ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Ασφάλεια Πληροφοριακών Συστημάτων

«Κρυπτογραφικά Συστήματα»

Τμήμα Πληροφορικής

Επ. Καθ. Π.Κοτζανικολάου
pkotzani@unipi.gr

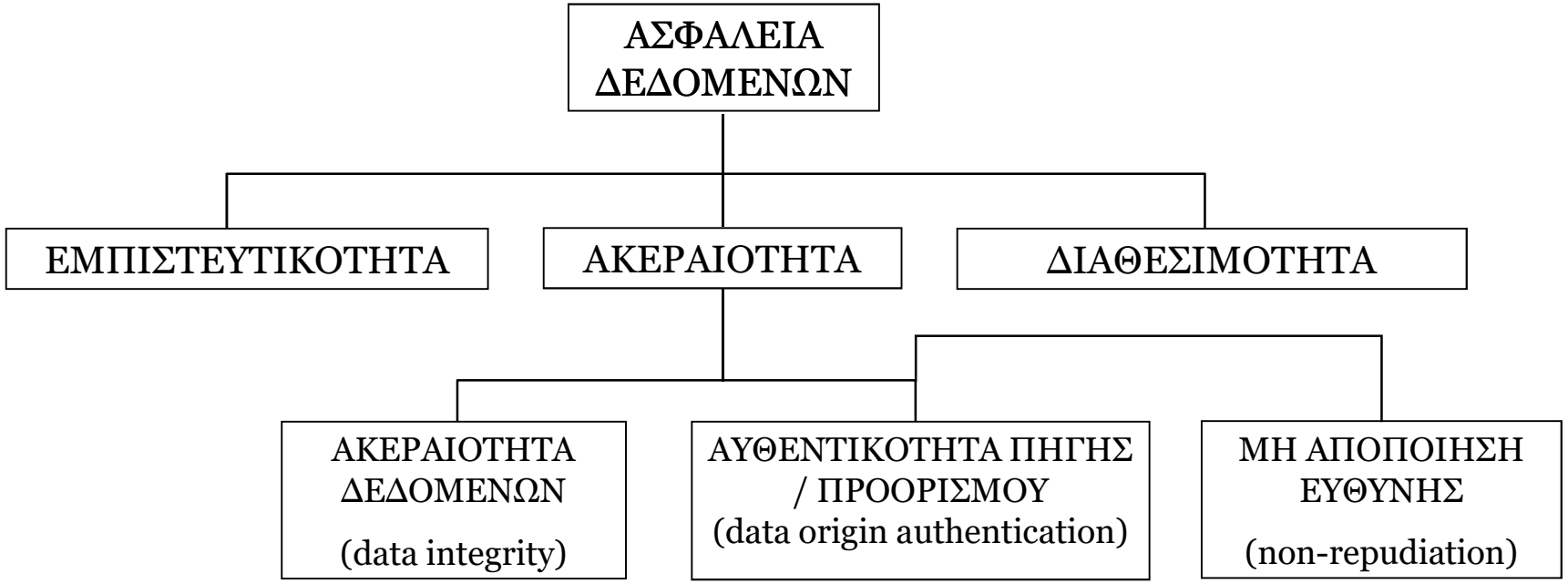
2η θεματική ενότητα

2. Κρυπτογραφικά συστήματα

- **Εισαγωγή**
- Μονόδρομες συναρτήσεις
- Κρυπτοσυστήματα μοναδιαίας κλείδας (συμμετρική κρυπτογράφηση)
- Κρυπτοσυστήματα δημόσιας κλείδας (ασύμμετρη κρυπτογράφηση)
- Υβριδικά συστήματα

Στόχοι της κρυπτογραφίας

- (Handbook of Applied Cryptography): *"Cryptography is the study of mathematical techniques related to aspects of information security such as* ***confidentiality***, ***data integrity***, ***authentication*** *and* ***non-repudiation****»*



Βασικοί όροι

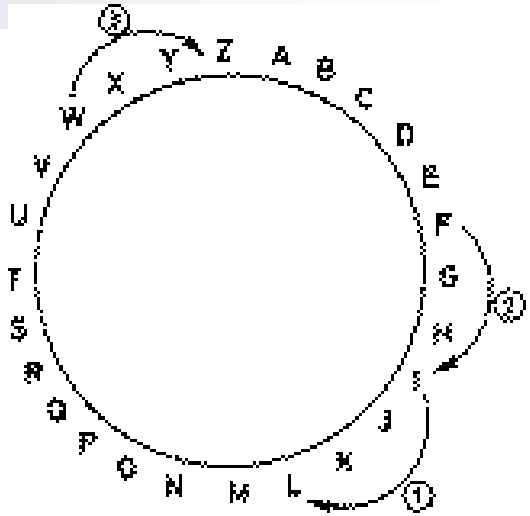
- Κρυπτογραφία: *Κρυπτόν & Γράφειν*
  - Σκοπός: Η επικοινωνία δύο οντοτήτων (π.χ. Alice και Bob) διαμέσου ενός μη ασφαλούς καναλιού, με ασφαλή τρόπο.
- Αλγόριθμος κρυπτογράφησης (encryption algorithm):
  - δέχεται ως είσοδο ένα αρχικό μήνυμα (plaintext) και δίνει στην έξοδο ένα τροποποιημένο μήνυμα (ciphertext)
- Αλγόριθμος αποκρυπτογράφησης (decryption algorithm):
  - δέχεται ως είσοδο ένα κρυπτογραφημένο μήνυμα (ciphertext) και δίνει στην έξοδο το αρχικό μήνυμα (plaintext)

Κλασσικοί κρυπτογραφικοί αλγόριθμοι

1. Αλγόριθμοι Αντικατάστασης (Substitution ciphers)
   - Κάθε χαρακτήρας (ή ομάδα χαρακτήρων) του αρχικού μηνύματος αντικαθίσταται από ένα άλλο συγκεκριμένο χαρακτήρας (ή ομάδα χαρακτήρων)

2. Αλγόριθμοι Αντιμετάθεσης (Transposition ciphers)
   - Κάθε χαρακτήρας του αρχικού κειμένου λαμβάνει μία άλλη θέση στο κρυπτογραφημένο μήνυμα (αναγραμματισμός του αρχικού μηνύματος)

Αλγόριθμοι Αντικατάστασης (Substitution)



- Ο αλγόριθμος του Καίσαρα (Ceasar cipher)
  - Αντικατάσταση ολίσθησης
- Αλγόριθμος Κρυπτογράφησης

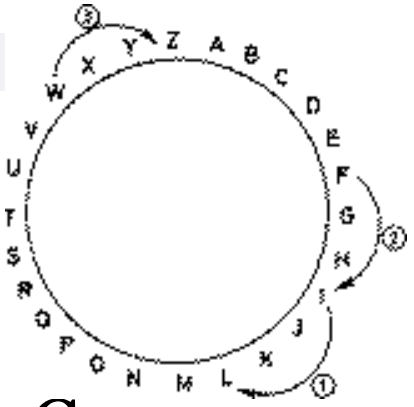
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	K	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Αλγόριθμος Αποκρυπτογράφησης

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

- Παράδειγμα:
  - Αρχικό μήνυμα: I CAME I SAW I CONQUERED
  - Κρυπτογραφημένο μήνυμα: L FDPH L VDZ L FRQTXHUHG

Ο αλγόριθμος ολίσθησης (The shift cipher)



- Η γενικότερη περίπτωση του αλγόριθμου Ceasar
  - Κρυπτογράφηση: $E_K(x) = x + K \bmod 26$
  - Αποκρυπτογράφηση: $D_K(x) = x - K \bmod 26$
- Πίνακας αντιστοίχησης γραμμάτων σε αριθμούς στην ομάδα 0-25 (Z_{25})

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

- Έστω ότι
  - K = 11 και M= we will meet at midnight
  - M = 22 4 22 8 11 11 12 4 4 19 0 19 12 8 3 13 8 13 …

The Shift cipher

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

- Προσθέτουμε το 11 (modulo 26) σε κάθε αριθμό

M = 22 4 22 8 11 11 12 4 4 19
0 19 12 8 3 13 8 6 7 19

C = 7 15 7 19 22 22 23 15 15 4
11 4 23 19 14 24 19 17 18 4

- Μετατρέπουμε σε αλφαβητικούς χαρακτήρες

HPHTWWXPPELEXTOYTRSE

- Αντίστοιχα για την αποκρυπτογράφηση
  - (- 11 (modulo 26)

The Shift cipher

- Ο αλγόριθμος shift δεν είναι ασφαλής
  - Αριθμός πιθανών κλειδιών: **26 κλειδιά**
- Ο «εχθρός» μπορεί εύκολα να δοκιμάσει όλα τα κλειδιά
- Κρυπτογράφημα (ciphertext) – mjaiamwlxsvitpegipixxiv
- Δοκιμή1: lizhzlvkwruhsodfhohwwhu (αποκρυπτογράφηση με K=1)
- Δοκιμή2: khygykujvotgrncegngvvgt (αποκρυπτογράφηση με K=2)
- Δοκιμή3: jgxfxjtiupsfombdfmfuufs (αποκρυπτογράφηση με K=3)
- Μήνυμα: ifwewishtoreplaceletter (αποκρυπτογράφηση με K=4)

Ο αλγόριθμος αντικατάστασης (The substitution cipher)

- Κάθε γράμμα αντικαθίσταται με ένα άλλο μοναδικό γράμμα (1-1 αντικατάσταση)

Κρυπτογράφηση

a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*
X	*N*	*Y*	*A*	*H*	*P*	*O*	*G*	*Z*	*Q*	*W*	*B*	*T*

n	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*
S	*F*	*L*	*R*	*C*	*V*	*M*	*U*	*E*	*K*	*J*	*D*	*I*

Αποκρυπτογράφηση

A	B	C	D	E	F	G	H	I	J	K	L	M
d	l	r	y	v	o	h	e	z	x	w	p	T

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	g	f	j	q	n	m	u	s	k	a	c	i

- Πλήθος πιθανών κλειδιών: Όσες οι αναδιατάξεις 26 στοιχείων

  $26! = (4 \text{ X } 10^{26})$

Αλγόριθμοι Αντιμετάθεσης (Transposition)
The Permutation cipher

- Οι θέσεις των γραμμάτων του μηνύματος, αλλάζουν με βάση την αναδιάταξη που ορίζει ένα κλειδί
- Έστω το κλειδί K είναι η ακόλουθη αναδιάταξη (μεγέθους 6)

