Ασφάλεια Τηλεπικοινωνιακών Συστημάτων

ΣΤΑΥΡΟΣ Ν ΝΙΚΟΛΟΠΟΥΛΟΣ| 03 ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΚΡΥΠΤΟΛΟΓΙΑ

Περιγραφή μαθήματος

- Η Κρυπτολογία είναι κλάδος των Μαθηματικών, που ασχολείται με:
- Ανάλυση Λογικών Μαθηματικών Συναρτήσεων.
- Μελέτη, σχεδίαση και ανάπτυξη κρυπτογραφικών πρωτοκόλλων.
- Μελέτη, σχεδίαση και ανάπτυξη κρυπτογραφικών αλγορίθμων.
- Μελέτη, σχεδίαση και ανάπτυξη κρυπταναλυτικών μεθόδων.

Ιστορική Αναδρομή

- **Κρυπτογράφηση**
- Τεχνικές Κρυπτογράφησης
- Αλγόριθμοι κρυπτογράφησης
- Κρυπτογραφικά πρωτόκολλα

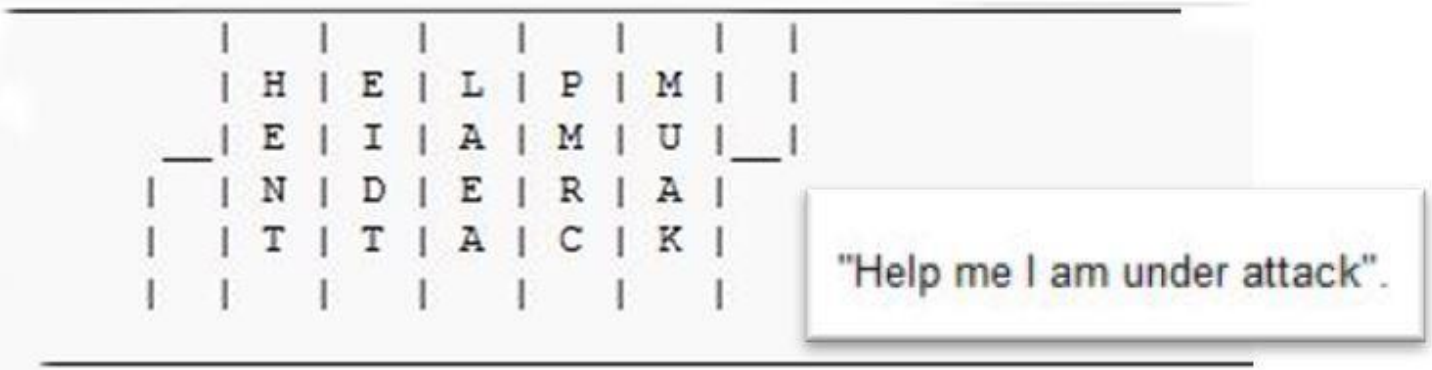
- **Κρυπτανάλυση**
- Μέθοδοι Κρυπτανάλυσης
- Τεχνικές Κρυπτανάλυσης

ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

ΚΡΥΠΤΟΓΡΑΦΙΑ: ΑΠΟ ΤΗΝ ΑΡΧΑΙΟΤΗΤΑ ΕΩΣ ΤΗ ΣΗΜΕΡΙΝΗ ΕΠΟΧΗ

Σκυτάλη


KILLKING
TOMORROW
MIDNIGHT


HELPME
EIAMUNDERATTACK
"Help me I am under attack".

Τετράγωνο του Πολύβιου

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Κώδικας του Ιουλίου Καίσαρα

$$c_i = E(p_i) = p_i + 3$$

A full translation chart of the Caesar cipher is shown here.

Plaintext	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
Ciphertext	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

Using this encryption, the message

TREATY IMPOSSIBLE

would be encoded as

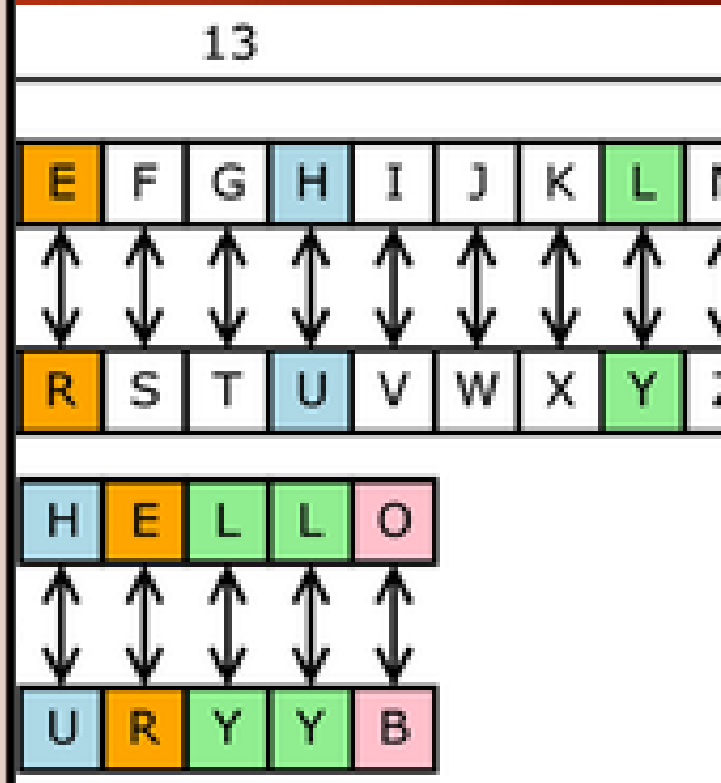
T	R	E	A	T	Y		I	M	P	O	S	S	I	B	L	E
w	u	h	d	w	b		l	p	s	r	v	v	l	e	o	h

