Κρυπτογραφία

Εργαστηριακό μάθημα 1

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.
- Ορολογία:
  - Plaintext : Το αρχικό κομμάτι πληροφορίας
  - Κρυπτόγραμμα (ciphertext): Το κρυπτογραφημένο μήνυμα
  - Encryption: Η διαδικασία της κρυπτογράφησης ενός μηνύματος
  - Decryption: η διαδικασία αποκρυπτογράφησής του

Στόχοι της κρυπτογραφίας

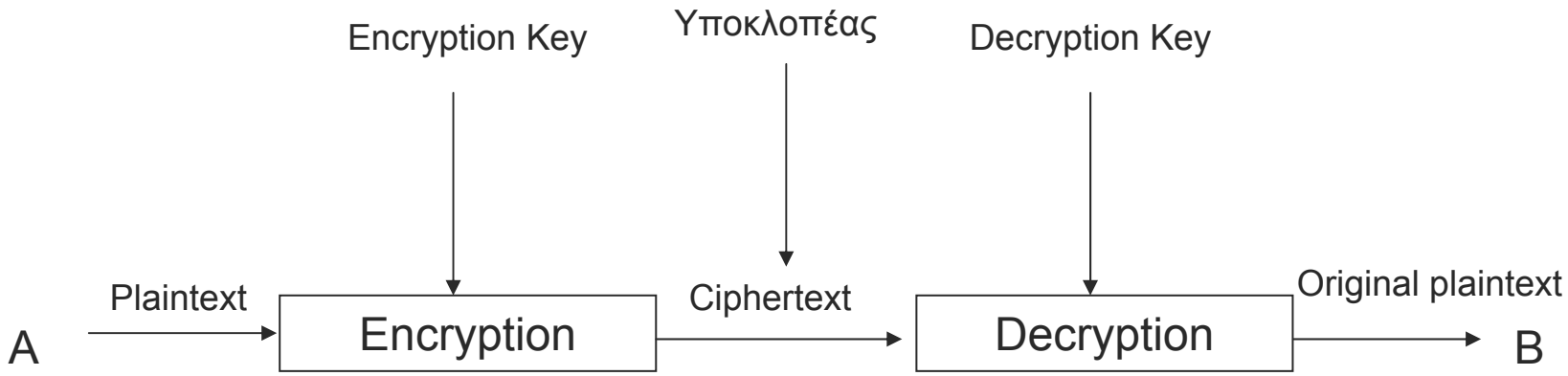
- Τα μηνύματα πρέπει να φτάνουν στο σωστό προορισμό
- Εμπιστευτικότητα: Μόνο ο παραλήπτης τους να μπορεί να τα λάβει και να τα δει (confidentiality)
- Πιστοποίηση της ταυτότητας του αποστολέα (authentication)
- Το μήνυμα δεν πρέπει να αλλοιωθεί κατά τη μεταφορά από μη εξουσιοδοτημένη οντότητα (data integrity)
- 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

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:

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

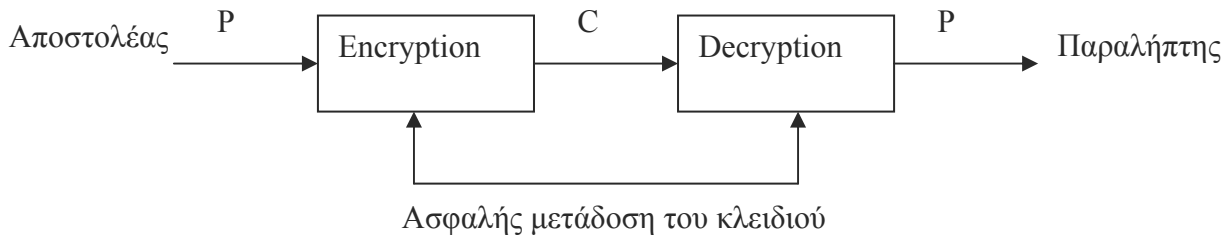
όπου M και C υποδηλώνουν το αρχικό και το κρυπτογραφημένο μήνυμα αντίστοιχα.

