ΤΕΙ ΗΠΕΙΡΟΥ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε
ΜΕΤΑΠΤΙΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ

Ασφάλεια

ΛΙΑΓΚΟΥ ΒΑΣΙΛΙΚΗ
ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ&
ΚΡΥΠΤΑΝΑΛΥΣΗ

Syllabus Διάλεξης

- Εισαγωγή στην Ασφάλεια Αλγορίθμων
- Συνδυασμός Τεχνικών Αντικατάστασης και Αναδιάταξης
- Παρωχημένες και Σύγχρονες Θεωρήσεις της Κρυπτογραφίας
- Μοντέλο Κρυπτογραφικής Επικοινωνίας (συμμετέχοντες)
- Τύποι & Ορισμοί Κρυπταναλυτικών επιθέσεων
- Ασφάλεια Κρυπτοσυστήματος
- Ορισμοί και Αποδείξεις Απόλυτης Ασφάλειας
- Εισαγωγή στην Υπολογιστική Ασφάλεια

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Σύγχρονη Κρυπτογραφία Εισαγωγή

- … στους ώμους «γιγάντων»
  - A. Kerckhoffs (επαναπροσδιορισμός του όρου «ασφάλεια κρυπτοσυστήματος»)
  - W. Friedman, L. Hill: Μαθηματικά στην υπηρεσία της Κρυπτολογίας
  - C. Shannon (1940s): Θεωρία Πληροφορίας (Information Theory)
  - A. Turing: Ο πνευματικός «πατέρας» του Η/Υ
- Τέλη δεκαετίας 60
  - Διάδοση Η/Υ και Δικτύων…
  - Εταιρικό ενδιαφέρον για προστασία ψηφιακών δεδομένων
  - Απουσία προτύπων κρυπτογράφησης
- Δεκαετίες 70s και 90s, Σημαντικές καινοτομίες στο χώρο…
  - 1976: Κρυπτογραφία Δημόσιου Κλειδιού – Diffie-Hellmann
  - 1977: Το πρότυπο συμμετρικής κρυπτογράφησης DES
  - 1978: Ο αλγόριθμος κρυπτογράφησης Δημόσιου Κλειδιού RSA
  - 1991: Το πρώτο πρότυπο ψηφιακής υπογραφής (βασισμένο στον αλγόριθμο RSA)

H. Mel, D. Baker.
Cryptography Decrypted.
Addison-Wesley, 2001

Κρυπτογραφία = Κρυπτογραφικά Κλειδιά και Κρυπτογραφικοί Αλγόριθμοι

- Ας κάνουμε τον εξής παραλληλισμό…
  - Μηχανισμός Κλειδαριάς (π.χ χρηματοκιβώτιο)= Κρυπτογραφικός Αλγόριθμος
    - Γνωστός σε όλους (Αρχή Kerckoffs)
  - Συνδυασμός = Κρυπτογραφικό Κλειδί

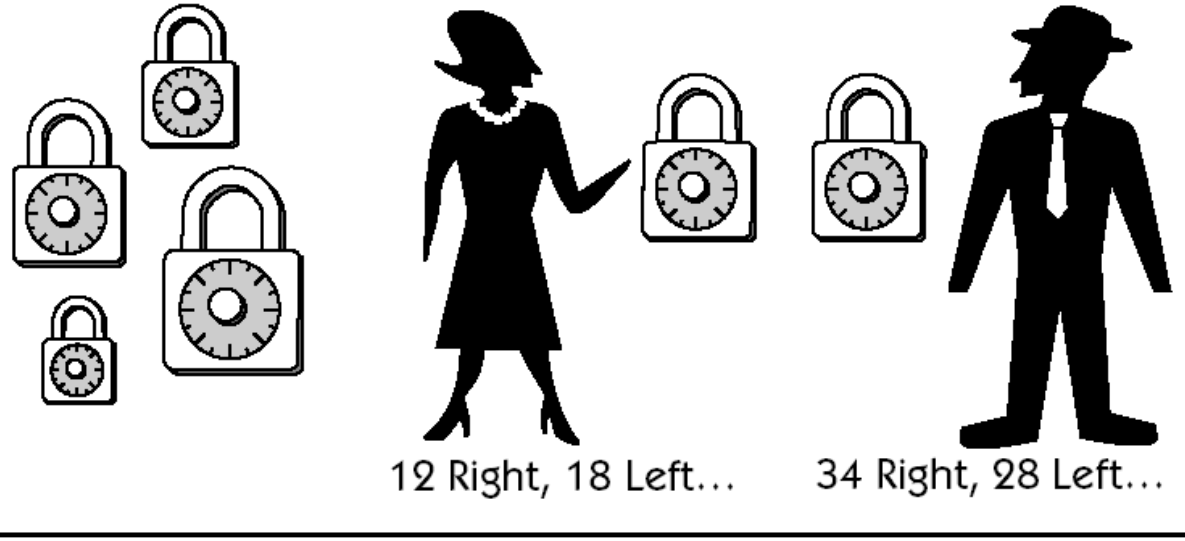


Figure 1-1 Alice's and Bob's individual locks are only two of many instances of the identical lock design.

H. Mel, D. Baker.
Cryptography Decrypted.
Addison-Wesley, 2001

Ερωτήματα

1. Πόσο ασφαλές είναι το σύστημα που θα επιλέξουμε;
   - Μεγαλύτερο πλήθος Κλειδιών = Μεγαλύτερη ασφάλεια (συνήθως)
     - (… εκτός και αν ο αλγόριθμος δεν είναι ασφαλής – δηλαδή υπάρχει πιο σύντομη επίθεση από την επίθεση ωμής βίας ;)
2. Τι προσπαθεί η Alice να προστατέψει, και για πόσο;
   - Ζητήματα ασφάλειας και πρακτικότητας
     - (π.χ. ένα σύστημα με μικρό αριθμό κλειδιών, μπορεί να είναι ασφαλές, αν η Alice θέλει να το προστατέψει για μικρό χρονικό διάστημα !

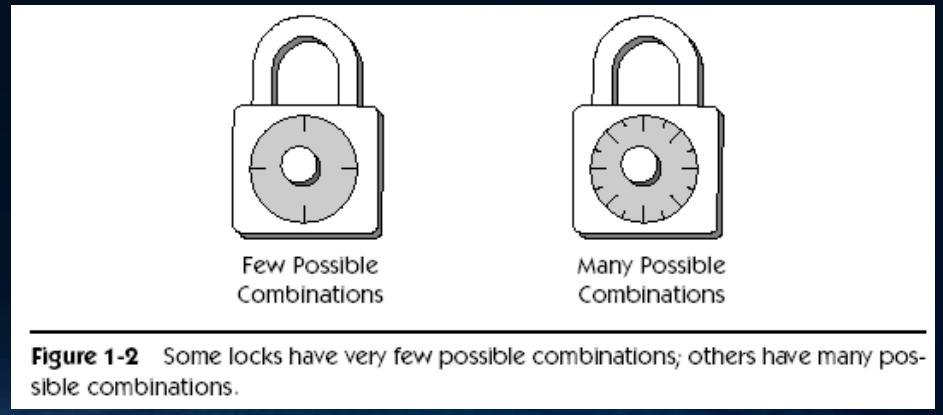


Figure 1-2 Some locks have very few possible combinations; others have many possible combinations.

Αντικατάσταση

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

Figure 2-3 Caesar's cipher variation: rotating each letter three places.

(Αλγόριθμος Ολίσθησης) Αριθμός διαθέσιμων κλειδιών = 25

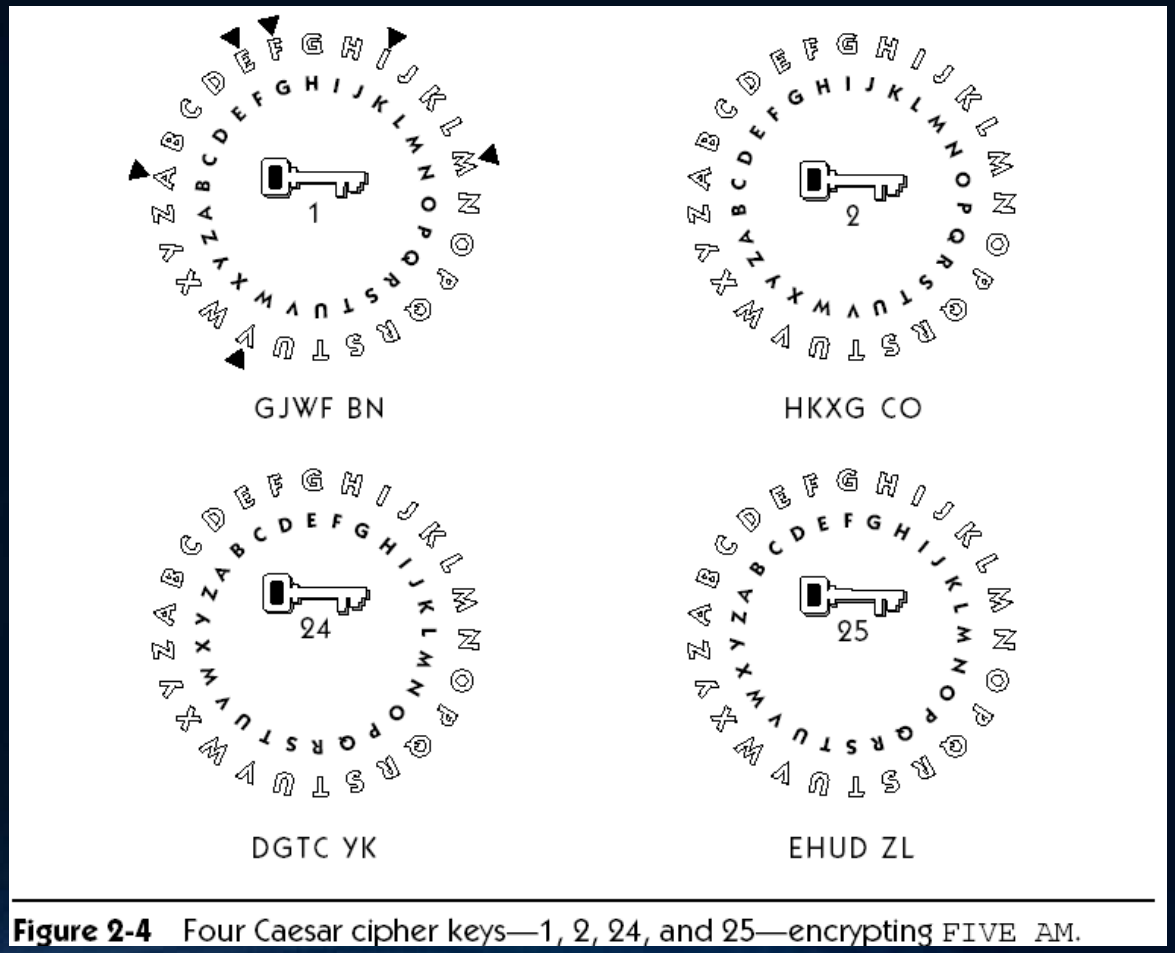


Figure 2-4 Four Caesar cipher keys—1, 2, 24, and 25—encrypting FIVE AM.

H. Mel, D. Baker.
Cryptography Decrypted.
Addison-Wesley, 2001

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

Παράδειγμα: Κρυπτανάλυση του Αλγορίθμου "Shift"

H. Mel, D. Baker. *Cryptography Decrypted*. Addison-Wesley, 2001

	I	L	Y	H	D	P
+1	J	M	Z	I	E	Q
+2	K	N	A	J	F	R
+3	L	O	B	K	G	S
+4	M	P	C	L	H	T
. . .						
+17	Z	D	P	Y	U	G
+18	A	E	Q	Z	V	H
+19	B	F	R	A	W	I
+20	C	H	S	B	X	J
+21	D	G	T	C	Y	K
+22	E	H	U	D	Z	L
+23	F	I	V	E	A	M
+24	G	J	W	F	B	N
+25	H	K	X	G	C	O
+26	I	L	Y	H	D	P

Figure 2-5 Caesar's cipher cryptanalysis: Meaningful text appears after 23 tries.

Παράδειγμα: Να κρυπταναλυθεί το κρυπτογράφημα “R F S T X”

F. Bauer, Decrypted Secrets- Methods & Maxims of Cryptology, 4th Edition, Springer, 2007

Μονογραμμική Μονοαλφαβητική Αντικατάσταση

Χρήση Μεικτού Αλφάβητου (mixed alphabet)

Α. Χρήση Κωδικού

- Ο αριθμός των «κλειδιών» αυξάνεται (Πόσο;)

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

Επεκτάσεις

1. Από ένα password, λήψη περισσότερων μεικτών αλφάβητων, με ολίσθηση:

$V \longleftrightarrow V$:	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	
	E	C	U	R	I	T	Y	A	B	D	F	G	H	J	K	L	M	N	O	P	Q	V	W	X	Z	S	,
$V \longleftrightarrow V$:	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	
	C	U	R	I	T	Y	A	B	D	F	G	H	J	K	L	M	N	O	P	Q	V	W	X	Z	S	E	etc.,

2. Το κρυπτοαλφάβητο αναδιατάσσεται ώστε να μοιάζει με αντιμετάθεση

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

- Η αντικατάσταση θα είναι:

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

Ουσιαστικά, οι επεκτάσεις δεν αυξάνουν πολύ την ασφάλεια του συστήματος (γιατί;)

John Hershey.
Cryptography Demystified.
McGraw-Hill, 2003

Γενικευμένος Αλγόριθμος Αντικατάστασης (ή: Αλγόριθμος Αντιμετάθεσης – Permutation Cipher)

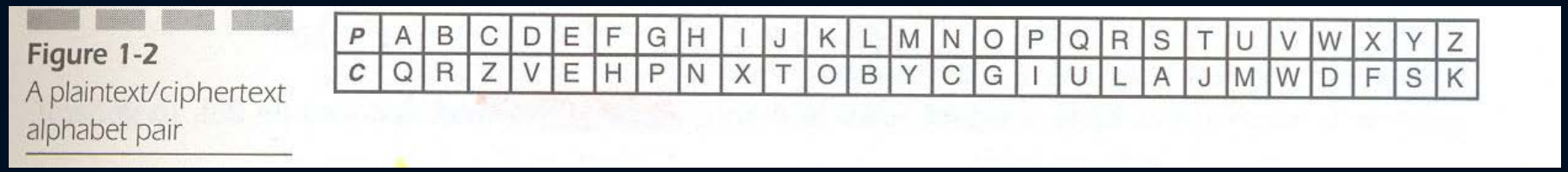


Figure 1-2
A plaintext/ciphertext alphabet pair

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

- Κρυπτοαλφάβητο = Τυχαία Αντιμετάθεση
  - Μονοαλφαβητικός: Χρήση ενός κρυπτο-αλφάβητου !
  - Το κρυπτο-αλφαβήτο (αντιμετάθεση) αποτελεί και το κλειδί του αλγορίθμου !
- Ποιο είναι το πλήθος των πιθανών κλειδιών;

$$25! \text{ Κλειδιά} = 1.5 \times 10^{25}$$

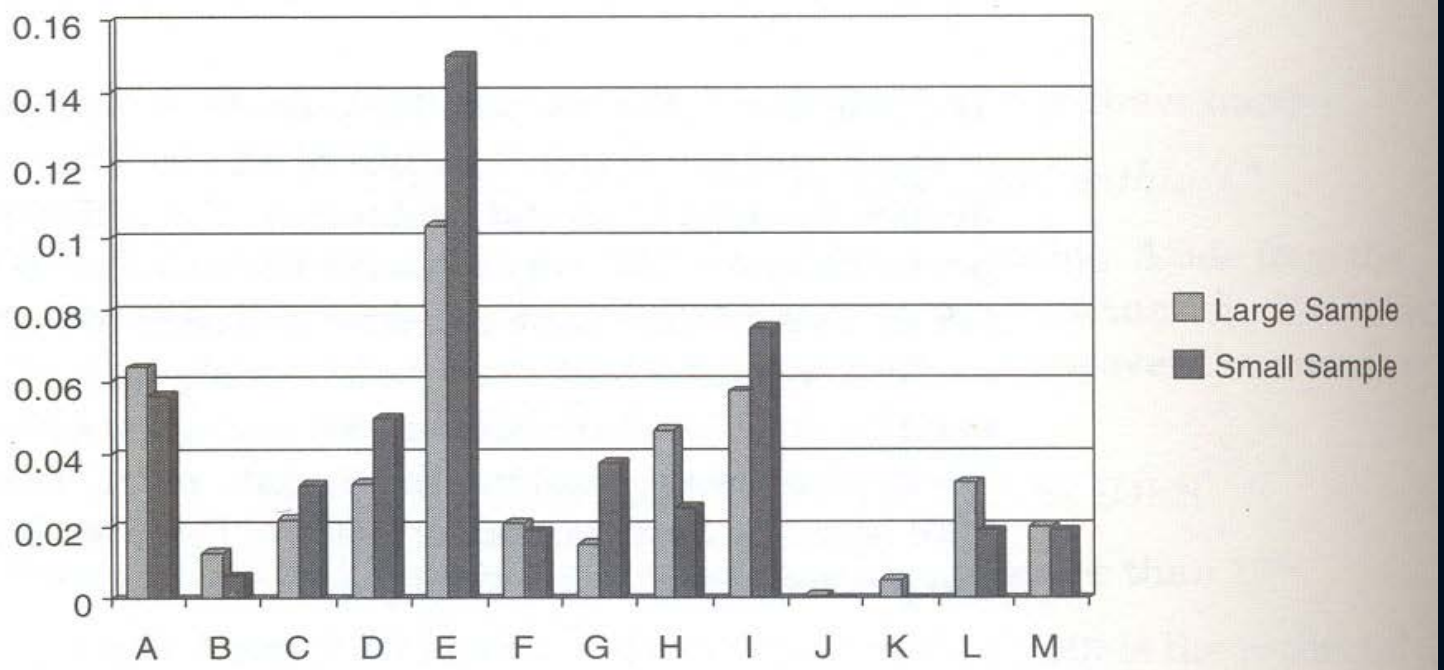
  - Το «A» μπορεί να κωδικοποιηθεί με 25 πιθανούς τρόπους
  - Το «B» μπορεί να κωδικοποιηθεί με 24 πιθανούς τρόπους
  - ...
  - Το «Z» μπορεί να κωδικοποιηθεί με 1 τρόπο

