

Symmetric Cryptography

Dimitris Mitropoulos
dimitro@di.uoa.gr

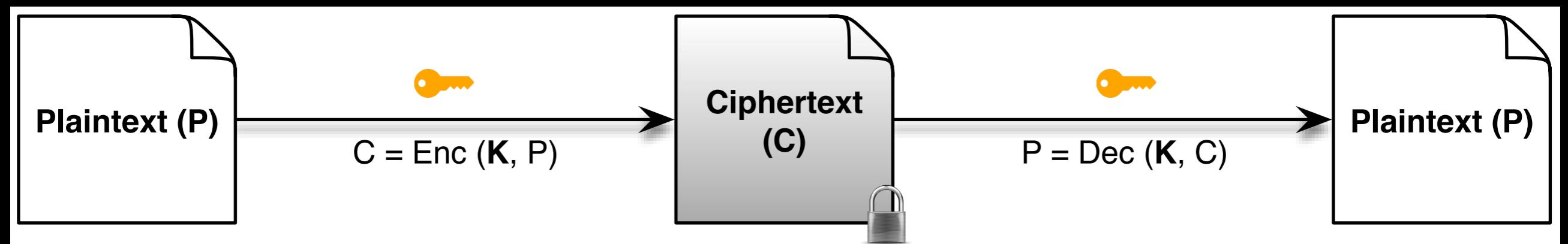
Ορολογία

- **Αρχικό Κείμενο (Plaintext)**: Αποτελεί το αρχικό μήνυμα (ή τα αρχικά δεδομένα) που εισάγεται στον αλγόριθμο κρυπτογράφησης.
- **Αλγόριθμος Κρυπτογράφησης (Encryption Algorithm)**: Ο αλγόριθμος που πραγματοποιεί τους απαραίτητους μετασχηματισμούς του αρχικού κειμένου για την επίτευξη της κρυπτογράφησης ενός μηνύματος.
- **Μυστικό Κλειδί (Secret Key)**: Εισάγεται και αυτό στον αλγόριθμο κρυπτογράφησης. Οι ακριβείς αντικαταστάσεις και τα αποτελέσματα των μετασχηματισμών που επιτελούνται από τον αλγόριθμο εξαρτώνται από αυτό.

Ορολογία (2)

- **Αλγόριθμος Παραγωγής Κλειδιού (Key-generation Algorithm):** ένας πιθανολογικός (probabilistic) αλγόριθμος που παράγει ένα κλειδί βασισμένο σε μια καθορισμένη κατανομή.
- **Κρυπτογράφημα ή Κρυπτογραφημένο Μήνυμα (Ciphertext):** Το μετασχηματισμένο μήνυμα που παράγεται ως έξοδος από τον αλγόριθμο κρυπτογράφησης.
- **Αλγόριθμος Αποκρυπτογράφησης (Decryption Algorithm):** Ο αλγόριθμος που πραγματοποιεί την αντίστροφη διαδικασία από τον αλγόριθμο κρυπτογράφησης. Λαμβάνει το κρυπτογραφημένο μήνυμα και το ίδιο μυστικό κλειδί και παράγει το αρχικό κείμενο.

Η **συμμετρική κρυπτογράφηση** βασίζεται στην ύπαρξη ενός και μόνο κλειδιού, το οποίο χρησιμοποιείται τόσο στην κρυπτογράφηση όσο και στην αποκρυπτογράφηση ενός μηνύματος. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα συναλλασσόμενα μέρη.



Correctness

(օրթօτητա)

$$P = \text{Dec}(K, \text{Enc}(K, P))$$

Αρχή Kerckhoffs

Ένα σύστημα κρυπτογράφησης θα πρέπει να είναι ασφαλές ακόμα και αν ο επιτιθέμενος γνωρίζει τα πάντα για αυτό εκτός από το κλειδί.

security by obscurity

Πλεονεκτήματα Αρχής Kerckhoffs

- Τα συστήματα που είναι δημόσια διαθέσιμα, υπόκεινται σε λεπτομερείς ελέγχους και είναι πιθανότερο να είναι αποτελεσματικότερα.
- Μπορεί κανείς να βρει ευκολότερα θέματα ασφάλειας που μπορεί να υπάρχουν στην εφαρμογή (και να τα αναφέρει στους υπεύθυνους!).
- Εάν η ασφάλεια του συστήματος εξαρτάται από την μυστικότητα του αλγόριθμου, τότε υπάρχει κίνδυνος να παραβιαστεί από κακόβουλους χρήστες με reverse engineering του κώδικα υλοποίησης (ή μπορεί να διαρρεύσει εκ των έσω).
- Η δημοσιοποίηση τέτοιων αλγορίθμων μπορεί να οδηγήσει σε νέα standards.

Caesar's Cipher

TREATY IMPOSSIBLE BEGIN THE ATTACK
NOW

WUHDWB LPSRVVLEOH EHJLQ WKH
DWWDFN QRZ

Μια παραλλαγή του συστήματος του
Καίσαρα (ROT13), χρησιμοποιούσαν
τα Windows XP για να
“κρυπτογραφούν” registry keys.

Παρατηρήσεις

- Στο σύστημα του Καίσαρα, η κρυπτογράφηση γίνεται πάντα με τον ίδιο τρόπο και δεν υπάρχει μυστικό κλειδί.
- Στον ROT k το σύστημα είναι παρόμοιο αλλά υπάρχει κλειδί ($k \in \{0, 1, \dots, 25\}$).

```
1 message = 'SQUIQHI SYFXUH YI KDRHUQAQRBU'
2 letters = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'
3
4 for key in range(len(letters)):
5     translated =
6     for symbol in message:
7         if symbol in letters:
8             num = letters.find(symbol)
9             num = num - key
10            if num < 0:
11                num = num + len(letters)
12            translated = translated + letters[num]
13        else:
14            translated = translated + symbol
15    print('Key #%s: %s' % (key, translated))
16
```

Το σύνολο των πιθανών κλειδιών (**key space**) ενός ασφαλούς συστήματος κρυπτογράφησης θα πρέπει να μην είναι ευάλωτο σε επιθέσεις “εξαντλητικής αναζήτησης” (exhaustive search / **brute force attacks**).

