Κρυπτογραφία

Γενική επισκόπηση

Ανασκόπηση ύλης

- Στόχοι της κρυπτογραφίας – Ιστορικό – Γενικά χαρακτηριστικά
- Κλασσική κρυπτογραφία
  - Συμμετρικού κλειδιού (block ciphers – stream ciphers)
  - Δημοσίου κλειδιού (στηριγμένη στη θεωρία υπολογισμού)
- Τεχνικές πιστοποίησης μηνύματος και πιστοποίησης ταυτότητας αποστολέα
- Εγκαθίδρυση και διαχείριση κλειδιού

Βιβλιογραφία

- “Handbook of Applied Cryptography”, A. J. Menezes, P. C. Van Oorschot και S. A. Vanstone, *CRC Press*, 1996

  (διαθέσιμο από το διαδίκτυο: http://www.cacr.math.uwaterloo.ca/hac/)
- *“Τεχνικές κρυπτογραφίας και κρυπτανάλυσης», Β.Α. Κάτος και Γ.Χ. Στεφανίδης*

Βασικοί όροι

- Με τον όρο κρυπτογραφία εννοούμε τη μελέτη μαθηματικών τεχνικών που στοχεύουν στην εξασφάλιση θεμάτων που άπτονται της ασφάλειας μετάδοσης της πληροφορίας, όπως εμπιστευτικότητα, πιστοποίηση ταυτότητας του αποστολέα και διασφάλιση του αδιάβλητου της πληροφορίας.
- Plaintext : Το αρχικό κομμάτι πληροφορίας
- Κρυπτόγραμμα (ciphertext): Το κρυπτογραφημένο μήνυμα
- Encryption: Η διαδικασία της κρυπτογράφησης ενός μηνύματος
- Decryption: η διαδικασία αποκρυπτογράφησής του

Κρυπτογραφική Ορολογία

- Εμπιστευτικότητα ή μυστικότητα (privacy): η διατήρηση της πληροφορίας κρυφής από όλους, εκτός από εκείνους που είναι εξουσιοδοτημένοι να τη δουν
- Ακεραιότητα των δεδομένων (data integrity): διασφάλιση του ότι η πληροφορία δεν έχει παραποιηθεί από μη εξουσιοδοτημένο μέσο
- Πιστοποίηση ταυτότητας (entity authentication ή identification): επιβεβαίωση της ταυτότητας ενός χρήστη
- Πιστοποίηση μηνύματος (message authentication): Επιβεβαίωση της πηγής της πληροφορίας
- Υπογραφή (signature): ένα μέσο προσάρτησης πληροφορίας ενός χρήστη στα μεταδιδόμενα δεδομένα, με στόχο την πιστοποίηση ταυτότητας

Στόχοι της κρυπτογραφίας

- Τα μηνύματα πρέπει να φτάνουν στο σωστό προορισμό
- Εμπιστευτικότητα: Μόνο ο παραλήπτης τους να μπορεί να τα λάβει και να τα δει (confidentiality)
- Πιστοποίηση της ταυτότητας του αποστολέα (authentication)
- Το μήνυμα δεν πρέπει να αλλοιωθεί κατά τη μεταφορά από μη εξουσιοδοτημένη οντότητα (data integrity)
- Όποια ενέργεια κάνει κάποιος (π.χ. πιστοποίηση ταυτότητας) δεν πρέπει αργότερα να μπορεί να την αρνηθεί (Non-repudiation)

Προσοχή!