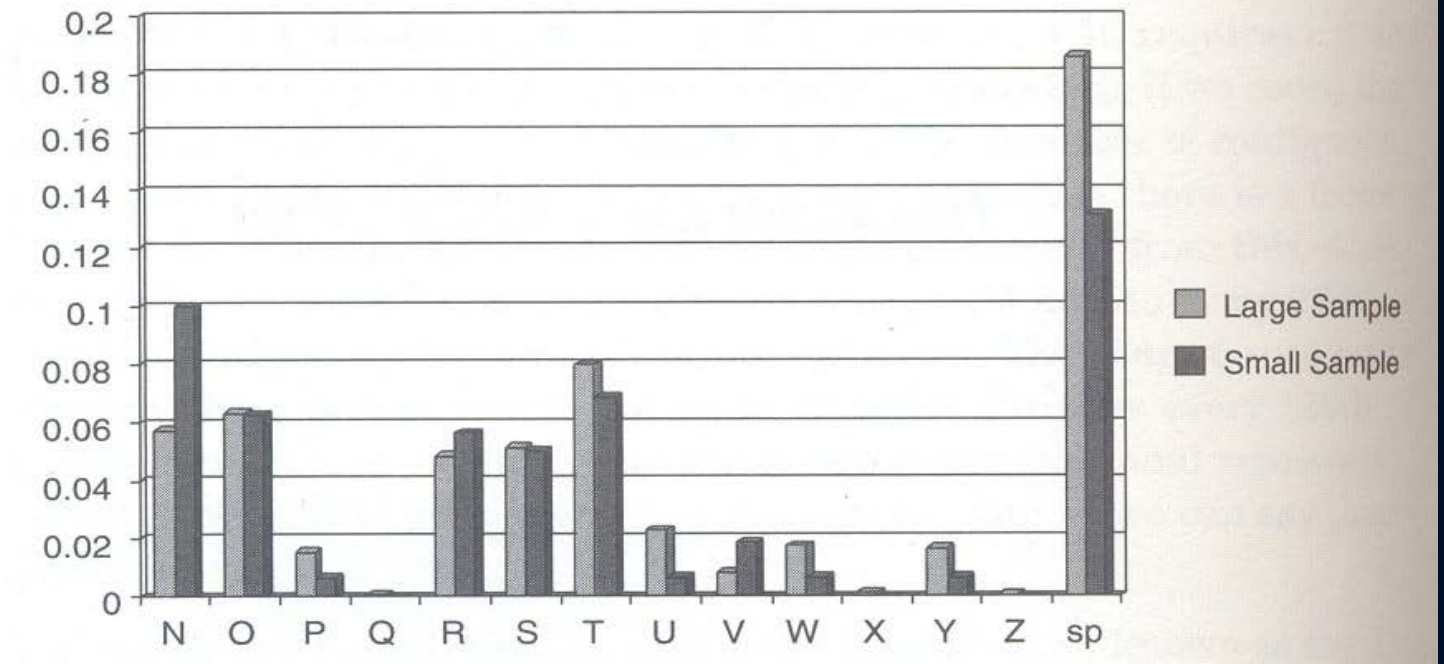
John Hershey. Cryptography Demystified. McGraw-Hill, 2003

Ανάλυση Συχνότητας Εμφάνισης Χαρακτήρων (Frequency analysis)

Plaintext Symbol	Probability	Plaintext Symbol	Probability	Plaintext Symbol	Probability
A	0.0642	J	0.0008	S	0.0514
B	0.0127	K	0.0049	T	0.0796
C	0.0218	L	0.0321	U	0.0228
D	0.0317	M	0.0198	V	0.0083
E	0.1031	N	0.0574	W	0.0175
F	0.0208	O	0.0632	X	0.0013
G	0.0152	P	0.0152	Y	0.0164
H	0.0467	Q	0.0008	Z	0.0005
I	0.0575	R	0.0484	space	0.1859

Αξιοποιώντας μεθόδους στατιστικής ανάλυσης, ο γενικευμένος αλγόριθμος αναδιάταξης μπορεί να σπάσει εύκολα υπό προϋποθέσεις





John Hershey.
Cryptography Demystified.
McGraw-Hill, 2003

F. Bauer, Decrypted Secrets- Methods & Maxims of Cryptology, 4th Edition, Springer, 2007

Πολυαλφαβητική Αντικατάσταση

- Αύξηση του πλήθους των κρυπτοαλφαβήτων

→Μεγαλύτερη ασφάλεια:

  - Κρυπτανάλυση στατιστικής ανάλυσης: πιο δύσκολη

- Συνεισφορά Trithemius:
  - Χρήση Στάνταρ Αλφάβητου με Κυκλική Ολίσθηση (Cyclically Shifted)

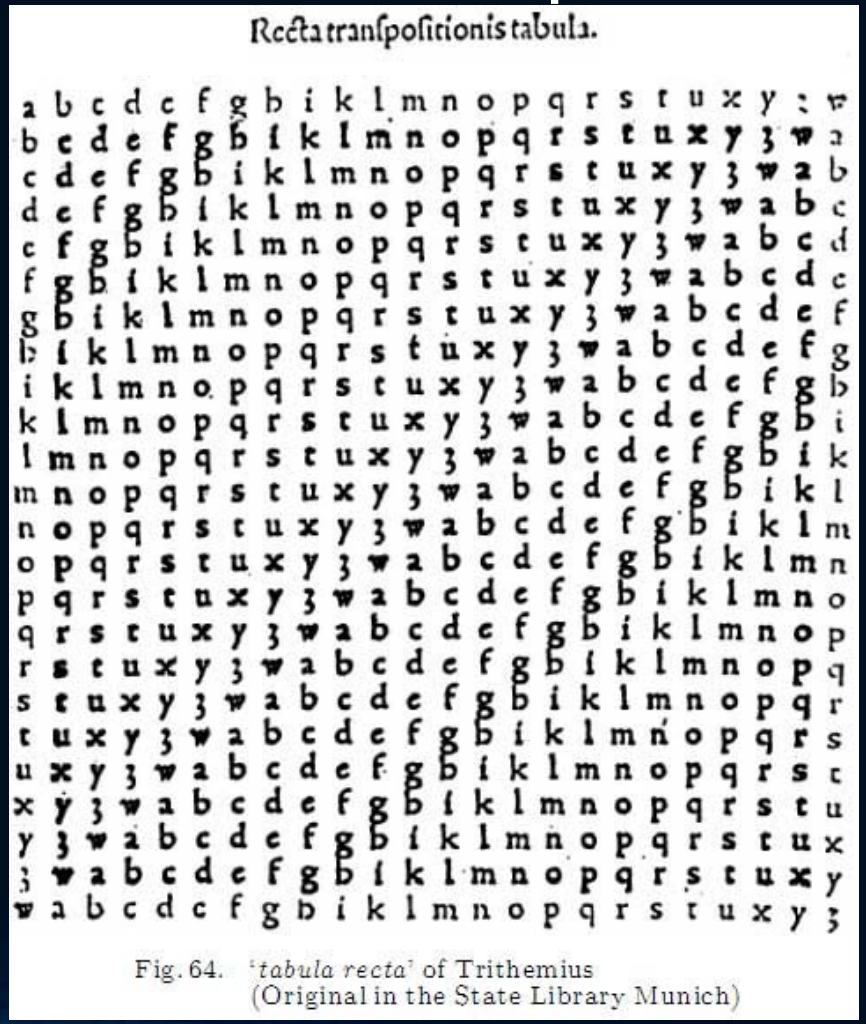


Fig. 64. '*tabula recta*' of Trithemius (Original in the State Library Munich)

Vigenere square

	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
1	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	A
2	C	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
3	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
4	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	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	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
23	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
24	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	X
25	Z	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
26	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

Keyword VOTEVOTEVOTEVOTEVOTE…
Plaintext ihavethreestinkydogs…
Ciphertext DVTZZHAVZSLXDBDCYCZW…

Immune to frequency analysis !

F. Bauer, Decrypted Secrets- Methods & Maxims of Cryptology, 4th Edition, Springer, 2007

Πολυαλφαβητική Αντικατάσταση

alphabet P generated by the mnemonic password NEWYORKCITY,

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

- Συνεισφορά Vigenere:
  1. Χρήση Μικτού Αλφάβητου με Κυκλική Ολίσθηση (Cyclically Shifted)
     - ~ δίσκος του Alberti
  2. Επιλογή του κρυπτοαλφάβητου (=αριθμός των ολισθήσεων) βάσει ενός περιοδικού κλειδιού

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

Ή:

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

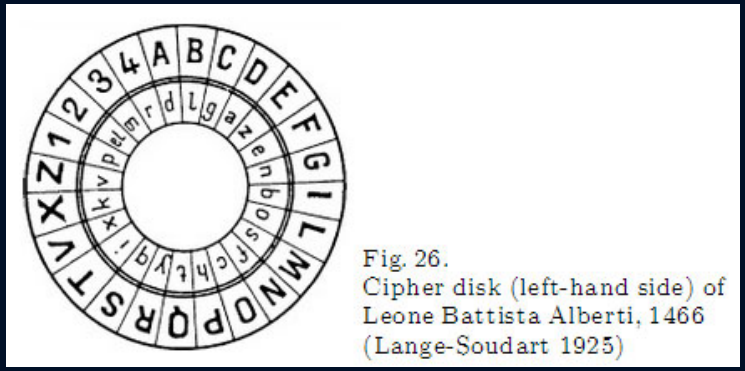
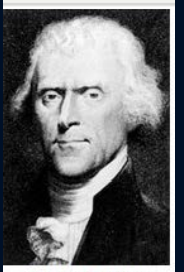


Fig. 26.
Cipher disk (left-hand side) of Leone Battista Alberti, 1466 (Lange-Soudart 1925)

F. Bauer, Decrypted Secrets- Methods & Maxims of Cryptology, 4th Edition, Springer, 2007


Thomas Jefferson
(1743–1826)

Πολυαλφαβητική Αντικατάσταση

- Επεκτάσεις:
  - Ανεξάρτητα Μικτά Αλφάβητα (unrelated mixed alphabets)

passwords serve to select a method from a class of methods and keys especially to select encryptions se…

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

Αν (για n=1) με βάση τα αλφάβητα που κατασκευάζονται με κυκλική ολίσθηση από ένα αρχικό αλφάβητο με N χαρακτήρες, τότε ο αριθμός των κλειδιών συμπίπτει με τον αριθμό των χαρακτήρων,

Το σώμα του κλειδιού αποτελεί μια μετάθεση και ανήκει στο κυκλικό σύνολο της τάξεως του N

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

Fig. 68. The twenty cycles of Bazeries

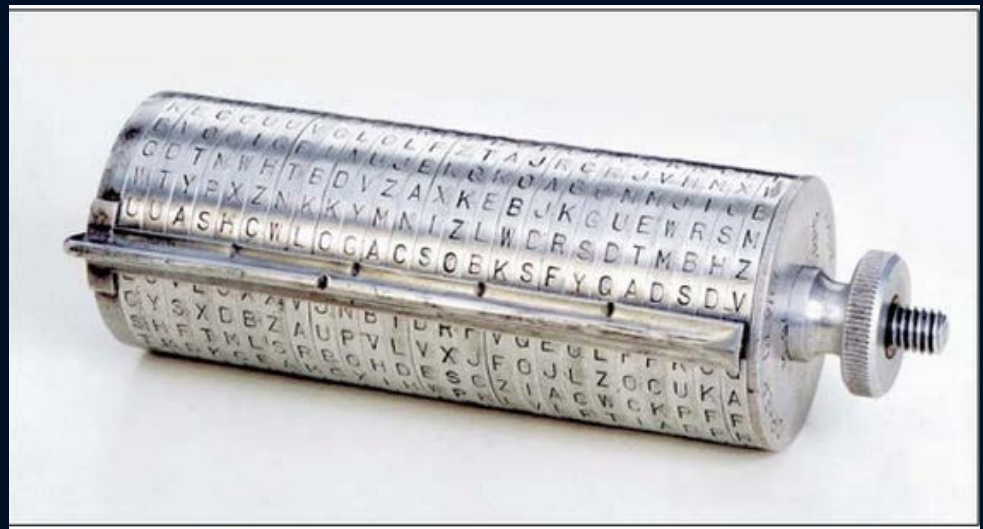


Plate D The U.S. Army Signal Corps Cipher Device M-94

This can still be cryptanalyzed:
- just N monoaphabetic substitution ciphers (N is length of key)
- so, just solve the N monoaphabetic problems as before

```
Keyword     VOTEVOTEVOTEVOTEVOTE…
Plaintext   ihavethreestinkydogs…
Ciphertext  DVTZZHAVZSLXDBDCYCZW…
```

DZZDY…
VHSBC…
TALDZ…
ZVXCW…

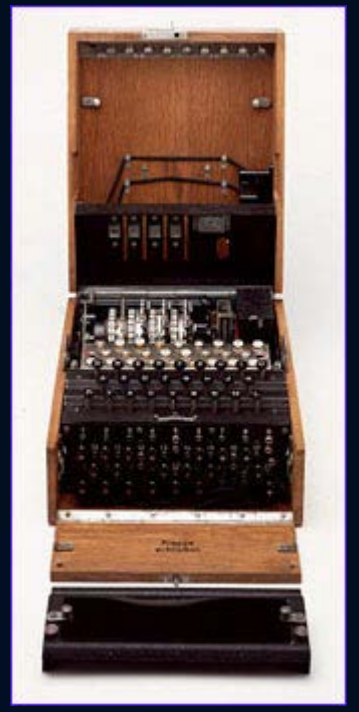
Do frequency analysis on these separately

OK, so make the key longer.
Make it as long as the message !

```
Keyword     VOTINGISIMPORTANTFOR…
Plaintext   ihavethreestinkydogs…
Ciphertext  DVTDRZPJMQPHAGKLWTUJ…
```

If there are patterns in the key (for example, words),
the message can still be decrypted with a bit of work.

Enigma: Repeated after $26^3 = 17{,}576$ letters
Successfully broken by Rajewski, Turing et al.
(a lot of work…protocol important)



However:

IF
If the key is as long as the message
AND
The key is completely random
THEN

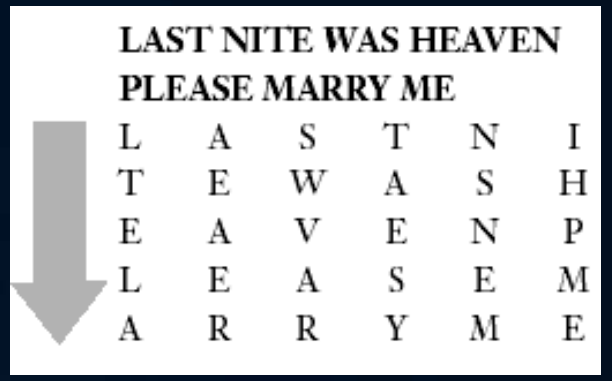
The encryption is perfect (can't be broken) !!!

This is called a "One Time Pad"

H. Mel, D. Baker. Cryptography Decrypted. Addison-Wesley, 2001

Αλγόριθμοι Αναδιάταξης* (Transposition Ciphers)

Απλή αντιμετάθεση



Διπλή αντιμετάθεση

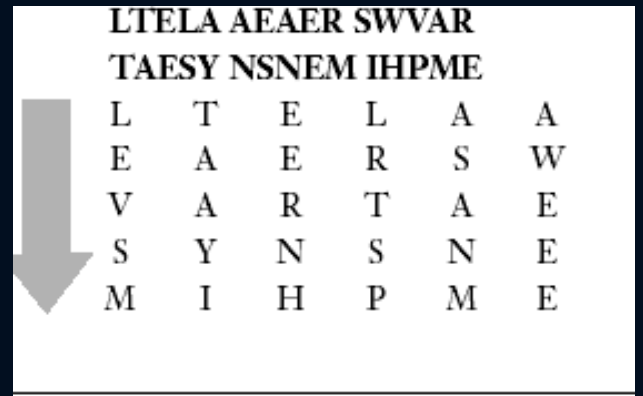


Figure 3-3 The output of Figure 3-2, enciphered.

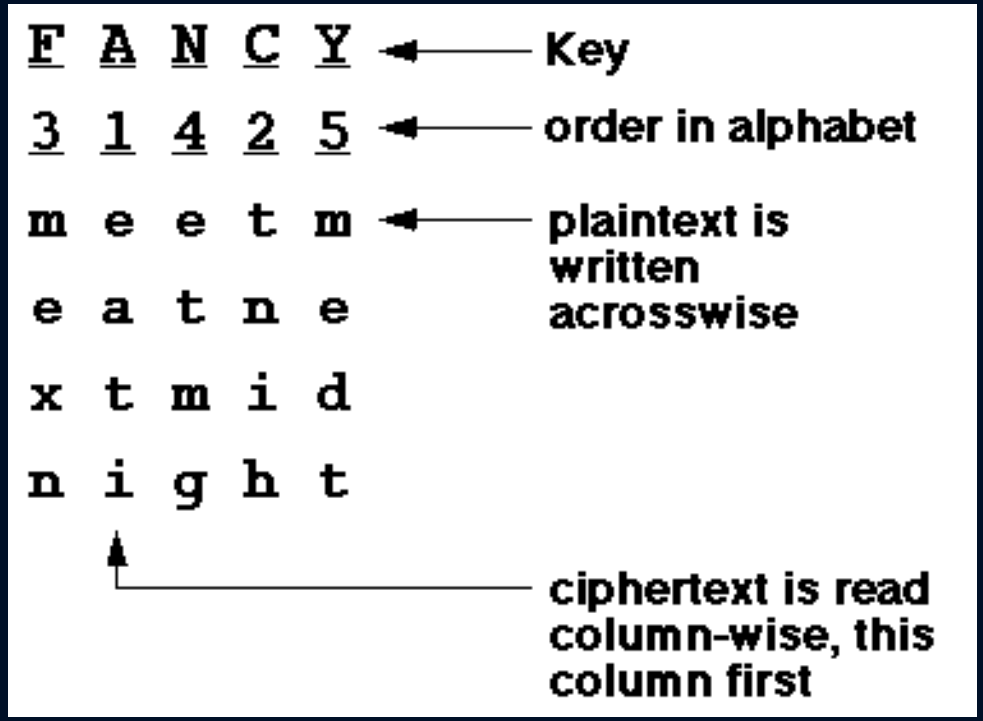
LTELAAEAERSWVARTAESYNSNEMIHPME

Κρυπτανάλυση = Εύρεση προτύπων (patterns)

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

Αλγόριθμοι Αναδιάταξης

Οι χαρακτήρες του αρχικού κειμένου δεν αλλάζουν μορφή, αλλάζει ωστόσο η θέση τους…



H. Mel, D. Baker.
Cryptography Decrypted.
Addison-Wesley, 2001

Αναδιάταξη στον Η/Υ

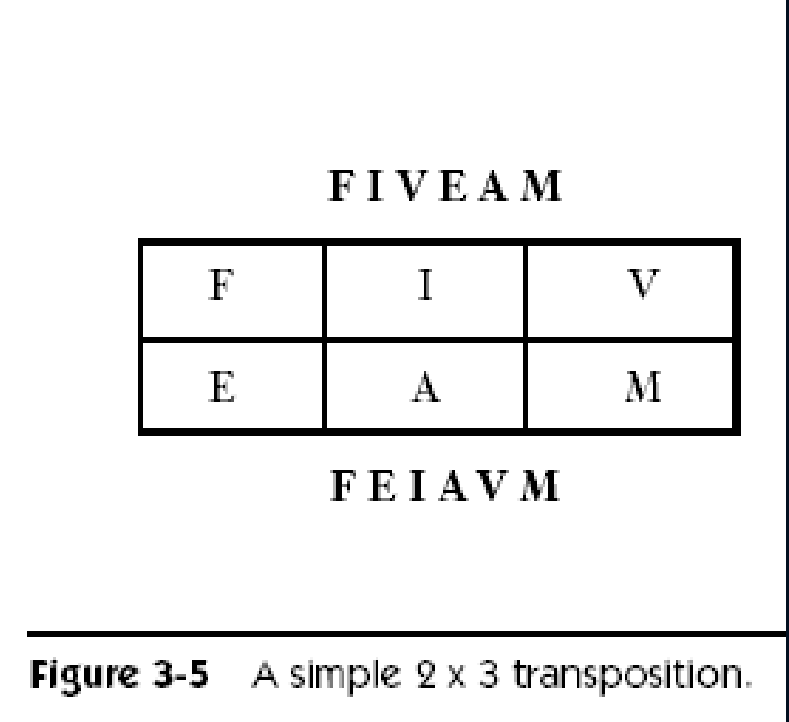


Figure 3-5 A simple 2 x 3 transposition.