Κώδικες Μετάθεσης

CIPHER ALPHABET

A	=	B	H	=	A	O	=	O	V	=	L
B	=	V	I	=	D	P	=	Y	W	=	P
C	=	G	J	=	Z	Q	=	F	X	=	U
D	=	Q	K	=	C	R	=	J	Y	=	I
E	=	K	L	=	W	S	=	X	Z	=	R
F	=	M	M	=	S	T	=	H			
G	=	N	N	=	E	U	=	T			

Figure 1



CIPHER ALPHABET
for the first letter

A = B	J = Z	S = X
B = V	K = C	T = H
C = G	L = W	U = T
D = Q	M = S	V = L
E = K	N = E	W = P
F = M	O = O	X = U
G = N	P = Y	Y = I
H = A	Q = F	Z = R
I = D	R = J	

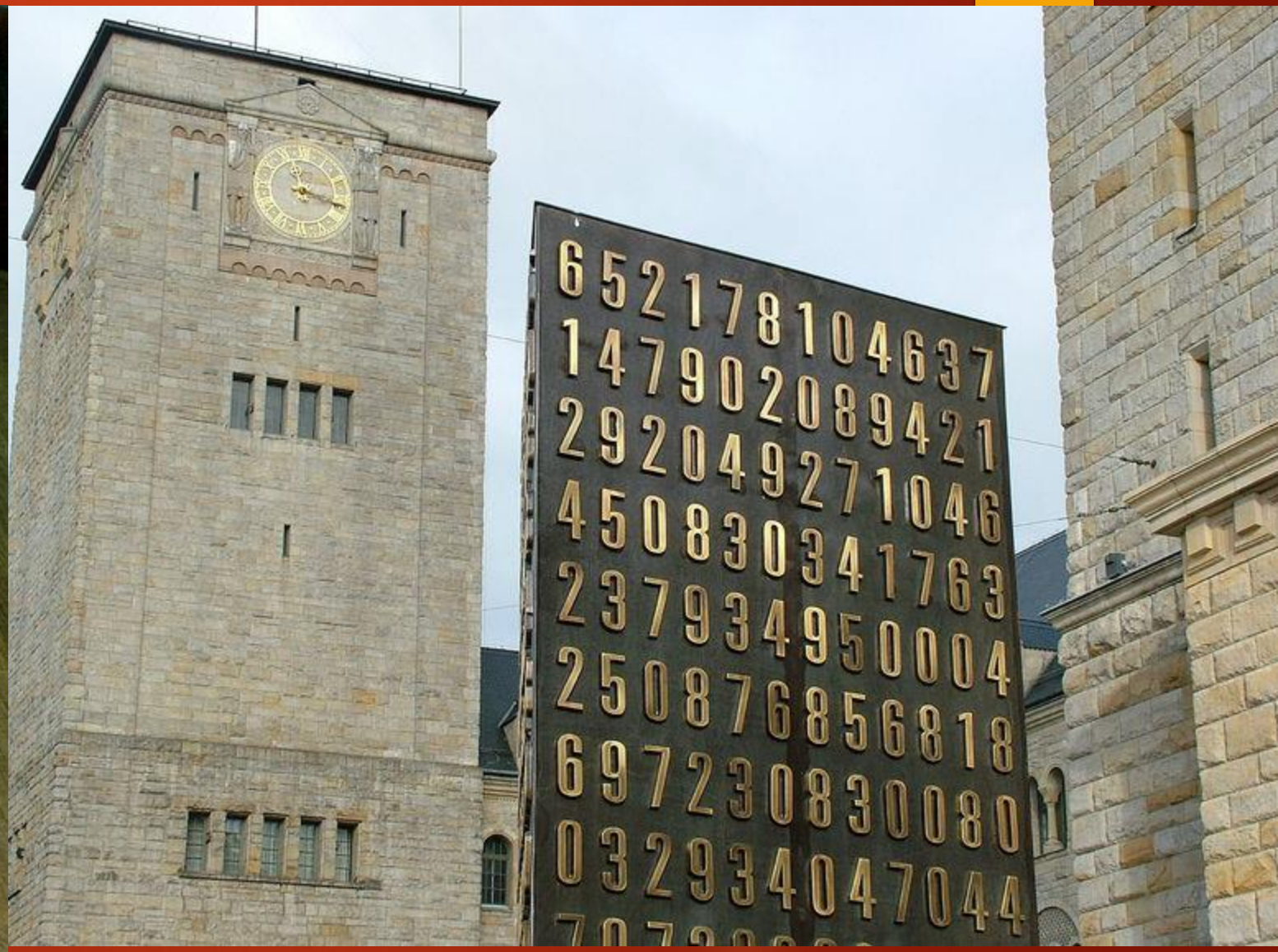
CIPHER ALPHABET
for the second letter

A = V	J = O	S = G
B = R	K = Q	T = M
C = A	L = Y	U = J
D = H	M = S	V = K
E = E	N = X	W = L
F = W	O = F	X = P
G = N	P = I	Y = B
H = D	Q = C	Z = T
I = U	R = Z	

Figure 2

Vigenère cipher

Enigma Machine



ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

4. ΚΡΥΠΤΟΛΟΓΙΑ

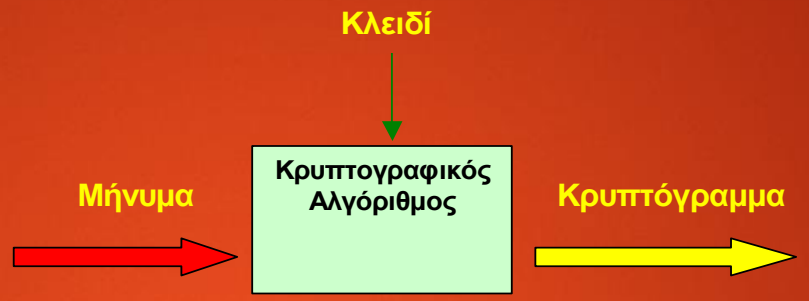
Κρυπτολογία : Είναι ο κλάδος που ασχολείται με τις αρχές της κρυπτογράφησης και της κρυπτανάλυσης.

ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

4. ΚΡΥΠΤΟΛΟΓΙΑ

Κρυπτογράφηση : είναι η τεχνική της μετατροπής των πληροφοριών, έτσι ώστε να είναι ακατάληπτες σε όλους, εκτός από αυτούς οι οποίοι γνωρίζουν την αντίστροφη διαδικασία.

ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ



Εικόνα 1- Κρυπτογράφηση ενός μηνύματος

Εικόνα 2 - Αποκρυπτογράφηση ενός μηνύματος

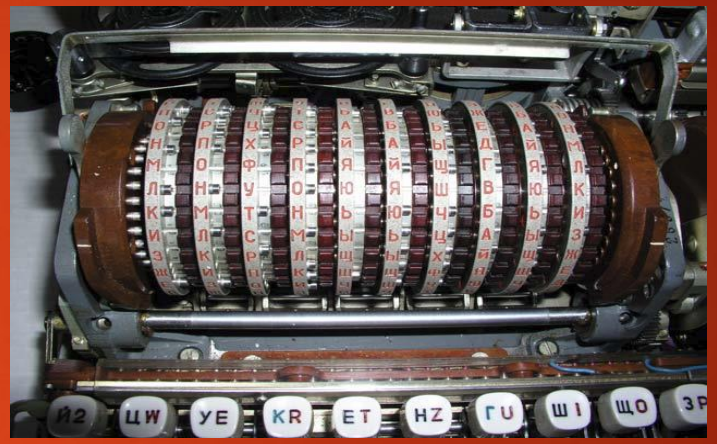
ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

4. ΚΡΥΠΤΟΛΟΓΙΑ

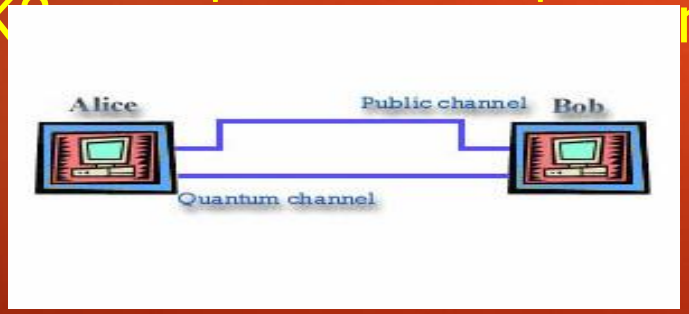
Κρυπτανάλυση : Είναι η μελέτη μεθόδων και τεχνικών για εξαγωγή αξιοποιήσιμης πληροφορίας από κρυπτογραφημένα δεδομένα, χωρίς αρχική γνώση του κλειδιού ή του συστήματος το οποίο χρησιμοποιήθηκε στην κρυπτογράφηση.

ΚΡΥΠΤΟΛΟΓΙΑ

- Χειρογραφικοί κώδικες
- Rotors
- Ψηφιακή κρυπτογράφηση
  - Συμμετρική (block, stream)
  - RSA, El Gamal
  - Hash codes



Κ η



ΑΡΧΕΣ του Kerckhoff

- Το σύστημα θα πρέπει να είναι πρακτικά αδιάσπαστο, αν όχι θεωρητικά αδιάσπαστο
- Πιθανή έκθεση του συστήματος δεν θα πρέπει να δημιουργεί πρόβλημα στην ασφάλεια. [Η ασφάλεια ενός κρυπτοσυστήματος θα πρέπει να βασίζεται στη γνώση των κλείδων και όχι στη γνώση του αλγορίθμου]
- Η κλείδα θα πρέπει να μπορεί να απομνημονευτεί
- Το κρυπτόγραμμα θα πρέπει να μπορεί να εκπεμφθεί με τηλέγραφο
- Η συσκευή κρυπτογράφησης θα πρέπει να είναι φορητή και λειτουργική από έναν χειριστή
- Το σύστημα θα πρέπει να είναι εύκολο στη χρήση και να μην απαιτεί απομνημόνευση πολύπλοκων κανόνων ή πληροφοριών

Η ασφάλεια ενός κρυπτοσυστήματος θα πρέπει να βασίζεται στη γνώση των κλείδων και όχι στη γνώση του αλγορίθμου]

- Δεν πρέπει να υπάρχει μυστικό τμήμα στα δομικά στοιχεία των αλγορίθμων.
- Το κλειστό κείμενο, οι χώροι κλείδων και το μήνυμα είναι ανοικτές πληροφορίες
- Χωρίς το σωστό κλειδί, η δυσκολία στην ανάκτηση του ανοικτού κειμένου από ένα κλειστό, είναι ένα πρόβλημα με δυσκολία όση το μήκος της κλείδας και μόνο.

ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

Όλοι οι κρυπτογραφικοί αλγόριθμοι επεξεργασίας πληροφοριών χωρίζονται σε δυο κατηγορίες:

1. Αμφίδρομοι κρυπτογραφικοί αλγόριθμοι, οι οποίοι ορίζουν τον ευθύ και τον αντίθετο μετασχηματισμό. Οι αμφίδρομοι κρυπτογραφικοί αλγόριθμοι χωρίζονται σε δυο υπό κατηγορίες:
   i. συμμετρικούς, στους οποίους χρησιμοποιείται το ίδιο κλειδί για την κρυπτογράφηση και για την αποκρυπτογράφηση πληροφοριών
   ii. μη συμμετρικούς, στους οποίους χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση πληροφοριών. Το κλειδί για την κρυπτογραφική ονομάζεται Δημόσια Κλειδί (Public Key) και για την αποκρυπτογράφηση Ιδιωτικό Κλειδί (Private Key).
2. Μη αμφίδρομοι κρυπτογραφικοί αλγόριθμοι (μονόδρομοι-One way), στους οποίους ορίζεται μόνο ο ευθύς μετασχηματισμός. Οι αλγόριθμοι αυτοί, γνωστοί και ως hash functions χρησιμοποιούνται ευρύτατα σε συστήματα ψηφιακών υπογραφών (digital signatures).