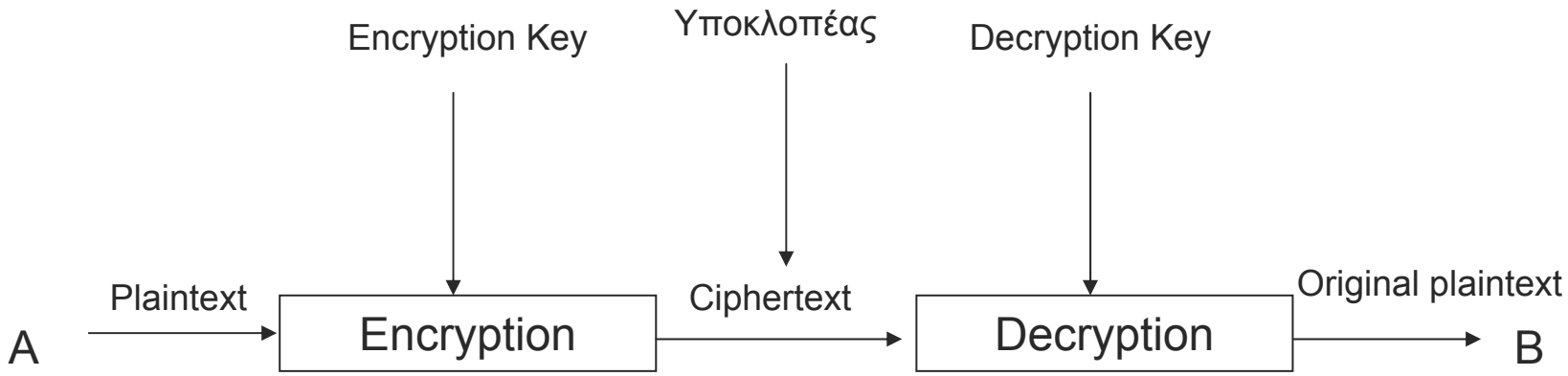
Η κρυπτογραφία δεν λύνει τα παραπάνω, απλά προσπαθεί να τα ικανοποιήσει

Περιοριστικοί αλγόριθμοι (restricted algorithms)

- Η ασφάλεια ενός τέτοιου αλγορίθμου εξασφαλίζεται μόνο αν ο αλγόριθμος παραμένει κρυφός!
- Ανεφάρμοστοι στην πράξη (μη ασφαλείς)

Αλγόριθμοι βασισμένοι σε **κλειδιά**

- Οι αλγόριθμοι κρυπτογράφησης χρησιμοποιούν ένα ή περισσότερα κλειδιά (keys).



Η ασφάλεια έγκειται στο ότι δεν είναι γνωστό το κλειδί – οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης μπορούν να είναι ευρέως γνωστοί (αρχή του Kerchoff)

Ένας απλός αλγόριθμος βασισμένος σε κλειδί

Κρυπτογράφηση

Πολλαπλασίασε το αρχικό μήνυμα επί 2 και πρόσθεσε το κλειδί

Αποκρυπτογράφηση

Αφαίρεσε το κλειδί και διαίρεσε το κρυπτόγραμμα διά 2

plaintext **= SECRET =** 19 5 3 18 5 20

Key = 3

Ciphertext = 41 13 9 39 13 43

Κατηγορίες αλγορίθμων ως προς το είδος του κλειδιού

- Αλγόριθμοι συμμετρικού (ή κρυφού) κλειδιού (symmetric key algorithms)
  - Χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση
- Αλγόριθμοι ασύμμετρου (ή δημοσίου) κλειδιού (Asymmetric (or public key) algorithms)
  - Χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση
  - Το κλειδί κρυπτογράφησης δεν μπορεί να εξαχθεί από το κλειδί αποκρυπτογράφησης

Μαθηματικός φορμαλισμός

Αν E και D συμβολίζουν τις συναρτήσεις κρυπτογράφησης και αποκρυπτογράφησης αντίστοιχα, τότε:

- $E_{K1}(m) = c$
- $D_{K2}(c) = m$

όπου m και c υποδηλώνουν το αρχικό και το κρυπτογραφημένο μήνυμα αντίστοιχα.

Οι δείκτες Ki υποδηλώνουν την εξάρτηση των συναρτήσεων από το κλειδί.

Οι συναρτήσεις έχουν την ιδιότητα: $D_{K2}(E_{K1}(m)) = m$

Σε αλγόριθμους συμμετρικού κλειδιού, ισχύει K1 = K2

«Επιθέσεις» εναντίον κρυπτογραφικών αλγορίθμων (Κρυπτανάλυση)

- Κρυπτανάλυση είναι η μελέτη μαθηματικών τεχνικών που στοχεύουν στην ακύρωση των κρυπτογραφικών μεθόδων, καθιστώντας τις έτσι μη κατάλληλες για κρυπτογραφικούς σκοπούς.
- Ένας αλγόριθμος θεωρείται μη ασφαλής αν είναι δυνατή η ανάκτηση του αρχικού μηνύματος ή του κλειδιού από το κρυπτόγραμμα, ή αν είναι δυνατή η ανάκτηση του κλειδιού από ζευγάρια plaintext-ciphertext.
- Είδη «επιθέσεων»
  - Ciphertext attack
    ο επιτιθέμενος γνωρίζει το κρυπτόγραμμα: στόχος η εύρεση είτε του αρχικού μηνύματος είτε του κλειδιού
  - Known-plaintext attack
    ο επιτιθέμενος γνωρίζει το κρυπτόγραμμα και το αντίστοιχο μήνυμα – στόχος του η εύρεση του κλειδιού
  - Chosen-plaintext attack
    Ο επιτιθέμενος είναι σε θέση να επιλέξει συγκεκριμένα ζεύγη «αρχικό μήνυμα – κρυπτόγραμμα» που θα γνωρίζει. Στόχος του η εύρεση του κλειδιού.