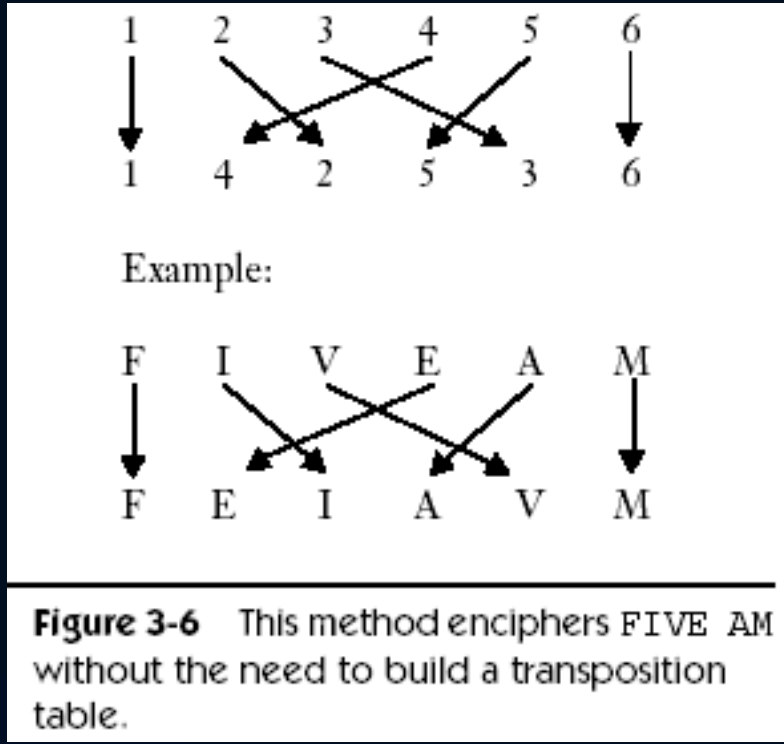
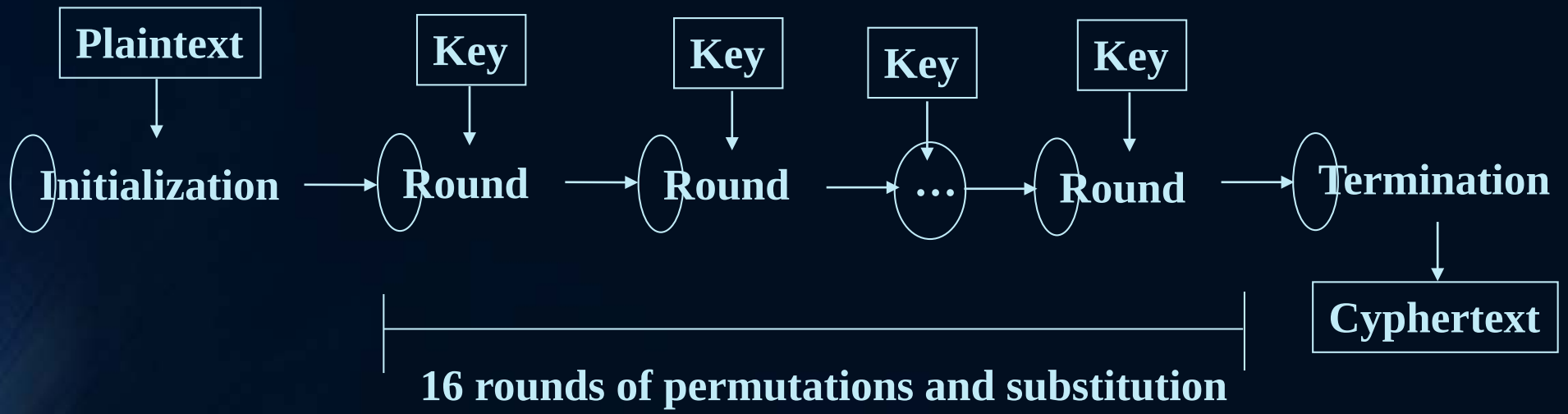


Figure 3-6 This method enciphers `FIVE AM` without the need to build a transposition table.

- Αντί να φτιάχνουμε έναν πίνακα αναδιάταξης με γραμμές και στήλες, είναι γρηγορότερο να πεις σε κάθε στοιχείο την καινούρια του θέση!

Παράδειγμα
Ο Αλγόριθμος DES – Αναδιάταξη P

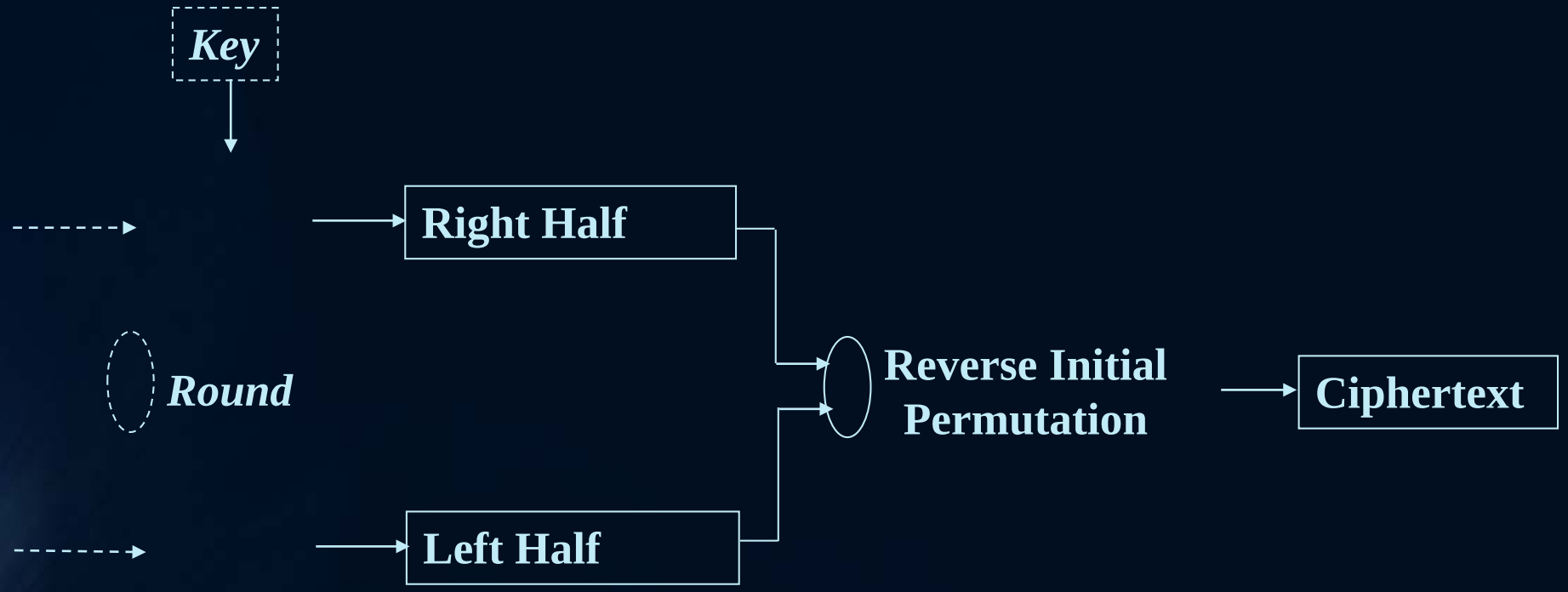


DES is a 64-bit block cipher. Both the plaintext and ciphertext are 64 bits wide.

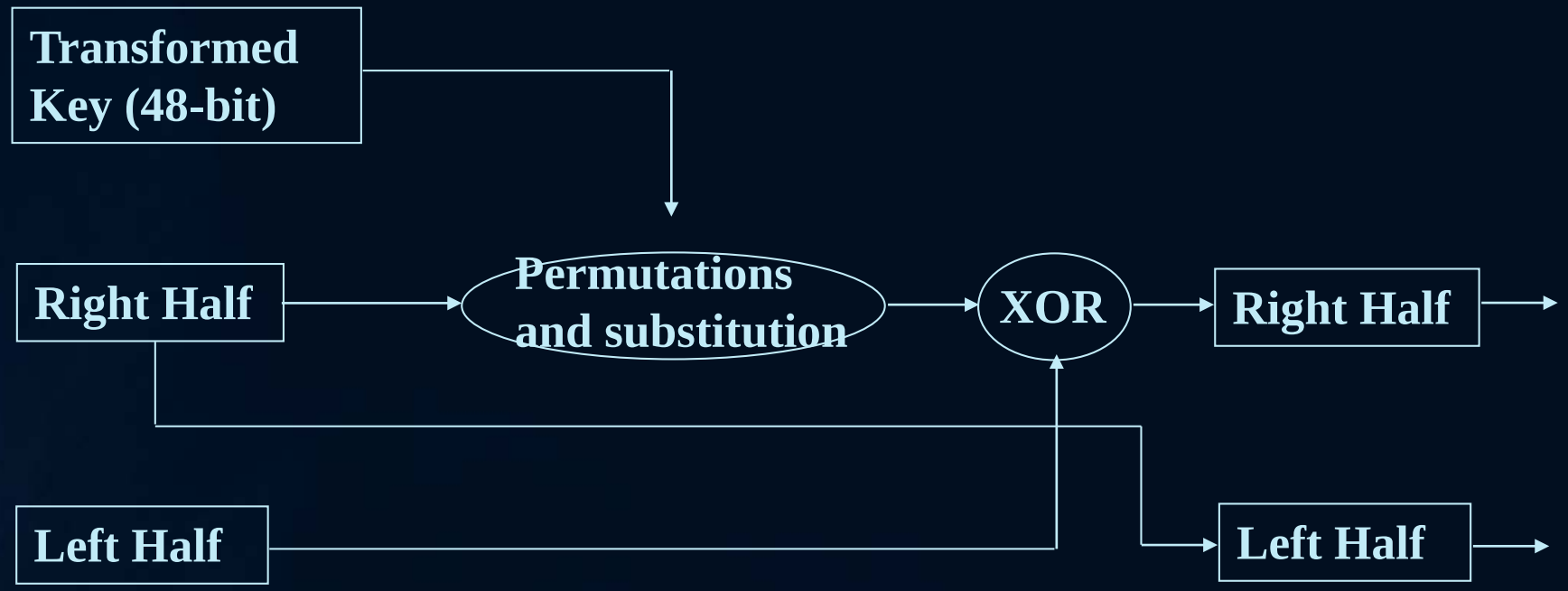
The key is 64-bits wide, but every eighth bit is a parity bit yielding a 54-bit key.

Initialization

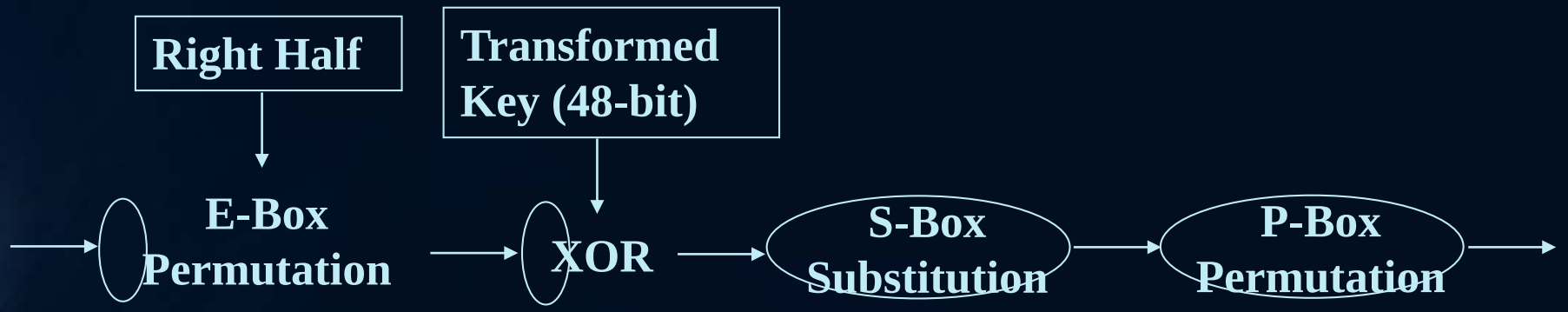
Termination



A Round

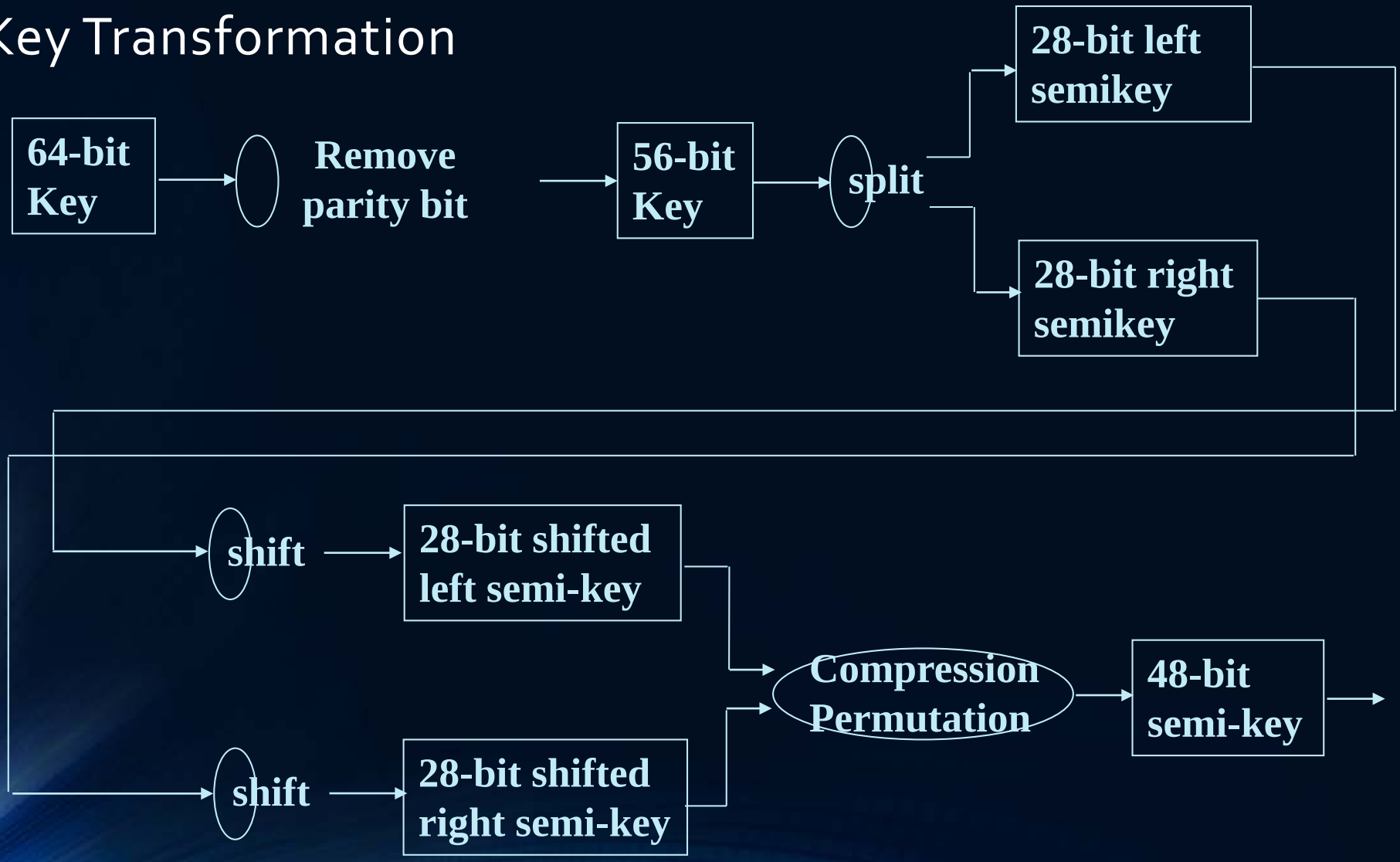

Transformed Key (48-bit)
Right Half
Permutations and substitution
XOR
Right Half
Left Half
Left Half