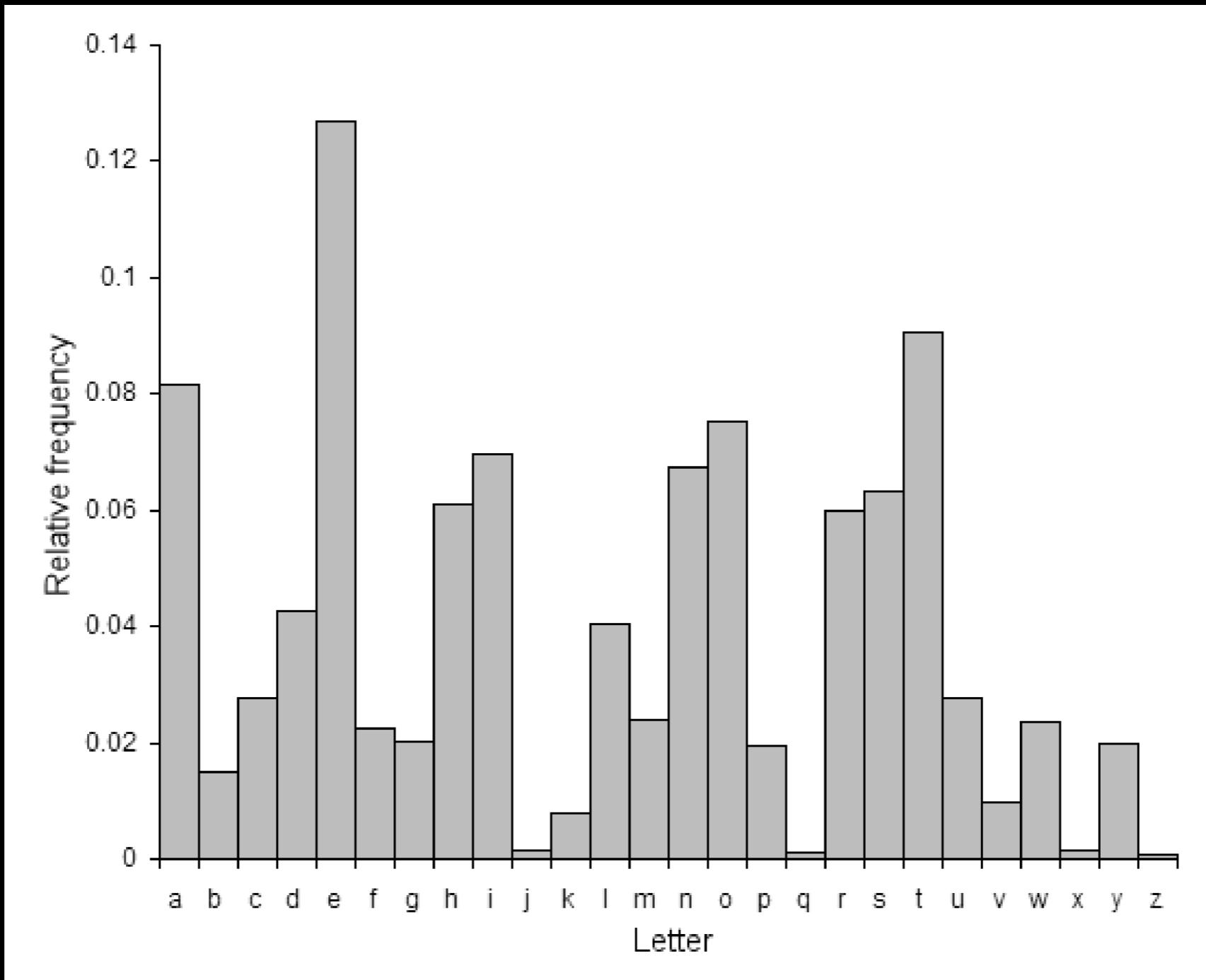
Key Space

- Για πεπερασμένο key space, λ.χ., $k \in \{0, 1\}^n$
- Brute-force επίθεση:
Δεδομένου του Ciphertext = Enc(k , Message):
Για όλα τα $k \in \{0, 1\}^n$
 $\text{Dec}(k, \text{Ciphertext}) = ?$ /* 2^n προσπάθειες */

Mono-alphabetic Substitution

```
201 monoalphabetic_cipher = {  
202     'a': 'm',  
203     'b': 'e',  
204     'c': 't',  
205     'd': 'n',  
206     'f': 'g',  
207     'h': 'l',  
208     'i': 'u',  
209     'j': 'o',  
210     'k': 'p',  
211     'l': 'q',  
212     'm': 'r',  
213     'o': 's',  
214     's': 'd',  
215     'u': 'v',  
216     'v': 'w',  
217     'w': 'x',  
218     'x': 'y',  
219     'y': 'z',  
220     'z': 'a'  
221 }  
222  
223  
224  
225  
226  
227  
228  
229
```

Frequency Analysis



Η εικόνα προέρχεται από το βιβλίο “Introduction to Modern Cryptography” των Jonathan Katz and Yehuda Lindell.

One Time Pad

- G. Vernam 1917, AT&T.
- Ιδανική ασφάλεια για τυχαίο κλειδί.

 Plaintext 010111011011100

 Key 1011010110101110

 Ciphertext 111010000010010

One Time Pad

Encryption

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

One Time Pad

Decryption

E	Q	N	V	Z	ciphertext
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)
H	E	L	L	O	→ message

One Time Pad

A Spy's Message

<i>Plain</i>	
<i>Key</i>	
<i>Cipher</i>	
heilhitler	
wc1nbtdefj	
DGYIBWPJA	

One Time Pad

What the Spy Claim He or She Said

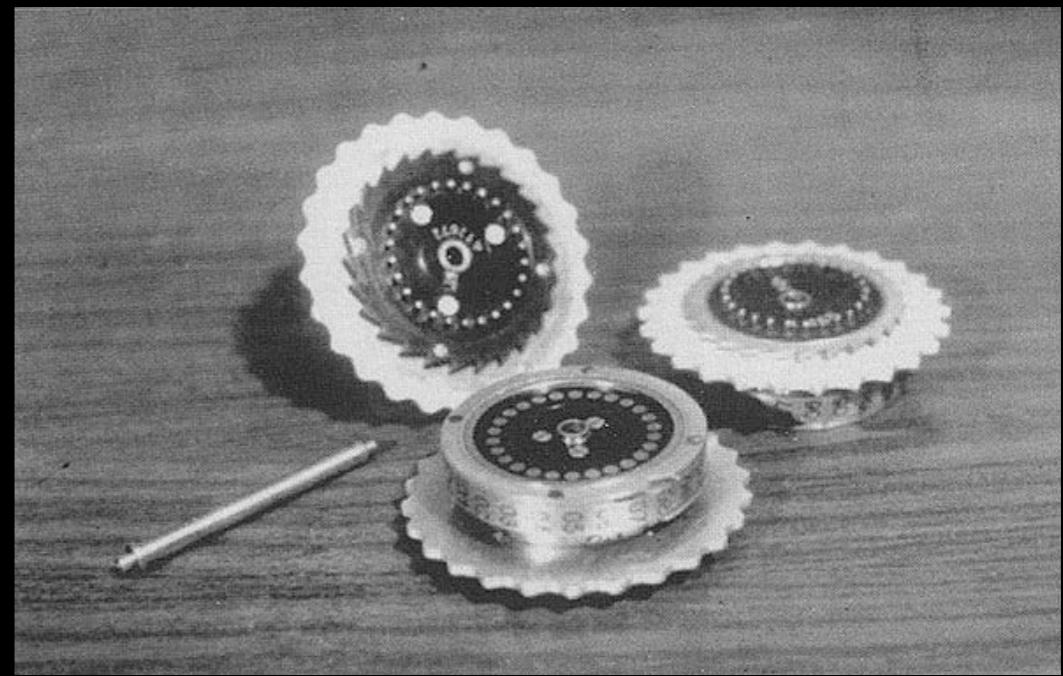
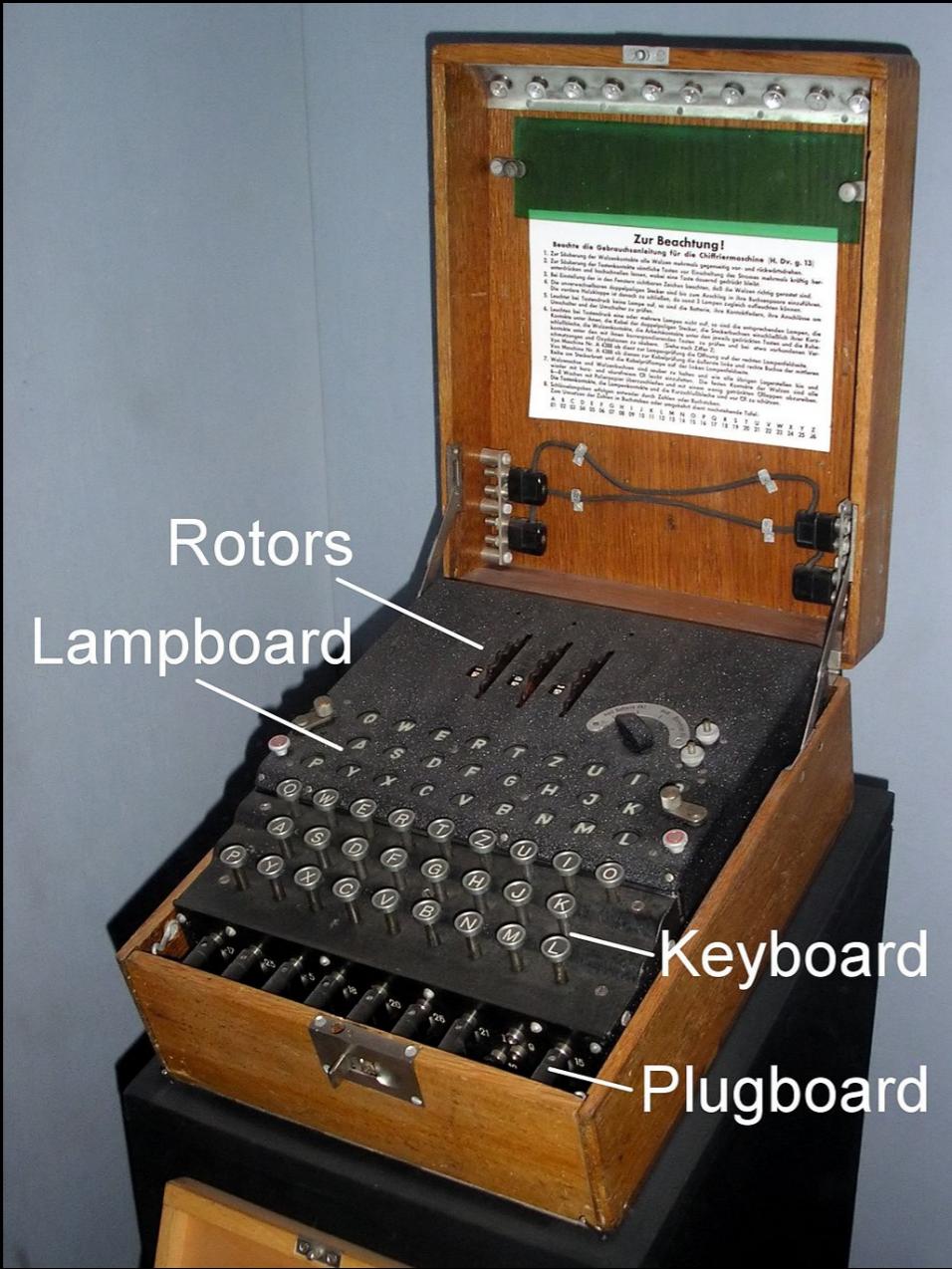
<i>Cipher</i>	DGYIBWPJA
<i>Key</i>	wggsbtdefj
<i>Plain</i>	hanghitler

