Cryptography and Network Security Chapter 2

Fifth Edition

by William Stallings

Κεφαλαιο 2 – Κλασσικες Τεχνικες Κρυπτογράφησης

- *"I am fairly familiar with all the forms of secret writings, and am myself the author of a trifling monograph upon the subject, in which I analyze one hundred and sixty separate ciphers," said Holmes..*

  —*The Adventure of the Dancing Men*, Sir Arthur Conan Doyle

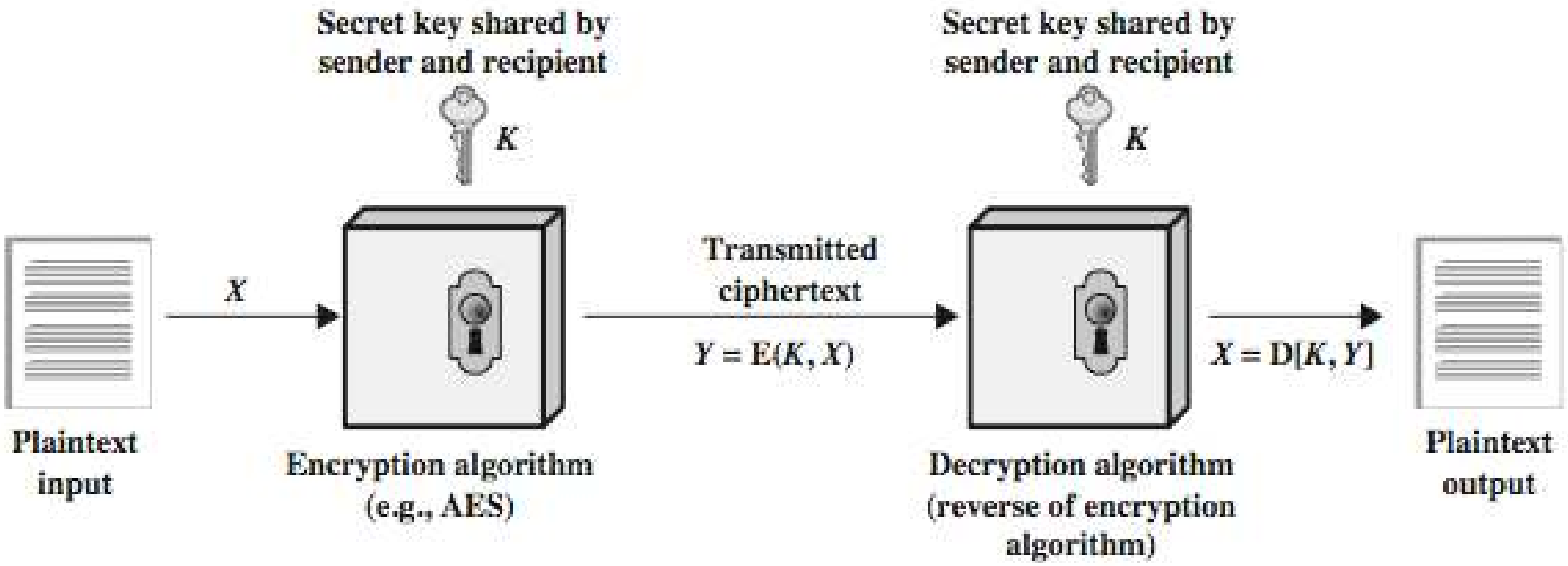
Συμμετρικη Κρυπτογραφια

- Αποκαλείται και Συμβατική ή Ιδιωτικου Κλειδιου (Private Key)
- Ο μεταδοτης και ο αποδέκτης μοιραζονται ενα κοινο κλειδι
- Ηταν ο μοναδικη γνωστη κρυπτογραφια μεχρι τη δεκαετια του 1970.
- Ειναι η ευρυτερα χρησιμοποιουμενη κρυπτογραφια.

Ορολογια

- **Απλο κειμενο (plaintext)** – το μη κρυπτογραφημενο μηνυμα
- **Κρυπτογραφημενο Κειμενο (ciphertext)** – το κρυπτογραφημενο μηνυμα
- **Αλγοριθμος κρυπτογραφησης (cipher)** - Μετατρεπει το plaintext σε ciphertext
- **Κλειδι (key)** – πληροφορια που χρησιμοποιείται απο τον αλγοριθμο κρυπτογραφησης και ειναι γνωστη μονο στο μεταδοτη και τον αποδεκτη
- **Κρυπτογραφηση (encryption, enciphering)** – η μετατροπη του plaintext σε ciphertext
- **Αποκρυπτογραφηση (decryprion, deciphering)** – η μετατροπη του ciphertext σε plaintext
- **Κρυπτογραφια (cryptography)** – η μελετη των μεθοδων κρυπτογραφησης και των αρχων της κρυπτογραφης και των αρχων που τις διεπουν
- **Κρυπταναλυση (cryptanalysis)** – μελετη των αρχων και των μεθοδων που αποσκοπουν στην αποκρυπτογραφηση χωρις να ειναι γνωστο το κλειδι.
- **Κρυπτολογια (cryptology)** – το επιστημονικο πεδιο που περιλαμβανει την κρυπτογραφια και την κρυπταναλυση