Permutations and Substitutions

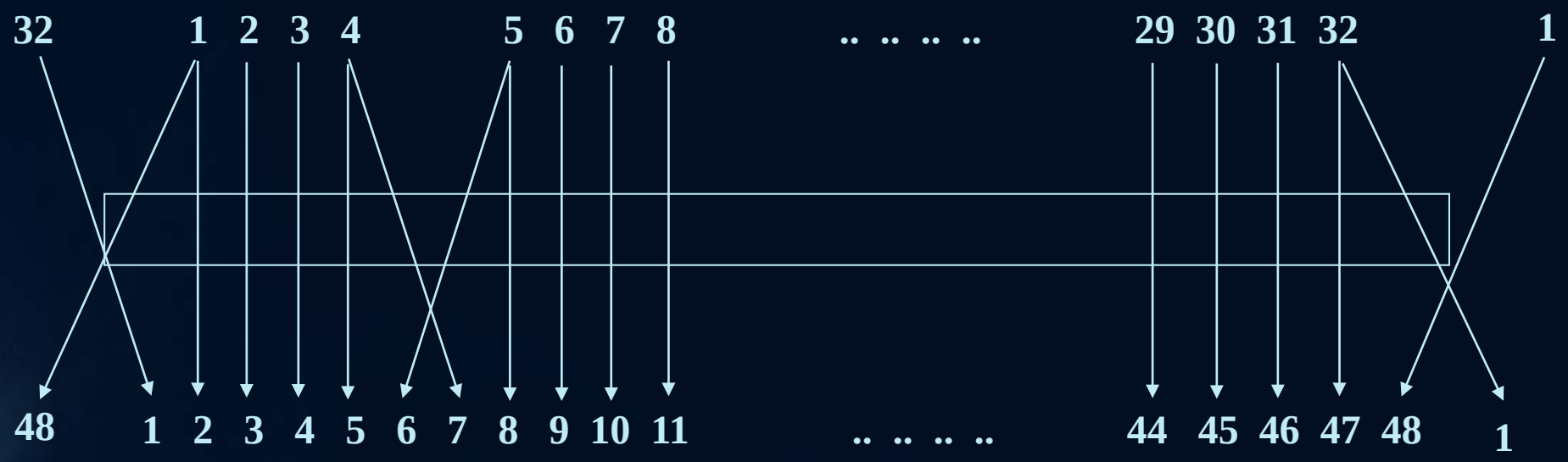


8 S-Boxes are used by the P-Box

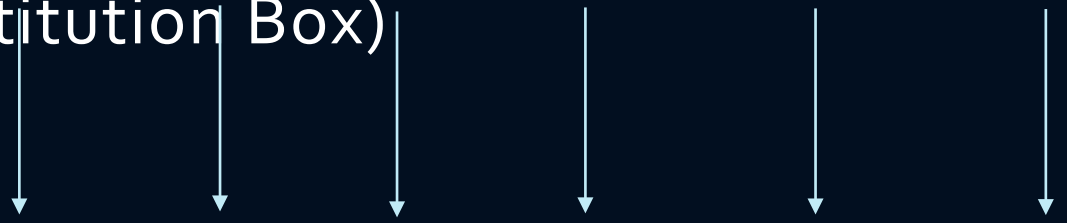
Key Transformation



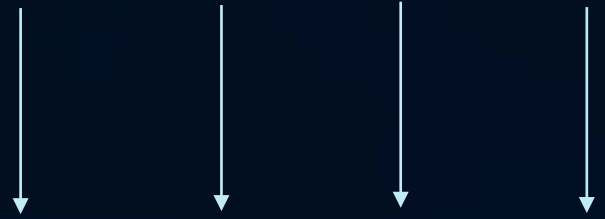
E-Box (Expansion Box)



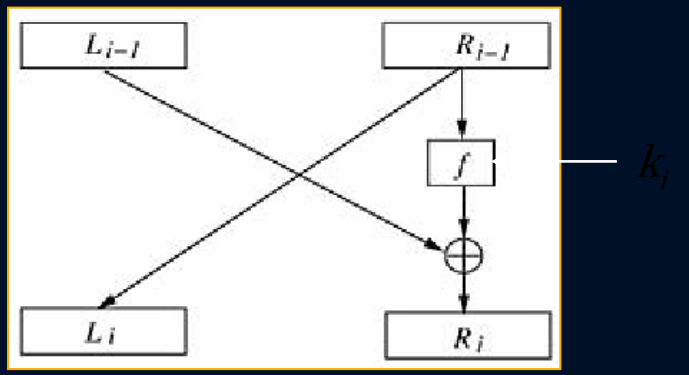
S-Box (Substitution Box)



- **There are 8 different S-Boxes, each of which provides a different 6:4 mapping. Where'd they come from? Some combination of IBM and NSA.**
- **The mappings are based on cryptanalysis and are ostensibly free of weaknesses, back-doors, &c.**



Stinson, D. Cryptography: Theory and Practice. Third Edition, CRC, 2005



Παράδειγμα

Ο Αλγόριθμος DES – Αναδιάταξη P

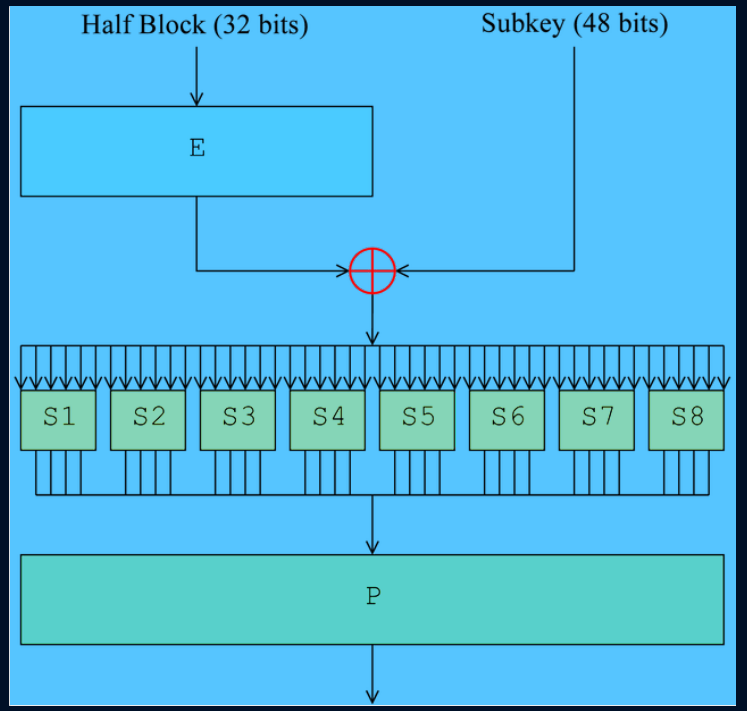
… Τα bit εξόδου όλων των S-box αναδιατάσσονται σύμφωνα με την *P*.

P			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

$P(C) = (c_{16}, c_7, c_{20}, c_{21}, c_{29}, \ldots, c_{11}, c_4, c_{25})$

π.χ. το bit string C = ($c_1, c_2, \ldots c_{32}$)

Η Συνάρτηση f (1 γύρος)



Ο αλγόριθμος DES, εφαρμόζει 16 κύκλους αναδιάταξης και αντικατάστασης σε κάθε ομάδα 8 χαρακτήρων (block = 64 bit)

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

Κρυπτογραφία – Παρωχημένες Θεωρήσεις

- Ο αποστολέας στέλνει ένα μήνυμα στον παραλήπτη
- Επιπλέον, ο αποστολέας επιθυμεί ασφάλεια !
  - Ασφάλεια = Εμπιστευτικότητα (Confidentiality)
- Κρυπτογραφία = Η «τέχνη» απόκρυψης μηνυμάτων
- Κρυπτανάλυση = Η «τέχνη» (μη εξουσιοδοτημένης) εύρεσης του αρχικού μηνύματος
  - Παράκαμψη του κρυπτογραφικού μηχανισμού
- Κρυπτολογία = Η μελέτη τεχνικών κρυπτογραφίας και κρυπτανάλυσης

«Κλασσική» αντίληψη περί ασφάλειας

N. Ferguson, B. Schneier. Practical Cryptography. Wiley, 2003

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Σύγχρονη Θεώρηση: Κρυπτογραφία και Ασφάλεια Πληροφορίας

... Κρυπτογραφία είναι η μελέτη μαθηματικών τεχνικών, σχετικών με πτυχές της Ασφάλειας Πληροφοριών όπως η Εμπιστευτικότητα (Confidentiality), η Ακεραιότητα (Integrity), η Αυθεντικοποίηση Οντότητας (Entity Authentication), η Αυθεντικοποίηση Μηνύματος (Data Origin Authentication), ο Καταλογισμός Ευθύνης (Non Repudiation) ...

Menezes et al

... Η κρυπτογραφία δεν αποτελεί το μόνο μέσο για την επίτευξη της Ασφάλειας Πληροφορίας, ωστόσο προσφέρει ένα σύνολο από τεχνικές (κρυπτογραφικά εργαλεία – cryptographic tools) προς αυτήν την κατεύθυνση...

... Ο ρόλος της κρυπτογραφίας εντοπίζεται στο κομμάτι της πρόληψης και της ανίχνευσης...

Ferguson-Schneier, 2003

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

Επιπρόσθετες Υπηρεσίες…

Συχνά, η κρυπτογραφία «προσπαθεί» να επιτελέσει και άλλες «εργασίες»…

1. Αυθεντικοποίηση Οντότητας
    1. Επαλήθευση της ταυτότητας ενός χρήστη (σε πραγματικό χρόνο)
    - Ποιος είσαι;

    Εργαλεία: Πρόκληση-Απάντηση, Απο-δείξεις Μηδενικής Γνώσης (ZKP),…
2. Αυθεντικοποίηση Μηνύματος
    2. Επαλήθευση της ταυτότητας αποστολέα του μηνύματος (όχι απαραίτητα σε πραγματικό χρόνο)
    - Ποιος δημιούργησε το μήνυμα που πήρα;

    Εργαλεία: Συναρτήσεις MAC, ψηφιακή υπογραφή,…
3. Ακεραιότητα (Integrity)
    - Ο παραλήπτης επαληθεύει ότι το μήνυμα δεν «αλλοιώθηκε» κατά τη μεταφορά.
    - Είναι το μήνυμα που έλαβα ίδιο με το αρχικό μήνυμα;

    Εργαλεία: Συναρτήσεις Hash,…
4. Καταλογισμός Ευθύνης (Non Repudiation)
    - Ο αποστολέας δε μπορεί να αρνηθεί ότι έστειλε ένα μήνυμα

    Εργαλεία: Ψηφιακή Υπογραφή,..

Menezes, Oorschot, Vanston
Applied Cryptography, CRC,

Κρυπτογραφία
: Μία Θεώρηση

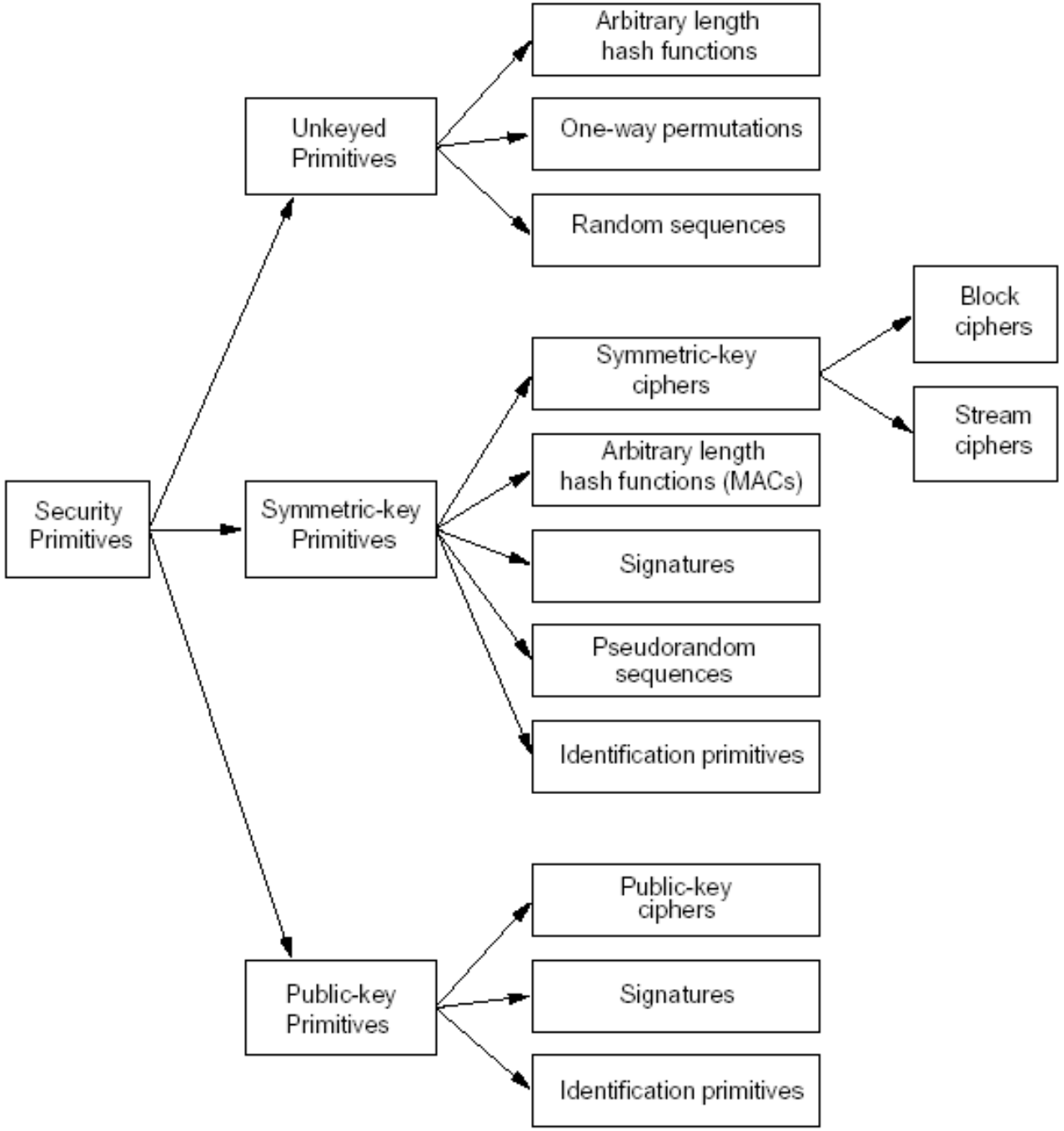
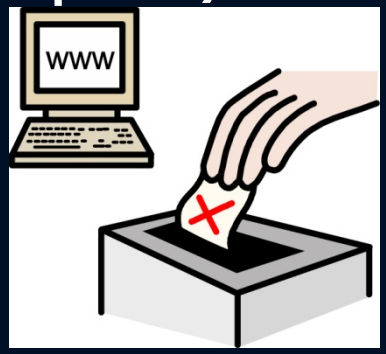


Figure 1.1: *A taxonomy of cryptographic primitives.*

Mao, W. Modern Cryptography: Theory and Practice. Prentice Hall, 2003

Ο Σύγχρονος Ρόλος της Κρυπτογραφίας



Modern Role of Cryptography:

Ensuring Fair Play of Games…

Mao, W. Modern Cryptography: Theory and Practice. Prentice Hall, 2003

Protocol 1.1: Coin Flipping Over Telephone

PREMISE

Alice and Bob have agreed:

i. a "magic function" f with properties specified in Property 1.1

ii. an even number x in $f(x)$ represents HEADS and the other case represents TAILS

[redacted]

1. Alice picks a large random integer x and computes $f(x)$; she reads $f(x)$ to Bob over the phone;
2. Bob tells Alice his guess of x as even or odd;
3. Alice reads x to Bob;
4. Bob verifies $f(x)$ and sees the correctness/incorrectness of his guess.

Ας μελετήσουμε το ακόλουθο πρόβλημα...

Δύο (ή περισσότερες) οντότητες,
διαθέτουν από μία βάση δεδομένων
με εμπιστευτικά (ευαίσθητα)
δεδομένα, και επιθυμούν την
εκτέλεση ενός αλγορίθμου εξόρυξης
δεδομένων στην ένωση των βάσεων,
χωρίς να αποκαλυφθούν τα
επιμέρους δεδομένα...

X_1

X_2

Σημείωση: Οι δύο οντότητες ΔΕΝ ΕΜΠΙΣΤΕΥΟΝΤΑΙ η μία την άλλη

(Lindell and Pinkas, 2000)

Ένα «Ιδανικό» πρωτόκολλο

Θα σας βοηθήσω !! Αν με εμπιστεύεστ ...

...