One Time Pad

Entrap the Spy

<i>Cipher</i>	DCYTIBWPJA
<i>Key</i>	wclnbtd e fj
<i>Plain</i>	hanghitler

The Enigma Machine



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

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

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

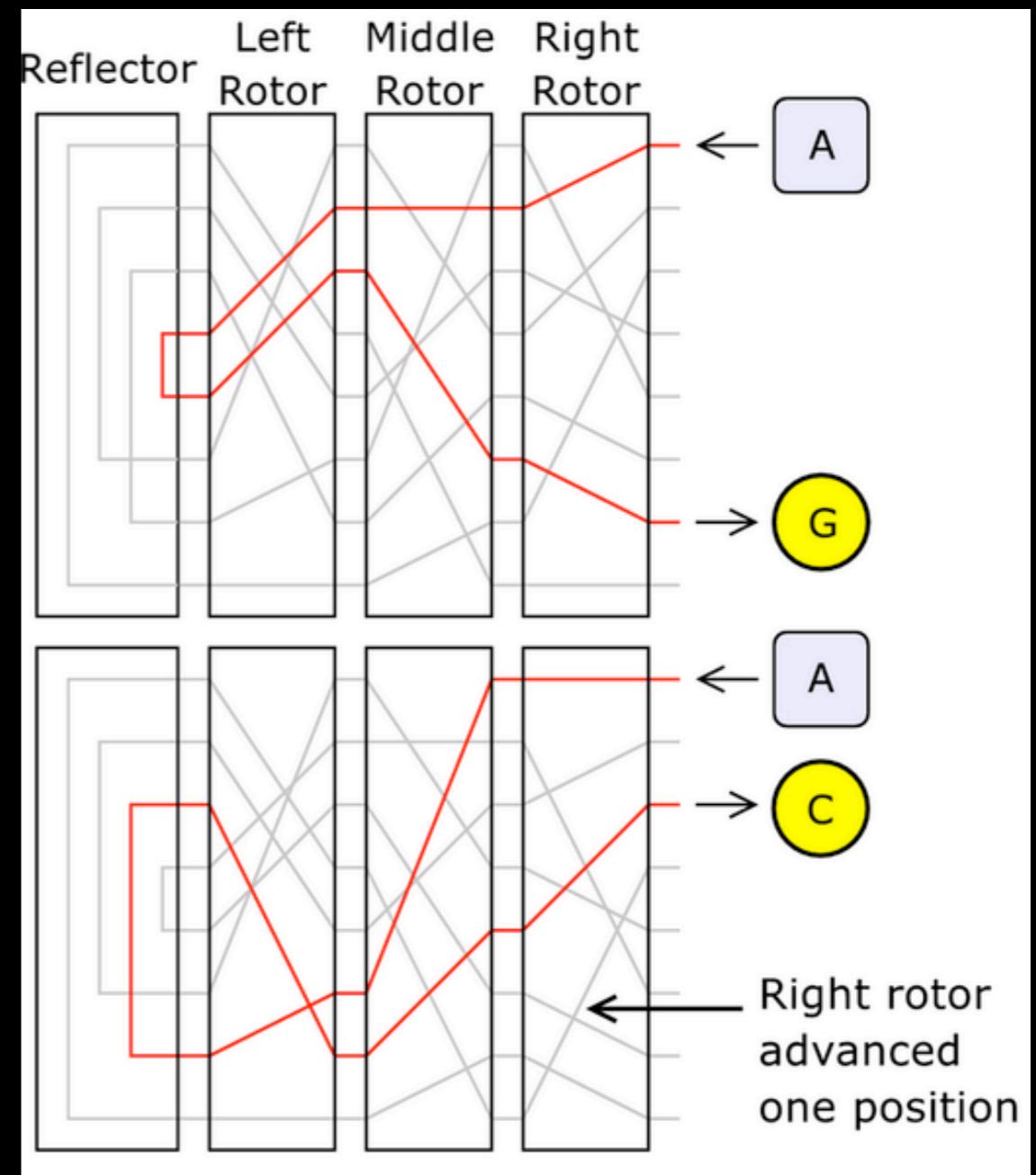
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
I I

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

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

Enigma Operation

- Ο “reflector” επιτρέπει την κρυπτογράφηση και αποκρυπτογράφηση με την ίδια διαμόρφωση (configuration).
- Η ιδιότητα που δίνει ο reflector είναι σημαντική για τον επιτιθέμενο.
- Με 3 rotators και τον reflector έχουμε $26 \times 26 \times 26 = 17,576$ διαφορετικά “alphanumeric substitutions”.



right-hand rotor:

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

center rotor:

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

left-hand rotor:

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

reflector:

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

Μεταθέσεις

(Permutations)

Αρχική διαμόρφωση:

$$\pi_1 \cdot \pi_2 \cdot \pi_3 \cdot \sigma \cdot \pi_3^{-1} \cdot \pi_2^{-1} \cdot \pi_1^{-1}$$

Μετά από μια κύλιση:

$$(\rho \cdot \pi_1 \cdot \rho^{-1}) \cdot \pi_2 \cdot \pi_3 \cdot \sigma \cdot \pi_3^{-1} \cdot \pi_2^{-1} \cdot (\rho \cdot \pi_1^{-1} \cdot \rho^{-1})$$

(Υπόψην: $\rho^{26} = 1$)

Enigma Cryptanalysis

- Reverse engineering των μεταθέσεων.
- Αποκάλυψη της αρχικής διαμόρφωσης.

