Πανεπιστήμιο Αιγαίου

Εισαγωγή στην Επιστήμη των Υπολογιστών και Επικοινωνιών

Ασφάλεια πληροφοριακών και επικοινωνιακών συστημάτων και προστασία της ιδιωτικότητας

Σπύρος Κοκολάκης (sak@aegean.gr)

Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων

Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Αιγαίου**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Στόχοι ασφάλειας

Πρώτα θα εξετάσουμε τους τρεις στόχους ασφάλειας:

- **εμπιστευτικότητα**,
- **ακεραιότητα**, και
- **διαθεσιμότητα**

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.

Ακεραιότητα

Οι πληροφορίες πρέπει να αλλάζουν συνεχώς. Όταν, για παράδειγμα, 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.

Διαθεσιμότητα

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. Σε μια εταιρεία, η μη διαθεσιμότητα των πληροφοριών είναι εξίσου επιζήμια με την έλλειψη εμπιστευτικότητας ή ακεραιότητας.

Επιθέσεις

Οι τρεις στόχοι της ασφάλειας, η εμπιστευτικότητα, η ακεραιότητα, και η διαθεσιμότητα, μπορεί να υπονομευθούν από επιθέσεις κατά της ασφάλειας.

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**.

Υπηρεσίες ασφάλειας

Έχουν οριστεί διάφορα πρότυπα υπηρεσιών ασφάλειας για την επίτευξη των στόχων ασφάλειας και την αποτροπή επιθέσεων κατά της ασφάλειας. Οι πέντε βασικές κατηγορίες υπηρεσιών είναι:

- Εμπιστευτικότητα δεδομένων
- Ακεραιότητα δεδομένων
- Πιστοποίηση αυθεντικότητας
- Μη απάρνηση
- Έλεγχος πρόσβασης

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).

Τεχνικές

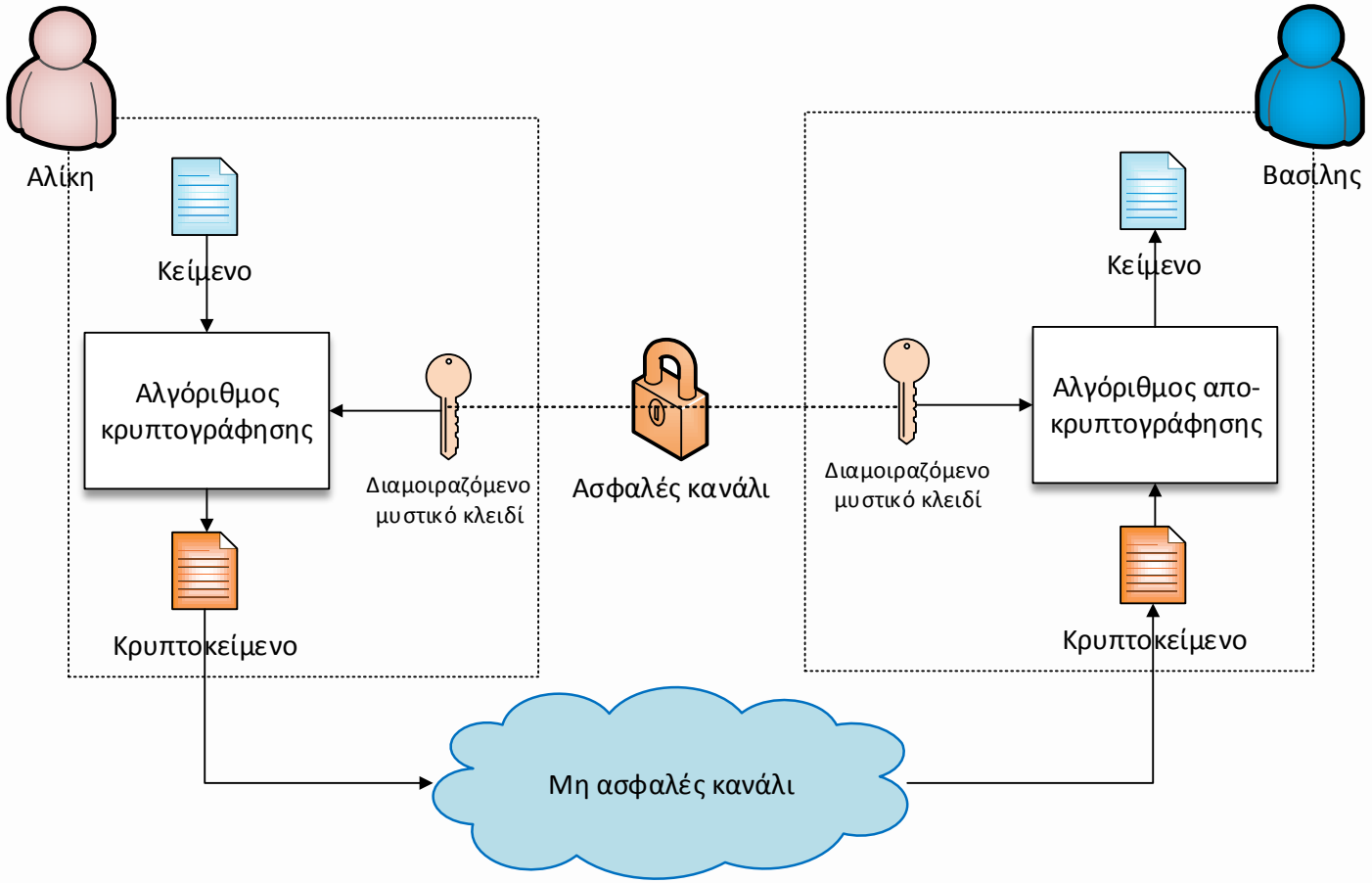
Κρυπτογραφία. Ορισμένες υπηρεσίες ασφάλειας μπορούν να υλοποιηθούν με χρήση κρυπτογραφίας. Η λέξη κρυπτογραφία προέρχεται από τις λέξεις "κρυπτός" και "γράφω".

