένο δημόσιο κλειδί ως δικό του. Για τον σκοπό αυτό, ο Bob μπορεί να απευθυνθεί σε μια **αρχή πιστοποίησης** ή ΑΠ (certification authority, CA), η οποία είναι μια κυβερνητική αρχή που αντιστοιχίζει δημόσια κλειδιά με οντότητες και εκδίδει πιστοποιητικά. Ακόμα και η ίδια η ΑΠ έχει ένα γνωστό δημόσιο κλειδί το οποίο όμως δεν μπορεί να πλαστογραφηθεί. Η ΑΠ εκδίδει ένα πιστοποιητικό για τον Bob. Για να αποτρέπεται η πλαστογράφηση του ίδιου του πιστοποιητικού, η ΑΠ το υπογράφει με το ιδιωτικό κλειδί της. Τώρα ο Bob μπορεί να δημοσιεύσει το υπογεγραμμένο πιστοποιητικό. Όποιος θέλει το δημόσιο κλειδί του Bob μπορεί να "κατεβάσει" το υπογεγραμμένο πιστοποιητικό και να χρησιμοποιήσει το δημόσιο κλειδί του κέντρου για να εξαγάγει το δημόσιο κλειδί του Bob.

16.48