Day	Ref	Wheels	Ring	Ground	Plugs
1	B	III IV II	MNN	ECM	AS BC DE GW HQ LJ OV RI XP ZT
2	B	IV VII VI	YIH	DKT	EQ IX JG OH PA RY UC VL WS ZD
3	C	V III I	MTK	PDE	AM EH FN KD PO VC WL XB YJ ZI
4	C	VI III IV	EBU	TFZ	CR EP JA MW NX SO TL UK VQ ZB
5	C	V III IV	RJD	LPD	AK BH DE JZ LS MC NT OG WI YR
6	B	I IV III	SUJ	DJM	CZ GV HO NJ PL SQ TX UI WE YA
7	B	VII IV VIII	NII	RRV	BQ EX GR IA JL KP OU VT WN YF
8	C	IV V II	ZUO	RMJ	CG EP FR IU LW ND QS TB VH ZK
9	B	VI V IV	RKD	IXM	CP EZ FB IM JT KS LG UD XA YO
10	B	III VIII II	ZHI	HEV	AH CY DP GU IZ KX MF QN VB WT

Vigenère Cipher

Για την κρυπτογράφηση ενός μηνύματος χρησιμοποιείται διαδοχικά ένα κλειδί μήκους n .

		PLAINTEXT LETTER																									
		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 LETTER	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	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	A	
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		
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		

Vigenère Cipher

Encryption

✉ Plaintext: ATTACKATDAWN

🔑 Key: LEMONLEMONLE

⊕ Ciphertext: LXFOPVEFRNHR

Spartan Scytale



Spartan Scytale Ciphertext

IryyatbHmvaEhedLurlP

Τενίκες Σχεδιασμού ενός Cipher Substitution (Αντικατάσταση)

- “Σπάσιμο” ενός μηνύματος σε μια συμβολοσειρά ενός αλφάβητου Σ .
- Αντικατάσταση του κάθε χαρακτήρα της συμβολοσειράς $\pi : \Sigma \rightarrow \Sigma$.
- $|\Sigma|!$ αντικαταστάσεις.

Τεντικές Σχεδιασμού ενός Cipher Transposition (Μετάθεση)

- “Σπάσιμο” ενός μηνύματος σε συμβολοσειρές ενός αλφάβητου Σ .
- Υποθέτουμε πως το μήκος του κλειδιού είναι n .
- Αντικατάσταση για κάθε χαρακτήρα του αλφάβητου στην συμβολοσειρά:

$$\pi : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$$

Τεντικές Σχεδιασμού ενός Cipher Composition (Σύνθεση)

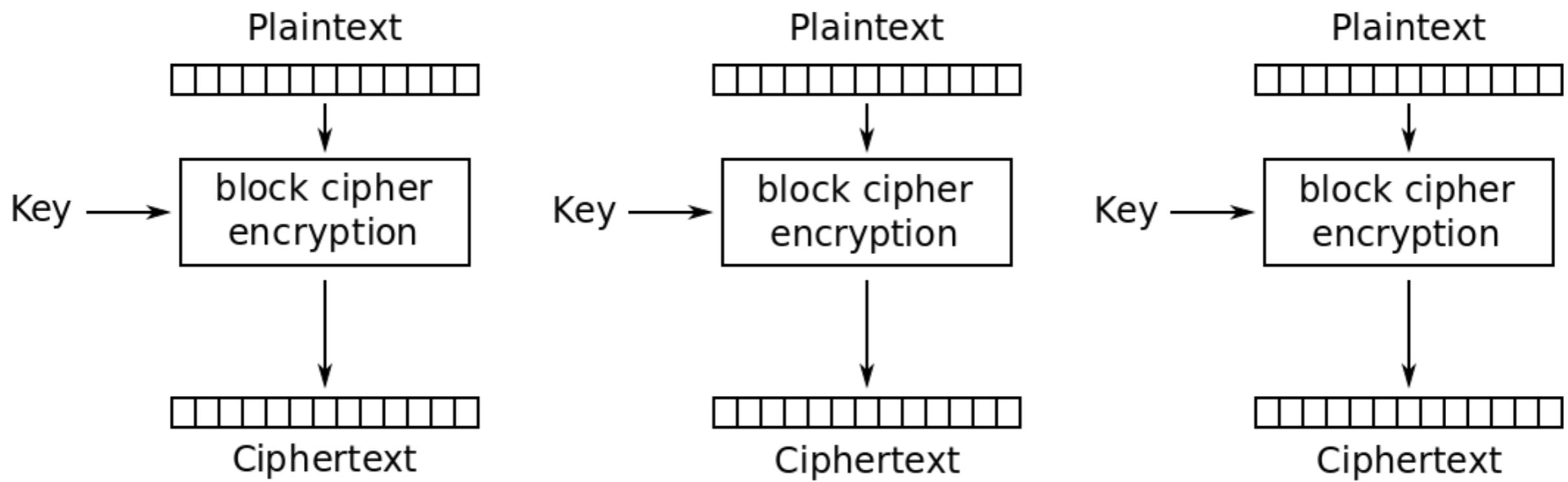
- Συνδυασμός αντικαταστάσεων και μεταθέσεων.
- Με αυτόν τον τρόπο αποκτά δυο σημαντικές ιδιότητες: **confusion** (σύγχυση) & **diffusion** (διάχυση).
- Ένα “καλό” cipher θα πρέπει να είναι “ανθεκτικό” σε γνωστές επιθέσεις και να υπακούει σε βασικές αρχές.

Block Ciphers

- Λειτουργούν με βάση ένα **block** που έχει έναν καθορισμένο αριθμό από **bits**.
- Χρειάζονται συγκεκριμένα **specifications** σχετικά με το πως θα λειτουργήσουν για να κρυπτογραφήσουν μεγαλύτερα μηνύματα (**mode of operation**).