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

- Έστω ότι το αρχικό μήνυμα είναι shesellsseashellsbytheseashore
- Χωρίζουμε το μήνυμα σε ομάδες έξι χαρακτήρων

  shesel lsseas hellsb ythese ashore

- Εφαρμόζοντας την αναδιάταξη, το κρυπτογράφημα γίνεται:

  EESLSH SALSES LSHBLE HSYEET HRAEOS

- Αποκρυπτογράφηση: χρήση της αντίστροφης αναδιάταξης K^{-1}

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

Σύγχρονη κρυπτογραφία

- Βασίζεται στην αρχή του Kerckhoff
  - Οι αλγόριθμοι είναι δημόσια γνωστοί
  - Η μόνη πληροφορία που παραμένει μυστική είναι ένα «*κλειδί*» κρυπτογράφησης ή/και αποκρυπτογράφησης
    - Αποκάλυψη κλειδιού = «σπάσιμο» ασφάλειας
    - Το μήκος του κλειδιού καθορίζει το επίπεδο ασφάλειας

Κρυπτοσύστημα (Cryptosystem)

1. Αλγόριθμος Κρυπτογράφησης (encryption algorithm)
2. Αλγόριθμος Αποκρυπτογράφησης (decryption algorithm)
3. Αλγόριθμος παραγωγής κλειδιού κρυπτογράφησης (key generation)
4. Κλειδί(α) κρυπτογράφησης (το μόνο μυστικό) (encryption /decryption key)

Βασικοί όροι

- Κρυπτογραφικό κλειδί: συμβολοσειρά πεπερασμένου μήκους
  - Παράμετρος στους αλγόριθμους κρυπτογράφησης και αποκρυπτογράφησης
- Αλγόριθμος κρυπτογράφησης ***E***:
  - Δέχεται ως είσοδο ένα μήνυμα ***M*** (plaintext) και ένα κλειδί K_A, και δίνει στην έξοδο ένα κρυπτογραφημένο μήνυμα ***C*** (ciphertext)

$$C = E_{K_A}(M)$$

Βασικοί όροι

- Αλγόριθμος αποκρυπτογράφησης ***D***:
  - Δέχεται ως είσοδο ένα κρυπτογραφημένο μήνυμα ***C*** (ciphertext) και το κλειδί K_B, και δίνει στην έξοδο το αρχικό μήνυμα ***M*** (plaintext)

$$M = D_{K_B}(C)$$

Μοντέλα ασφάλειας

- Άνευ όρων ασφάλεια (Unconditional security)
- Υπολογιστική ασφάλεια (Computational security)
- Αποδείξιμη ασφάλεια (Provable security)
- Ευρεστική ασφάλεια (Heuristic security)

Άνευ όρων ασφάλεια (Unconditional security)

- Ένα κρυπτοσύστημα είναι άνευ όρων ασφαλές, εάν:
  1. Ο αντίπαλος (adversary) έχει *απεριόριστη υπολογιστική ισχύ* στη διάθεσή του (συνεπώς η ασφάλεια είναι ανεξάρτητη των δυνατοτήτων του).
  2. Το κρυπτογράφημα δεν παρέχει καμία πληροφορία σχετικά με το αρχικό κείμενο.
- (Σχεδόν) αδύνατο.
  - Παράδειγμα αλγορίθμου: **one-time pad.**
  - Πρακτικές δυσκολίες στην εφαρμογή του.

Ο Αλγόριθμος one-time pad

- Οι δύο χρήστες έχουν ανταλλάξει ένα σύνολο από τυχαία κλειδιά με τις εξής ιδιότητες:
  - Κάθε κλειδί είναι μίας χρήσης
  - Αν K_i είναι το i-στο κλειδί και M_i i-στο αρχικό μήνυμα (plaintext) τότε $\mathbf{|K_i| = |M_i|}$
- Αλγόριθμος κρυπτογράφησης
  - $\mathbf{C_i = M_i \ XOR \ K_i}$
- Αλγόριθμος αποκρυπτογράφησης
  - $\mathbf{M_i = C_i \ XOR \ K_i}$

Υπολογιστική ασφάλεια (Computational security)

- Ένα κρυπτοσύστημα έχει υπολογιστική ασφάλεια, εάν:
  - Η επεξεργαστική ισχύς που θα χρειαζόταν ο αντίπαλος για να το παραβιάσει, *είναι σημαντικά μεγαλύτερη από την εκτιμώμενη υπολογιστική ισχύ που έχει στη διάθεσή του*.
- Λιγότερο ασφαλές αλλά πρακτικό και υλοποιήσιμο.

Αποδείξιμη ασφάλεια (Provable security)

- Επέκταση του προηγούμενου μοντέλου.
  - Η δυσκολία της παραβίασης μπορεί να αναχθεί σε κάποιο γνωστό δύσκολο πρόβλημα.
  - Η παραβίαση της ασφάλειας του αλγορίθμου είναι (τουλάχιστον) τόσο δύσκολη, όσο η επίλυση του προβλήματος.
- Συνήθως χρησιμοποιούνται προβλήματα θεωρίας αριθμών.
  - Παραγοντοποίηση ακεραίων.
  - Εύρεση διακριτού λογαρίθμου.

Ευρεστική ασφάλεια (Heuristic security)

- **Δεν υπάρχει κάποια απόδειξη** της ασφάλειας του κρυπτογραφικού αλγορίθμου/πρωτοκόλλου.
- Υπάρχει μόνο κάποια **ένδειξη της ασφάλειας** του αλγορίθμου **έναντι σε γνωστές επιθέσεις.**
- Αρκετά ασθενές μοντέλο, αλλά καλύτερο από το τίποτα.

Κρυπτανάλυση

- Κρυπτολογία (Cryptology) = Κρυπτογραφία + Κρυπτανάλυση
  - Κρυπτανάλυση (Cryptanalysis): Μελέτη μεθόδων για την ανάκτηση του αρχικού μηνύματος M, *χωρίς πρόσβαση στο κλειδί κρυπτογράφησης K*.
- Κρυπτανάλυση μονο-αλφαβητικών αλγορίθμων
  - Στατιστική ανάλυση της γλώσσας του αρχικού κειμένου
  - Διαφορετικές πιθανότητες εμφάνισης για κάθε γράμμα της αλφαβήτου

Συχνότητα Εμφάνισης (Ελληνικά)

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

letter	probability	letter	probability
A	0.082	N	0.067
B	0.015	O	0.075
C	0.028	P	0.019
D	0.043	Q	0.001
E	0.127	R	0.060
F	0.022	S	0.063
G	0.020	T	0.091
H	0.061	U	0.028
I	0.070	V	0.010
J	0.002	W	0.023
K	0.008	X	0.001
L	0.040	Y	0.020
M	0.024	Z	0.001

Συχνότητα (Αγγλικά)

- Πιθανότητες εμφάνισης γραμμάτων
  - E, - με πιθανότητα ~ 0.120
  - T, A, O, I, N, S, H, R - με πιθανότητα (0.06-0.09)
  - D, L – με πιθανότητα ~ 0.04
  - C, U, M, W, F, G, Y, P, B - με πιθανότητα (0.015 – 0.028)
  - V, K, J, X, Q, Z – με πιθανότητα < 0.01
- Διπλών χαρακτήρων
  - TH ,HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OF
- Τριπλών χαρακτήρων
  - THE, ING, AND, HER, ERE, END,
  - THA NTH, WAS, ETH, FOR, DTH

Κρυπτανάλυση του αλγόριθμου κρυπτογράφησης "Substitution Cipher"

- Φτιάχνουμε έναν πίνακα συχνοτήτων εμφάνισης
- Ο πιο «συχνός» χαρακτήρας: Z
  - Υποθέτουμε ότι D(Z) = e
- Οι αμέσως πιο «συχνοί» χαρακτήρες
  - {M, C, D, F, J, R, Y, N}
- Συνέχεια εξετάζουμε τα δίψηφα που εμφανίζονται πιο συχνά
  - ZW, DZ (4 φορές)
    - Το ZW εμφανίζεται συχνά, το WZ καθόλου, ενώ το W σπάνια
      - Αρα, «ίσως» D(W)= d
  - NZ, ZU (3 φορές)
    - …

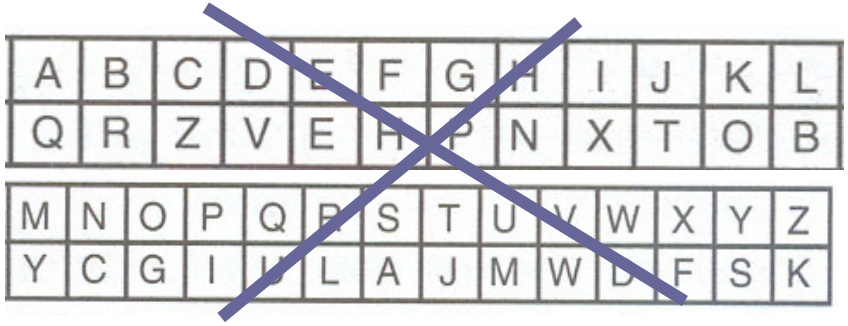
Κρυπτανάλυση του αλγόριθμου κρυπτογράφησης "Substitution Cipher"

```
          end                  e       ne dh   e
YIFQF MZRWQ FYVEC FMDZP CVMRZ WNMDZ VEJBT
          h            e       e           nh d
XCDDU MJNDI FEFMD ZCDMQ ZKCEY FCJMY RNCWJ
   en      e   h  eh       n          n        ed
CSZRE XCHZU NMXZN ZUCDR JXYYS MRTME YIFZW
    e     e    ne nd he e     ed        n h    h
DYVZV YFZUM RZCRW NZDZJ JXZWG CHSMR NMDHN
          e       ed           d  he    n
CMFQC HZJMX JZWIE JYUCF WDJNZ DIR
```

- "Ισως" D(C) = A
- ...