16 Tons

X_1

X_2

$F(X_1,X_2)$

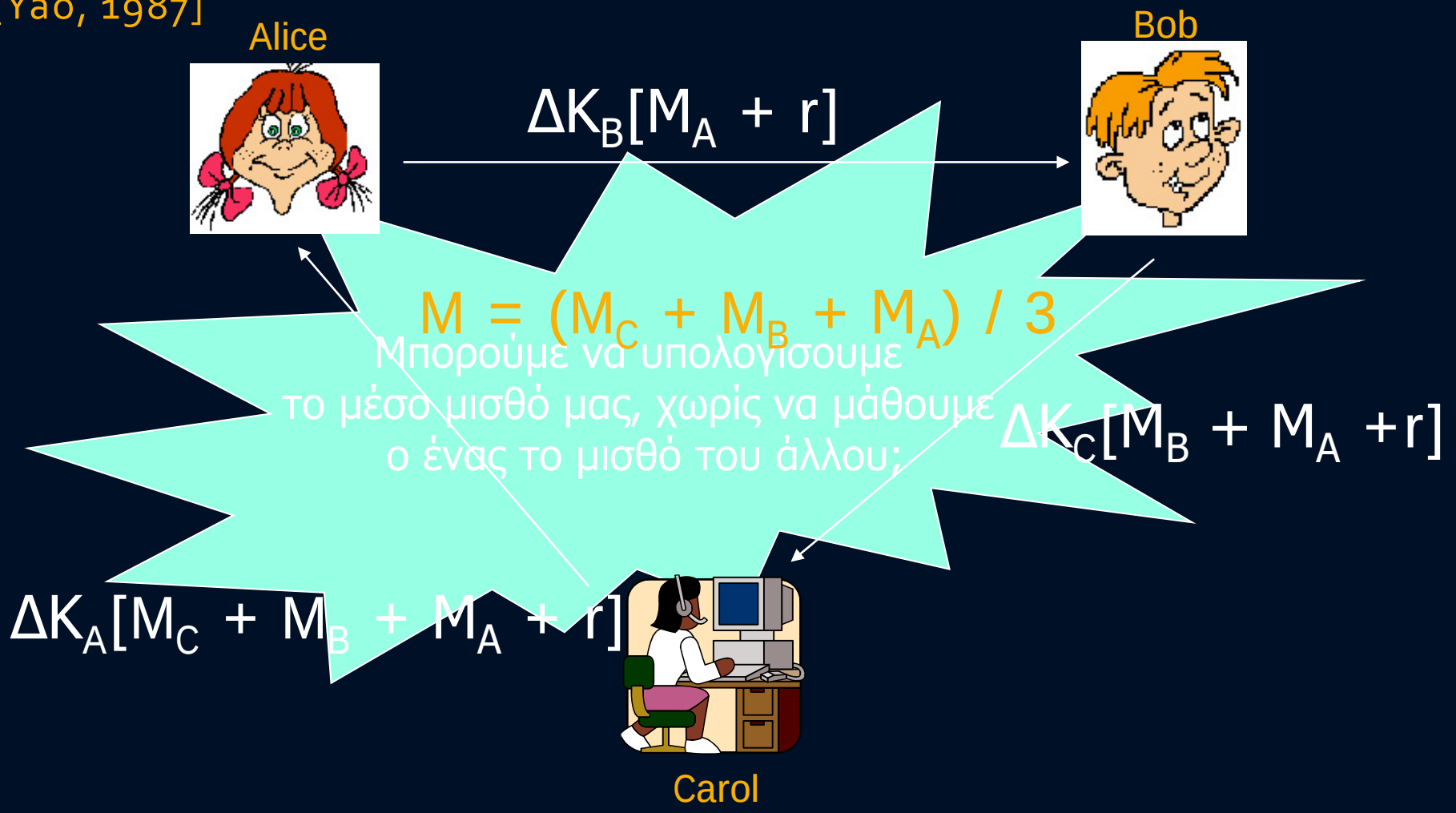
$F(X_1,X_2)$

Στόχος: Η υλοποίηση συστημάτων που «μοιάζουν» με το ιδανικό σύστημα…

Πώς? Με τη χρήση κρυπτογραφικών τεχνικών και μεθόδων …

Secure Multiparty Computation (SMC)

[Yao, 1987]



Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Μοντέλο Κρυπτογραφικής Επικοινωνίας

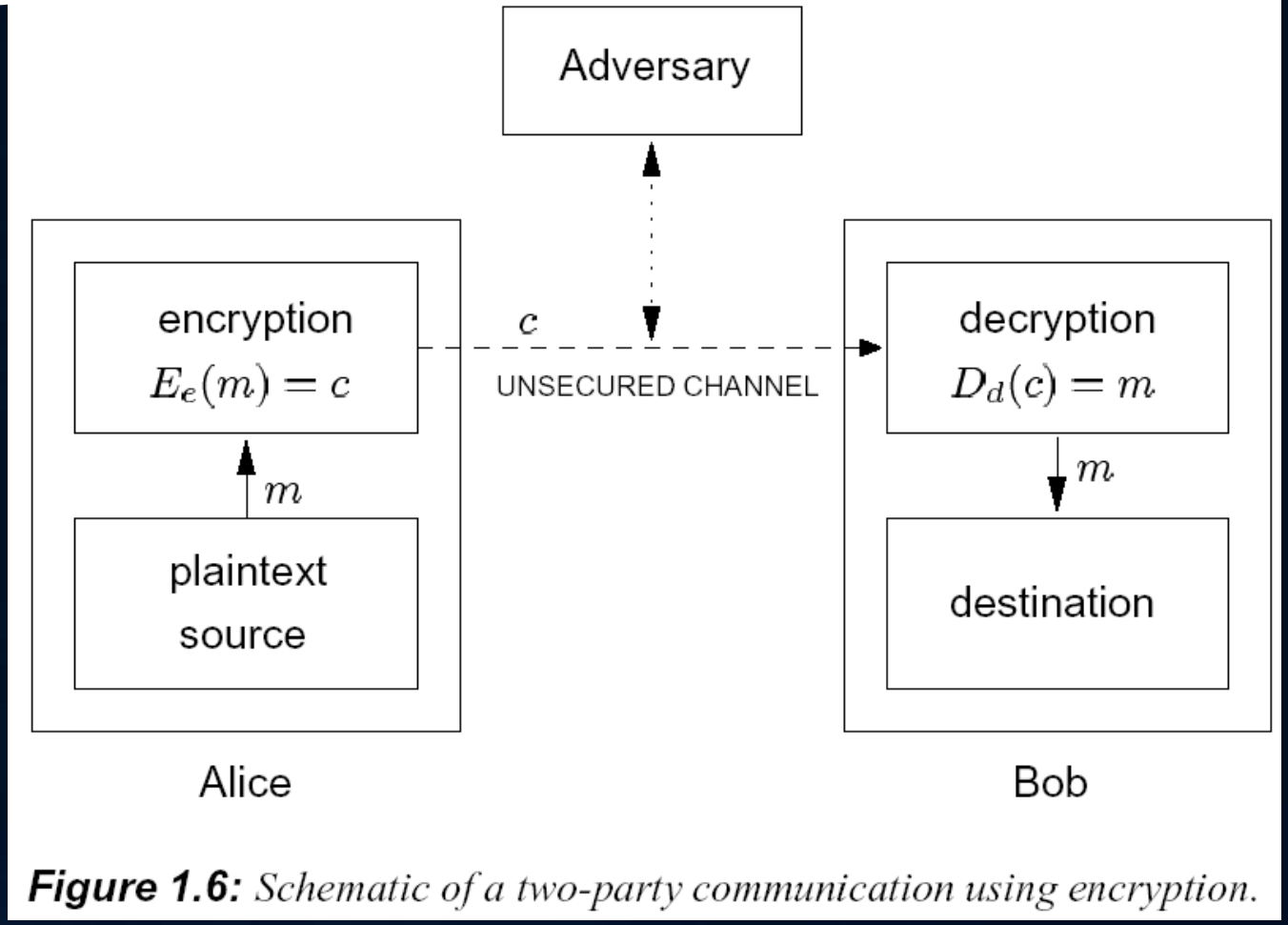


Figure 1.6: *Schematic of a two-party communication using encryption.*

- Συστατικά Στοιχεία: Αλγόριθμοι, Υποκείμενα, Κανάλια Επικοινωνίας

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Αλγόριθμοι Κρυπτογράφησης

=*Συναρτήσεις*

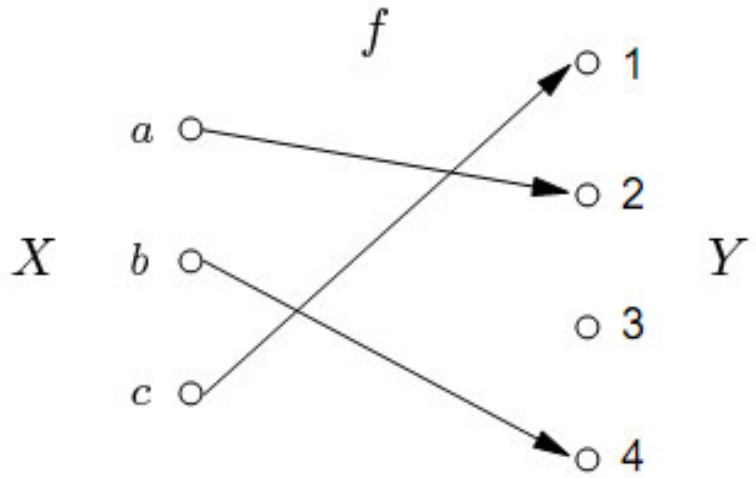


Figure 1.2: *A function f from a set X of three elements to a set Y of four elements.*

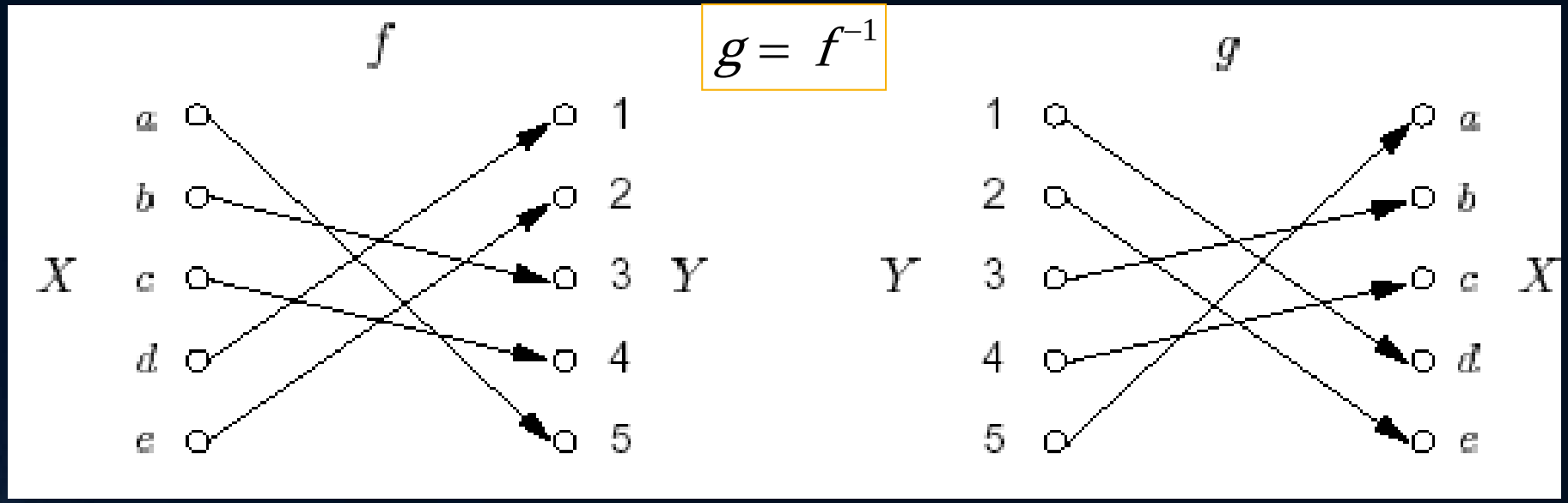
1.4 Example (*function*) Take $X = \{1, 2, 3, \ldots, 10\}$ and let f be the rule that for each $x \in X$, $f(x) = r_x$, where r_x is the remainder when x^2 is divided by 11. Explicitly then

$$f(1) = 1 \quad f(2) = 4 \quad f(3) = 9 \quad f(4) = 5 \quad f(5) = 3$$
$$f(6) = 3 \quad f(7) = 5 \quad f(8) = 9 \quad f(9) = 4 \quad f(10) = 1.$$

The image of f is the set $Y = \{1, 3, 4, 5, 9\}$. □

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Αλγόριθμοι Κρυπτογράφησης και Αποκρυπτογράφησης
= *Αντιστρέψιμες Συναρτήσεις*



- Παράδειγμα: οι συναρτήσεις *f* και *g* περιγράφουν ένα μετασχηματισμό για την κρυπτογράφηση και την αποκρυπτογράφηση αντίστοιχα

Μία συνάρτηση *f* που είναι 1-1 (injective) και Επί (Surjective) αντιστρέφεται.

Η αντιστρέψιμη συνάρτηση *f: X→ X* ονομάζεται αντιμετάθεση (permutation)

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Αλγόριθμοι Κρυπτογράφησης και Αποκρυπτογράφησης
= *Συναρτήσεις*

1.18 Example (*permutation*) Let $\mathcal{S} = \{1, 2, 3, 4, 5\}$. A permutation p: $\mathcal{S} \longrightarrow \mathcal{S}$ is defined as follows:

$$p(1) = 3,\ p(2) = 5,\ p(3) = 4,\ p(4) = 2,\ p(5) = 1.$$

A permutation can be described in various ways. It can be displayed as above or as an array:

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}, \qquad (1.1)$$

Μια συνάρτηση $f: X \rightarrow X$ που αντιστρέφεται ονομάζεται και αντιμετάθεση (permutation)

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Αλγόριθμοι Κρυπτογράφησης

Συναρτήσεις

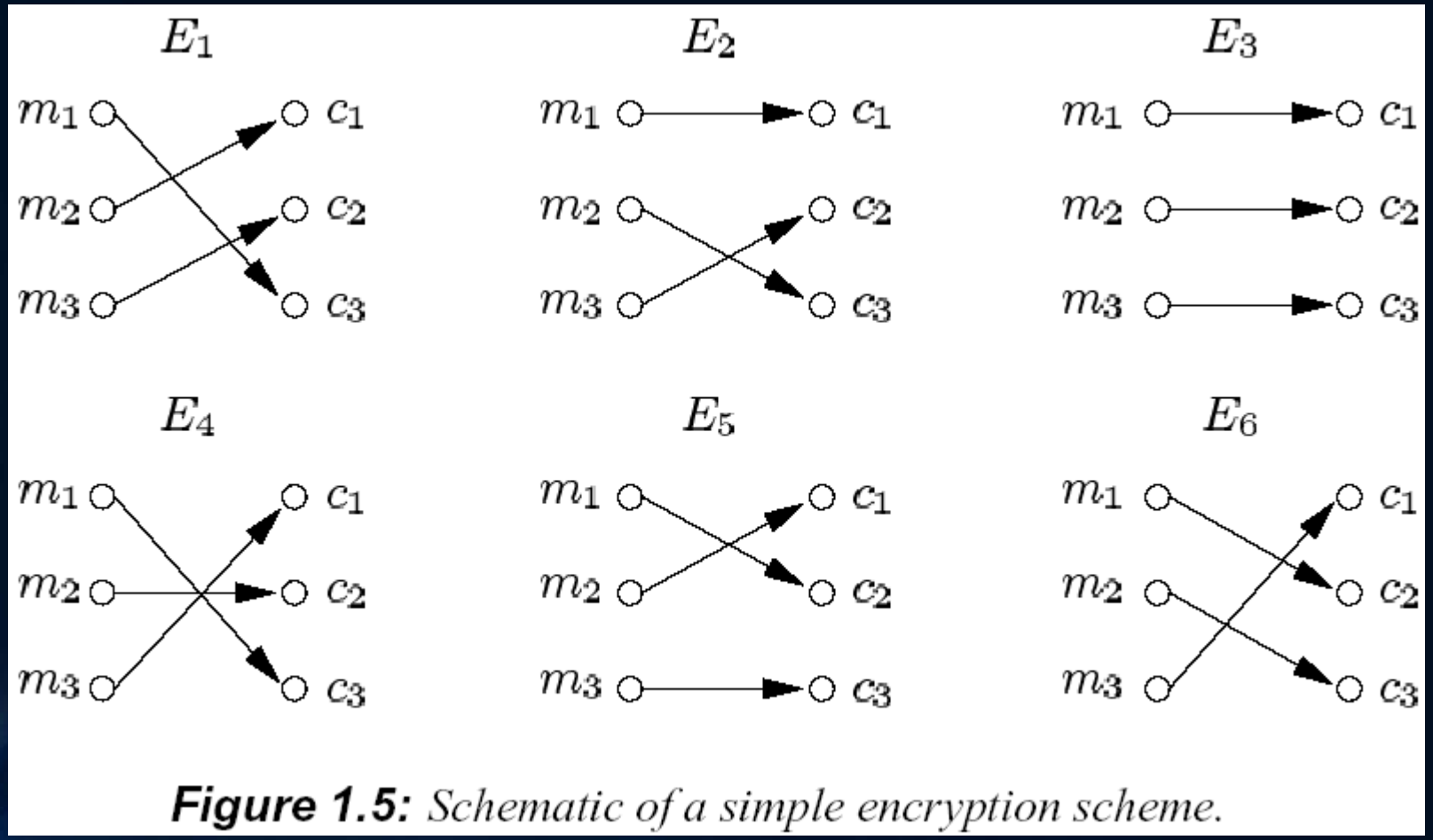
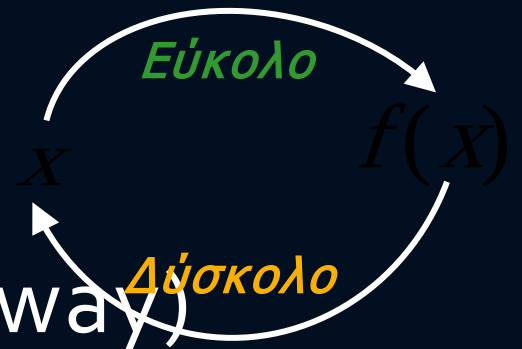


Figure 1.5: *Schematic of a simple encryption scheme.*

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



Μονόδρομες Συναρτήσεις (One-way)

- Μονόδρομες Συναρτήσεις
  - Εύκολος ο υπολογισμός τους
  - «Δύσκολη» η αντιστροφή τους

It would take millions of years to compute x from f(x), even if all the computers in the world were assigned to the problem

Δεν έχει αποδειχθεί η ύπαρξη τους

- Ποια θα μπορούσε να είναι η χρήση των μονόδρομων συναρτήσεων;
  1. Ακεραιότητα και Αυθεντικοποίηση
     - Θα εξεταστεί στη συνέχεια
  2. Κρυπτογράφηση
     - Ένσταση: κανείς δε θα μπορούσε να ανακτήσει το M !!

Μονόδρομες Συναρτήσεις & Κρυπτογράφηση

- Μονόδρομες συναρτήσεις κρυφής εισόδου (trapdoor one way)
  - One-way: Εύκολος ο υπολογισμός
  - Αντιστροφή: Δύσκολη, εκτός και εάν κάποιος γνωρίζει τη μυστική πληροφορία (trapdoor)
  - Οι αλγόριθμοι δημοσίου κλειδιού βασίζονται στην ύπαρξη τους
    - π.χ. Η κρυπτογράφηση με τον αλγόριθμο RSA θεωρείται μονόδρομη συνάρτηση
    - Η μυστική πληροφορία για την αντιστροφή του RSA είναι οι πρώτοι παράγοντες του n

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Μοντέλο Επικοινωνίας
Υποκείμενα

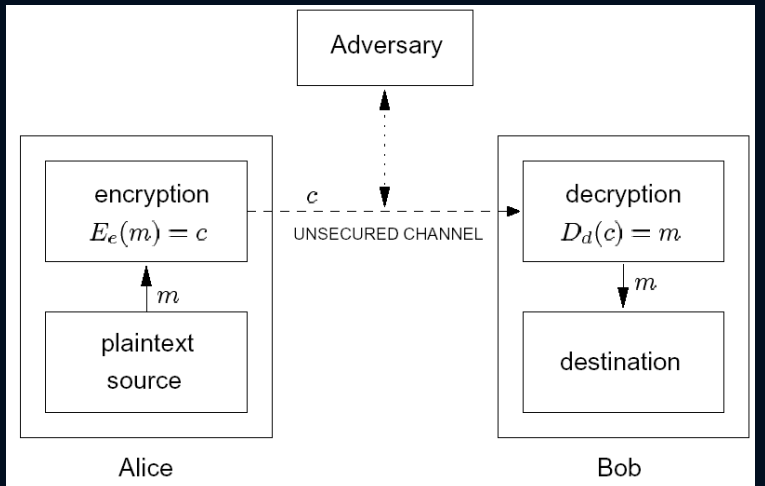


Figure 1.6: *Schematic of a two-party communication using encryption.*

- Υποκείμενα που *στέλνουν*, *λαμβάνουν*, ή *τροποποιούν* πληροφορία
  - Alice, Bob, Eve, Mallory, Trent, ...