Mode of Operation

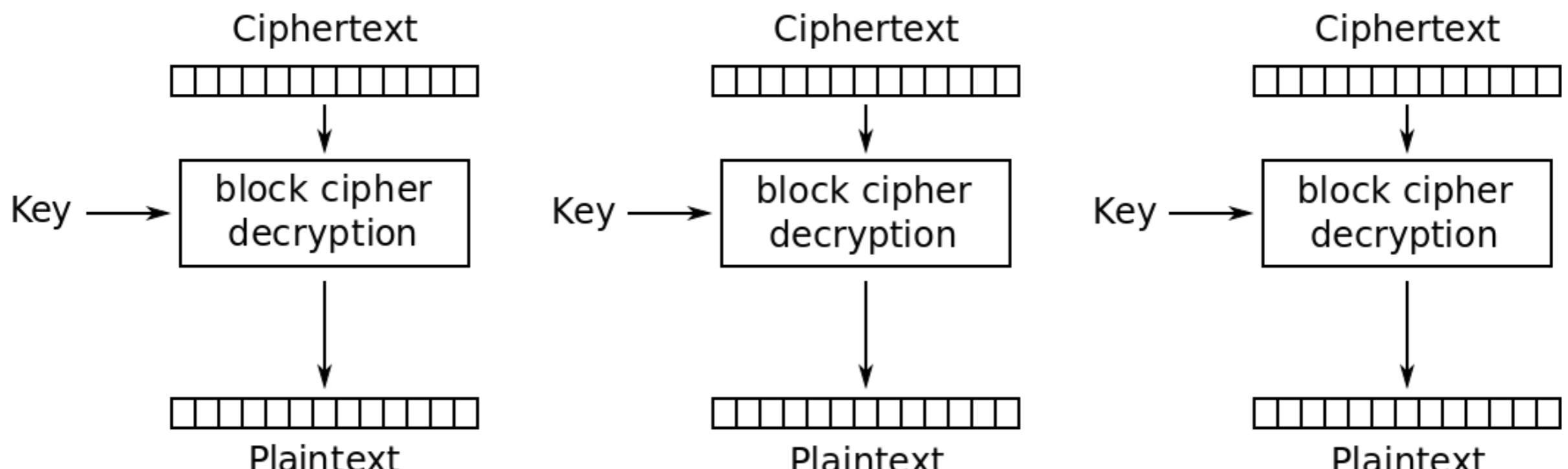
Electronic Codebook - Encryption



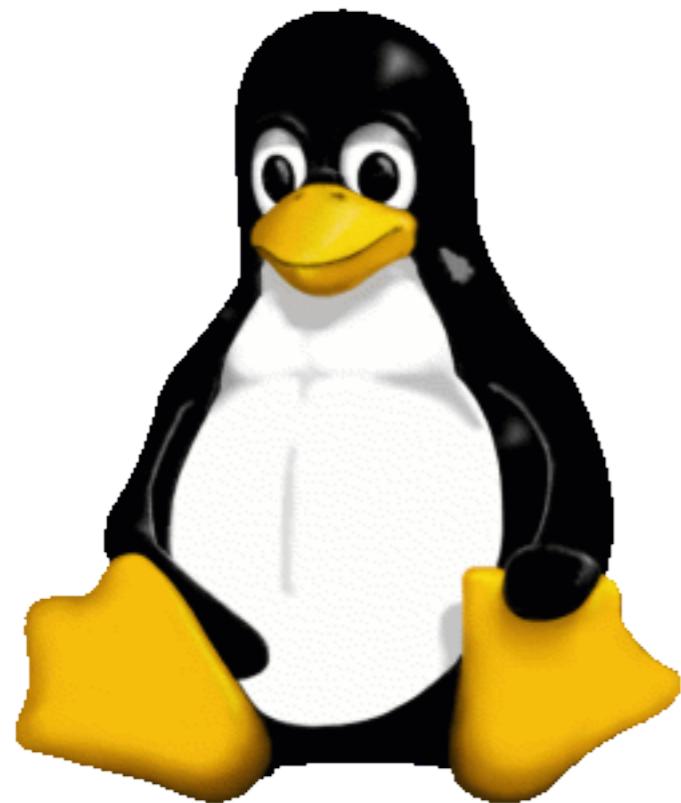
Electronic Codebook (ECB) mode encryption