Κρυπτανάλυση με χρήση προηγούμενων γνωστών μηνυμάτων (Known-plaintext attack)

- Έστω ότι ο αλγόριθμος κρυπτογράφησης είναι «ασφαλής»



- Ασφάλεια του κρυπτοσυστήματος
  - Στόχος: Ο μόνος τρόπος για να παραβιαστεί, είναι η δοκιμή όλων των πιθανών κλειδιών
    - Υπολογιστική Ασφάλεια

- Επίθεση «Known-Plaintext»
  1. Η Eve διαθέτει ένα ή περισσότερα κρυπτογραφημένα μηνύματα, και τα αντίστοιχα αρχικά μηνύματα !
  2. Στη συνέχεια η Eve δοκιμάζει όλα τα πιθανά κλειδιά (brute force)
- Πολυπλοκότητα της επίθεσης;
  - Ανάλογη με το μήκος του κλειδιού
  - 128 bit: Τρέχον standard για συμμετρική κρυπτογράφηση

Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.

Αλγόριθμοι μυστικού κλειδιού

Ασφάλεια Αλγορίθμων

Average Time Estimates for a Hardware Brute-Force Attack in 1995

Length of Key in Bits						
Cost	**40**	**56**	**64**	**80**	**112**	**128**
$100 K	2 seconds	35 hours	1 year	70,000 years	10^{14} years	10^{19} years
$1 M	.2 seconds	3.5 hours	37 days	7000 years	10^{13} years	10^{18} years
$10 M	.02 seconds	21 minutes	4 days	700 years	10^{12} years	10^{17} years
$100 M	2 milliseconds	2 minutes	9 hours	70 years	10^{11} years	10^{16} years
$1 G	.2 milliseconds	13 seconds	1 hour	7 years	10^{10} years	10^{15} years
$10 G	.02 milliseconds	1 second	5.4 minutes	245 days	10^{9} years	10^{14} years
$100 G	2 microseconds	.1 second	32 seconds	24 days	10^{8} years	10^{13} years
$1 T	.2 microseconds	.01 second	3 seconds	2.4 days	10^{7} years	10^{12} years
$10 T	.02 microseconds	1 millisecond	.3 second	6 hours	10^{6} years	10^{11} years

AES Cryptanalysis

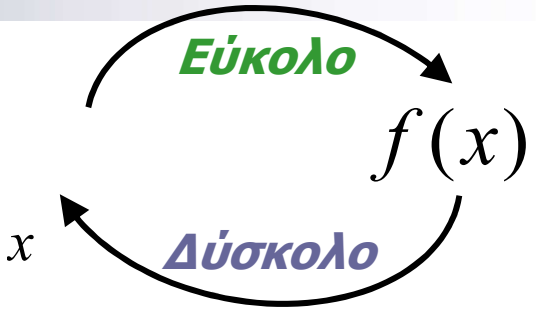
"… Actually you have 2^127*(time for AES operation) time, the 127 is in place of the 128 because on average you will only need to work through half the key space. So assuming you can perform 2^56 AES operations per second (and this itself an exceedingly fast rate) it would take 2^127/2^56 seconds, this works out to 75,000,000,000,000 years. I do not consider the project to have an achievable timeframe for success. This is the best cryptoanalysts know how to do with AES right now; for security this is a good thing, for your project it is a bad thing.. "

Joe Ashwood

2. Κρυπτογραφικά συστήματα

- Εισαγωγή
- **Μονόδρομες συναρτήσεις**
- Κρυπτοσυστήματα μοναδιαίας κλείδας (συμμετρική κρυπτογράφηση)
- Κρυπτοσυστήματα δημόσιας κλείδας (ασύμμετρη κρυπτογράφηση)
- Υβριδικά συστήματα

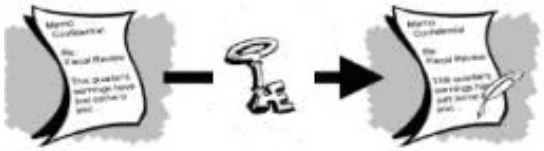
Μονόδρομες Συναρτήσεις (One-way functions)



- Εύκολος ο υπολογισμός, δύσκολη η αντιστροφή
- Ποια θα μπορούσε να είναι η χρήση των μονόδρομων συναρτήσεων?
  - Κρυπτογράφηση;
  - … κανείς δεν θα μπορούσε να αποκρυπτογραφήσει το μήνυμα !
- Χρειαζόμαστε ***μονόδρομες συναρτήσεις κρυφής εισόδου*** (trapdoor one way functions)
  - Αντιστροφή: Δύσκολη, εκτός και εάν κάποιος γνωρίζει τη μυστική πληροφορία (trapdoor information)
  - Οι αλγόριθμοι κρυπτογραφίας βασίζονται στην ύπαρξή τους
    - Η μυστική πληροφορία είναι το κρυπτογραφικό κλειδί

Κρυπτογραφικές συναρτήσεις κατακερματισμού (hash functions)

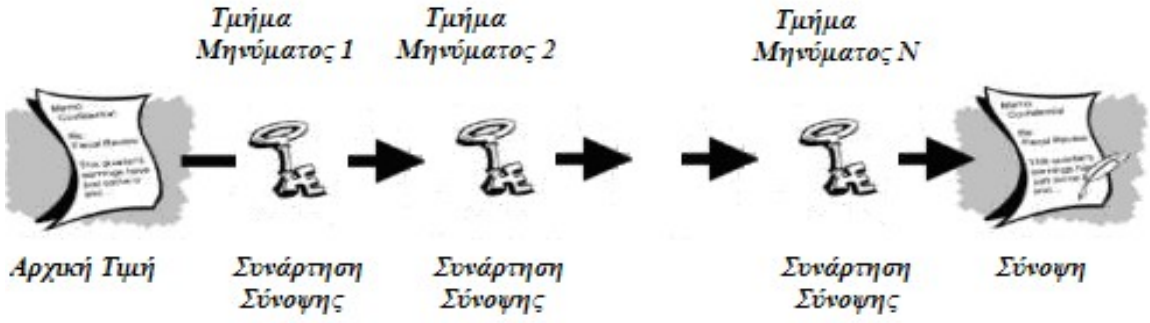
- Μονόδρομη συνάρτηση ***H*** με τις εξής ιδιότητες:
  - Συμπίεση εισόδου: Για είσοδο μήνυμα ***m*** μεταβλητού μήκους, επιστρέφει έξοδο ***h = H(m)*** σταθερού μήκους.
  - Για κάθε ***m*** είναι εύκολο να υπολογιστεί η τιμή ***h= H(m)***
  - Ανθεκτική σε συγκρούσεις (collision-resistant):
    - Για μία συγκεκριμένη τιμή ***h*** είναι υπολογιστικά δύσκολο να βρεθεί τιμή ***m*** τέτοια ώστε ***H(m) = h***
    - Είναι **δύσκολο** να βρεθούν δύο τιμές εισόδου ***m≠m΄*** τέτοιες ώστε ***H(m) = H(m΄)***



Αρχικό Κείμενο *Συνάρτηση Κατακερματισμού* *Σύνοψη*

Συναρτήσεις συμπίεσης

- Βήματα Συναρτήσεων Συμπίεσης:
  - Το αρχικό μήνυμα ***M*** (οποιουδήποτε μήκους) χωρίζεται σε τμήματα (blocks) καθορισμένου μήκους $\boldsymbol{m_1, m_2, ..., m_k,}$
  - Το μήκος του block εξαρτάται από τη συνάρτηση. Το αρχικό μήνυμα συμπληρώνεται (padded) για λόγους ασφαλείας, ώστε το μήκος του μηνύματος να είναι πολλαπλάσιο του μήκους του block.
  - Κάθε block $\boldsymbol{m_i}$ του αρχικού μηνύματος *περνά από τη συνάρτηση συμπίεσης* και λαμβάνεται έξοδος *περιορισμένου μήκους.*
    - $Hash(m_i) = h_i,$ *για κάθε* $i \in [1, k]$.
    - $Hash(M) = h_1 \; XOR \; h_2 \; ... \; XOR \; h_k$



Αλγόριθμοι συναρτήσεων hash

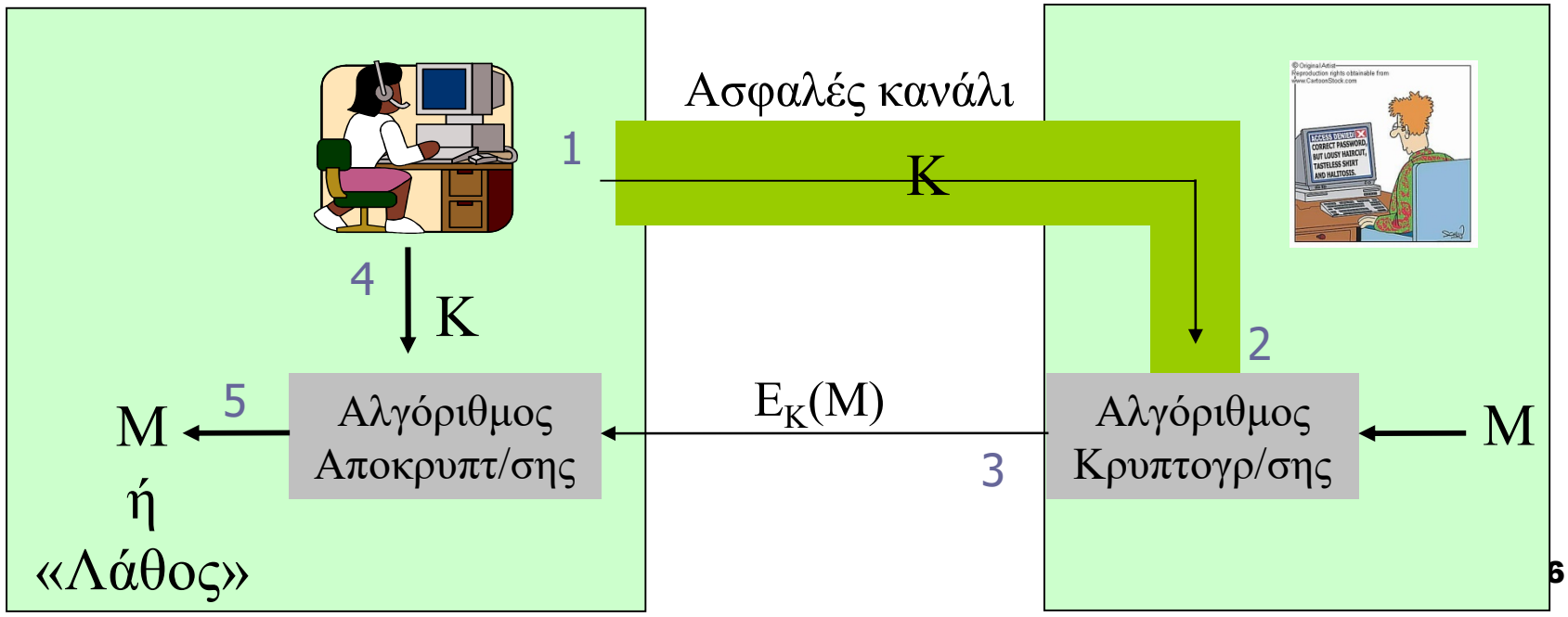
- SHA, SHA-1, SHA-2, SHA-3 (Secure Hash Algorithm)
  - Οι SHA και SHA-1 αναπτύχθηκαν από το NIST.
  - Ο SHA-1 αποτελεί επανέκδοση του SHA που διόρθωνε μια ατέλεια του τελευταίου.
  - Ο SHA-1 παίρνει είσοδο μήνυμα μήκους μικρότερο από 264 bits και παράγει σύνοψη 160 bit.
  - Ο SHA-2 παράγει σύνοψη 256 ή 512 bit.
  - Ο SHA-3 δεν αντικαθιστά τον SHA-2 αλλά αποτελεί ένα εναλλακτικό αλγόριθμο με διαφορετική σχεδιαστική φιλοσοφία.
- MD2, MD4, MD5 (Message Digest)
  - Παίρνουν στην είσοδο μήνυμα αυθαίρετου μήκους και δίνουν στην έξοδο μια σύνοψη 128 bit.
  - Ο MD2 είχε σχεδιαστεί για μηχανές 8 bit, σε αντίθεση με τους MD4 και MD5 που προορίζονται για μηχανές 32 bit.