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".

Κρυπτογραφία συμμετρικού κλειδιού

Στο επόμενο σχήμα παρουσιάζεται η γενική ιδέα της κρυπτογραφίας συμμετρικού κλειδιού. Η Αλίκη μπορεί να στείλει ένα μήνυμα στο Βασίλη μέσω ενός μη ασφαλούς καναλιού με την πεποίθηση ότι κάποιος άλλος χρήστης δεν θα μπορέσει να κατανοήσει το περιεχόμενο του μηνύματος "κρυφακούγοντας" στο κανάλι.

Κρυπτογραφία συμμετρικού κλειδιού



Κρυπτογραφία συμμετρικού κλειδιού

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

Κλασικοί κρυπταλγόριθμοι

Οι κλασικοί κρυπταλγόριθμοι χρησιμοποιούσαν δύο τεχνικές για την απόκρυψη πληροφοριών από εισβολείς:

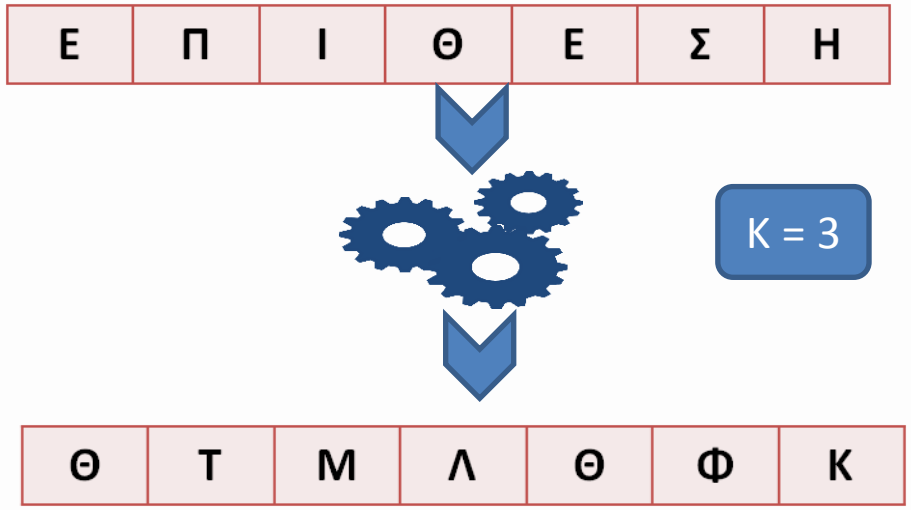
- αντικατάσταση και
- αναδιάταξη

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.