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

Αλγόριθμοι συμμετρικού κλειδιού



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

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 γράμμα του αλφαβήτου του κρυπτογράμματος.
  - **Αλγόριθμοι μετάθεσης ή αναδιάταξης (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.**

Ειδική περίπτωση αλγορίθμων αντικατάστασης: αλγόριθμοι μετατόπισης

- Κάθε γράμμα μετατοπίζεται κατά k θέσεις δεξιά τους (όπου k το κλειδί του αλγορίθμου)
  - Παράδειγμα αλγόριθμου μετατόπισης: Caesar cipher
    - Κάθε γράμμα αντικαθίσταται από εκείνο που βρίσκεται 3 θέσεις (modulo 26 για το αγγλικό αλφάβητο) δεξιά του.
    - Η ασφάλεια των αλγορίθμων μετατόπισης είναι μικρή (π.χ. για το αγγλικό αλφάβητο, τα πιθανά κλειδιά είναι μόλις 25).

Caesar Cipher - Παραδείγματα

- Παράδειγμα 1
  - Plaintext: ABCXYZ
  - Ciphertext: DEFABC
- Παράδειγμα 2
  - Plaintext: This is not secure
  - Ciphertext: Wklv lv qrw vhfxuh

Στη γενική περίπτωση, ένας αλγόριθμος μετατόπισης ολισθαίνει κάθε γράμμα κατά k θέσεις όπου το k μπορεί να πάρει οποιαδήποτε τιμή.

• Μη ασφαλείς αλγόριθμοι – το πλήθος των δυνατών κλειδιών είναι πολύ μικρό!!!

Μονοαλφαβητικοί αλγόριθμοι αντικατάστασης

- Κάθε σύμβολο του μηνύματος αντιστοιχίζεται σε ένα συγκεκριμένο σύμβολο του αλφαβήτου του κρυπτογράμματος, με μία «1-1» και επί συνάρτηση.
- Παράδειγμα: Α -> Λ, Β -> Ω, Γ -> Δ κ.ο.κ.
- Το πλήθος των κλειδιών είναι πολύ μεγάλο!! (ίσο με το πλήθος των δυνατών αντιστοιχίσεων που μπορούν να υπάρξουν)
  - Για το ελληνικό αλφάβητο που έχει 24 γράμματα, οι πιθανές αντιστοιχίσεις είναι 23!
- Ένας μονοαλφαβητικός αλγόριθμος αντικατάστασης είναι εύκολο να σπάσει, με ελέγχους της συχνότητας εμφάνισης των γραμμάτων

Συχνότητες εμφάνισης γραμμάτων της ελληνικής γλώσσας

Γράμμα	Συχνότητα Εμφάνισης (%)	Γράμμα	Συχνότητα Εμφάνισης (%)
Α	12	Λ	3,3
Ο	9,8	Η	2,9
Τ	9,1	Γ	2
Ε	8	Δ	1,7
Ν	7,9	Ω	1,6
Ι	7,8	Χ	1,4
Π	5,024	Θ	1,3
Ρ	5,009	Φ	1,2
Σ	4,9	Β	0,8
Μ	4,4	Ξ	0,6
Υ	4,3	Ζ	0,5
Κ	4,2	Ψ	0,2

Πρέπει το κείμενο να είναι μεγάλο, ώστε οι συχνότητες εμφάνισης των γραμμάτων στο κείμενο να ταυτίζονται με αυτές του πίνακα.

Ευρύτερη περίπτωση: Πολυαλφαβητικοί αλγόριθμοι αντικατάστασης

- Κάθε γράμμα του αρχικού μηνύματος δεν αντικαθίσταται από κάποιο συγκεκριμένο, αλλά το από ποιο θα αντικατασταθεί καθορίζεται από κάποιο κλειδί
- Αν και δείχνει πιο ασφαλής από έναν απλό αλγόριθμο αντικατάστασης, εν τούτοις αν βρεθεί το μήκος του κλειδιού υπόκειται στις ίδιες μεθόδους κρυπτανάλυσης, βασισμένες στις συχνότητες εμφάνισης των γραμμάτων
- Παράδειγμα: Vigenere Cipher

Vigenere Cipher

- Ανακαλύφτηκε από τον Γάλλο κρυπτογράφο Blaise de Vigenere
- Χρησιμοποιεί μία φράση-κλειδί για να κρυπτογραφήσει ένα μήνυμα
- Κάθε χαρακτήρας του κλειδιού αποφασίζει το πόσες θέσεις θα ολισθήσει ο αντίστοιχος χαρακτήρας του αρχικού κειμένου. Για παράδειγμα:
  - A: ολίσθηση 0 θέσεων δεξιά
  - B: ολίσθηση 1 θέσης δεξιά
  - C: ολίσθηση 2 θέσεων δεξιά
  - …
- Αν η φράση-κλειδί έχει μικρότερο μήκος από το αρχικό μήνυμα, η φράση-κλειδί επαναλαμβάνεται.