Mode of Operation

Electronic Codebook - Decryption

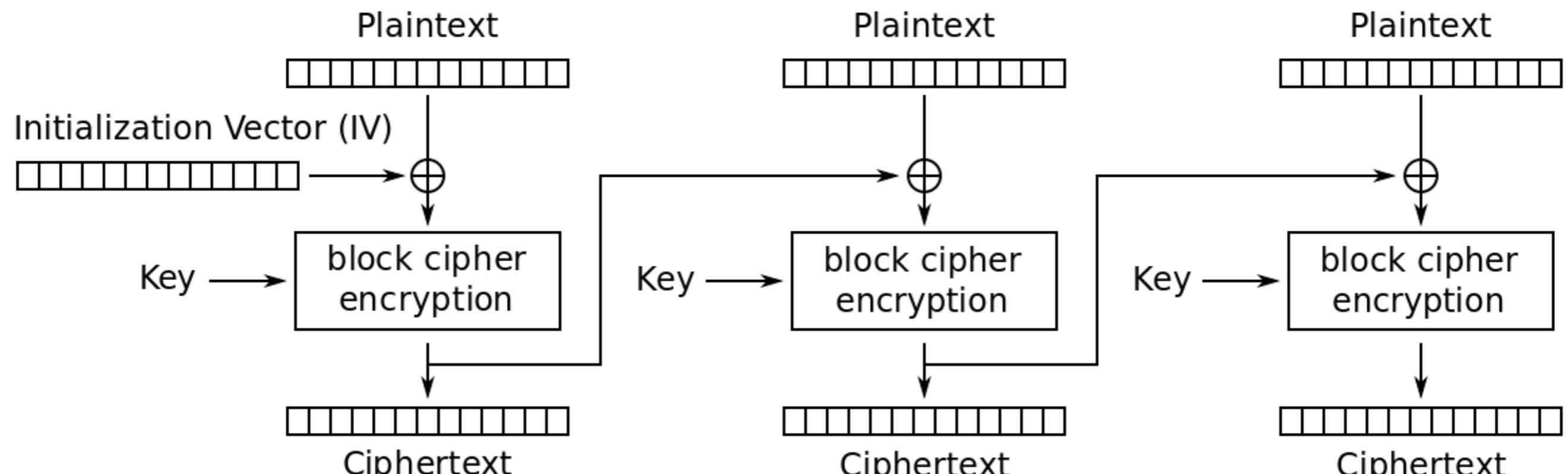


Electronic Codebook (ECB) mode decryption



Mode of Operation

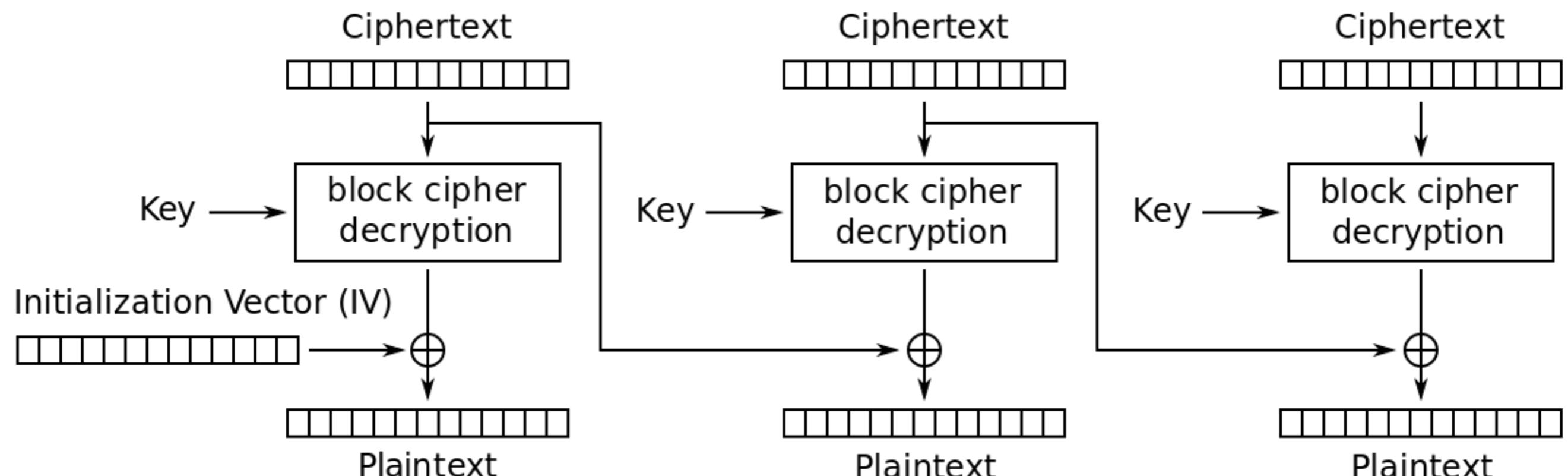
Cipher Block Chaining - Encryption



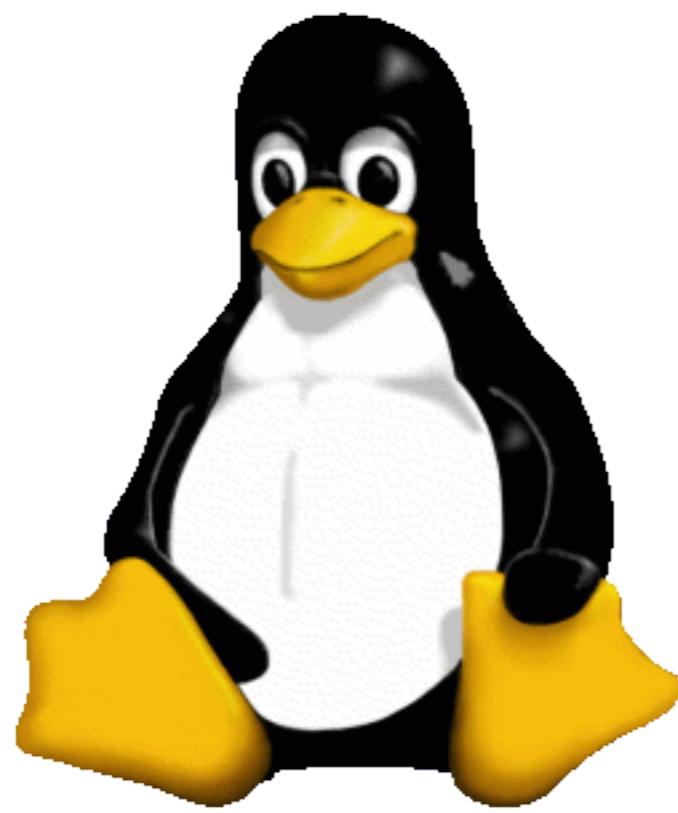
Cipher Block Chaining (CBC) mode encryption

Mode of Operation

Cipher Block Chaining - Decryption



Cipher Block Chaining (CBC) mode decryption

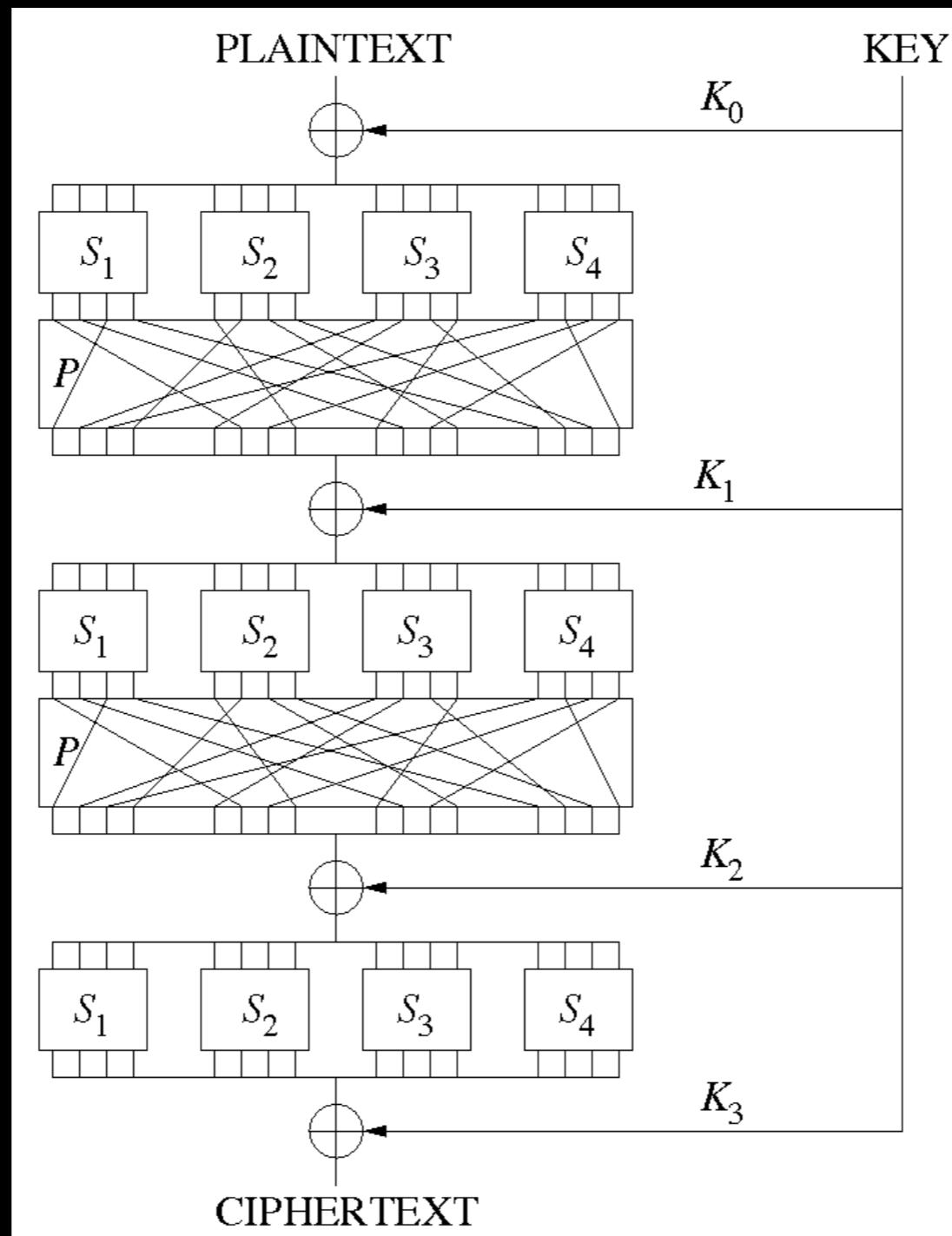


S-box

(Substitution-box)