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

Ο «αλγόριθμος του Καίσαρα»



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.

Κρυπταλγόριθμοι αναδιάταξης (παράδειγμα)

Έστω ότι θέλουμε να κρυπτογραφήσουμε το εξής μήνυμα: "Η ΑΠΟΒΑΣΗ ΘΑ ΓΙΝΕΙ ΣΤΗ ΝΟΡΜΑΝΔΙΑ". Για να εφαρμόσουμε την παραπάνω μέθοδο αναδιάταξης θα αφαιρέσουμε τα κενά και θα χωρίσουμε το μήνυμα σε τμήματα με μήκος επτά συμβόλων, ως εξής: " ΗΑΠΟΒΑΣ ΗΘΑΓΙΝΕ ΙΣΤΗΝΟΡ ΜΑΝΔΙΑΩ" Στο τέλος του τέταρτου τμήματος προσθέσαμε ένα αυθαίρετα επιλεγμένο σύμβολο, το Ω, ώστε να συμπληρωθεί το τμήμα των επτά συμβόλων.

Κρυπταλγόριθμοι αναδιάταξης (παράδειγμα)

Εφαρμόζοντας την παρακάτω αναδιάταξη της παράγουμε το εξής κρυπτοκείμενο: ΠΟΑΗΑΣΒΑΓΝΗΘΕΙΤΗΟΙΣΡΝΝΔΑΜΑΩΙ. Η αποκρυπτογράφηση γίνεται, απλά, αντιστρέφοντας τη διαδικασία της κρυπτογράφησης

1	2	3	4	5	6	7
4	5	1	2	7	3	6

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 ένα 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.

Advanced Encryption Standard

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 παλαιότερου προτύπου (Data Encryption Standard - DES), όπως το μικρό μέγεθος κλειδιού.

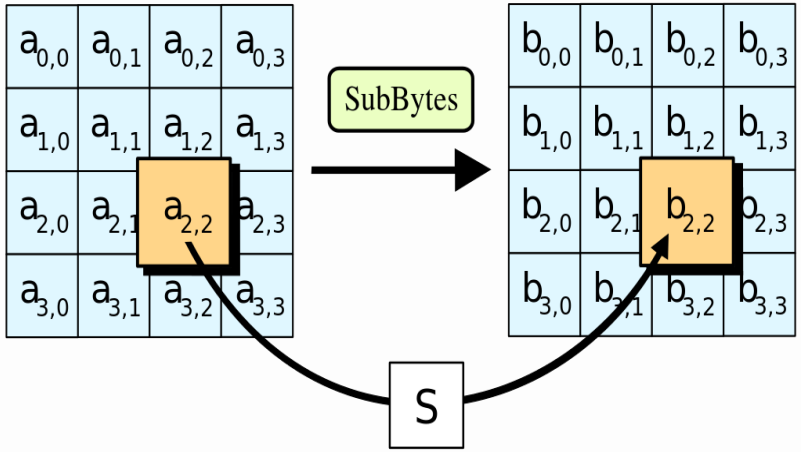
Advanced Encryption Standard

Στον AES κάθε μήνυμα χωρίζεται σε τμήματα σταθερού μήκους 128 bits. Το κάθε τμήμα κρυπτογραφείται με ένα κλειδί που μπορεί να έχει μήκος 128, 192, ή 256 bits.

Η κρυπτογράφηση γίνεται σε κύκλους, που ο καθένας περιλαμβάνει από τρεις έως τέσσερεις μετασχηματισμούς, οι οποίοι συνδυάζουν σύνθετες αντικαταστάσεις και μετατοπίσεις των δυαδικών ψηφίων. Εκτελούνται 10, 12, ή 14 κύκλοι, ανάλογα με το μέγεθος του κλειδιού.