Symmetric Cipher Model



Προϋποθεσεις

- Δυο απαιτησεις για ασφαλη χρηση της συμμετρικης κρυπτογραφιας:
  - Να ειναι ισχυρος ο αλγοριθμος κρυπτογραφησης
  - Το Μυστικο κλειδι να ειναι γνωστο μονο στο μεταδοτη και στον αποδεκτη
- Συμβολικα γράφουμε:

  $Y = E(K, X)$

  $X = D(K, Y)$
- Υποθετουμε οτι ο αλγοριθμος κρυπτογραφησης ειναι γνωστος
- Πρεπει να υπαρχει προνοια (π.χ. ενα ασφαλες καναλι) για τη διανομη του κλειδιου

Κρυπτογραφια

- Μπορουμε να χαρακτηρισουμε τα κρυπτογραφικα συστηματα αναλογα με:
  - Το ειδος των κρυπτογραφικων λειτουργιων που χρησιμοποιουνται
    - Αντικαταστασης (substitution)
    - Αντιμεταθεσης (transposition)
    - Γινομενου (product)
  - Τον αριθμο των κλειδιων που χρησιμοποιουνται
    - Μοναδικου κλειδιου (single-key) ή ιδιωτικου κλειδιου (private key)
    - Δυο κλειδιων (two-key) ή Δημοσιου Κλειδιου (public key).
  - Τον τροπο επεξεργασιας του plaintext
    - Τμηματων (block)
    - Ροης (stream)

Κρυπταναλυση

- Στοχος ειναι να ανακαλυφθει το κλειδι και οχι μονο το μηνυμα
- Γενικες προσεγγισεις:
  - Κρυπταναλυτικη επιθεση (cryptanalytic attack)
  - Επιθεση ωμης βιας (brute-force attack)

Κρυπταναλυτικες επιθεσεις

- **ciphertext only**
  - only know algorithm & ciphertext, is statistical, know or can identify plaintext
- **known plaintext**
  - know/suspect plaintext & ciphertext
- **chosen plaintext**
  - select plaintext and obtain ciphertext
- **chosen ciphertext**
  - select ciphertext and obtain plaintext
- **chosen text**
  - select plaintext or ciphertext to en/decrypt

More Definitions

- **Ασφάλεια Άνευ Ορων (unconditional security)**
  - **Δεν εχει σημασια ποση υπολογιστκη ισχυς ειναι διαθεσιμη**, ο αλγοριθμος κρυπτογραφησης δεν μπορει να σπασει, λογω του οτι το ciphertext παρεχει ανεπατκη πληροφορια για να προσδιοριστει μονοσημαντα το αντιστοιχο plaintext.
- **Υπολογιστικη Ασφάλεια (computational security)**
  - **Δοθεντων περιορισμενων υπολογιστικων πορων** ο αλγοριθμος κρυπτογραφησης δεν μπορει να σπασει.

Brute Force Search

- Δοκιμαζεται καθε δυνατο κλειδι
- Προϋποθέτει οτι ειναι γνωστο ή αναγνωριζεται το plaintext

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/μs	Time required at 10^6 decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} μs = 6.4×10^{12} years	6.4×10^6 years

Κλασσικοι Κρυπτογραφικοι Αλγοριθμοι Αντικαταστασης

- Τα γράμματα του plaintext αντικαθιστανται απο αλλα γραμματα ή αριθμους ή συμβολα
- Ή αν το plaintext ειναι μια ακολουθια απο bits, τοτε η αντικασταση αφορα ομαδες απο bits που αντικαθιστανται απο άλλες ομαδες bits

Ο Αλγοριθμος του Καισαρα (Caesar Cipher)

- Αντικαθιστα καθε γραμμα με το γραμμα που ειναι τρεις θεσεις πιο πισω στο αλφαβητο.