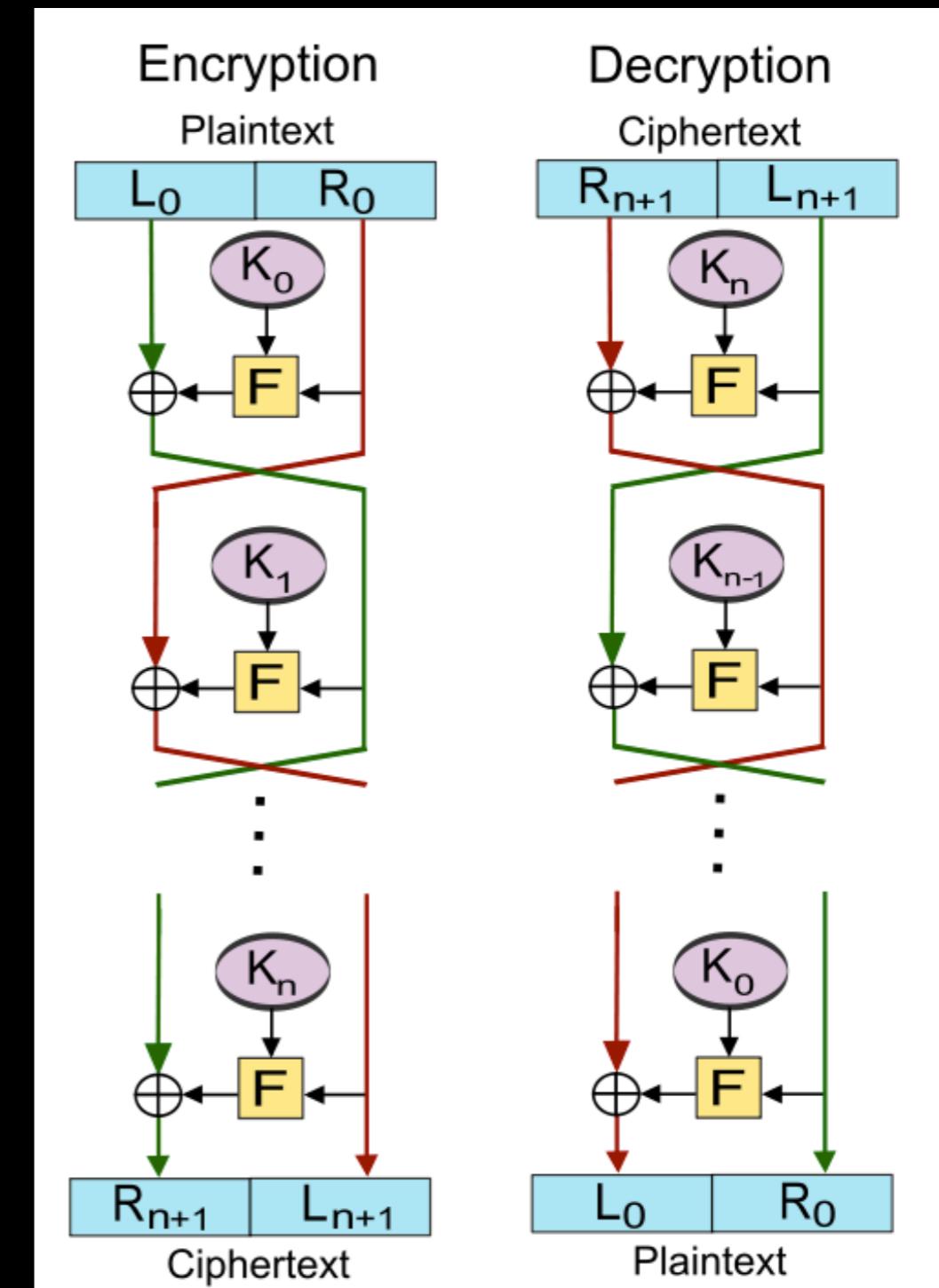
S ₅		Middle 4 bits of input															
		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Outer bits	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

Substitution - Permutation Network (SP network)



Feistel Ciphers

- Μια **συμμετρική δομή** που χρησιμοποιείται για την δημιουργία block ciphers.
- Η κρυπτογράφηση και η άποκρυπτογράφηση μπορεί να γίνει από το **ίδιο** “κύκλωμα” (circuit).

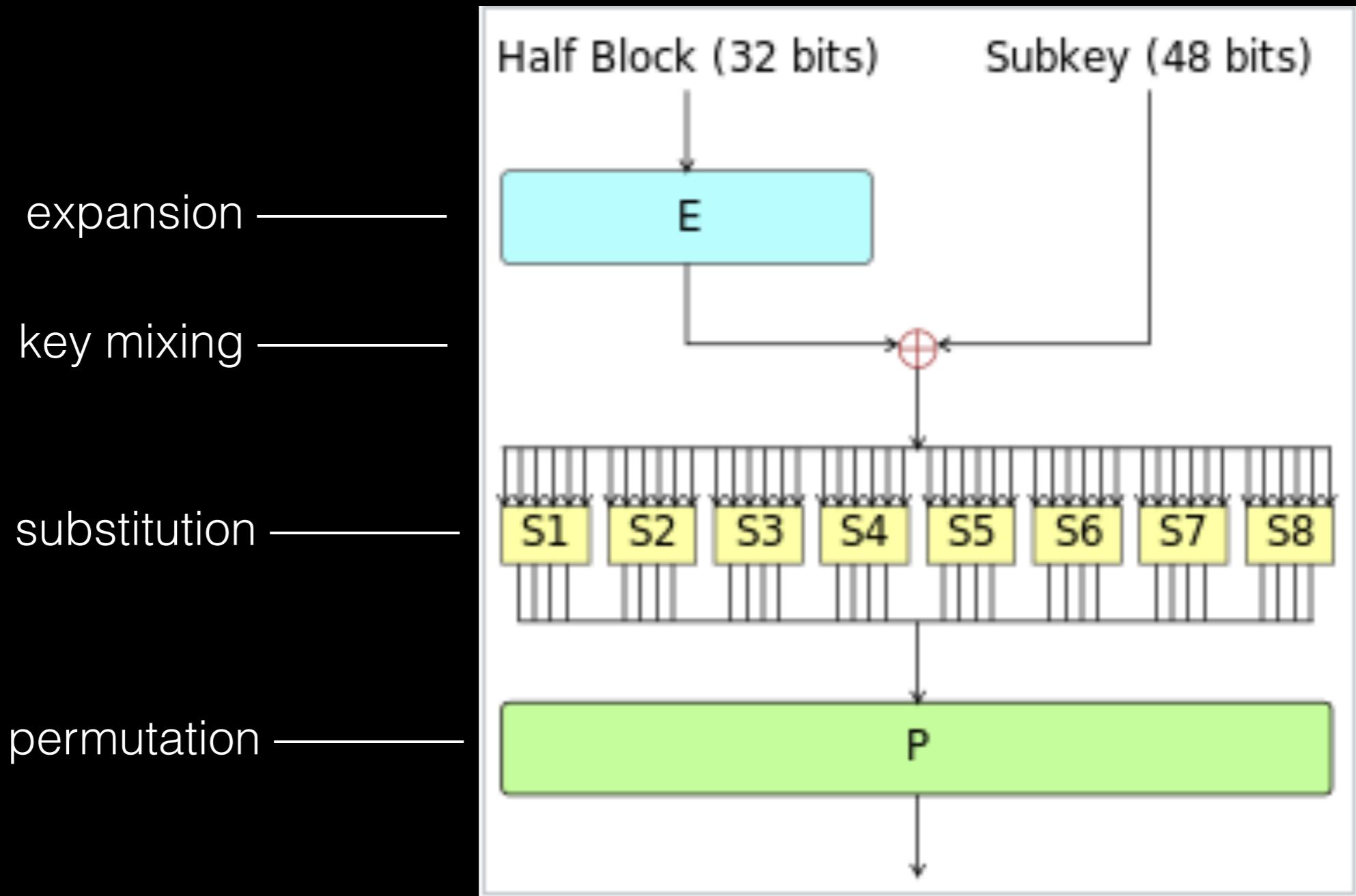


Data Encryption Standard (DES)

- Δημιουργήθηκε από την IBM.
- Μήκος κλειδιού: 56 bits.
- Block size: 64 bits.
- Το μήκος του κλειδιού θεωρήθηκε από την αρχή μικρό.