Advanced Encryption Standard

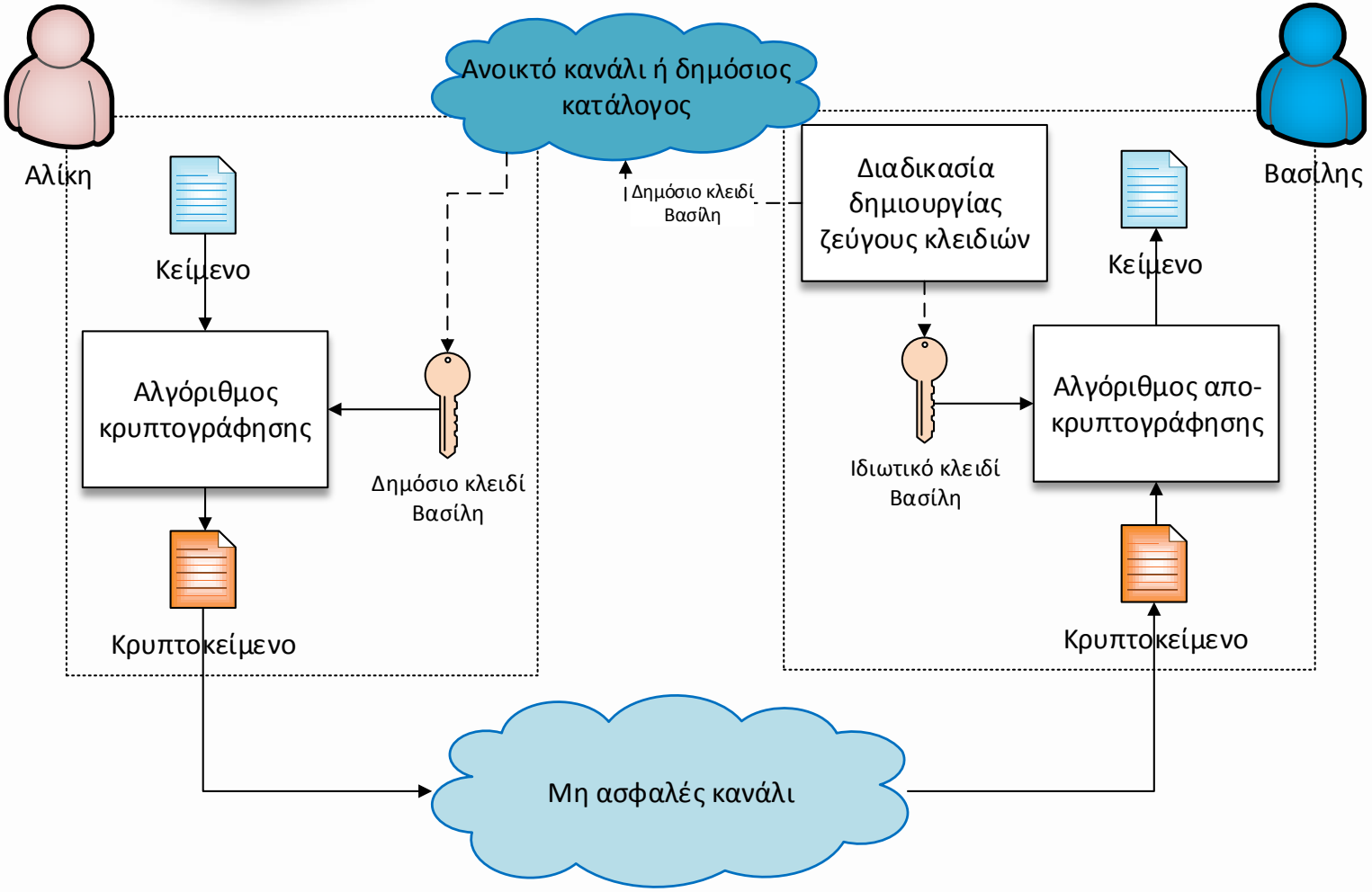
Το πρώτο από τα τέσσερα στάδια κάθε κύκλου στον AES. Αντικατάσταση κάθε λέξης στον αριστερό πίνακα με την αντίστοιχη λέξη στο δεύτερο πίνακα. (Πηγή: Wikipedia)



Κρυπτογραφία ασύμμετρου κλειδιού

Σε αντίθεση με την κρυπτογραφία συμμετρικού κλειδιού, στην κρυπτογραφία ασύμμετρου κλειδιού χρησιμοποιούνται ξεχωριστά κλειδιά, 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.

Κρυπτογραφία ασύμμετρου κλειδιού



Σύγκριση μεθόδων

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.