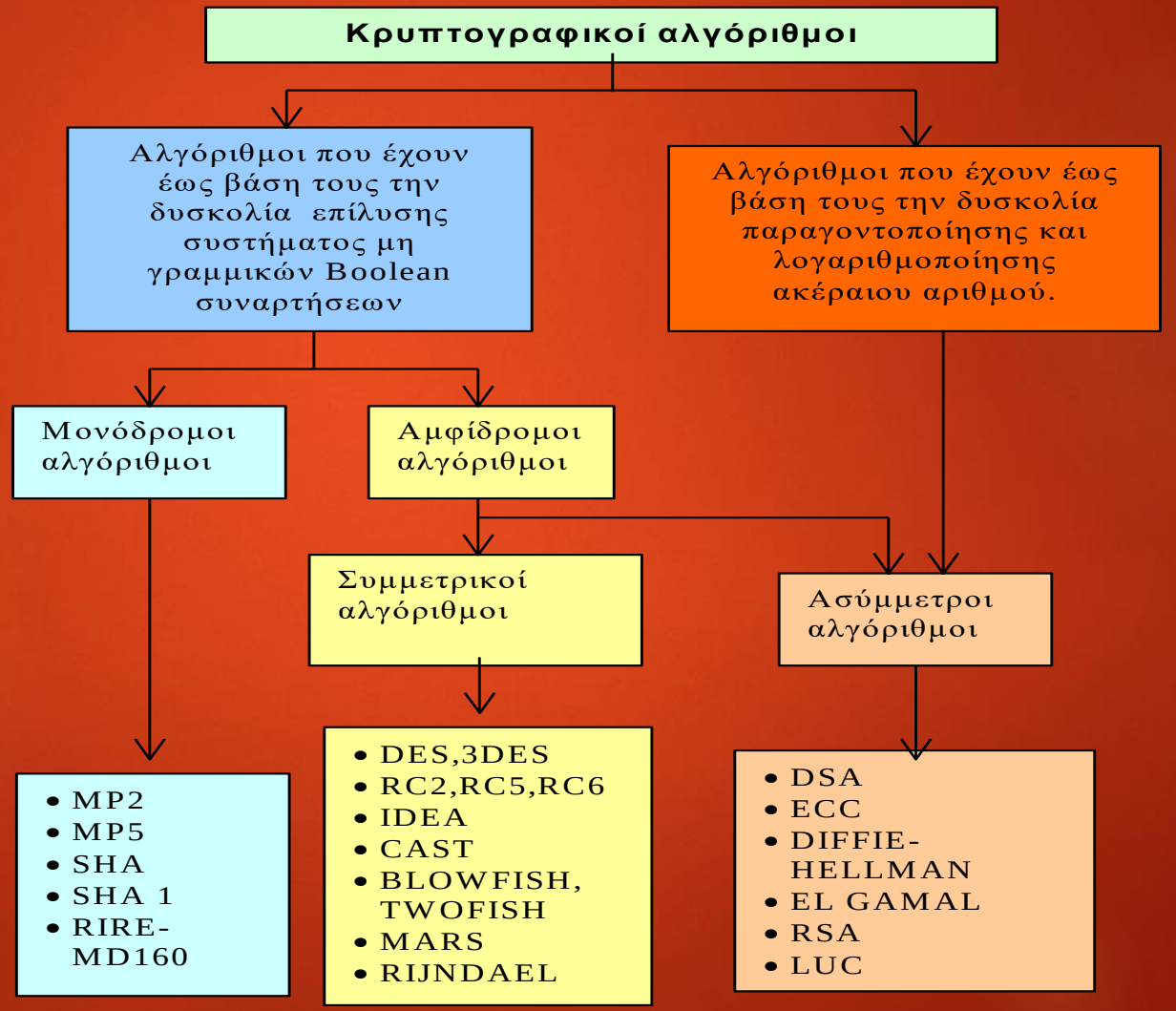
ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΗΛΕΚΤΡΟΝΙΚΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ

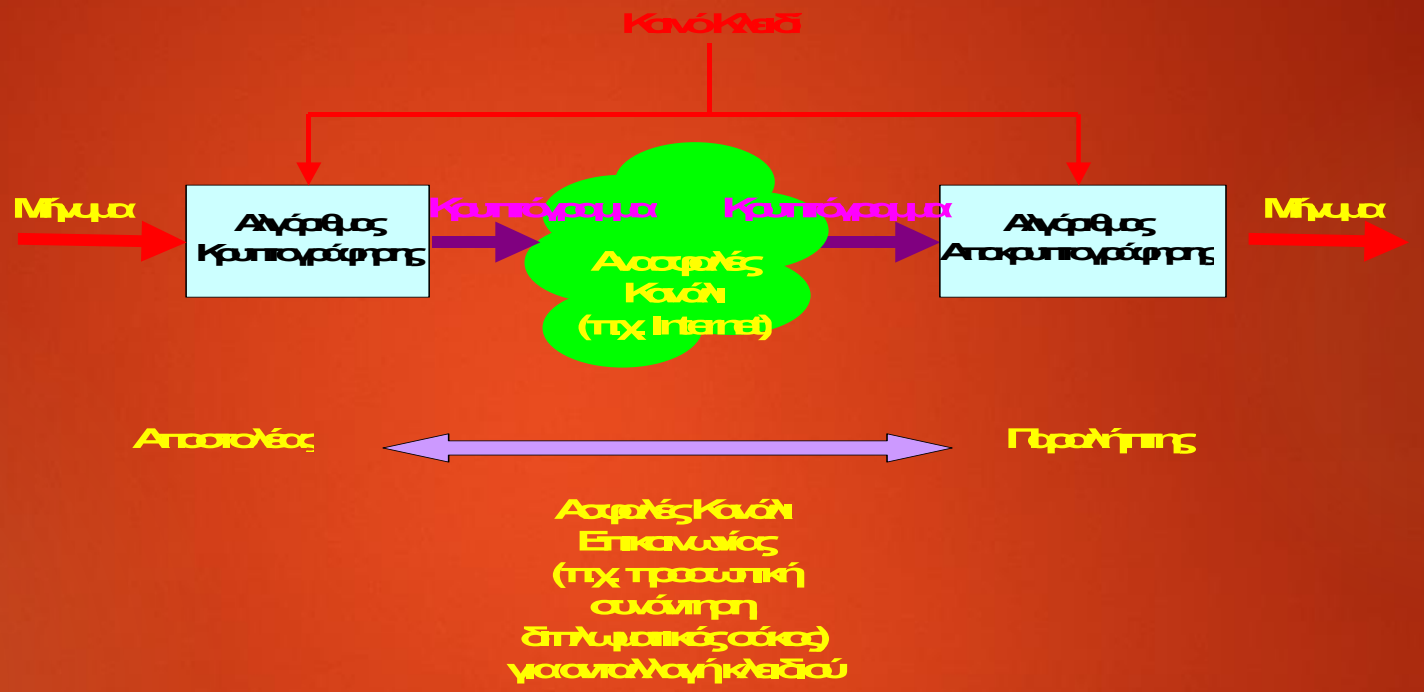
Συμμετρική	Ασύμμετρη
-Μυστική κλείδα.	-Δημόσια κλείδα και Προσωπική κλείδα.
-Ίδια κλείδα για κρυπτογράφηση και αποκρυπτο-γράφηση.	-Διαφορετικές κλείδες για κρυπτογράφηση και αποκρυπτογράφηση.

ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

Στο Σχήμα 3 παρουσιάζεται η τοπολογία των κρυπτογραφικών αλγόριθμων.



ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

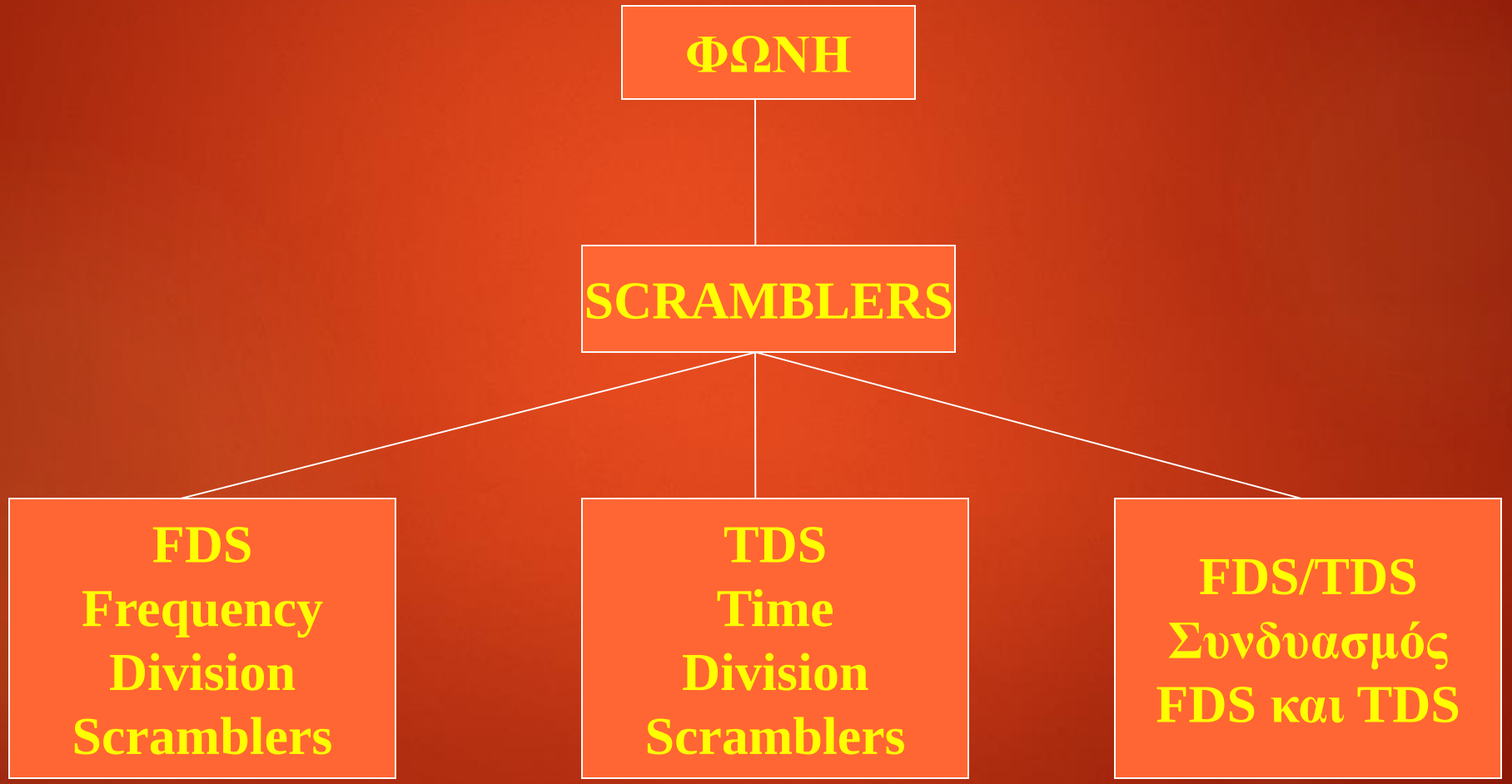


Εικόνα 4 – Η λειτουργία ενός συμμετρικού κρυπτοσυστήματος

ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ-1

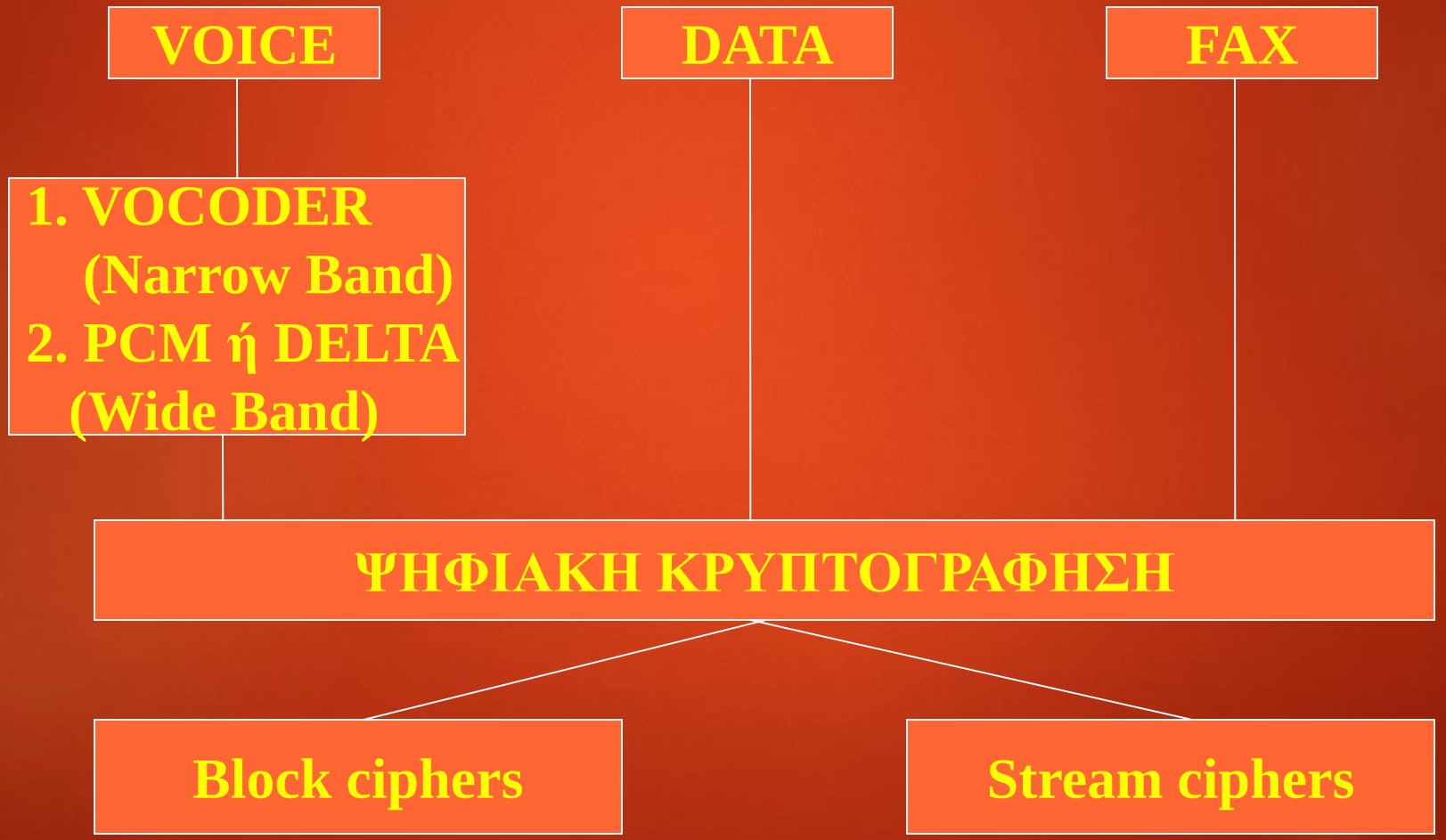
ΑΝΑΛΟΓΙΚΗ ΜΕΘΟΔΟΣ



ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

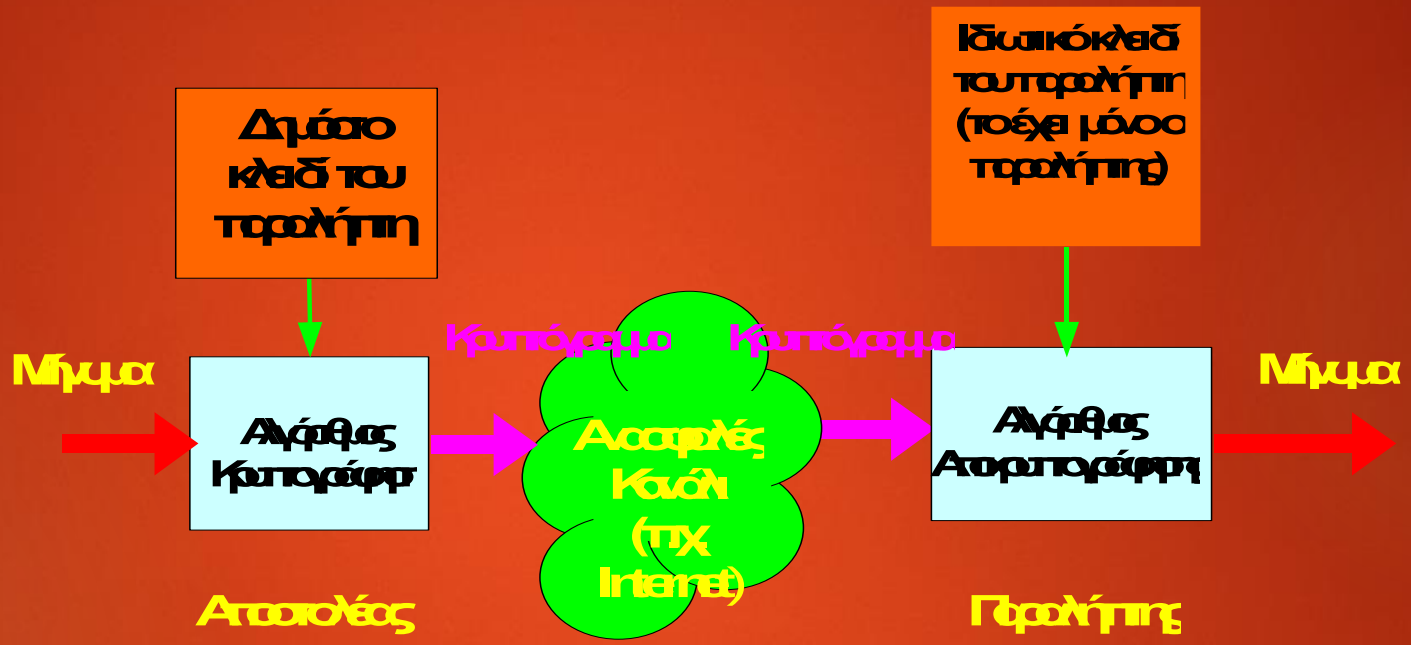
ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ-2

ΨΗΦΙΑΚΗ ΜΕΘΟΔΟΣ



ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ



ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Δύο ξεχωριστές κλείδες

1) **Δημόσια κλείδα (public key)**
2) **Προσωπική κλείδα (private key)**

Κρυπτογράφηση με την Δημόσια κλείδα Του παραλήπτη

Εκπομπή

Αποκρυπτογράφηση με την Προσωπική κλείδα Του παραλήπτη

ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ

(Αυθεντικότητα-Ακεραιότητα)

Αρχικό κείμενο

Υπολογισμός του hash code

Κρυπτογράφηση του hash code με την προσωπική κλείδα του αποστολέα και επισύναψη στο κείμενο

Αποστολή

Αποκρυπτογράφηση του hash code με την Δημόσια κλείδα του αποστολέα (έλεγχος αυθεντικότητας)

Υπολογισμός και σύγκριση των hash codes (έλεγχος ακεραιότητας)

ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΣΥΝΔΥΑΣΜΟΣΣΥΜΜΕΤΡΙΚΗΣ ΚΑΙ ΑΣΥΜΜΕΤΡΗΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

(Εμπιστευτικότητα-Αυθεντικότητα-Ακεραιότητα)

Αρχικό κείμενο

Παραγωγή του hash code (Ακεραιότητα)

Κρυπτογράφηση του hash code με την Προσωπική κλείδα του αποστολέα (Αυθεντικότητα)

Κρυπτογράφηση του κειμένου χρησιμοποιώντας Συμμετρική κλείδα μιας χρήσης (Εμπιστευτικότητα)