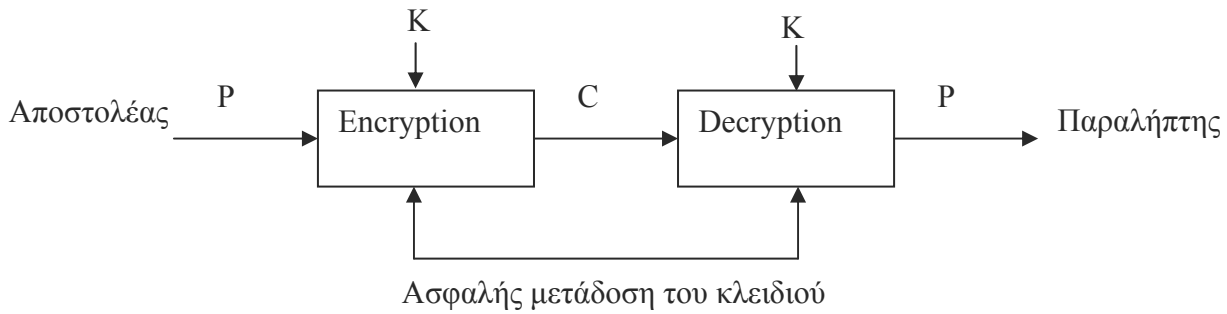
Ασφαλή συστήματα κρυπτογράφησης

- Απεριόριστα ασφαλές (Unconditionally secure)
  - Ένα σύστημα κρυπτογράφησης χαρακτηρίζεται απεριόριστα ασφαλές αν, ανεξάρτητα του πόσο μεγάλου τμήματος του κρυπτογράμματος είναι γνωστό, δεν υπάρχει αρκετή πληροφορία για την ανάκτηση του αρχικού μηνύματος κατά μοναδικό τρόπο, όση υπολογιστική ισχύ κι αν διαθέτει ο επιτιθέμενος (δεν μπορεί να υπάρξει).
- Υπολογιστικά ασφαλές (Computationally secure)
  - Ένα σύστημα κρυπτογράφησης χαρακτηρίζεται υπολογιστικά ασφαλές αν είναι υπολογιστικά αδύνατο να «σπάσει».

Βασικές αρχές του Shannon

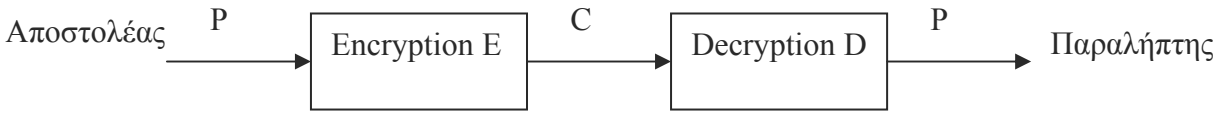
- Διάχυση (Diffusion): κάθε γράμμα του αρχικού μηνύματος πρέπει να επηρεάζει όσο γίνεται περισσότερα γράμματα του κρυπτογράμματος.
- Σύγχυση (Confusion): Η σχέση μεταξύ αρχικού μηνύματος και κρυπτογράμματος πρέπει να είναι σύνθετη, έτσι ώστε ο επιτιθέμενος να μην είναι σε θέση να προβλέψει αλλαγές στο κρυπτόγραμμα, με δεδομένες κάποιες μεταβολές στο αρχικό μήνυμα.
- Οι αρχές αυτές εφαρμόζονται στην πράξη, αφού λαμβάνονται υπ όψιν στην κατασκευή κρυπτογραφικών αλγορίθμων

Συμμετρικά κρυπτοσυστήματα



- Ο αποστολέας και ο παραλήπτης πρέπει από την αρχή να συμφωνήσουν στη χρήση ενός κοινού κλειδιού K.
- Ένα «ασφαλές κανάλι επικοινωνίας» πρέπει να υπάρχει για την επικοινωνία τους προκειμένου να ενημερώσει ο ένας τον άλλον για τον κλειδί.