- Παραδειγμα:

```
meet me after the toga party
PHHW PH DIWHU WKH WRJD SDUWB
```

Caesar Cipher

- Μπορουμε να ορισουμε το μετασχηματισμο ως εξης:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Αντιστοιχουμε σε καθε γραμμα εναν αριθμο.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Και ο αλγοριθμος του Καισαρα οριζεται ως εξης:

  $c = E(k, p) = (p + k) \bmod (26)$

  $p = D(k, c) = (c - k) \bmod (26)$

Κρυπταναλυση του Κωδικα του Καισαρα

- Υπαρχουν μονο 26 δυνατοι κωδικες
  - Το Α αντιστοιχει σε ενα απο τα Α,Β,..Ζ
- Ο επιτιθεμενος μπορει να τους δοκιμασει ολους και να βρει ποιος εφαρμοζεται.
- Δηλ. **brute force search**
- Χρειαζεται να αναγνωριζει ο επιτιθεμενος το plaintext

Μονοαλφαβητικος Κρυπτογραφικος Αλγοριθμος (Monoalphabetic Cipher)

- Αντι να μεταθετουμε το αλφαβητο, μπορουμε να ανακατευουμε τα γραμματα αυθαιρετα.

- Καθε γραμμα του plaintext απεικονιζεται σε ενα τυχαίο γραμμα του ciphertext.

- Αρα, το κλειδι εχει μηκος 26 γραμματα

```
Plain letter:  abcdefghijklmnopqrstuvwxyz
Cipher letter: DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext:  ifwewishtoreplaceletters
Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA
```

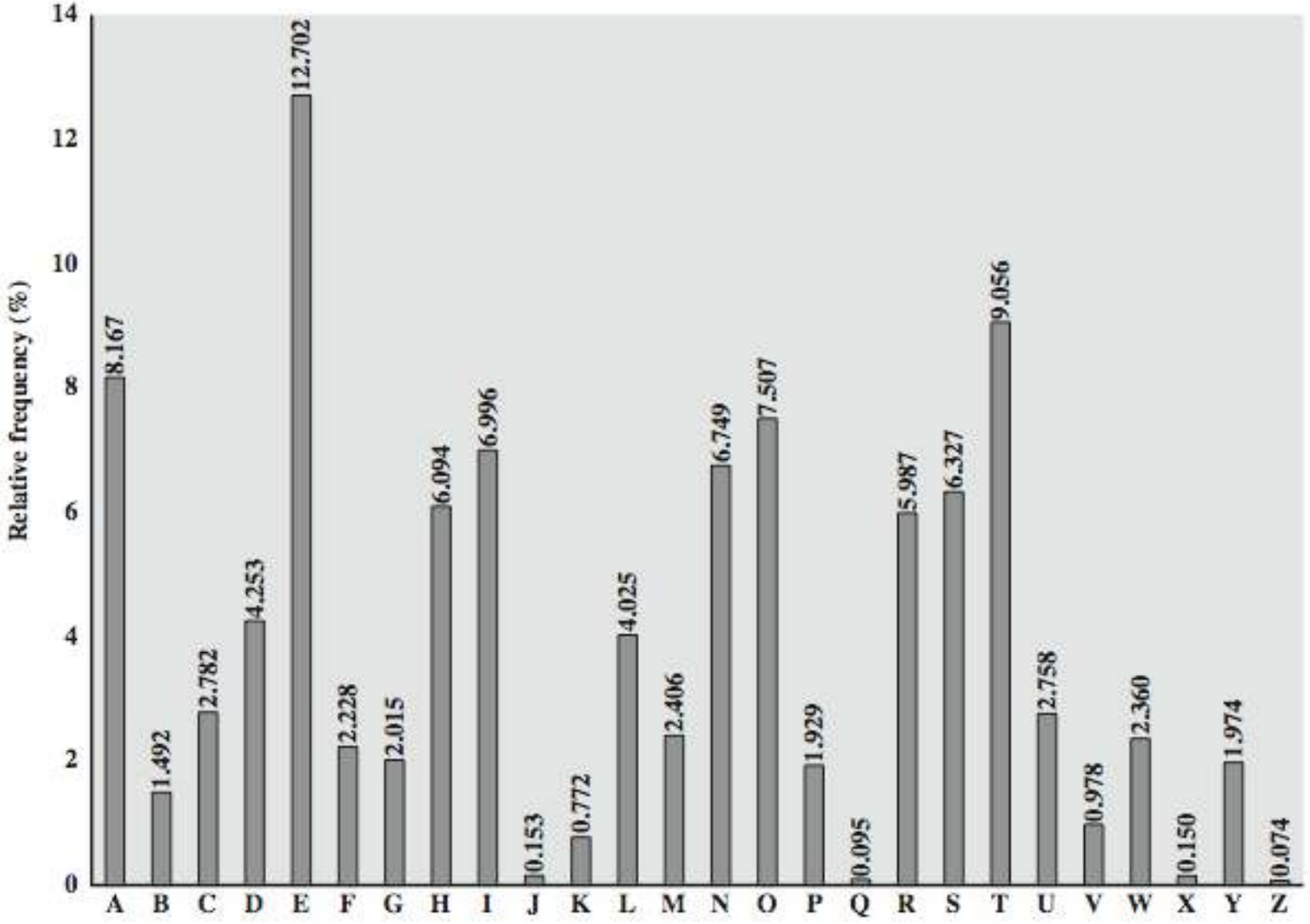
Ασφαλεια του Μονοαλφαβητικου Κρυπτογραφικου Αλγοριθμου