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 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. Ενώ η κρυπτογραφία συμμετρικού κλειδιού βασίζεται στην αντικατάσταση και τη μετάθεση συμβόλων, η κρυπτογραφία ασύμ-μετρου κλειδιού βασίζεται στην εφαρμογή μαθηματικών συναρτήσεων σε αριθμούς.

Άλλες υπηρεσίες ασφάλειας

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.

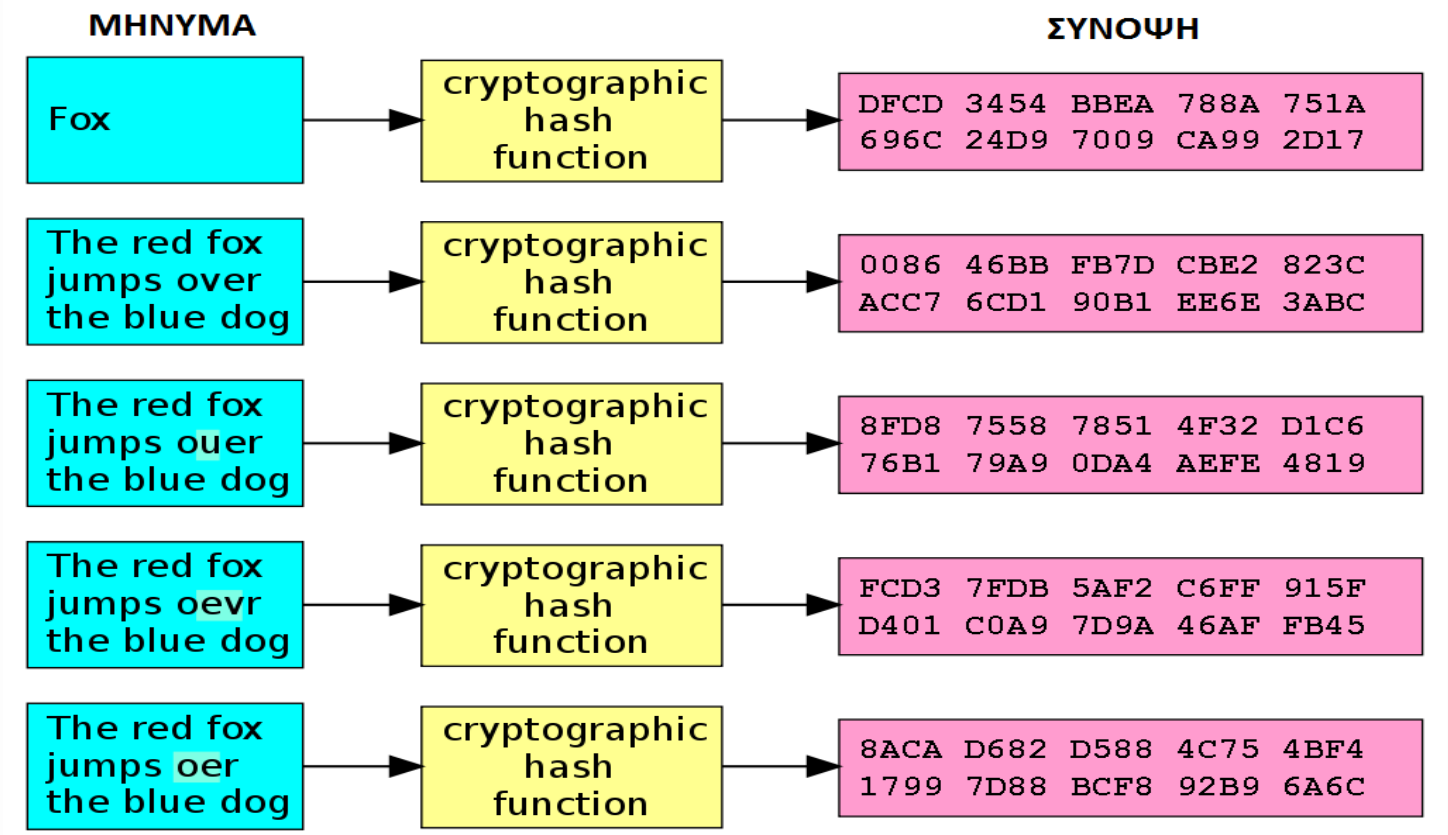
Ακεραιότητα μηνύματος

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**.

Ακεραιότητα μηνύματος

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.