1. Ο νόμιμος (εξουσιοδοτημένος) αποστολέας (π.χ. Alice)
2. Ο νόμιμος (εξουσιοδοτημένος) παραλήπτης (π.χ. Bob)
3. Ο εχθρός του συστήματος (μη εξουσιοδοτημένος)
   - Στοχεύει κατά της ασφάλειας του συστήματος
     - Η Eve υποκλέπτει (eavesdropping - παθητική επίθεση)
     - Ο Mallory τροποποιεί, διαγράφει, εισάγει μηνύματα (ενεργητική επίθεση)

Σημείωση: Ο εχθρός του συστήματος μπορεί να είναι και ένας εκ των Alice, Bob !!!!!!

4. Μία ή περισσότερες Τρίτες Έμπιστες Οντότητες (TTP) – Ο Trent

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Κρυπτανάλυση –Τύποι Επιθέσεων

Δύο ειδών επιθέσεις

- Παθητικές Επιθέσεις (Passive Attacks)
  - Ο εχθρός υποκλέπτει το κανάλι
    - Οι παθητικές επιθέσεις στοχεύουν κατά της Εμπιστευτικότητας
- Ενεργητικές Επιθέσεις (Active Attacks)
  - Ο εχθρός επιχειρεί να διαγράψει, εισαγάγει, ή τροποποιήσει τα μηνύματα που μεταδίδονται στο κανάλι
    - Οι ενεργητικές επιθέσεις μπορεί να στοχεύουν κατά της Εμπιστευτικότητας, Ακεραιότητας ή Αυθεντικοποίησης

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

Κρυπτανάλυση –Τύποι Επιθέσεων

Παθητικές Επιθέσεις

Θεωρούμε ότι ο κρυπταναλυτής γνωρίζει τους αλγορίθμους…

1. Ciphertext-only attack
   - Ο κρυπταναλυτής έχει στην κατοχή του ένα ή περισσότερα κρυπτογραφημένα μηνύματα και προσπαθεί να ανακτήσει κάποιο αρχικό μήνυμα ή το κλειδί που χρησιμοποιήθηκε
2. Known-Plaintext attack
   - Ο κρυπταναλυτής έχει στην κατοχή του ένα ή περισσότερα κρυπτογραφημένα μηνύματα καθώς και το(α) αντίστοιχα αρχικά μηνύματα και προσπαθεί να ανακτήσει το κλειδί που χρησιμοποιήθηκε.
3. Chosen Plaintext attack
   - Ο κρυπταναλυτής επιλέγει ένα ή περισσότερα μηνύματα και στη συνέχεια αποκτά τα αντίστοιχα κρυπτογραφημένα μηνύματα. Έπειτα, προσπαθεί να ανακτήσει κάποιο άλλο μήνυμα ή το κλειδί που χρησιμοποιήθηκε.

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

Κρυπτανάλυση –Τύποι Επιθέσεων

Παθητικές Επιθέσεις

…

- Άλλες επιθέσεις
  - Adaptive chosen plaintext
  - Chosen ciphertext
  - Adaptive chosen ciphertext

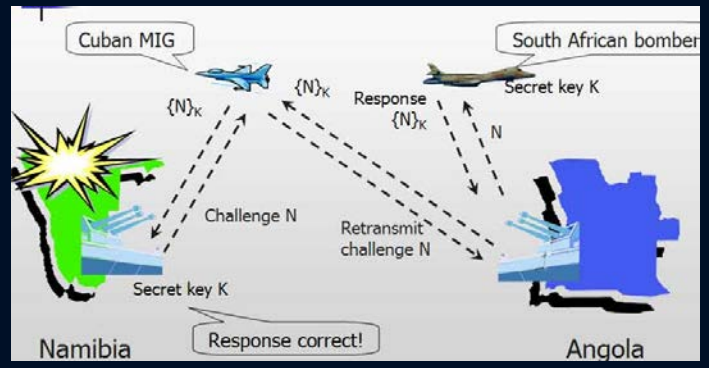
Προς το παρόν δεν θα μας απασχολήσουν !

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Τύποι Επιθέσεων

Άλλες (πιο μοντέρνες) Επιθέσεις

1. Επίθεση γνωστού κλειδιού (Known Key attack)
   - Ο εχθρός αποκτά πρόσβαση σε κάποιο κλειδί (τρέχον ή παλαιότερο) και προσπαθεί να εξαπολύσει μια επίθεση



2. Επίθεση Επανάληψης (Replay Attack)
   - Ο εχθρός υποκλέπτει μια σύνοδο (session) επικοινωνίας και μετά τη χρησιμοποιεί (ολόκληρη ή κάποιο τμήμα της) σε μια καινούρια σύνοδο… - Ενεργητική Επίθεση

3. Επίθεση Πλαστοπροσωπίας (Impersonation Attack)
   - Ο εχθρός εμφανίζεται αντί άλλου, με σκοπό αθέμιτο (λεξικό Τεγόπουλου-Φυτράκη) - Ενεργητική Επίθεση

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Μοντέλο Επικοινωνίας

Κανάλια Μετάδοσης

- Κανάλι (Channel)
  - Μέσο μεταφοράς της πληροφορίας από ένα υποκείμενο σε κάποιο άλλο
- Φυσικά Προστατευμένο Κανάλι (Physically Secured Channel)
  - Κανάλι στο οποίο ο εχθρός δεν έχει φυσική πρόσβαση
- Μη Ασφαλές Κανάλι (Unsecured Channel)
  - Κανάλι στο οποίο είναι εφικτή η μη εξουσιοδοτημένη πρόσβαση από κάποιον τρίτο με σκοπό υποκλοπή, αλλοίωση, διαγραφή ή εισαγωγή.
- Ασφαλές Κανάλι (Secured Channel)
  - Κανάλι στο οποίο ΔΕΝ είναι εφικτή η μη εξουσιοδοτημένη … (ομοίως)
    - Ένα μη ασφαλές κανάλι μπορεί να γίνει ασφαλές χρησιμοποιώντας κρυπτογραφικές τεχνικές, ή εφαρμόζοντας φυσική προστασία !

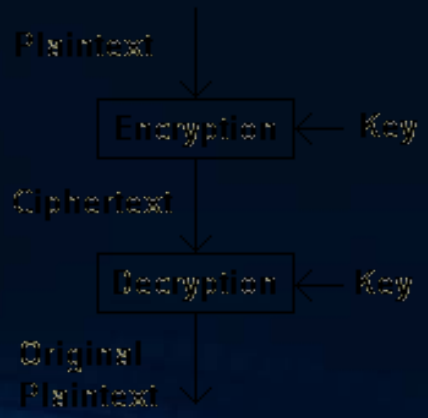
Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.

Ασφάλεια Κρυπτοσυστήματος

Μυστικότητα Αλγορίθμου

- Κρυπτογραφικός αλγόριθμος (cipher)
  - Μία μαθηματική συνάρτηση για κρυπτογράφηση και αποκρυπτογράφηση

1. Η ασφάλεια του συστήματος θα πρέπει να βασίζεται στη μυστικότητα του αλγορίθμου;
   - Πρόβλημα: Τι θα γίνει αν ο αλγόριθμος γίνει γνωστός;
2. Η ασφάλεια του συστήματος βασίζεται στην ύπαρξη ενός κλειδιού
   - (A. Kerchoffs - 1883)



Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Ασφάλεια Κρυπτοσυστήματος

Ο κανόνας του Kerckhoffs (1883)

1. the system should be, if not theoretically unbreakable, unbreakable in practice;
2. compromise of the system details should not inconvenience the correspondents;
3. the key should be rememberable without notes and easily changed;
4. the cryptogram should be transmissible by telegraph;
5. the encryption apparatus should be portable and operable by a single person; and
6. the system should be easy, requiring neither the knowledge of a long list of rules nor mental strain.

Η ασφάλεια του συστήματος δεν πρέπει να βασίζεται στη μυστικότητα του αλγορίθμου...

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

Ασφάλεια Κρυπτοσυστήματος (Συνέχεια)

- Η ασφάλεια είναι «σχετική». Παραδείγματα:
  1. Αν το «κόστος» παραβίασης ενός αλγορίθμου είναι μεγαλύτερο από την αξία των υπό προστασία δεδομένων, τότε είμαστε (πιθανόν) ασφαλείς !!
  2. Αν ο χρόνος που απαιτείται για να «σπάσει» ο αλγόριθμος είναι μεγαλύτερος από το χρόνο, κατά τον οποίο πρέπει να μείνουν μυστικά τα δεδομένα, τότε είμαστε (πιθανόν) ασφαλείς!!
  3. Αν η ποσότητα των δεδομένων που κρυπτογραφούνται με ένα κλειδί είναι μικρότερη από την ελάχιστη ποσότητα κρυπτ/μένου κειμένου που χρειάζεται ο κρυπταναλυτής, τότε είμαστε (πιθανόν) ασφαλείς !!

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Ασφάλεια Κρυπτοσυστήματος

Απόλυτη Ασφάλεια (1) και Υπολογιστική Ασφάλεια (2)

1. Απόλυτη Ασφάλεια (Unconditional - Perfect Secrecy)
   - Έστω πανίσχυρος κρυπταναλυτής βλέπει κρυπτογραφημένο μήνυμα
     - Πανίσχυρος = «Άπειροι υπολογιστικοί πόροι»
   - … Ο Μ δεν μπορεί να «βρει» το αρχικό κείμενο
     - Περίπτωση: One-time Pad

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Ασφάλεια Κρυπτοσυστήματος

Απόλυτη Ασφάλεια

1. Απόλυτη Ασφάλεια (Unconditional - Perfect Secrecy)
   - Έστω πανίσχυρος κρυπταναλυτής βλέπει κρυπτογραφημένο μήνυμα
     - Πανίσχυρος = «Άπειροι υπολογιστικοί πόροι»
   - … Ο Μ δεν μπορεί να «βρει» το αρχικό κείμενο
     - Περίπτωση: One-time Pad
   - Ας δώσουμε έναν άλλο ορισμό

Ένα σχήμα κρυπτογράφησης είναι ασφαλές, όταν η βεβαιότητα του κρυπταναλυτή για το αρχικό μήνυμα ΠΡΙΝ δει το κρυπτογράφημα, δεν μεταβάλλεται ΜΕΤΑ (αφού δει το κρυπτογράφημα).

Διαίσθηση για τον Ορισμό:

- Παρατηρώντας το κρυπτογράφημα, ο εχθρός δεν "κερδίζει" σε γνώση

one-time pad

Για να αποφύγει στατιστικής ανάλυσης επιθέσεις—δεν υπάρχουν πρότυπα

- Το ιδιωτικό κλειδί δημιουργείται τυχαία και χρησιμοποιείται μόνο μία φορά για να κρυπτογραφήσει ένα μήνυμα , με μήκος αντίστοιχο του μηνύματος
- Αποκρυπτογραφούμε χρησιμοποιώντας μια αντιστοιχία one-time pad και το κλειδί.
- Αδύνατον να «σπάσει ο κώδικας» αναλύοντας μια διαδοχή των μηνυμάτων.
- Κάθε κρυπτογράφηση είναι μοναδική και δεν έχει καμία σχέση με την επόμενη κρυπτογράφηση, ώστε να μπορεί να ανιχνευθεί κάποια μοτίβο.
- Στο one-time pad, αυτός που αποκρυπτογραφεί πρέπει να έχει πρόσβαση στο ίδιο κλειδί που χρησιμοποιείται για να κρυπτογραφήσει
  - πώς θα διανεμηθεί το κλειδί
- Αν το μυστικό κλειδίαποκαλύπτεται, τα μηνύματα κρυπτογραφούνται με αυτό μπορεί εύκολα να αποκρυπτογραφηθεί.

Ομοιόμορφη κατανομή συχνότητ γραμμάτων

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

http://en.wikipedia.org/wiki/One_time_pad#Example

and the message is "HELLO", then the coding is done as follows:

```
   23 (X)   12 (M)    2 (C)   10 (K)   11 (L) key
+   7 (H)    4 (E)   11 (L)   11 (L)   14 (O) message
= 30        16       13       21       25     key + message
=  4 (E)   16 (Q)   13 (N)   21 (V)   25 (Z) key + message (mod 26)
```

plaintext. Here, the key is *subtracted* from the ciphertext, again using modular arithmetic:

```
    4 (E)   16 (Q)   13 (N)   21 (V)   25 (Z) ciphertext
-  23 (X)   12 (M)    2 (C)   10 (K)   11 (L) key
= -19        4       11       11       14     ciphertext - key
=   7 (H)    4 (E)   11 (L)   11 (L)   14 (O) ciphertext - key (mod 26)
```

the key material sequence "TQURI" giving the plaintext "LATER", an equally plausible message:

```
    4 (E)   16 (Q)   13 (N)   21 (V)   25 (Z) ciphertext
-  19 (T)   16 (Q)   20 (U)   17 (R)    8 (I) possible key
= -15        0       -7       4        17     ciphertext-key
=  11 (L)    0 (A)   19 (T)    4 (E)   17 (R) ciphertext-key (mod 26)
```

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Απόλυτη Ασφάλεια (Perfect Secrecy)

Ορισμός

Μοντέλο Απειλών (Threat Model)

- **Τύπος Εχθρού:** Παθητικός (ciphertext-only),
- **Υπολογιστική Ισχύς**: άπειρη
- **Εκ των προτέρων γνώση**: Ο εχθρός γνωρίζει την κατανομή πιθανότητας στο σύνολο των υποψήφιων μηνυμάτων

ΟΡΙΣΜΟΣ 2.1. *Ένα σχήμα κρυπτογράφησης* (Gen, Enc, Dec) *σε ένα σύνολο μηνυμάτων* M *είναι απόλυτα ασφαλές αν για κάθε κατανομή πιθανότητας στο* M, *κάθε μήνυμα* $m \in M$ *και κάθε κρυπτογράφημα* $c \in C$ *για το οποίο* $\Pr[C = c] > 0$ *ισχύει:*

$$\Pr[M = m \mid C = c] = \Pr[M = m]$$

Stinson, D. Cryptography: Theory and Practice. Third Edition, CRC, 2005

Απόλυτη Ασφάλεια (Perfect Secrecy)

Ένα παράδειγμα (όχι απόλυτη ασφάλεια)

Παράδειγμα. *Έστω* $M=\{a,b\}$ *με* $P[a]=1/4$, $P[b]=3/4$. *Έστω* $K=\{K_1,K_2,K_3\}$ *με* $P[K_1]=1/2$, $P[K_2]=P[K_3]=1/4$. *Έστω* $C=\{1,2,3,4\}$ και ας υποθέσουμε ότι οι συναρτήσεις κρυπτογράφησης ορίζονται ως: $Enc_{K_1}(a)=1$, $Enc_{K_1}(b)=2$, $Enc_{K_2}(a)=2$, $Enc_{K_2}(b)=3$, $Enc_{K_3}(a)=3$, $Enc_{K_3}(b)=4$. *Το κρυπτοσύστημα αναπαρίσταται ως εξής:*

	a	b
K_1	1	2
K_2	2	3
K_3	3	4

Για να υπολογίσουμε τη συνάρτηση κατανομής στο C, αξιοποιούμε τη σχέση:

$$P[C=c]=\sum_{k:c\in\{Enc_k(m):m\in M\}} P(K=k)P[m=Dec_k(c)] \qquad (1)$$

½*1/4 $P[1]=\frac{1}{8}$ $P[2]=\frac{3}{8}+\frac{1}{16}=\frac{7}{16}$ ½*3/4+1/4*1/4

¼*3/4+1/1*14 $P[3]=\frac{3}{16}+\frac{1}{16}=\frac{1}{4}$ $P[4]=\frac{3}{16}$ ¼*3/4

Stinson, D. Cryptography: Theory and Practice. Third Edition, CRC, 2005

	a	b
K_1	1	2
K_2	2	3
K_3	3	4

Απόλυτη Ασφάλεια (Perfect Secrecy)

Ένα παράδειγμα (όχι απόλυτη ασφάλεια)

Παράδειγμα. Έστω $M=\{a,b\}$ με $P[a]=1/4$, $P[b]=3/4$. Έστω $K=\{K_1,K_2,K_3\}$ με $P[K_1]=1/2$, $P[K_2]=P[K_3]=1/4$. Έστω $C=\{1,2,3,4\}$ και ας υποθέσουμε ότι οι συναρτήσεις κρυπτογράφησης ορίζονται ως: $Enc_{K_1}(a)=1$, $Enc_{K_1}(b)=2$, $Enc_{K_2}(a)=2$, $Enc_{K_2}(b)=3$, $Enc_{K_3}(a)=3$, $Enc_{K_3}(b)=4$.