2. Κρυπτογραφικά συστήματα

- Εισαγωγή
- Μονόδρομες συναρτήσεις
- **Κρυπτοσυστήματα μοναδιαίας κλείδας (συμμετρική κρυπτογράφηση)**
- Κρυπτοσυστήματα δημόσιας κλείδας (ασύμμετρη κρυπτογράφηση)
- Υβριδικά συστήματα

Συμμετρική κρυπτογράφηση

- Το ίδιο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση ($K_A = K_B = K$)
- Δύο κατηγορίες:
  - Αλγόριθμοι κρυπτογράφησης τμήματος (**block ciphers**)
  - Αλγόριθμοι κρυπτογράφησης ροής (**stream ciphers**)



Αλγόριθμοι κρυπτογράφησης τμήματος (block ciphers)

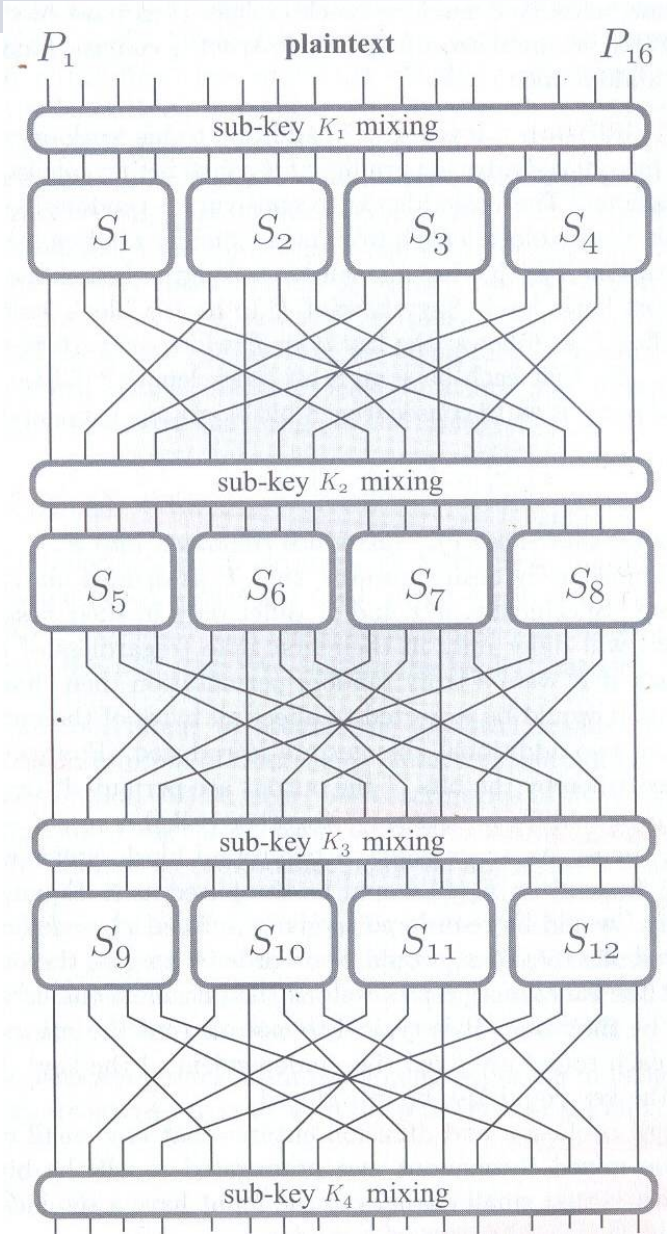
- Μετατρέπει ένα τμήμα μη κρυπτογραφημένου κειμένου, καθορισμένου μεγέθους (plaintext), σε ίδιου μεγέθους τμήμα κρυπτογραφημένου κειμένου (ciphertext)
- Το καθορισμένο μήκος καλείται *μέγεθος τμήματος (block size)*
  - Συνήθως block size = key size
- Οι αλγόριθμοι τμημάτων λειτουργούν επαναληπτικά, κρυπτογραφώντας ένα τμήμα διαδοχικά, αρκετές φορές
- Σε κάθε γύρο, ο ίδιος μετασχηματισμός εφαρμόζεται στα δεδομένα χρησιμοποιώντας ένα υπό-κλειδί.
- Το σύνολο των υπό-κλειδιών προέρχεται από το μυστικό κλειδί που χορήγησε ο χρήστης, με ειδική συνάρτηση.

Συμμετρικοί Αλγόριθμοι Ομάδας Σύγχυση και Διάχυση

- Στόχος: Η συμπεριφορά σαν μία ***τυχαία αντιμετάθεση*** (random permutation)
- Σύμφωνα με τον Shannon, για να το πετύχουμε χρησιμοποιούμε τεχνικές:
  1. Σύγχυσης (Confusion) - π.χ. Αντικατάσταση
  2. Διάχυσης (Diffusion) π.χ. Αναδιάταξη

... και επαναλαμβάνουμε τόσες φορές ώστε να προσομοιώσουμε (όσο γίνεται) τη λειτουργία μιας τυχαίας αντιμετάθεσης, δηλαδή:

- Κάθε (έστω μικρή) αλλαγή θα επηρεάσει όλα τα bit εξόδου (avalanche effect)



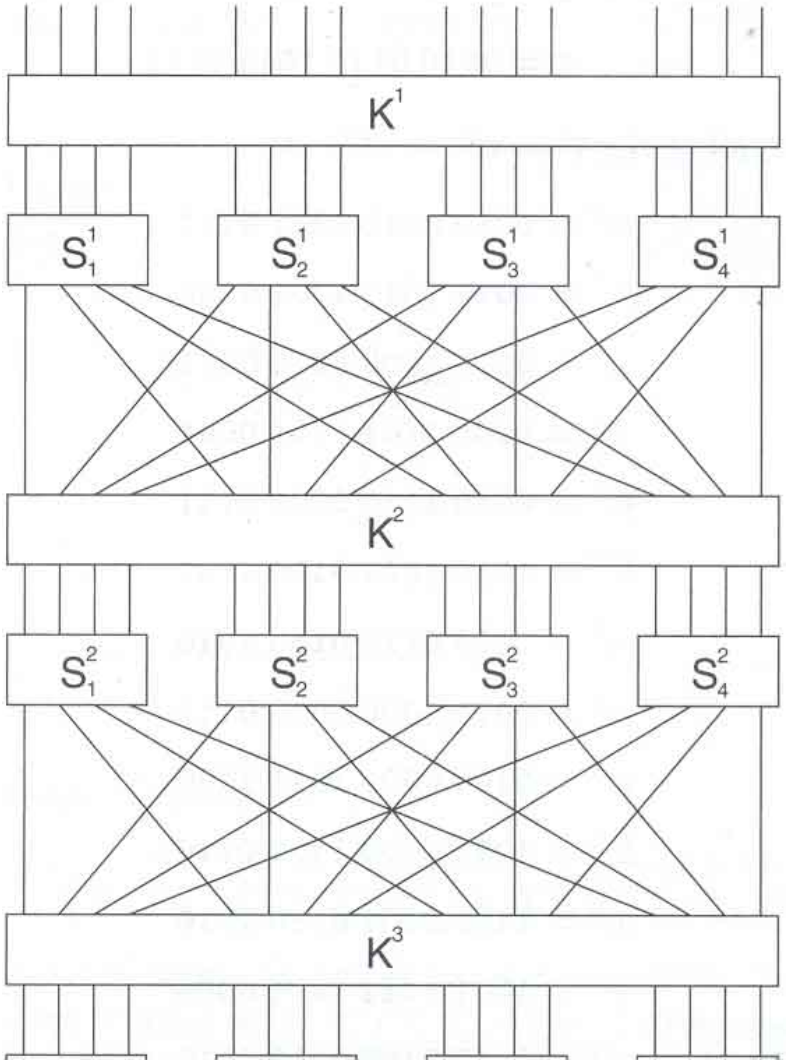
A substitution-permutation (SP) network

Συμμετρικοί Αλγόριθμοι Ομάδας

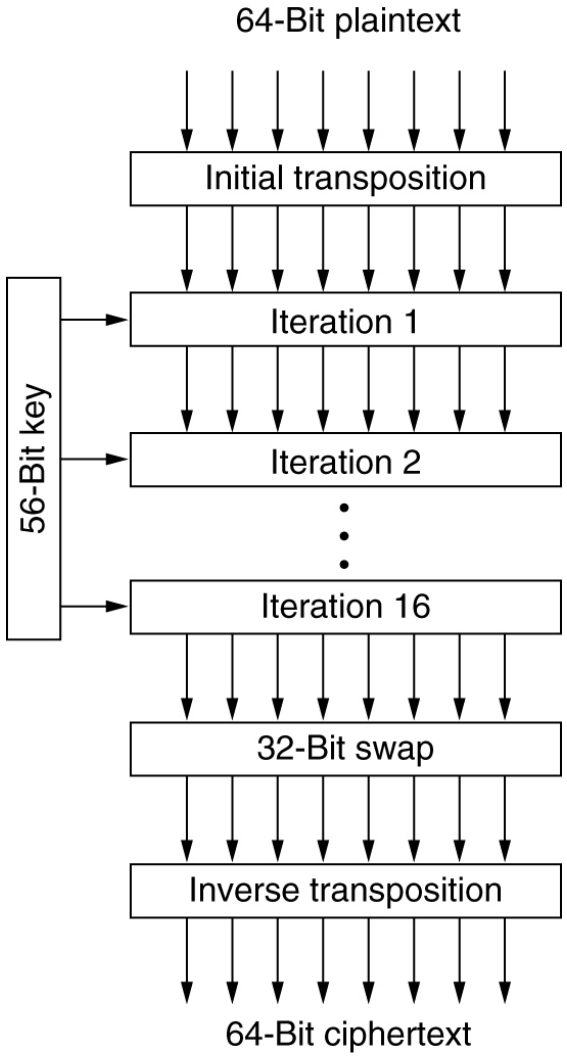
Το φαινόμενο της χιονοστιβάδας (avalanche effect)