Συνάρτηση κατακερματισμού



Παράδειγμα εφαρμογής κρυπτογραφικής συνάρτησης κατακερματισμού (πηγή: http://en.wikipedia.org/wiki/Cryptographic_hash_function)

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.

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 Αλίκη στέλνει ένα μήνυμα στο Βασίλη, αυτός πρέπει να επιβεβαιώνει ότι το μήνυμα προέρχεται πράγματι από την Αλίκη. Για να επιτρέπει την πιστοποίηση της αυθεντικότητας των μηνυμάτων, η Αλίκη 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.

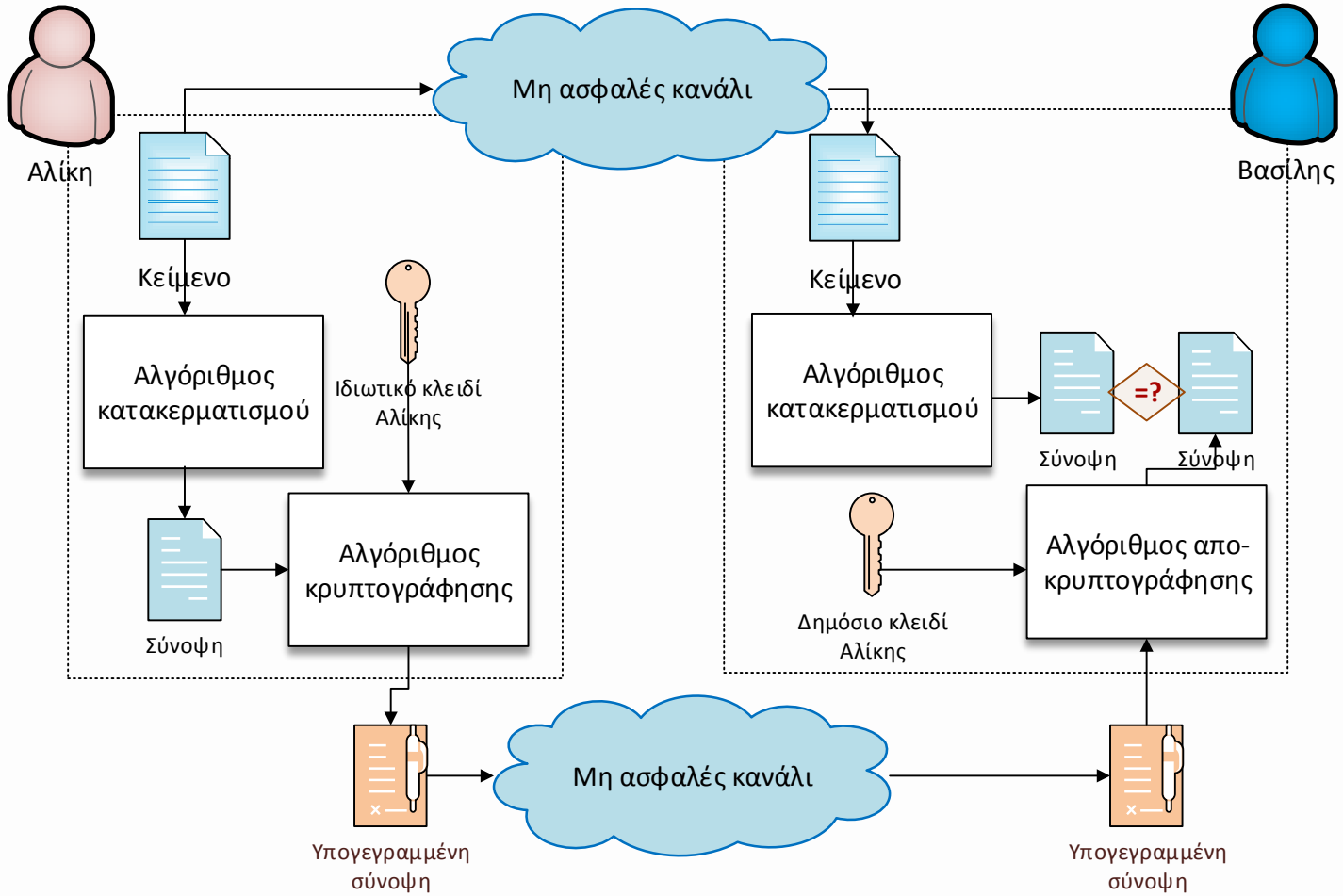
Πιστοποίηση αυθεντικότητας μηνύματος

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).