Κρυπτοσυστήματα Δημοσίου κλειδιού



- Προτάθηκαν το 1976
- Κάθε συμμετέχων στο σύστημα κατέχει ένα ζευγάρι κλειδιών e και d, που το ένα αντιστρέφει το άλλο: $D_d(E_e(m))=m$
- Το κλειδί e σε κάθε χρήστη είναι ευρέως γνωστό σε όλους, ενώ το d κρατείται μυστικό και το ξέρει μόνο ο κάτοχός του. Απαραίτητη προϋπόθεση για την ασφάλεια του συστήματος είναι το εξής: η γνώση του δημοσίου κλειδιού δεν πρέπει να επιτρέπει τον προσδιορισμό του ιδιωτικού κλειδιού.
- Σύγκριση με τους αλγορίθμους συμμετρικού κλειδιού: Η ανταλλαγή κλειδιών μεταξύ αποστολέα και παραλήπτη αντικαθίσταται από την ύπαρξη ενός διαφανούς καταλόγου, στον οποίο όλοι έχουν πρόσβαση, και περιέχει τα δημόσια κλειδιά e όλων των συμμετοχόντων.

Τρόπος λειτουργίας συστημάτων δημοσίου κλειδιού

- Έστω e_A, d_A και e_B,d_B τα δημόσια και ιδιωτικά κλειδιά των Α, Β αντίστοιχα.
- Όταν ο Α θέλει να στείλει ένα μήνυμα m στον Β, το δημόσιο κλειδί κρυπτογράφησης του παραλήπτη Β χρησιμοποιείται για τη δημιουργία του κρυπτογράμματος Ee_B (m). Αφού το e_B είναι πλήρως διαθέσιμο σε κάποιον δημόσιο κατάλογο στον οποίο έχουν όλοι πρόσβαση, ο οποιοσδήποτε μπορεί να κρυπτογραφήσει ένα μήνυμα με προορισμό τον Β. Ωστόσο, μόνο ο Β, ο οποίος έχει πρόσβαση στο ιδιωτικό του κλειδί αποκρυπτογράφησης d_B μπορεί να ανακατασκευάσει το αρχικό μήνυμα, εφαρμόζοντας τον αντίστροφο μετασχηματισμό:

$$D_{dB}(Ee_B(m)).$$

Μειονέκτημα συστημάτων δημοσίου κλειδιού

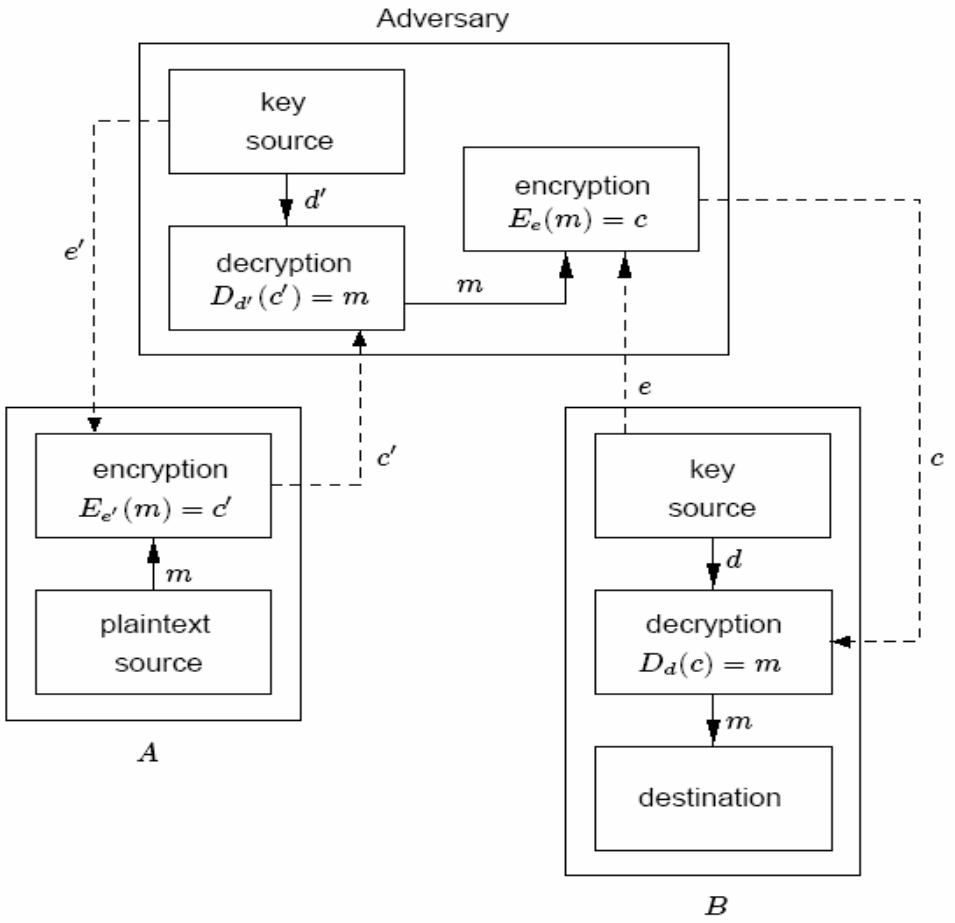
- Ο οποιοσδήποτε μπορεί να προσποιηθεί ότι είναι κάποιος άλλος χρήστης!! Αν ο επιτιθέμενος «σταματήσει» το μήνυμα που στέλνει ο Α στον Β, γράψει ένα δικό του και το στείλει στον Β κρυπτογραφημένο με το δημόσιο κλειδί του Β, ο Β δεν θα γνωρίζει τον πραγματικό αποστολέα του μηνύματος που λαμβάνει.