- Για να ισχύει το φαινόμενο της χιονοστιβάδας, θα πρέπει:
  1. Κάθε S-box σχεδιάζεται ώστε αλλάζοντας 1 bit εισόδου επηρεάζει τουλάχιστον 2 bit εξόδου του S-box
  2. Οι αναδιατάξεις (mixes) σχεδιάζονται ώστε τα bit εξόδου κάθε S-box διαχέονται σε διαφορετικά S-box κατά τον επόμενο γύρο.
- Επιπλέον, θέλω όλα τα bit κλειδιού να επηρεάζουν όλα τα bit εξόδου !!!

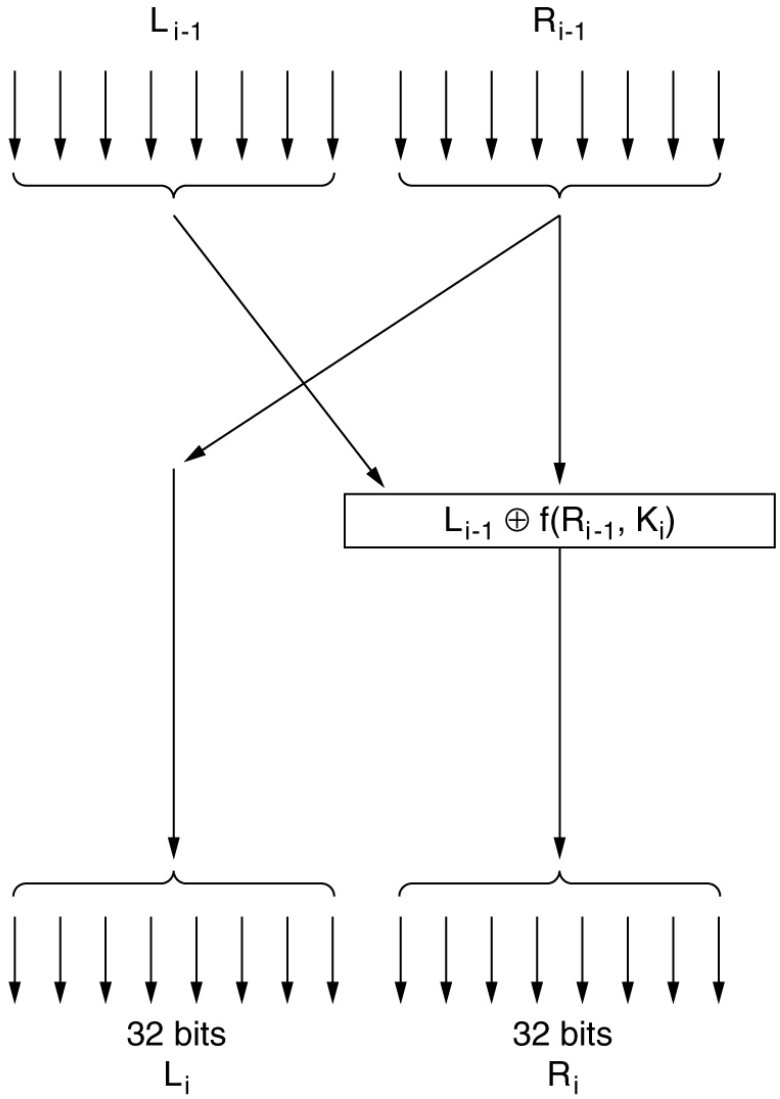
Για μπλόκ 128 bit, χρειάζονται τουλάχιστον 7 γύροι (rounds)



Παράδειγμα: Αλγόριθμος DES



(a)

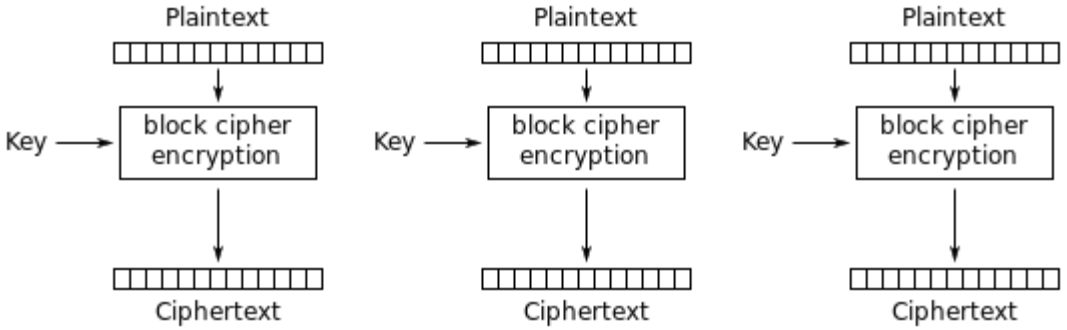


(b)

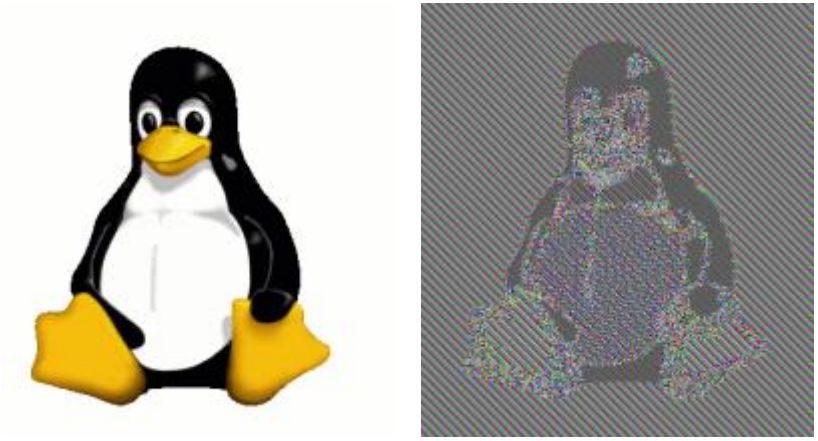
Παραδείγματα block ciphers και μήκος κλειδιού

- Data Encryption Standard (DES): 64 bit (56 στην πράξη)
- 3DES: 2 x 64 = 128 bit (112)
- Advanced Encryption Standard (AES): 128, 192, 256 bit (3 λειτουργίες)
- Ανάλυση αλγορίθμου AES (επίδειξη αλγορίθμου)

Καταστάσεις λειτουργίας AES: (ECB mode)



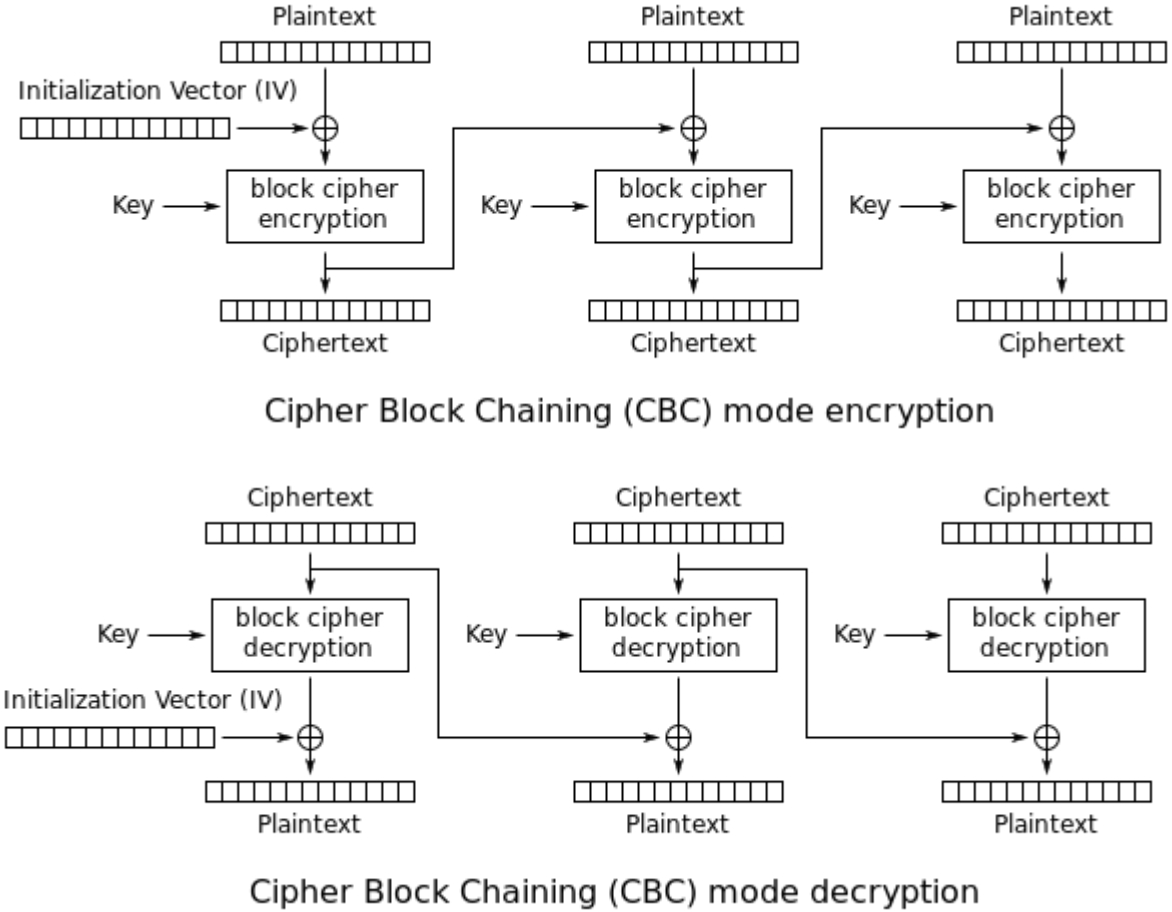
Electronic Codebook (ECB) mode encryption