Για την κατανομή δεσμευμένης πιθανότητας στο M, αξιοποιούμε τη σχέση:

$$P[C=c\mid M=m]=\sum_{k:m=Dec_k(c)}P(K=k) \qquad (2)$$

και υπολογίζουμε:

$$P[M=m\mid C=c]=\frac{P[C=c\mid M=m]\times P[M=m]}{P[C=c]}\overset{(1),(2)}{=}\frac{\sum_{k:m=Dec_k(c)}P(K=k)\times P[M=m]}{\sum_{k:c\in\{Enc_k(m):m\in M\}}P(K=k)P[m=Dec_k(c)]} \qquad (3)$$

$P[1]=\frac{1}{8}$ $\quad P[a\mid 1]=1$ $\quad P[b\mid 1]=0$

$P[2]=\frac{3}{8}+\frac{1}{16}=\frac{7}{16}$ $\quad P[a\mid 2]=\frac{1}{7}$ $\quad P[b\mid 2]=\frac{6}{7}$

$P[3]=\frac{3}{16}+\frac{1}{16}=\frac{1}{4}$ $\quad P[a\mid 3]=\frac{1}{4}$ $\quad P[b\mid 3]=\frac{3}{4}$

$P[4]=\frac{3}{16}$ $\quad P[a\mid 4]=0$ $\quad P[b\mid 4]=1$

Τι παρατηρείτε;

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Απόλυτη Ασφάλεια

Ισοδύναμοι Ορισμοί

ΛΗΜΜΑ 2.2. *Ένα σχήμα κρυπτογράφησης* (Gen, Enc, Dec) *σε ένα σύνολο μηνυμάτων* M *είναι απόλυτα ασφαλές αν και μόνο αν για κάθε κατανομή πιθανότητας στο* M*, κάθε μήνυμα* $m \in M$ *και κάθε κρυπτογράφημα* $c \in C$*:*

$$\Pr[C = c \mid M = m] = \Pr[C = c]$$

ΛΗΜΜΑ 2.3. *Ένα σχήμα κρυπτογράφησης* (Gen, Enc, Dec) *σε ένα σύνολο μηνυμάτων* M *είναι απόλυτα ασφαλές αν και μόνο αν για κάθε κατανομή πιθανότητας στο* M*, κάθε* $m_0, m_1 \in M$ *και κάθε* $c \in C$*:*

$$\Pr[C = c \mid M = m_0] = \Pr[C = c \mid M = m_1]$$

Ένας άλλος τρόπος να πούμε ότι το κρυπτογράφημα δεν “προδίδει” πληροφορία για το μήνυμα

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Απόλυτη Ασφάλεια

Ισοδύναμη Ορισμού Perfect Indistinguishability

Πείραμα $\mathrm{Priv}K^{εαν}_{A,Π}$ Μη Διάκρισης από Παθητικό Εχθρό (με Άπειρη Υπολογιστική Δύναμη)

1. *Ο εχθρός A εξάγει ένα ζεύγος τιμών $m_0, m_1 \in M$.*
2. *Εκτελώντας τον Gen, παράγεται ένα τυχαίο κλειδί k και στη συνέχεια γίνεται επιλογή ενός τυχαίου bit $b \leftarrow \{0,1\}$. (Αυτά εκτελούνται από μια φανταστική οντότητα που εκτελεί το πείραμα μαζί με τον A.) Στη συνέχεια, υπολογίζεται και δίνεται στον A ένα κρυπτογράφημα $c \leftarrow Enc_k(m_b)$.*
3. *Ο A εξάγει ένα bit b'.*
4. *Η έξοδος του πειράματος ορίζεται ως 1 αν $b' = b$, αλλιώς ορίζεται ως 0. Αν η έξοδος είναι 1 γράφουμε $\mathrm{Priv}K^{εαν}_{A,Π} = 1$, και σε αυτήν την περίπτωση λέμε ότι ο A ήταν επιτυχής.*

ΟΡΙΣΜΟΣ 2.4 *Ένα σχήμα κρυπτογράφησης (Gen, Enc, Dec) σε ένα σύνολο μηνυμάτων M είναι απόλυτα ασφαλές αν για κάθε εχθρό A ισχύει:*

$$\Pr[\mathrm{Priv}K^{εαν}_{A,Π} = 1] = \frac{1}{2}$$

ΠΡΟΤΑΣΗ 2.5 *Έστω (Gen, Enc, Dec) ένα κρυπτογραφικό σχήμα σε ένα σύνολο μηνυμάτων M. Τότε το (Gen, Enc, Dec) είναι απόλυτα ασφαλές ως προς τον ορισμό 2.1 αν και μόνο αν είναι απόλυτα ασφαλές ως προς τον ορισμό 2.4.*

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Απόλυτη Ασφάλεια

Ο αλγόριθμος One-Time Pad (Vernam Cipher)

One-Time Pad (Vernam Cipher)

1. Ορίζουμε έναν ακέραιο $\ell > 0$. Τότε το σύνολο των μηνυμάτων M, το σύνολο των κλειδιών K και το σύνολο των κρυπτογραφημάτων C ισούνται με το $\{0,1\}^{\ell}$ (δηλ. το σύνολο όλων των δυαδικών συμβολοσειρών μήκους ℓ).
2. Ο αλγόριθμος δημιουργίας κλειδιού *Gen* δουλεύει ως εξής: Επιλέγουμε μια συμβολοσειρά από το $K = \{0,1\}^{\ell}$ σύμφωνα με την ομοιόμορφη κατανομή (δηλ. κάθε μία από τις 2^{ℓ} συμβολοσειρές στο K επιλέγεται ως το κλειδί με πιθανότητα $2^{-\ell}$).
3. Η κρυπτογράφηση *Enc* δουλεύει ως ακολούθως: δεδομένου ενός κλειδιού $k \in \{0,1\}^{\ell}$ και ενός μηνύματος $m \in \{0,1\}^{\ell}$, δώσε στην έξοδο: $c := k \oplus m$.
4. Η αποκρυπτογράφηση *Dec* δουλεύει ως ακολούθως: δεδομένου ενός κλειδιού $k \in \{0,1\}^{\ell}$ και ενός κρυπτογραφήματος $c \in \{0,1\}^{\ell}$, δώσε στην έξοδο: $m := k \oplus c$.

Παράδειγμα

- **Αρχικό μήνυμα (plaintext)**
  - Το μήνυμα IF, κωδικοποιείται (ASCII) ως 1001001 1000110
- **Κλειδί (pad)**
  - Έστω το κλειδί 1010110 0110001
- **Κρυπτογράφηση (encryption)**

1001001 1000110	plaintext
1010110 0110001	key
0011111 1110111	ciphertext

- **Αποκρυπτογράφηση (decryption)**

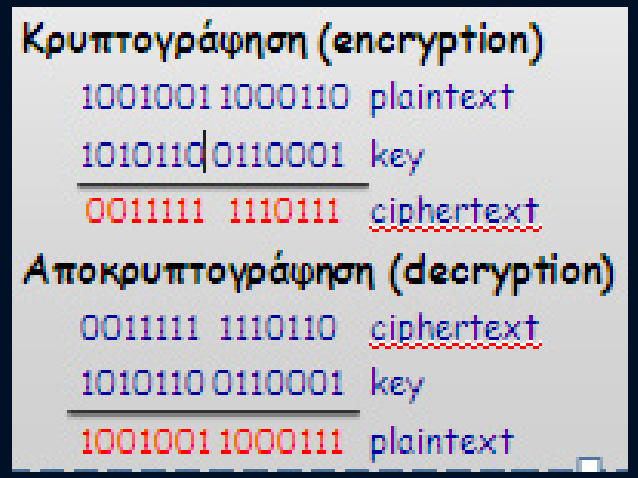
0011111 1110110	ciphertext
1010110 0110001	key
1001001 1000111	plaintext

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Γιατί ο Αλγόριθμος one-time pad είναι απόλυτα ασφαλής; (Shannon)

- Διαισθητικά, θέλουμε να δείξουμε ότι το *c* δεν αποκαλύπτει καμία πληροφορία για το μήνυμα *m*. Αυτό ισχύει γιατί:
  1. Για κάθε πιθανό *m*, υπάρχει ένα κλειδί *k* τέτοιο ώστε $c = Enc_k(m)$.

     Συγκεκριμένα, $k = m \oplus c$
  1. Κάθε κλειδί επιλέγεται τυχαία (και κρυφά από τον εχθρό), επομένως κανένα από τα παραπάνω κλειδιά δεν είναι πιο πιθανό!



- π.χ. βλέποντας το κρυπτογράφημα, μπορούμε να θεωρήσουμε ότι κάποιο αρχικό μήνυμα είναι περισσότερο πιθανό από κάποιο άλλο?

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

Αλγόριθμος Μιας Χρήσης (One-time Pad)
(*Vernam cipher - 1917)*

Περίπτωση («πώς θα μεταμφιέσουμε ένα κρυπτογραφημένο μήνυμα»)

- Η Alice κρυπτογραφεί για τον Bob ένα μήνυμα P με το κλειδί K (που «μοιράζεται» με τον Bob).
- Η Alice επιλέγει επίσης ένα «αθώο» μήνυμα D και ένα «πλαστό» κλειδί K′ (ώστε αν τη συλλάβουν να αθωωθεί !!!!!:

Η Alice υπολογίζει ένα K′ τέτοιο ώστε:

$K' = C \oplus D$

Η Αστυνομία κατάσχει το C, αξιώνει από την Alice το κλειδί και αποκρυπτογραφεί:

$C \oplus K' = D$

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Απόλυτη Ασφάλεια

Ο αλγόριθμος One-Time Pad (Vernam Cipher)

One-Time Pad (Vernam Cipher)

1. Ορίζουμε έναν ακέραιο $\ell > 0$. Τότε το σύνολο των μηνυμάτων M, το σύνολο των κλειδιών K και το σύνολο των κρυπτογραφημάτων C ισούνται με το $\{0,1\}^{\ell}$ (δηλ. το σύνολο όλων των δυαδικών συμβολοσειρών μήκους ℓ).
2. Ο αλγόριθμος δημιουργίας κλειδιού *Gen* δουλεύει ως εξής: Επιλέγουμε μια συμβολοσειρά από το $K = \{0,1\}^{\ell}$ σύμφωνα με την ομοιόμορφη κατανομή (δηλ. κάθε μία από τις 2^{ℓ} συμβολοσειρές στο K επιλέγεται ως το κλειδί με πιθανότητα $2^{-\ell}$).
3. Η κρυπτογράφηση *Enc* δουλεύει ως ακολούθως: δεδομένου ενός κλειδιού $k \in \{0,1\}^{\ell}$ και ενός μηνύματος $m \in \{0,1\}^{\ell}$, δώσε στην έξοδο: $c := k \oplus m$.
4. Η αποκρυπτογράφηση *Dec* δουλεύει ως ακολούθως: δεδομένου ενός κλειδιού $k \in \{0,1\}^{\ell}$ και ενός κρυπτογραφήματος $c \in \{0,1\}^{\ell}$, δώσε στην έξοδο: $m := k \oplus c$.

ΘΕΩΡΗΜΑ 2.6 *Το σχήμα κρυπτογράφησης one-time pad είναι απόλυτα ασφαλές.*

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

Κλειδί Μιας Χρήσης (One-time Pad)
(*Vernam cipher)*

- Shanon (1942): Απόλυτη Ασφάλεια (Perfect Secrecy), εφόσον:
  1. Μήκος κλειδιού ίσο με μήκος μηνύματος: |K|=|M|
  2. Οι χαρακτήρες του κλειδιού είναι επιλεγμένοι με τυχαίο τρόπο
  3. Κάθε κλειδί χρησιμοποιείται *μία μόνο* φορά !!!
- Ερωτήματα – Θέματα πρακτικότητας
  - Πόσο εφικτή είναι η παραγωγή (μεγάλης ποσότητας) τυχαιότητας
  - Πόσο πρακτική είναι η αλλαγή κλειδιού για κάθε μήνυμα;
  - …

John Hershey.
Cryptography Demystified.
McGraw-Hill, 2003

Τεχνικές Κρυπτανάλυσης

One-time Pad

- Τι θα γίνει αν χρησιμοποιήσουμε δύο φορές το ίδιο κλειδί για να κρυπτογραφήσουμε δύο διαφορετικά μηνύματα;

Έστω

$C_1 = P_1 \oplus K$

και

$C_2 = P_2 \oplus K$

Τότε, ισχύει:

$C_1 \oplus C_2 = P_1 \oplus P_2$

- Μπορεί η Eve να χρησιμοποιήσει αυτήν την πληροφορία και να ανακτήσει τα αρχικά μηνύματα;

John Hershey.
Cryptography Demystified.
McGraw-Hill, 2003

Τεχνικές Κρυπτανάλυσης

One-time Pad – Μελέτη περίπτωσης

Table 3-1
A straightforward binary representation of plaintext

Plaintext	Binary	Plaintext	Binary	Plaintext	Binary
A	00000	J	01001	S	10010
B	00001	K	01010	T	10011
C	00010	L	01011	U	10100
D	00011	M	01100	V	10101
E	00100	N	01101	W	10110
F	00101	O	01110	X	10111
G	00110	P	01111	Y	11000
H	00111	Q	10000	Z	11001
I	01000	R	10001	space	11010

- Έστω κάποιος χρησιμοποίησε το ίδιο κλειδί για να κρυπτογραφήσει δύο διαφορετικά μηνύματα P_1 και P_2, δημιουργώντας έτσι τα CT_1 και CT_2

CT1: 11010 11111 01010 00111 10100 00000 00001 10111 01101
11000 01100 10101 00010 01000 00011 11000 11111
CT2: 01101 01110 00000 00101 01011 01100 11110 00001 11010
01100 11100 10111 10111 10011 10111 01000 11100

John Hershey.
Cryptography Demystified.
McGraw-Hill, 2003

Τεχνικές Κρυπτανάλυσης

One-time Pad – Μελέτη περίπτωσης

- Έστω $C = C_1 \oplus C_2 = P_1 \oplus P_2 =$

10111 10001 01010 00010 11111 01100 11111 10110 10111
10100 10000 00010 10101 11011 10100 10000 00011

- Ο Κρυπταναλυτής πιθανολογεί την ύπαρξη μιας συχνής λέξης (π.χ. FOR) σε ένα από τα δύο κείμενα, και κάνει XOR στο C.
  - Αν το αποτέλεσμα βγάζει νόημα, τότε ο κρυπταναλυτής θα έχει ανακτήσει «μέρος» και των δύο αρχικών μηνυμάτων !!!

10111 10001 01010 00010 11111 01100 11111 10110 10111
00101 01110 10001
10010 11111 11011
S ϕ^3 ϕ

Τεχνικές Κρυπτανάλυσης

One-time Pad – Μελέτη περίπτωσης

John Hershey.
Cryptography Demystified.
McGraw-Hill, 2003

- Ο Κρυπταναλυτής δοκιμάζει το FOR σε άλλη θέση…

```
10111 10001 01010 00010 11111 01100 11111 10110 10111
      00101 01110 10001
      10100 00100 10011
        U     E     T
```

- Ίσως !!! Δοκιμάζουμε και ένα κενό (space) μετά το FOR:

```
10111 10001 01010 00010 11111 01100 11111 10110 10111
      00101 01110 10001 11010
      10100 00100 10011 00101
        U     E     T     F
```

- Ο Κρυπταναλυτής δοκιμάζει το FOR σε άλλη θέση…

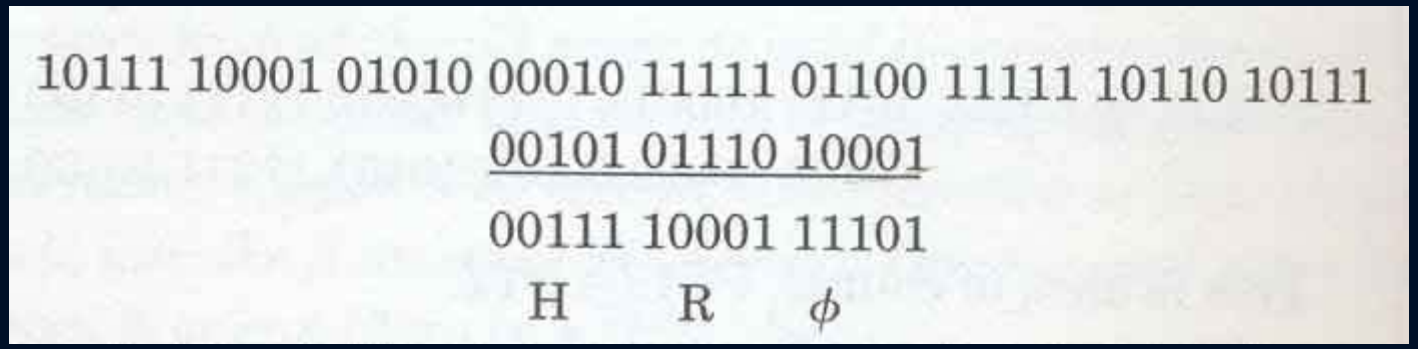
```
10111 10001 01010 00010 11111 01100 11111 10110 10111
            00101 01110 10001
            01111 01100 01110
              P     M     O
```

John Hershey.
Cryptography Demystified.
McGraw-Hill, 2003

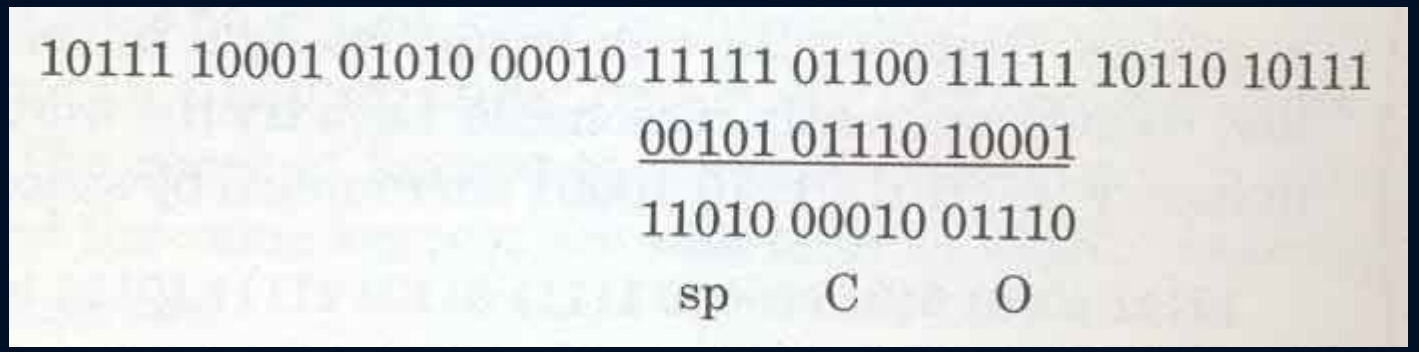
Τεχνικές Κρυπτανάλυσης

One-time Pad – Μελέτη περίπτωσης

- Ο Κρυπταναλυτής δοκιμάζει το FOR σε άλλη θέση…



- Ο Κρυπταναλυτής δοκιμάζει το FOR σε άλλη θέση…

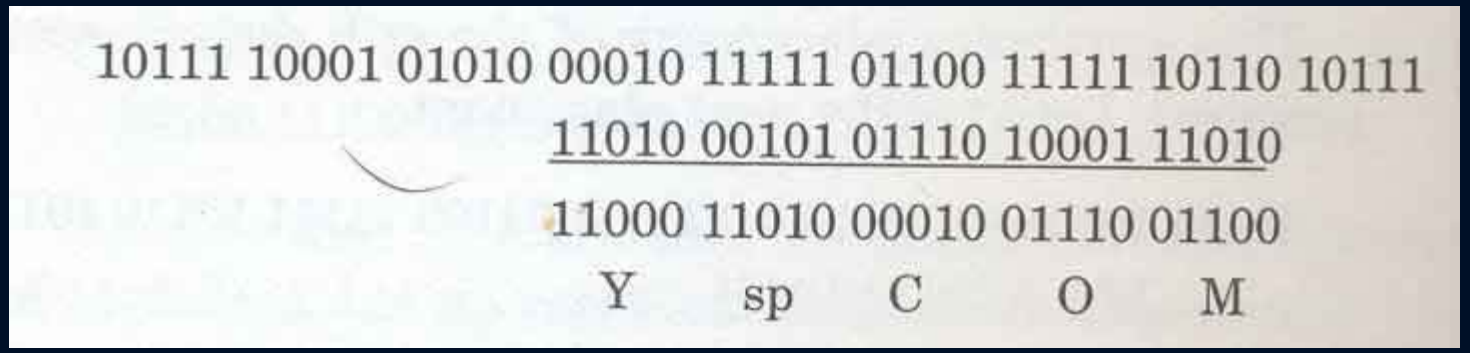


John Hershey.
Cryptography Demystified.
McGraw-Hill, 2003

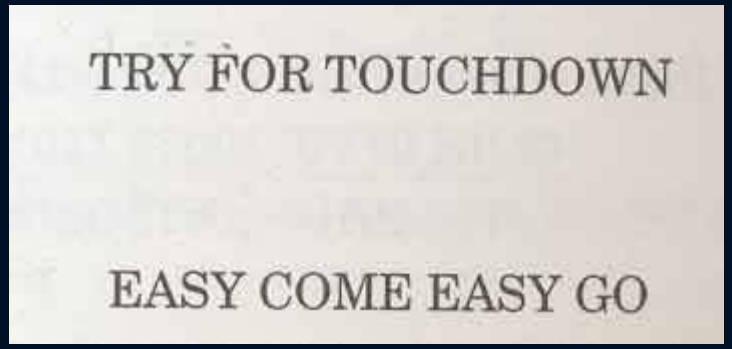
Τεχνικές Κρυπτανάλυσης

One-time Pad – Μελέτη περίπτωσης

- Ο Κρυπταναλυτής προσθέτει δυο κενά (spaces) εκατέρωθεν του FOR:



- Μετά από (όχι πολύωρες) προσπάθειες, προκύπτουν τα δύο μηνύματα :



J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Απόλυτη Ασφάλεια

Το Θεώρημα του Shannon

ΘΕΩΡΗΜΑ 2.8 *(Το θεώρημα του Shannon). Εστω* (Gen, Enc, Dec) *ένα κρυπτογραφικό σχήμα σε ένα σύνολο μηνυμάτων* M *για το οποίο* $|M| = |K| = |C|$. *Το σχήμα είναι απολύτως ασφαλές αν και μόνο αν:*

1. *Κάθε* $k \in K$ επιλέγεται με ίση πιθανότητα $1/|K|$ από τον αλγόριθμο Gen.
2. *Για κάθε* $m \in K$ και κάθε $c \in C$, υπάρχει ένα μοναδικό κλειδί $k \in K$ τέτοιο ώστε $Enc_k(m)$ *δίνει στην έξοδο το* c.

Αλγόριθμος Μιας Χρήσης (One-time Pad)
Μια Γενίκευση

- Plaintext space = Ciphtertext space = Keyspace = $(Z_m)^n$
- **Αρχικό μήνυμα (plaintext)**
  - $X = (x_1\ x_2\ \ldots\ x_n)$
- **Κλειδί (pad)**
  - $K = (k_1\ k_2\ \ldots\ k_n)$
- **Κρυπτογράφηση (encryption)**
  - $e_k(X) = (x_1+k_1\ \ x_2+k_2\ \ldots\ x_n+k_n) \bmod m$
- **Αποκρυπτογράφηση (decryption)**
  - $d_k(Y) = (y_1-k_1\ \ y_2-k_2\ \ldots\ y_n-k_n) \bmod m$

O. Goldreigh. Foundations of Cryptography, Vol II Basic Applications, 2004.

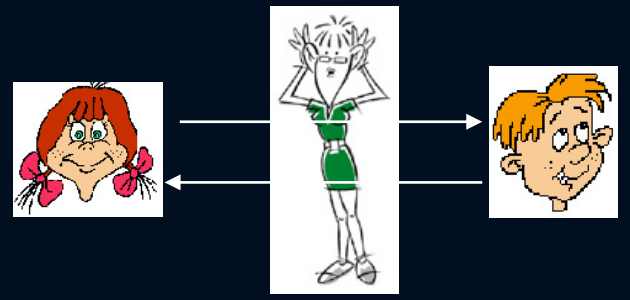
Ασφάλεια Κρυπτογραφικών Συστημάτων

- Δύο βασικές ιδιότητες:

  1. Σημασιολογική ασφάλεια (semantic security): Το κρυπτογραφημένο μήνυμα δεν αποκαλύπτει καμιά πληροφορία για το αρχικό μήνυμα

  2. Μη δυνατότητα διάκρισης (indistinguishability): Δεδομένων δύο μηνυμάτων m_1, m_2 και των κρυπτογραφήσεων τους c_1, c_2, είναι αδύνατο για την Eve να διακρίνει ποια κρυπτογράφηση αντιστοιχεί σε ποιο μήνυμα !

Βλέποντας το κρυπτογραφημένο μήνυμα, η Eve δεν μαθαίνει κάτι για το αρχικό μήνυμα.



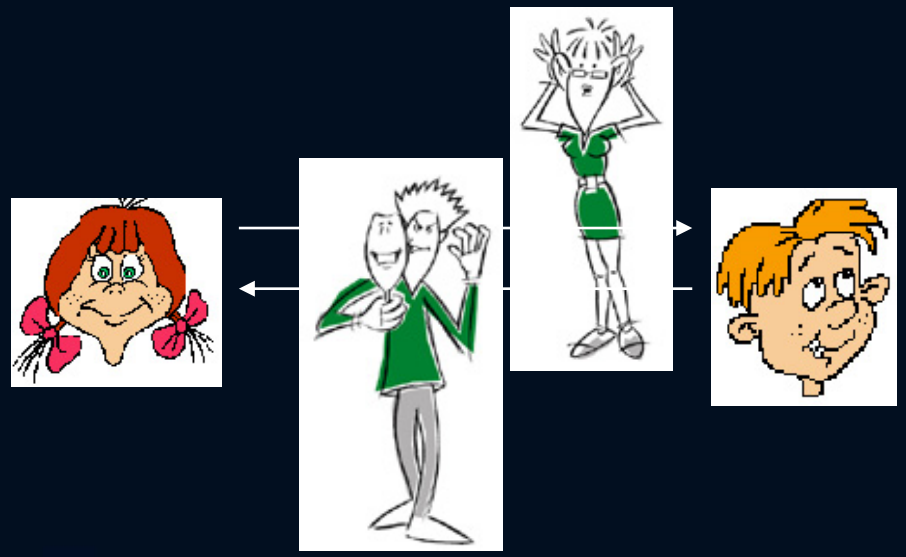
- Οι ιδιότητες αυτές θεωρούνται ισοδύναμες

O. Goldreigh. Foundations of Cryptography, Vol II Basic Applications, 2004.

Υπολογιστική Ασφάλεια vs Απόλυτη Ασφάλεια

«Χαλαρώνοντας» τους ορισμούς ασφάλειας

- Οδεύοντας από την τέλεια (απόλυτη) ασφάλεια προς την πρακτική (υπολογιστική) ασφάλεια, στους ορισμούς ασφάλειας που μελετούμε, μπορούμε να αντικαταστήσουμε φράσεις όπως:
  - «... ο εχθρός δεν μπορεί να ... »
  - «... είναι αδύνατο για τον εχθρό ... »
- με τη φράση
  - «... είναι υπολογιστικά ανέφικτο για τον εχθρό...»



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

Υπολογιστική Ασφάλεια Αλγορίθμων

2. Υπολογιστική Ασφάλεια (Computational Security)

- Όλα τα (πρακτικά) κρυπτοσυστήματα είναι ευάλωτα σε επιθέσεις εξαντλητικής αναζήτησης (exhaustive search), ή ωμής βίας (brute force)
  - Brute-force: Ο κρυπταναλυτής «δοκιμάζει» κάθε πιθανό κλειδί !
- Ένα σύστημα είναι υπολογιστικά ασφαλές, όταν η επίθεση brute-force εμφανίζει πολύ υψηλή πολυπλοκότητα
  - π.χ. ("πολύς" υπολογιστικός χρόνος, μικρή πιθανότητα εύρεσης)

*Σημείωση: Ένας αλγόριθμος θεωρείται **μη ασφαλής**, εάν κάποιος τρίτος, χωρίς γνώση του κλειδιού που χρησιμοποιήθηκε, αποκτήσει πρόσβαση στο αρχικό κείμενο, σε «εύλογο» χρονικό διάστημα !*

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Υπολογιστική Ασφάλεια Αλγορίθμων

Το μεγάλο «στοίχημα» για τους σχεδιαστές αλγορίθμων:

Η βέλτιστη μέθοδος για να «σπάσει» ένας αλγόριθμος πρέπει να είναι η εξαντλητική αναζήτηση για το σωστό κλειδί. Σε αυτήν την περίπτωση, η ασφάλεια του αλγορίθμου εξαρτάται από το μήκος (σε bit) του κλειδιού που ο αλγόριθμος υποστηρίζει.

«Το σωστό κλειδί υπάρχει κάπου εκεί...»

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

Ασφάλεια Αλγορίθμων

- Μέτρηση της πολυπλοκότητας μιας επίθεσης
  - Πολυπλοκότητα Δεδομένων (Data Complexity)
    - Ποσότητα δεδομένων που δίνονται ως είσοδος στον αλγόριθμο κρυπτανάλυσης
  - Υπολογιστική Πολυπλοκότητα (Processing Complexity)
    - Χρόνος για τη διενέργεια της επίθεσης
  - Αποθηκευτική Πολυπλοκότητα (Storage Complexity)
    - Ποσότητα αποθηκευτικού χώρου που απαιτείται για τη διενέργεια της επίθεσης
- Συνήθως λαμβάνεται υπόψη η <u>υπολογιστική πολυπλοκότητα</u>
  - Εκφράζεται ως ο (ελάχιστος) αριθμός των «βημάτων» (operations) που απαιτούνται για τη διενέργεια (επιτυχούς) επίθεσης
    - Ο Παράγοντας Εργασίας (Work Factor)
  - π.χ. Ο παράγων εργασίας για την εύρεση του μυστικού κλειδιού σε ένα (συμμετρικό) σύστημα με κλειδιά μήκους 128 bit είναι 2^{128}

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

«Μεγάλοι» Αριθμοί

Reference	Magnitude
Seconds in a year	$\approx 3 \times 10^7$
Age of our solar system (years)	$\approx 6 \times 10^9$
Seconds since creation of solar system	$\approx 2 \times 10^{17}$
Clock cycles per year, 50 MHz computer	$\approx 1.6 \times 10^{15}$
Binary strings of length 64	$2^{64} \approx 1.8 \times 10^{19}$
Binary strings of length 128	$2^{128} \approx 3.4 \times 10^{38}$
Binary strings of length 256	$2^{256} \approx 1.2 \times 10^{77}$
Number of 75-digit prime numbers	$\approx 5.2 \times 10^{72}$
Electrons in the universe	$\approx 8.37 \times 10^{77}$

Table 1.2: *Reference numbers comparing relative magnitudes.*

Time until the next ice age	$14{,}000$ (2^{14}) year
Time until the sun goes nova	10^9 (2^{30}) years
Age of the planet	10^9 (2^{30}) years
Age of the Universe	10^{10} (2^{34}) years
Number of atoms in the planet	10^{51} (2^{170})
Number of atoms in the sun	10^{57} (2^{190})
Number of atoms in the galaxy	10^{67} (2^{223})
Number of atoms in the Universe (dark matter excluded)	10^{77} (2^{265})
Volume of the Universe	10^{84} (2^{280}) cm^3
If the Universe is Closed:	
Total lifetime of the Universe	10^{11} (2^{37}) years
	10^{18} (2^{61}) second
If the Universe is Open:	
Time until low-mass stars cool off	10^{14} (2^{47}) years
Time until planets detach from stars	10^{15} (2^{50}) years
Time until stars detach from galaxies	10^{19} (2^{64}) years
Time until orbits decay by gravitational radiation	10^{20} (2^{67}) years
Time until black holes decay by the Hawking process	10^{64} (2^{213}) years
Time until all matter is liquid at zero temperature	10^{65} (2^{216}) years
Time until all matter decays to iron	10^{1026} years
Time until all matter collapses to black holes	10^{1076} years

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

N. Ferguson, B. Schneier. Practical Cryptography. Wiley, 2003.

Κρυπτογραφία και Κρυπτογραφικές Τεχνικές

Ορισμένες Παρατηρήσεις…

1. Κρυπτογραφία: Σημαντικό «κομμάτι» της Ασφάλειας Πληροφορίας

   « Στόχος της κρυπτογραφίας είναι η παροχή πρόσβασης σε κάποιους, καθώς επίσης και η μη παροχή πρόσβασης σε κάποιους άλλους» (Schneier, 2003)

2. Η κρυπτογραφική προστασία δεν αποτελεί πανάκεια…
   - π.χ. Υπερχείλιση καταχωρητών (buffer overflows), worms, κ.λ.π

Ένα σύστημα ασφάλειας είναι τόσο ασφαλές όσο το πιο αδύνατο του σημείο

3. Εντούτοις, οι κρυπτογραφικοί μηχανισμοί πρέπει να υλοποιούνται σωστά…
   - Μια επίθεση που παρακάμπτει την κρυπτογραφική προστασία, είναι δύσκολο να γίνει αντιληπτή… !!!!

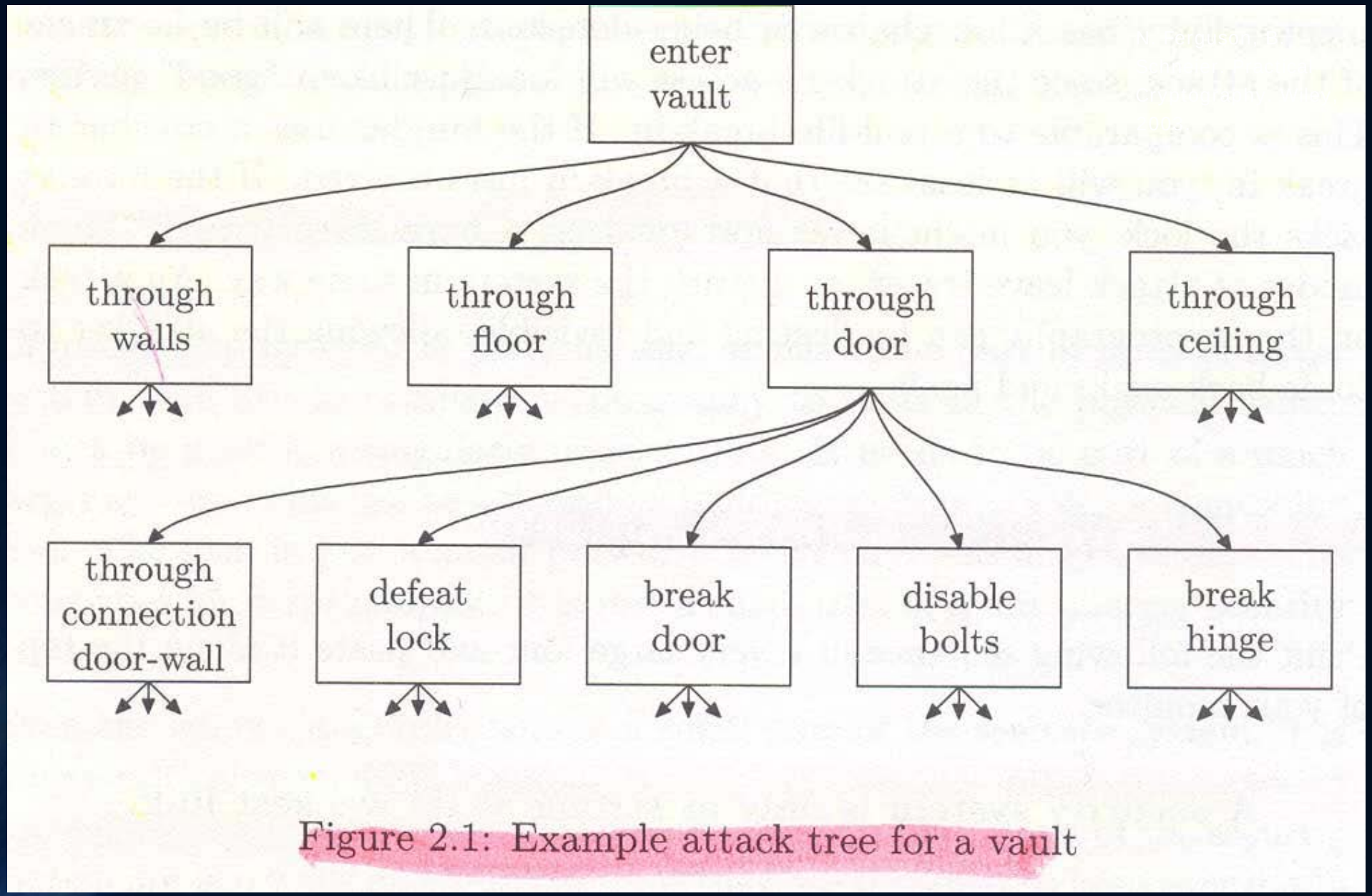
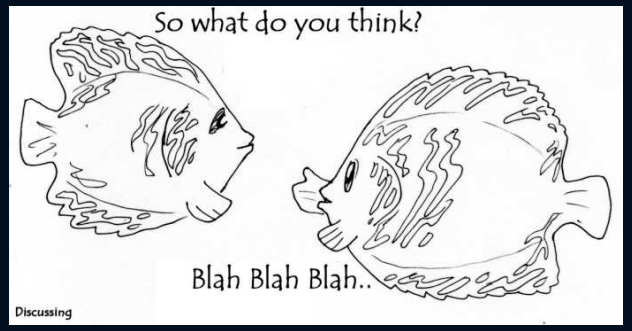


Figure 2.1: Example attack tree for a vault

Συζήτηση



"Cryptography is the mathematics of making a system secure, which is different from actually making a system secure."

B. Schneier