- Εχουμε τωρα συνολικα 26! = 4 x 10^{26} κλειδια
- Ισως καποιος να σκεφτει οτι με τοσα διαφορετκα κλειδια ειναι ασφαλης
- **!!!ΛΑΘΟΣ!!!**
- Το προβλημα ειναι τα χαρακτηριστικα της γλωσσας

Πλεονασμος της γλωσσας και Κρυπτανάλυση (Language Redundancy and Cryptanalysis)

- Τα γραμματα δεν εχουν ολα τη ιδια συχνοτητα εμφανισης
- Το Αγγλικο Ε ειναι το συχνοτερα εμφανιζομενο, και ακολουθουν τα: T,R,N,I,O,A,S
- Αλλα γραμματα, οπως τα Z,J,K,Q,X εμφανιζονται σχετικα σπανια
- Υπαρχουν πινακες για τις συχνοτητες εμφανισης απλων γραμματων, ζευγων γραμματων ή τριαδων γραμματων για διαφορες γλωσσες

English Letter Frequencies



Κρυπτογραφικοι Αλγοριθμοι Αντιμεταθεσης

- Κρυβουν το μηνυμα αλλαζοντας τη σειρα των γραμμάτων
- Χωρις να αλλαζουν τα γραμματα που χρησιμοποιουνται

Rail Fence cipher

- Τα γραμματα του μηνυματος γραφονται διαγωνια σε εναν αριθμο γραμμων.

- Και στη συνεχεια διαβαζεται το ciphertext κατα γραμμες.
- π.χ. το μηνυμα γραφεται ως εξης:

```
m e m a t r h t g p r y
  e t e f e t e o a a t
```

- και παιρνουμε το εξης ciphertext:

```
MEMATRHTGPRYETEFETEOAAT
```

Κρυπτογραφικοι Αλγοριθμοι Αντιμεταθεσης στηλών (Columnar Transposition Ciphers)

1. Γραφονται τα γραμματα του μηνυματος σε γραμμές, με εναν προκαθορισμενο αριθμο στηλων
2. Στη συνεχεια, διαβαζεται το ciphertext κατα στηλες, αλλα με διαφορετικη σειρα των στηλων, η οποια καθοριζεται απο καποιο κλειδι.
3. Τελος, διαβαζονται οι γραμμες.

- Key: 4312567

```
          4 3 1 2 5 6 7
Plaintext: a t t a c k p
           o s t p o n e
           d u n t i l t
           w o a m x y z
Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

Κρυπτογραφικοι Αλγοριθμοι Γινομενου (Product Ciphers)

- Οι αλγοριθμοι αντικαταστασης ή αντιμεταθεσης δεν ειναι ασφαλεις λογω των χαρακτηριστικων της γλωσσας.

- Για να αντιμετωπισουμε το προβλημα αυτο χρησιμοποιουμε περισσοτερους απο εναν αλγοριθμους στη σειρα.

Στεγανογραφία (Steganography)

- Είναι μια εναλλακτική λυση ως προς την κρυπτογραφηση
- Κρυβει την υπαρξη του μηνυματος
  - Χρησιμοποιεί μόνο ένα υποσυνολο των γραμματων/λεξεων (τα οποία μαρκαρονται με καποιον τροπο) σε ενα μεγαλύτερο μηνυμα.
- Μεγαλο μειονεκτημα της ειναι εχει μεγαλο overhead για σχετικα λιγα bits πληροφοριας.
- Πλεονεκτημα της ειναι οτι μπορει να χρησιμοποιηθει απο αυτους που δε θελουν να φαινεται οτι επικοινωνουν κρυπτογραφημενα.

Συνοψη

- Μελετησαμε:
  - Κλασσικες τεχνικες κρυπτογραφησης και ορολογια
  - Μονοαλφαβητικοι αλγπριθμοι αντικαταστασης
  - Κρυπταναλυση με βαση τη συχνοτητα εμφανισης των γραμματων
  - Κρυπτογραφικος αλγοριθμος Rail Fence
  - Κρυπτογραφικοι αλγοριθμοι αντιμεταθεσης
  - Κρυπτογραφικοι αλγοριθμοι γινομενου
  - Σταγανογραφια