- Κάθε μπλοκ κρυπτογραφείται ανεξάρτητα από τα υπόλοιπα
- Καθόλου ασφαλές

Πηγή: https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Electronic_Codebook_.28ECB.29

Καταστάσεις λειτουργίας AES: (CBC mode)



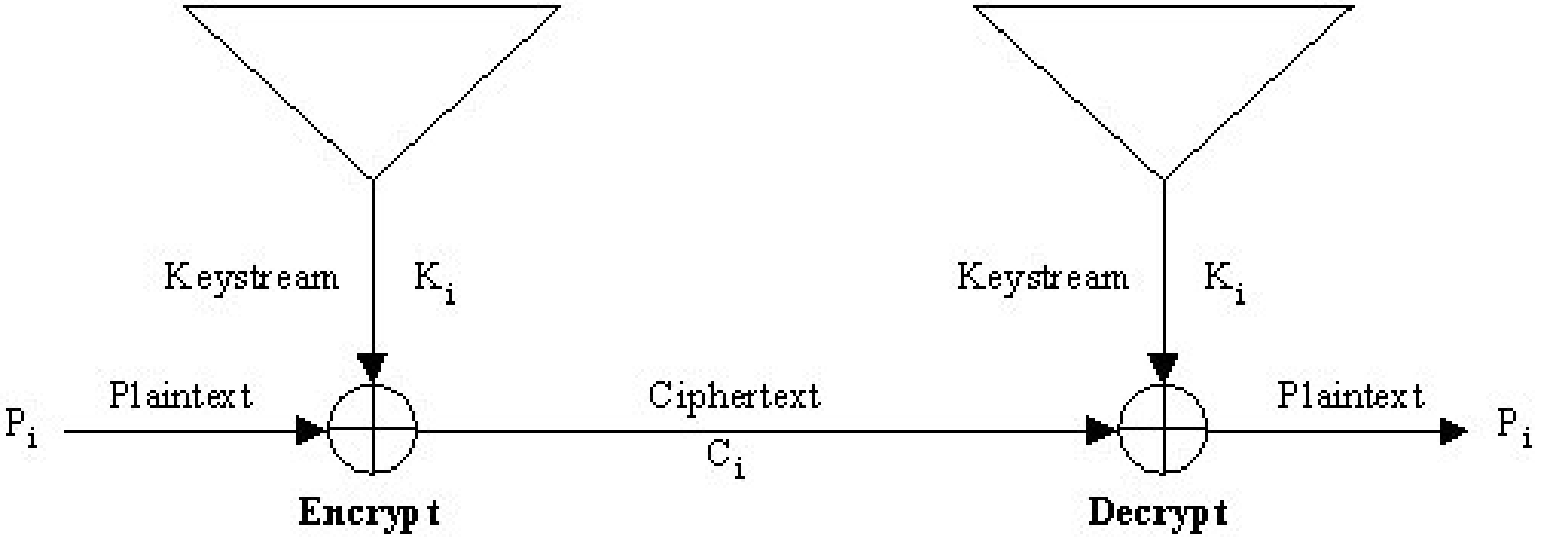
- Κάθε μπλοκ γίνεται XOR με το προηγούμενο, πριν κρυπτογραφηθεί
- Για να είναι κάθε κρυπτογράφηση μοναδική, χρησιμοποιεί ένα Initialization Vector (IV) για το 1ο μπλοκ
- Η κρυπτογράφηση γίνεται σειριακά

Πηγή: https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Electronic_Codebook_.28ECB.29

Αλγόριθμοι κρυπτογράφησης ροής (stream ciphers)

- Εξαιρετικά ταχείς αλγόριθμοι (πολύ ταχύτεροι από τους αλγόριθμους τμημάτων)
- Οι αλγόριθμοι ροών λειτουργούν με μικρότερες μονάδες απλού κειμένου (συνήθως με bits)
- Ένας αλγόριθμος ροής παράγει μια ακολουθία από bits που χρησιμοποιείται σαν κλειδί και καλείται ροή κλειδιού (keystream) η οποία παράγεται (ψευδο-) τυχαία
- Η κρυπτογράφηση επιτυγχάνεται με το συνδυασμό της ροής κλειδιού με το plaintext, συνήθως μέσω πράξης X-OR

Παραδείγματα αλγορίθμων ροής



A5: 40 bit

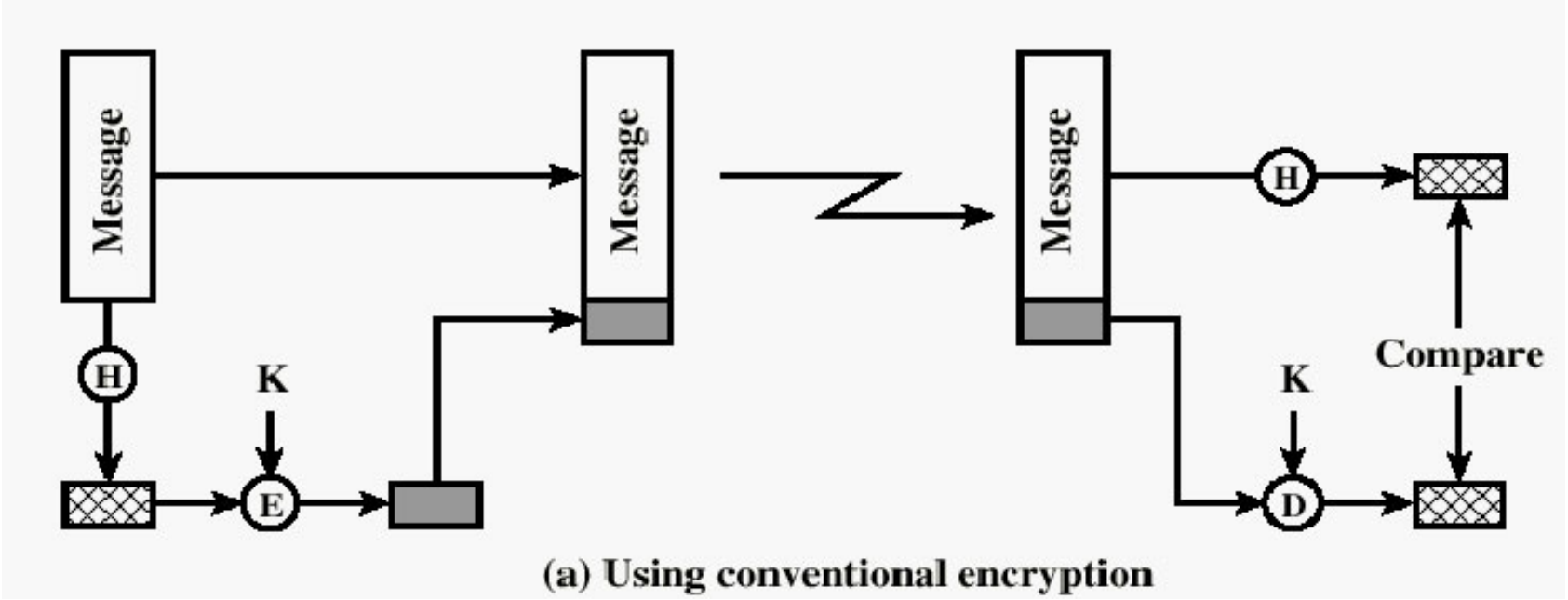
RC4, RC5: 40 - 2048 bit

Ακεραιότητα μηνύματος με συμμετρική κρυπτογραφία και συναρτήσεις κατακερματισμού

1. Η Alice στέλνει στον Bob ένα μήνυμα **m**, και την τιμή hash $h = H(m)$
2. Ο Bob λαμβάνει το μήνυμα, υπολογίζει εκ νέου την τιμή hash του μηνύματος που έλαβε και τη συγκρίνει με την $H(m)$
   - Εάν είναι ίσες, τότε το μήνυμα είναι το σωστό
- Εάν αλλαχτεί έστω και ένα bit του μηνύματος, η τιμή hash θα είναι διαφορετική
  - π.χ. αν το μέγεθος της συνάρτησης Hash είναι 256 bit, η πιθανότητα να βρεθεί ένα m' ώστε $H(m) = H(m')$ είναι 1 στις 2^{256}

- Αν η συνάρτηση hash συνδυαζόταν και με ένα μυστικό κλειδί, τότε θα μπορούσε να προσφέρει και <u>αυθεντικοποίηση</u>

Message Authentication Code (MAC)



(a) Using conventional encryption

- Η Alice υπολογίζει την τιμή hash του μηνύματος ***m***
- Στη συνέχεια κρυπτογραφεί το ***H(m)*** με ένα συμμετρικό κλειδί ***K***
- Στέλνει το αποτέλεσμα, καθώς και το αρχικό μήνυμα, στον Bob

Alice $\xrightarrow{m, E_K(H(m))}$ Bob

- Ο Bob υπολογίζει το ***H(m)*** και χρησιμοποιεί το ***K*** για να αποκρυπτογραφήσει το $E_K(H(M))$ και συγκρίνει τις δύο τιμές hash

Χαρακτηριστικά συμμετρικής κρυπτογραφίας

- Πλεονεκτήματα
  - Μεγάλη απόδοση (efficiency): μέχρι 100-αδες MB/sec για h/w implementations
  - Μικρό μήκος κλειδιού
- Μειονεκτήματα
  - Αριθμός κλειδιών: για n χρήστες, (n-1) κλειδιά ανά χρήστη, συνολικά n(n-1)/2 κλειδιά
  - Ανταλλαγή κλειδιών
  - Δυσκολία εντοπισμού παραβίασης