  Άρα
- Ανάγκη πιστοποίησης της ταυτότητας κάθε χρήστη.

Σχηματική αναπαράσταση υποκλοπής σε σύστημα Δημοσίου Κλειδιού

• Ο επιτιθέμενος ξεγελά τον Α ότι είναι ο Β, στέλνοντάς του το δικό του δημόσιο κλειδί e'. Έτσι, ο Α στέλνει τα μηνύματα κρυπτογραφημένα ως προς το e'. Συνεπώς, ο επιτιθέμενος μπορεί και «διαβάζει» όλα τα μηνύματα που στέλνει ο Α στον Β

•Ο Β δεν μπορεί να αντιληφθεί την παρουσία του επιτιθέμενου, μια που αυτός του στέλνει κανονικά το μήνυμα. Ο Β, λαμβάνοντας ένα μήνυμα, δεν μπορεί να ξέρει με σιγουριά ποιος του το έστειλε.



Ψηφιακή υπογραφή (Digital Signature)

- Εξασφαλίζει πιστοποίηση της ταυτότητας.
- Έστω ότι ο Α στέλνει ένα υπογεγραμμένο μήνυμα στον Β. Η υπογραφή του Α πρέπει να ικανοποιεί τα εξής:
  1. Ο Β να είναι σε θέση να επικυρώσει το γνήσιο της υπογραφής.
  2. Πρέπει να είναι αδύνατη η πλαστογράφηση της υπογραφής του Α

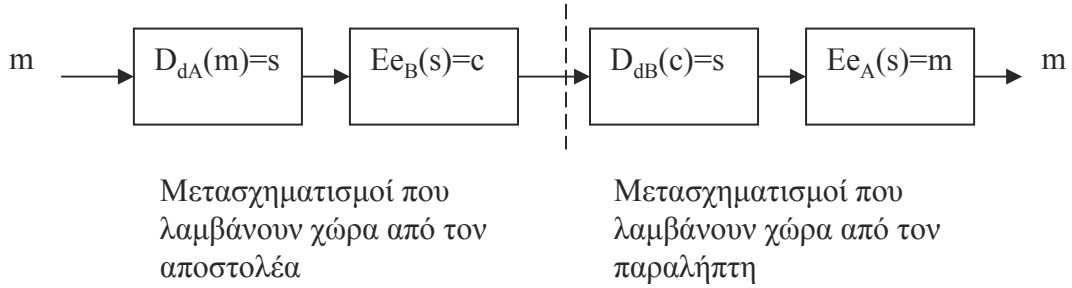
Χρήση συστημάτων δημοσίου κλειδιού για υπογραφή μηνυμάτων

1. Ο Α υπογράφει το m με το ιδιωτικό του κλειδί d_A, υπολογίζοντας το $c=D_{dA}(m)$
2. Ο Β ελέγχει το γνήσιο της υπογραφής του Α με το δημόσιο κλειδί $e_{A,}$,υπολογίζοντας το $E_{eA}(c) =m$
3. Σαν επαλήθευση, το $E_{eA}(c)$ πρέπει να ανακτά το ίδιο Μ με αυτό που ανακτά ο Β.