Παράδειγμα

- Κλειδί: lucky
- Αρχικό μήνυμα: simple message
- Κλειδί μετά την επανάληψη: luckyl uckyluc
- Πλήθος θέσεων ολίσθησης: 11 (l), 20(u), 2(c), 10(k), 24 (y), 11(l), 20(u), 2(c), 10(k), 24(y), 11(l), 20(u), 2(c). Αυτό το πλήθος θέσεων ολίσθησης εξαρτάται από τη θέση του αντίστοιχου γράμματος του κλειδιού στο αγγλικό αλφάβητο. Για παράδειγμα, το l είναι το 12^{ο} γράμμα, άρα η μετατόπιση του αντίστοιχου γράμματος του αρχικού μηνύματος είναι κατά 11 θέσεις δεξιά κ.ο.κ.
- Ολίσθηση των χαρακτήρων: s→d, i→c, m→o, p→z, l→j, …
- Κρυπτόγραμμα: dcozjpggcqlag

Σχόλια για τον αλγόριθμο Vigenere

- Το κλειδί πρέπει να είναι μεγάλο, όχι μόνο για αποφυγή της δυνατότητας εξαντλητικής αναζήτησης αλλά και για την απόκρυψη της συχνότητας των γραμμάτων.
- Μέθοδος κρυπτανάλυσης: αναζήτηση του μεγέθους του κλειδιού (αν υπολογιστεί το μήκος του κλειδιού, το πρόβλημα ανάγεται σε αλγόριθμο απλής αντικατάστασης).
- **Έλεγχος του Kasiski**: με δεδομένο ότι στο αρχικό κείμενο υπάρχουν λογικά πολλά τμήματα που επαναλαμβάνονται (π.χ. στην ελληνική γλώσσα λέξεις όπως «το», «οι», «σε», «με», «του», «από» κτλ εμφανίζονται πολλές φορές σε ένα κείμενο), τότε αν στο κρυπτόγραμμα εμφανιστούν δύο τέτοια τμήματα, πιθανότατα αυτά αντιστοιχούν σε ίδιο μήνυμα, στο οποίο έχει εφαρμοστεί το ίδιο κλειδί. Έτσι είναι πιθανό να υπολογιστεί το μήκος του κλειδιού.
- **Παράδειγμα:** Έστω το κρυπτόγραμμα ΑΚΨΟΜΙ**ΗΗΙ**ΛΟ**ΗΗΙ**ΞΑΚΨΝΔΚ
  το ΑΚΨ επανεμφανίζεται σε απόσταση 15 χαρακτήρων, ενώ το ΗΗΙ σε απόσταση 5 χαρακτήρων. Άρα, πιθανά μήκη κλειδιού ως προς την επανεμφάνιση του ΑΚΨ είναι τα 3,5,15 (οι διαιρέτες του 15), ενώ ως προς το ΗΗΙ είναι 5 (μια που το 5 δεν έχει διαιρέτες). Άρα, το πιο πιθανό μήκος κλειδιού είναι το 5 («ικανοποιεί» και την επανεμφάνιση του ΑΚΨ και την επανεμφάνιση του ΗΗΙ).

Αλγόριθμοι μετάθεσης

- «Ανακάτωμα» των bits ή των χαρακτήρων του μηνύματος, με βάση κάποια συνάρτηση ‘1-1’ και επί πάνω στο αλφάβητο (συνάρτηση αναδιάταξης).
- (Η συνάρτηση αυτή αποτελεί και το κλειδί)

INFORMATION TECHNIQUES FOR IPR

↓

I R I T N E R

N O M T O E H I U S O I R

F A N C Q F P

↓

IRITNERNOMTOEHIUSOIRFANCQFP

- Επίσης όχι ασφαλείς.

Το κλειδί στους αλγορίθμους μετάθεσης

- Αλλάζουνε οι θέσεις των γραμμάτων του μηνύματος, με βάση κάποια αναδιάταξη που ορίζεται από το κλειδί.
- Παράδειγμα: έστω η λέξη ΜΑΘΗΜΑ και κλειδί το [421653]. Αυτό σημαίνει ότι το τέταρτο γράμμα θα γίνει 1ο, το δεύτερο θα παραμείνει δεύτερο, το πρώτο θα γίνει 3ο κ.ο.κ. Άρα, το κρυπτόγραμμα θα είναι ΗΑΜΑΜΘ.
- Για μήνυμα μήκους Ν, όλα τα πιθανά κλειδιά είναι Ν! (όσες δηλαδή και οι αναδιατάξεις Ν στοιχείων).