2. Κρυπτογραφικά συστήματα

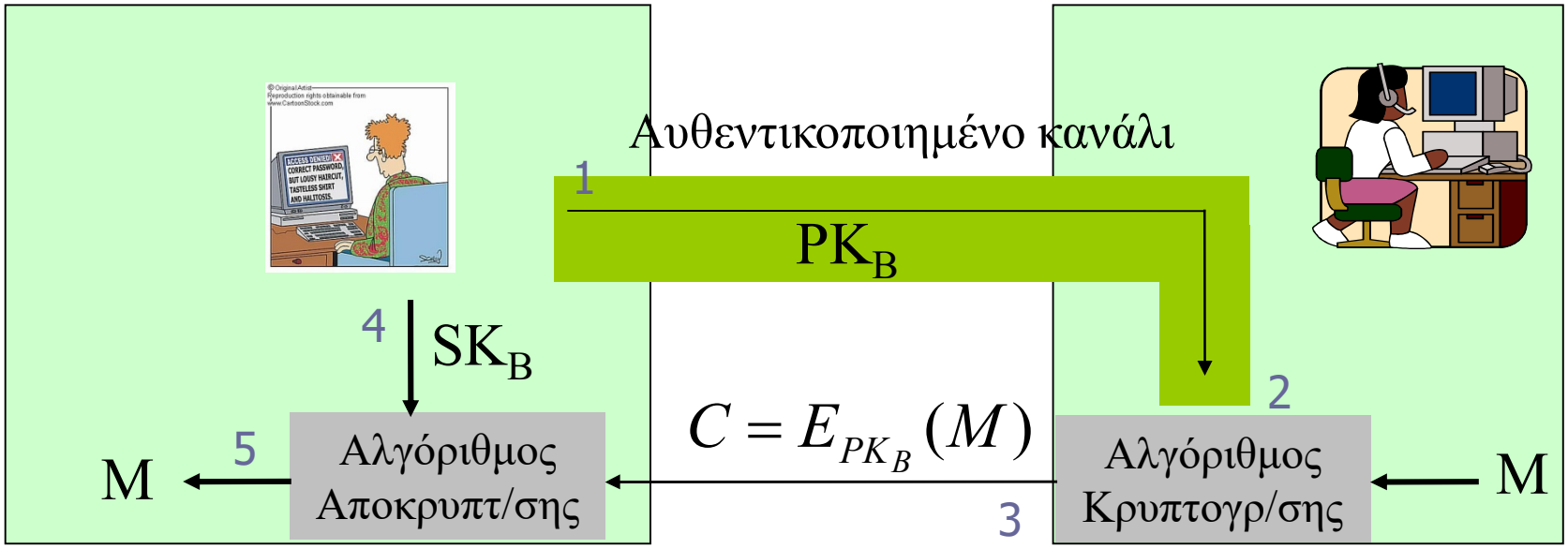
- Εισαγωγή
- Μονόδρομες συναρτήσεις
- Κρυπτοσυστήματα μοναδιαίας κλείδας (συμμετρική κρυπτογράφηση)
- **Κρυπτοσυστήματα δημόσιας κλείδας (ασύμμετρη κρυπτογράφηση)**
- Υβριδικά συστήματα

Ασύμμετρη κρυπτογράφηση ή κρυπτογραφία δημόσιου κλειδιού

- Κρυπτογραφία Δημοσίου Κλειδιού = Ασύμμετρη Κρυπτογραφία
- Δύο διαφορετικά αλλά ***μαθηματικά συσχετιζόμενα*** κλειδιά:
  - Δημόσιο κλειδί (Public key) PK_A: γνωστό σε όλους (με αυτό γίνεται η κρυπτογράφηση)
  - Ιδιωτικό κλειδί (Secret key) SK_A: γνωστό μόνο στον κάτοχο
- Η γνώση του δημόσιου δεν οδηγεί σε αποκάλυψη του ιδιωτικού κλειδιού

Αλγόριθμοι Δημόσιου Κλειδιού (κρυπτογράφηση)

- Η Alice χρησιμοποιεί το Δημόσιο Κλειδί PK_B του Bob για να κρυπτογραφήσει το M
- Ο Bob χρησιμοποιεί το Ιδιωτικό Κλειδί του SK_B για να αποκρυπτογραφήσει το μήνυμα



Μαθηματικό υπόβαθρο ασύμμετρης κρυπτογραφίας

- Χρειαζόμαστε *μονόδρομες συναρτήσεις με καταπακτή (trapdoor one-way function)*
- Βασίζονται σε δυσεπίλυτα υπολογιστικά προβλήματα
  1. Παραγοντοποίηση μεγάλων ακεραίων (RSA)
     - Αν p, q πρώτοι αριθμοί, και $n = p\,q$, είναι δύσκολο να υπολογιστούν οι όροι p και q από το n
  2. Εύρεση διακριτού λογαρίθμου (Diffie-Hellman)
     - Αν p μεγάλος πρώτος και $y = g^x \pmod p$ είναι δύσκολο από το y να υπολογιστεί το x

Αλγόριθμος RSA (1)

- Δημιουργία κλειδιών
  - ***p, q*** μεγάλοι πρώτοι αριθμοί, και $n = p\ q$
  - Συνάρτηση Euler: $\varphi(n) = (p-1)\ (q-1)$
  - Επιλέγω ***e*** τέτοιο ώστε ΜΚΔ(e, φ) =1
  - Επιλέγω ***d*** : $e\ d = 1\ mod\ \varphi(n)$
- Δημόσιο κλειδί: $PK_A = e$
- Μυστικό κλειδί: $SK_A = d$

Αλγόριθμος RSA (2)

- Αλγόριθμος κρυπτογράφησης
  - Μήνυμα $\boldsymbol{m}$ (όπου m < n)
  - $\boldsymbol{E_e(m) = m^e \ (mod\ n) = c}$
- Αλγόριθμος αποκρυπτογράφησης
  - $\boldsymbol{D_d(c) = c^d \ (mod\ n) = m}$
- Γιατί λειτουργεί:
  - $\boldsymbol{c^d \ (mod\ n) = (m^e)^d \ (mod\ n) = m^1 \ (mod\ n)}$
  - Οι πράξεις στον εκθέτη γίνονται modulo φ(n)

Ακεραιότητα μηνύματος με ασύμμετρη κρυπτογραφία και συναρτήσεις κατακερματισμού

1. Η Alice θέλει να στείλει στον Bob ένα μήνυμα **m**, και να αποδείξει ότι:
   - Μόνο η Alice έχει στείλει το μήνυμα
   - Το μήνυμα δεν έχει τροποποιηθεί
   - Υπολογίζει την τιμή hash $h = H(m)$
   - Χρησιμοποιεί το μυστικό κλειδί της και υπολογίζει την RSA υπογραφή $SIG_{SKa}(h) = h^d \, (mod n) = \sigma$
   - Στέλνει το m και την υπογραφή σ
2. Ο Bob λαμβάνει το μήνυμα m, και το σ και:
   - Υπολογίζει εκ νέου την τιμή hash $h = H(m)$
   - Χρησιμοποιεί το δημόσιο κλειδί της Alice και επαληθεύει την υπογραφή σ: $VER_{PKa}(\sigma) = \sigma^e \, (mod n) = (h^d)^e \, (mod n)$
   - Εάν $VER_{PKa}(\sigma) == h$, τότε η υπογραφή είναι έγκυρη

Πρωτόκολλο Diffie-Hellman: Ανταλλαγή διαμοιραζόμενου κλειδιού

- Βασίζεται στο πρόβλημα εύρεσης διακριτού λογαρίθμου
- Ζεύγη μυστικού / δημόσιου κλειδιού
- Alice: $\boldsymbol{SK_A = a, PK_A = g^a \bmod p}$
- Bob: $\boldsymbol{SK_B = b, PK_B = g^b \bmod p}$
- Ανταλλάσουν τα δημόσια κλειδιά τους
- Το μυστικό διαμοιραζόμενο κλειδί μεταξύ τους είναι: $\boldsymbol{K = g^{ab} \bmod p}$

Χαρακτηριστικά ασύμμετρης κρυπτογραφίας

- Πλεονεκτήματα
  - Αριθμός κλειδιών: Αρκούν n κλειδιά ανά χρήστη (αντί για n(n-1)/2)
  - Εύκολη ανταλλαγή διαμοιραζόμενων κλειδιών
  - Ευκολία εντοπισμού παραβίασης
- Μειονεκτήματα
  - Μικρή απόδοση (efficiency): 100 με 1000 φορές πιο αργή από τη συμμετρική κρυπτογράφηση
  - Μεγαλύτερο μήκος κλειδιού

2. Κρυπτογραφικά συστήματα

- Εισαγωγή
- Μονόδρομες συναρτήσεις
- Κρυπτοσυστήματα μοναδιαίας κλείδας (συμμετρική κρυπτογράφηση)
- Κρυπτοσυστήματα δημόσιας κλείδας (ασύμμετρη κρυπτογράφηση)
- **Υβριδικά συστήματα**

Υβριδική κρυπτογραφία

- Συνδυασμός συμμετρικών και ασύμμετρων αλγορίθμων
  - Ασύμμετρη κρυπτογραφία για την ασφαλή ανταλλαγή ενός κοινού συμμετρικού κλειδιού K_{AB}
  - Χρήση του συμμετρικού κλειδιού K_{AB} για τη συμμετρική κρυπτογράφηση και τον έλεγχο ακεραιότητας του κανονικού μηνύματος
- Τα πρωτόκολλα ασφάλειας χρησιμοποιούν συνήθως υβριδική κρυπτογραφία. Γνωστά πρωτόκολλα:
  - PGP
  - IPSec
  - SSL/TLS

Υβριδική κρυπτογραφία

Ανταλλαγή συμμετρικού κλειδιού με χρήση δημόσιου κλειδιού

A

PK_A, SK_A

B

PK_B, SK_B

1. Επιλογή ενός μυστικού, συμμετρικού κλειδιού K_{AB}
2. Κρυπτογράφηση κλειδιού K_{AB} με το δημόσιο κλειδί του Β και αποστολή

$E_{PK_B}(K_{AB})$ →

3. Αποκρυπτογράφηση με τη χρήση του ιδιωτικού κλειδιού SK_B :
   $D_{SK_B}[E_{PK_B}(K_{AB})] = K_{AB}$
4. Συμμετρική κρυπτογράφηση μηνύματος m_1 με το κλειδί K_{AB} :
   $E_{K_{AB}}(m_1) = c_1$

← c_1

5. Συμμετρική αποκρυπτογράφηση του c_1 με το κλειδί K_{AB} :
   $D_{K_{AB}}(c_1) = D_{K_{AB}}(E_{K_{AB}}(m_1)) = m_1$

c_2 →

...