- Απαιτήσεις:
  - $D_{dA}(E_{eA}(m))=E_{eA}(D_{dA}(m))=m$ για κάθε m
- Το παραπάνω καλείται αναστρέψιμο σχήμα Δημοσίου Κλειδιού

Ταυτόχρονη μυστικότητα και έλεγχος υπογραφής σε ένα κρυπτοσύστημα Δημοσίου κλειδιού

Έστω χρήστες A, B με δημόσια και ιδιωτικά κλειδιά e_A,d_A, e_B,d_B αντίστοιχα. Με E και D συμβολίζουμε γενικότερα τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης αντίστοιχα



Αποκρυπτογράφηση:

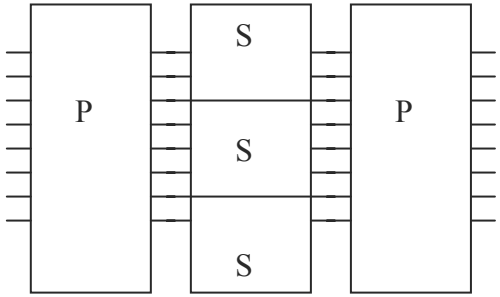
- $E_{eA}(s) = E_{eA}(D_{dB}(c)) =$
  $= E_{eA}(D_{dB}(E_{eB}(s))) =$
  $= E_{eA}(D_{dB}(E_{eB}(D_{dA}(m)))) =$
  $= E_{eA}(D_{dA}(m)) = m$

Ιστορική αναδρομή – Αλγόριθμοι αντικατάστασης και μετάθεσης

- Πριν την εμφάνιση των υπολογιστών, η κρυπτογραφία εφαρμοζόταν σε μηνύματα αποτελούμενα από γράμματα της αλφαβήτου
  - **Αλγόριθμοι αντικατάστασης (substitution ciphers)**: κάθε γράμμα του αρχικού μηνύματος αντικαθίσταται από κάποιο άλλο συγκεκριμένο του αλφαβήτου του κρυπτογράμματος.
  - **Αλγόριθμοι μετάθεσης (transposition (permutation) ciphers)**: το κρυπτόγραμμα είναι αναγραμματισμός του αρχικού μηνύματος.
- Είναι αλγόριθμοι **συμμετρικού κλειδιού**
- **Αυτές οι τεχνικές είναι παρούσες σχεδόν σε όλους τους σύγχρονους αλγορίθμους κρυπτογράφησης.**

Συνδυασμός αντικατάστασης και μετάθεσης – **Product Cipher** (αλγόριθμος γινομένου)

- Ένα product κρυπτογραφικό σύστημα αποτελείται από σύνθεση συναρτήσεων $F_1,\ldots,F_t$, όπου κάθε F_i μπορεί να είναι είτε αλγόριθμος αντικατάστασης (substitution) είτε αλληλομεταθεσης (permutation).
- Παραδείγματα (ευρέως χρησιμοποιούμενα)
  - DES, AES (θα τους δούμε αργότερα)



•Η αντικατάσταση εισάγει «σύγχυση» (confusion)

•Η μετάθεση εισάγει διάχυση (diffusion)

Κατηγοριοποίηση κρυπτογραφικών συστημάτων

- Block ciphers (αλγόριθμοι τμήματος/μπλοκ)
  - Το αρχικό μήνυμα χωρίζεται blocks, όπου το καθένα κρυπτογραφείται ξεχωριστά.
    - Πλεονεκτήματα:
      - υψηλή διάχυση
      - Ο επιτιθέμενος δεν μπορεί να προσθέσει bits (λόγω του σταθερού μήκους μπλοκ που έχουν αυτοί οι αλγόριθμοι)
- Stream ciphers (αλγόριθμοι ροής)
  - Το μήνυμα κρυπτογραφείται bit προς bit (ή byte προς byte)
    - Πλεονεκτήματα:
      - Πολύ υψηλή ταχύτητα (εφαρμογή σε τηλεδιασκέψεις κτλ)
      - Δεν υπάρχει διάδοση σφάλματος (αφού το κάθε bit μηνύματος επηρεάζει μόνο ένα bit του κρυπτογράμματος).