Ψηφιακές υπογραφές

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: δηλ. πρέπει να διασφαλίζει ότι το μήνυμα προέρχεται από την Αλίκη και όχι από κάποιον τρίτο. Για το σκοπό αυτό, ο Βασίλης μπορεί να ζητήσει από την Αλίκη να υπογράφει ηλεκτρονικά τα μηνύματα. Η ηλεκτρονική υπογραφή μπορεί να αποδεικνύει την αυθεντικότητα της Αλίκης ως αποστολέα του μηνύματος. Αυτού του είδους η υπογραφή αναφέρεται ως ψηφιακή υπογραφή.

Διαδικασία ψηφιακής υπογραφής



Υπηρεσίες

Μια ψηφιακή υπογραφή παρέχει τρεις από τις πέντε υπηρεσίες ασφάλειας που αναφέραμε στην αρχή:

- πιστοποίηση αυθεντικότητας μηνύματος,
- ακεραιότητα μηνύματος, και
- μη απάρνηση.

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.

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.

Πιστοποίηση αυθεντικότητας προέλευσης δεδομένων και οντότητας

- 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.

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
- Κάτι που κατέχεται
- Κάτι που ενυπάρχει

Διαχείρισης κλειδιών

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.

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 Αλίκη και ο Βασίλης θέλουν να επικοινωνούν, πρέπει να βρουν έναν τρόπο να ανταλλάσσουν ένα μυστικό κλειδί. Αν η Αλίκη θέλει να επικοινωνεί με ένα εκατομμύριο άτομα, πώς μπορεί να ανταλλάσσει με αυτά ένα εκατομμύριο κλειδιά; Είναι προφανές ότι χρειαζόμαστε έναν αποδοτικό τρόπο να διατηρούμε και να διανέμουμε κλειδιά.

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 Αλίκη στείλει μια αίτηση στο ΚΔΚ με την οποία δηλώνει ότι χρειάζεται ένα μυστικό κλειδί συνεδρίας μεταξύ της ίδιας και του Βασίλη.
2. Το ΚΔΚ ενημερώνει το Βασίλη για την αίτησή της.
3. Αν ο Βασίλης συμφωνήσει, δημιουργείται μια συνεδρία μεταξύ τους.

Διανομή δημόσιων κλειδιών

Στην κρυπτογραφία ασύμμετρου κλειδιού, οι χρήστες δεν χρειάζονται κάποιο διαμοιραζόμενο συμμετρικό κλειδί. Αν η Αλίκη θέλει να στείλει ένα μήνυμα στο Βασίλη, πρέπει μόνο να γνωρίζει το δημόσιο κλειδί του, το οποίο είναι γνωστό στο κοινό και διαθέσιμο σε όλους. Παρόμοια, αν ο Βασίλης χρειάζεται να στείλει ένα μήνυμα στην Αλίκη, 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.

Δημοσιοποίηση στο κοινό

Η απλούστερη προσέγγιση είναι η ανακοίνωση των δημόσιων κλειδιών στο κοινό. Έτσι, ο Βασίλης μπορεί να τοποθετήσει το δημόσιο κλειδί του στην ιστοσελίδα του ή να το δημοσιεύσει σε διάφορα έντυπα. Όταν η Αλίκη θελήσει να στείλει ένα μήνυμα στο Βασίλη, 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.

Αρχή πιστοποίησης

Με την προηγούμενη προσέγγιση, ένα κέντρο θα μπορούσε να φορτιστεί σημαντικά αν το πλήθος των αιτήσεων είναι μεγάλο. Μια εναλλακτική λύση είναι η δημιουργία **πιστοποιητικών δημόσιων κλειδιών**. Ο Βασίλης 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** (Certification Authority, CA).

Σύνοψη

- Στόχοι ασφάλειας
- Κρυπτογραφία
  - Κρυπτογραφία ασύμμετρου κλειδιού
  - Συμμετρική κρυπτογραφία
- Ψηφιακές υπογραφές
- Υποδομή Δημοσίου Κλειδιού
- Διαχείριση κλειδιών