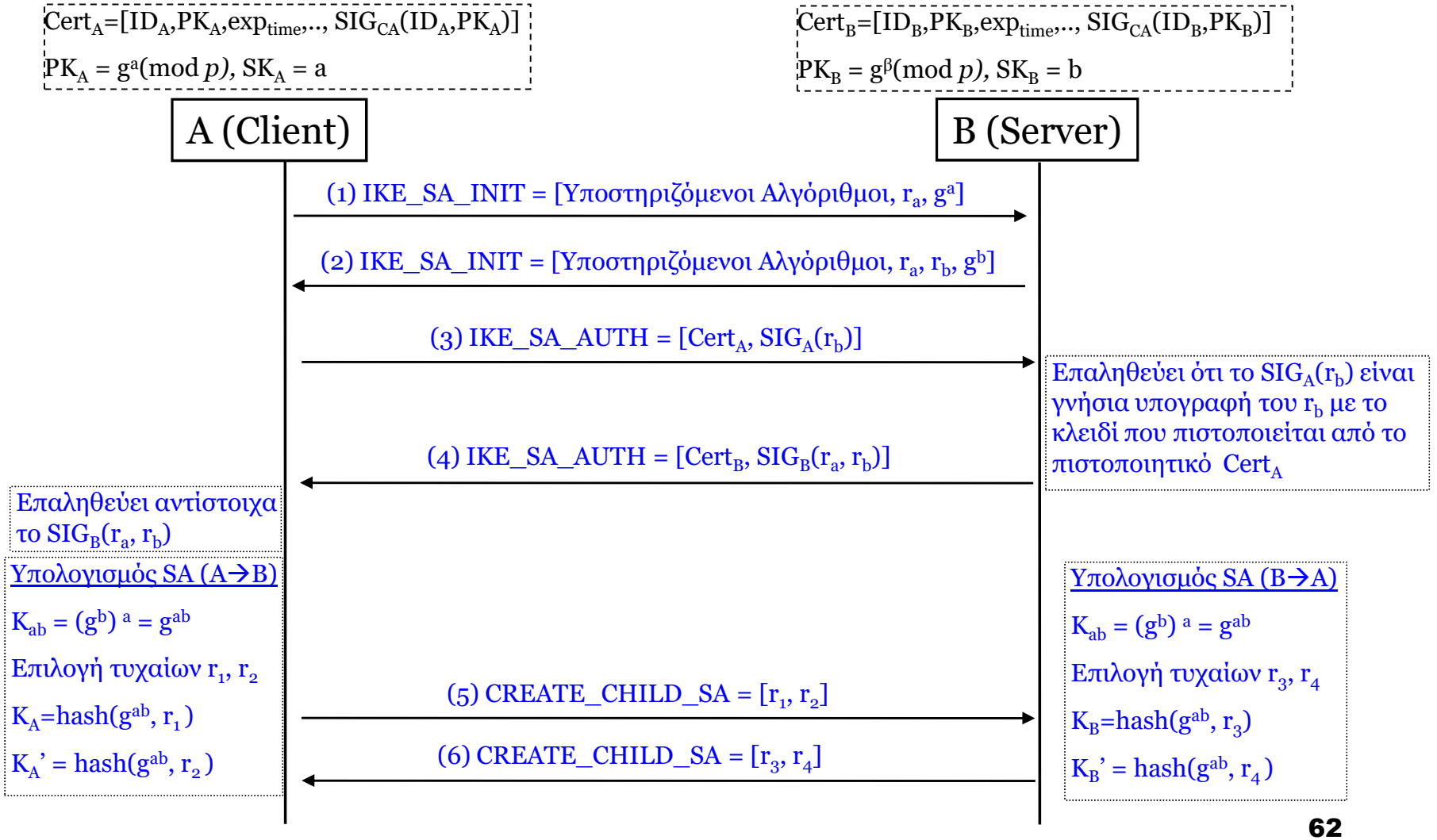
←

...

Παραδείγματα υβριδικής κρυπτογραφίας

- Πρωτόκολλο IPSec
  - Παρέχει εμπιστευτικότητα, ακεραιότητα και αυθεντικότητα μηνύματος στο επίπεδο δικτύου (IP).
- Πρωτόκολλο PGP (Pretty Good Privacy)
  - Παρέχει αυθεντικοποίηση χρήστη, εμπιστευτικότητα και ακεραιότητα μηνύματος σε web, e-mail κτλ
- Πρωτόκολλο SSL / TLS
  - Παρέχει εμπιστευτικότητα, ακεραιότητα και αυθεντικότητα μηνύματος σε διαδικτυακή επικοινωνία

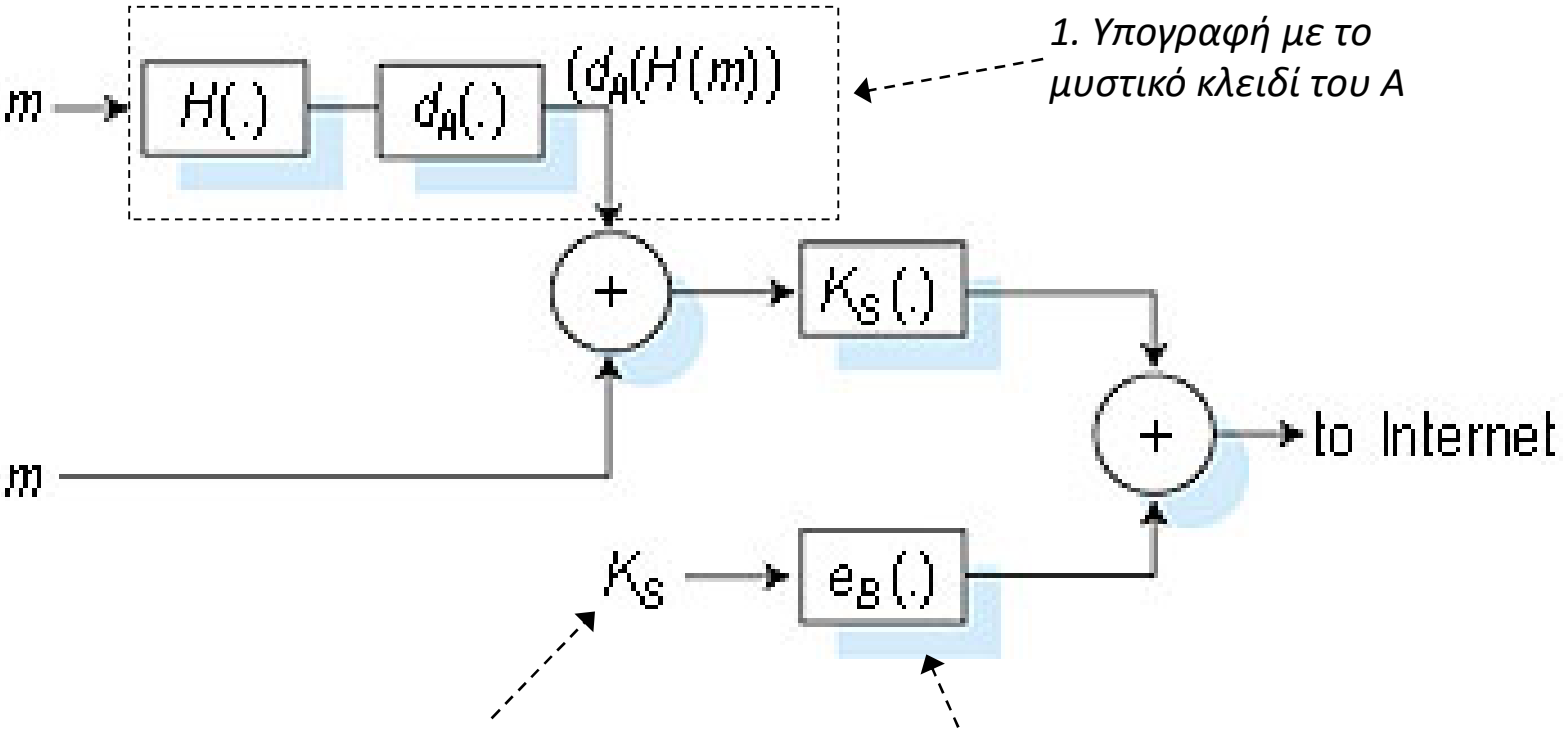
Ανταλλαγή κλειδιών στο IPSec: Το πρωτόκολλο Internet Key Exchange (IKE)



Κρυπτογράφηση και υπογραφή δεδομένων: GPG (GNU PG)

- Το PGP είναι πλέον εμπορικό προϊόν
- GPG: GNU PGP
  - Βασίζεται στο πρότυπο Open PGP
  - Παρέχει αντίστοιχες υπηρεσίες με το PGP
  - http://www.gnupg.org/

Υβριδική κρυπτογράφηση και υπογραφή email



Το πρωτόκολλο SSL

- Χειραψία (Handshake): Η Alice και ο Bob χρησιμοποιούν τα πιστοποιητικά τους και τα αντίστοιχα ιδιωτικά κλειδιά τους για αμοιβαία αυθεντικοποίηση και για ανταλλαγή κοινού μυστικού κλειδιού
- Παραγωγή κλειδιών (Key Derivation): Η Alice και ο Bob χρησιμοποιούν το κοινό κλειδί για να δημιουργήσουν ένα σύνολο από κλειδιά για όλη την επικοινωνία
- Μεταφορά δεδομένων (Data Transfer): Τα δεδομένα που θα μεταφερθούν χωρίζονται σε μία σειρά εγγραφών (data records)
- Τερματισμός σύνδεσης (Connection Closure): Χρησιμοποιούνται ειδικά μηνύματα για τον ασφαλή τερματισμό της σύνδεσης

Βιβλιογραφία

1. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, “Handbook of Applied Cryptography”, CRC press, (5th ed) 2001.
2. Δ. Πολέμη, Χ. Δημητριάδης, Σ. Παπαστεργίου, Α. Καλιαντζόγλου, Εργαστηριακά θέματα ασφάλειας, 2006.
3. Εμ. Μάγκος, Σημειώσεις μαθήματος κρυπτογραφίας, Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο.
4. Σ. Κάτσικας Δ. Γκρίτζαλης, Σ. Γκρίτζαλης, «Ασφάλεια Πληροφοριακών Συστημάτων», Εκδόσεις Νέων Τεχνολογιών, 2003.