Κρυπτογράφηση της Συμμετρικής κλείδας Με χρήση της δημόσιας κλείδας του παραλήπτη

Αποστολή

ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΣΥΝΔΥΑΣΜΟΣΣΥΜΜΕΤΡΙΚΗΣ ΚΑΙ ΑΣΥΜΜΕΤΡΗΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

(Εμπιστευτικότητα-Αυθεντικότητα-Ακεραιότητα)

Αποκρυπτογράφηση Συμμετρικής κλείδας με χρήση Προσωπικής κλείδας του παραλήπτη

Αποκρυπτογράφηση του κειμένου με χρήση της συμμετρικής κλείδας

Αποκρυπτογράφηση του hash code με χρήση της Δημόσιας κλείδας του αποστολέα (έλεγχος αυθεντικότητας)

Υπολογισμός και σύγκριση των hash codes (έλεγχος ακεραιότητας)

ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

Κρυπτανάλυση

ΚΡΥΠΤΑΝΑΛΥΣΗ - 1

Ιστορική αναδρομή

1. Κώδικες μετάθεσης

-Ίδια συχνότητα γραμμάτων με το ανοικτό κείμενο.

-Μέθοδος αναγραμματισμού.

2. Κώδικες αντικατάστασης

-Πίνακες συχνότητας γραμμάτων.

-Δοκιμές με κοινές λέξεις.

3. Πολύαλφαβητικοί κώδικες.

-Μέθοδος Kasiski (1863).

4. Εναλλασσόμενες κλείδες.

-Μέθοδος της "πιθανής λέξης",
Bateries (1890) και Friedman (1918).

5. Σύνθετοι κώδικες (Rotors)

- μέθοδος της "επιλεγμένης λέξης"
(διάσπαση της Enigma, Β' Παγκόσμιος Πόλεμος)

6. Κρυπτανάλυση του DES (Diffie and Hellman , 1977)

7. Κρυπτανάλυση του DES (Διάσπαση σε 22.5 ώρες, 1999)

ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

Κρυπτανάλυση

Στόχοι – επιτυχίες της Κρυπτανάλυσης

- Διάκριση κρυπτογράφησης από θόρυβο
- Πιθανοκρατική εκμετάλλευση του κλειστού κειμένου
- Τοπική εξαγωγή ανοικτού κειμένου
- Γενική εξαγωγή ανοικτού κειμένου
- Ολική διάσπαση

Υπολογιστική Ισχύς που απαιτείται:

- Χρόνος
- Μνήμη
- Όγκος Δεδομένων

ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΚΡΥΠΤΑΝΑΛΥΣΗ - 2

Symmetric algorithms:
Boomerang attack
Brute force attack
Davies' attack
Differential cryptanalysis
Impossible differential cryptanalysis
Improbable differential cryptanalysis
Integral cryptanalysis
Linear cryptanalysis
Meet-in-the-middle attack
Mod-n cryptanalysis
Related-key attack
Sandwich attack
Slide attack
XSL attack

Classical cryptanalysis:
Frequency analysis
Index of coincidence
Kasiski examination

Hash functions:
Birthday attack
Rainbow table
Attack models
Chosen-ciphertext attack
Chosen-plaintext attack
Ciphertext-only attack
Known-plaintext attack
Side channel attacks:
Power analysis
Timing attack
Network attacks:
Man-in-the-middle attack
Replay attack
External attacks:
Black-bag cryptanalysis
Rubber-hose cryptanalysis

Αρχές της κρυπτογραφίας

- **απαιτήσεις ανάλογα με το είδος πληροφορίας [1]**

είδος πληροφορίας	χρονικός ορίζοντας	ελάχιστο μήκος κλειδιού
τακτικές πληροφορίες μάχης	**λεπτά/ώρες**	**56 - 64 bits**
ανακοινώσεις προϊόντων, επιτόκια	**εβδομάδες**	**64 bits**
επιχειρηματικά σχέδια	**έτη**	**64 bits**
εμπορικά μυστικά (πχ συνταγή Coca-Cola)	**δεκαετίες**	**112 bits**
τεχνολογία υδρογονοβόμβας (H-bomb)	**> 40 έτη**	**128 bits**
ταυτότητες κατασκόπων	**> 50 έτη**	**128 bits**
διπλωματικά επεισόδια	**> 65 έτη**	**> 128 bits**
απογραφές πληθυσμού	**> 100 έτη**	**> 128 bits**

1 → **Applied Cryptography, 2nd** Edition **Bruce Schneier,** John Wiley & Sons, 1996, **ISBN** 0-471-11709-9

Μεγέθη κρυπτανάλυσης

- **πολύ μεγάλοι & πολύ μικροί αριθμοί**

φυσικό μέγεθος	τάξη
η πιθανότητα να σκοτωθείς από κεραυνό (στις ΗΠΑ ανά ημέρα)	2^{-33}
η πιθανότητα να κερδίσεις το πρώτο βραβείο στο λόττο (στις ΗΠΑ)	2^{-22}
η πιθανότητα πνιγμού στις ΗΠΑ (ανά έτος)	2^{-16}
ο χρόνος ημιζωής του άνθρακα - 14	2^{+12} έτη
ο χρόνος μέχρι τον επόμενο παγετώνα	2^{+14} έτη
η ηλικία του πλανήτη Γη	2^{+32} έτη
ο χρόνος, ώσπου να σβήσει (εκραγεί) ο ήλιος	2^{+32} έτη
η ηλικία του σύμπαντος	2^{+34} έτη
το πλήθος ατόμων στον πλανήτη Γη	2^{+170}
το πλήθος ατόμων στο γαλαξία μας (Milky Way ☺)	2^{+223}
η ενέργεια που ακτινοβολεί ο ήλιος σε ένα έτος	$3 \times 10^{+27}$ kWh
ο χρόνος, ώσπου η ύλη να καταρρεύσει (αν το σύμπαν είναι ανοικτό)	10^{+1076} έτη

Μεγέθη κρυπτανάλυσης

- **Παράδειγμα:**
  - έστω ένα σύστημα κρυπτογραφημένο με κλειδί μήκους **256 bits**
  - για μια απευθείας επίθεση στο σύστημα θα απαιτηθεί μετρητής (counter) ίσου μήκους (δηλαδή 256 bits)
    - για να παράγει όλες τις δυνατές τιμές του κλειδιού
  - αν η μετάβαση του μετρητή από την τιμή **N** στην **N+1**
    - διαρκεί **1 ns** και κοστίζει σε ενέργεια **1 eV** (~4.45×10^{-26} kWh)
  - τότε μόνο για τη δημιουργία των δυνατών κλειδιών:
    - θα παρέλθουν **$3{,}67 \times 10^{60}$ έτη > ηλικία του σύμπαντος**
    - θα καταναλωθούν **$5{,}15 \times 10^{51}$ kWh > συνολική ενέργεια που θα έχει εκπέμψει ο ήλιος σε όλη τη διάρκεια ζωής του**

ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΚΡΥΠΤΑΝΑΛΥΣΗ - 3

Μέθοδος των εξαντλητικών δοκιμών

(Απαιτούμενος χρόνος με χρήση Η/Υ)

Μέγεθος κλειδιού	**Απλή έρευνα**		**Παράλληλη έρευνα (10)**	
(bits)	1ms	1 μs	1ms	1 μs
24	2.33 h	8.4 s	8.4 ms	8.4 ns
32	24.9 d	35.8 m	2.15 s	2.15 ms
40	17.4 y	6.4 d	9.2 m	550 ms
48	>100 y	4.46 y	1.63 d	2.35 m
56		>100 y	1.14 y	10.0 h
64			>100 y	107 d
70				18,7 y
128				>> 100 y

Πίνακας 1: Κρυπτανάλυση με εξαντλητική έρευνα

ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΚΡΥΠΤΑΝΑΛΥΣΗ - 4

Μέτρα εναντίον της Κρυπτανάλυσης

α) Επικαιροποιημένη χρήση κρυπτογραφικών πρωτοκόλλων.

β) Επικαιροποιημένη χρήση κρυπτογραφικών αλγορίθμων

γ) Επικαιροποιημένη χρήση κρυπτογραφικών παραμέτρων

γ) Παραγωγή, χρήση και συχνή αλλαγή κλείδων.

δ) Επικρυπτογράφηση.