DES

Feistel Function

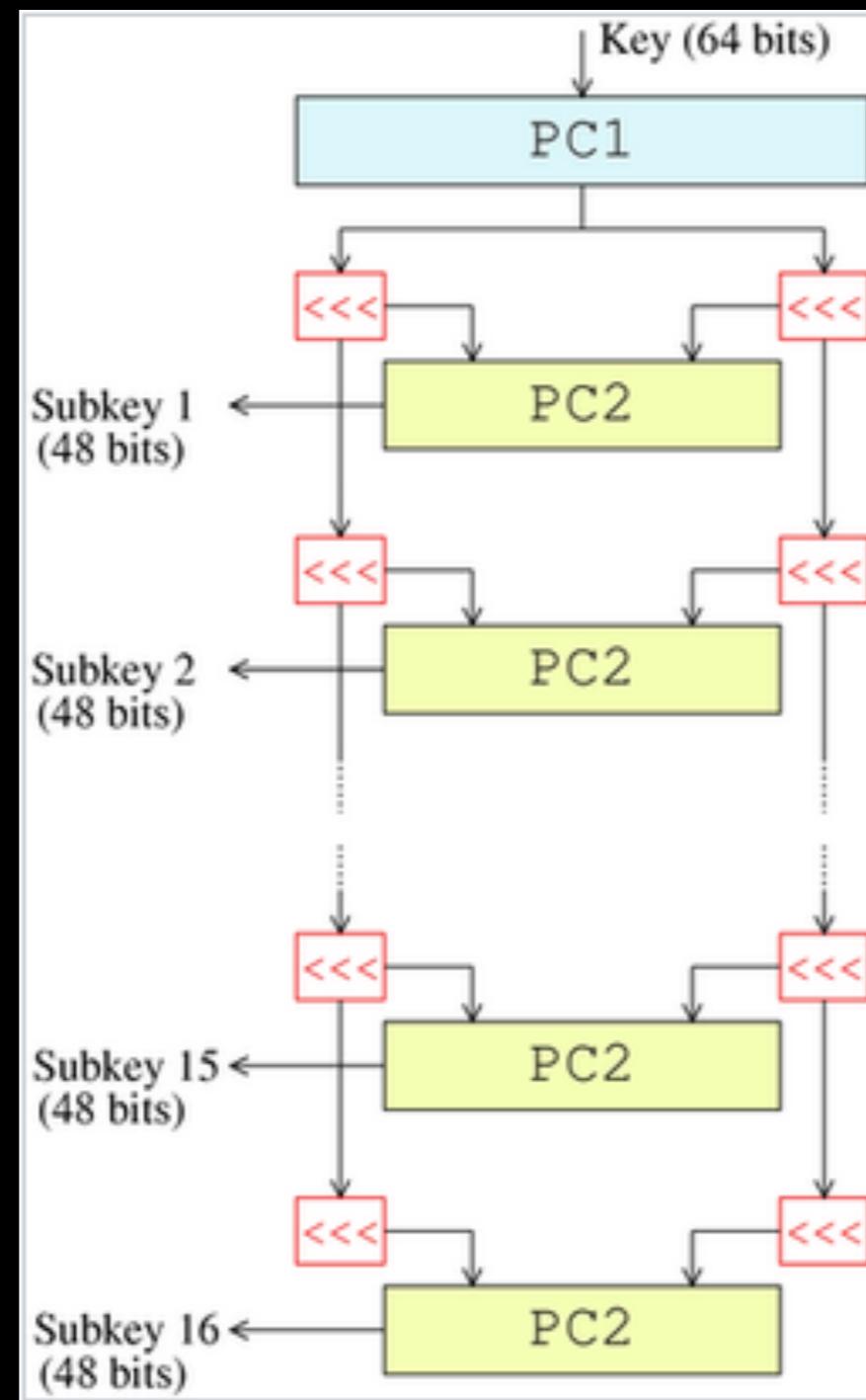


DES

Key Schedule

bit shift ($\pi.X. \ll\ll$) —————

————— permutation



Attacks on DES

Brute Force

- 1997: 4 μήνες (DESCHALL project)
- 1998: 56 ώρες (DES Cracker)
- 1999: 22 ώρες (distributed.net)

Attacks on DES

Linear Cryptanalysis

- Εξετάζουμε σχέσεις όπως “το 2o bit συν το 5o bit της εισόδου είναι ίσο με το 1o bit συν το 8o bit της εξόδου με πιθανότητα 13/16”.
- Συνδυάζοντας τέτοιες σχέσεις θέλουμε να φτάσουμε σε μια αλγεβρική σχέση μεταξύ input bits, output bits και key bits, που να ισχύει με πιθανότητα άνω του μισού ($p = 0.5 + 1 / M$).

Advanced Encryption Standard (AES)

- Μήκος κλειδιού: 128, 192, 256 bits.
- Block size: 128 bits.
- Βασίζεται σε SP networks και σε πίνακες από **bytes**.

AES (2)

$$\begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix}$$

Πηγή εικόνας: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

AES

(High Level Design)

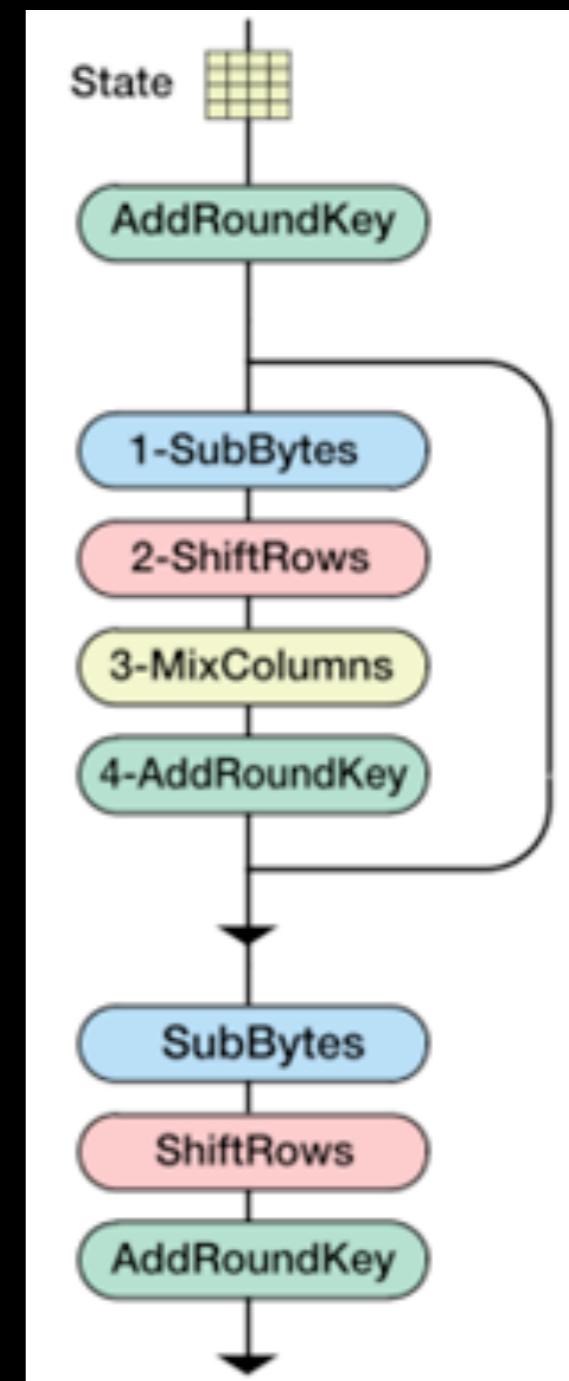
Το Round Key προέρχεται από συγκεκριμένες διεργασίες που περιλαμβάνουν το αρχικό κλειδί.

Substitution

Transposition

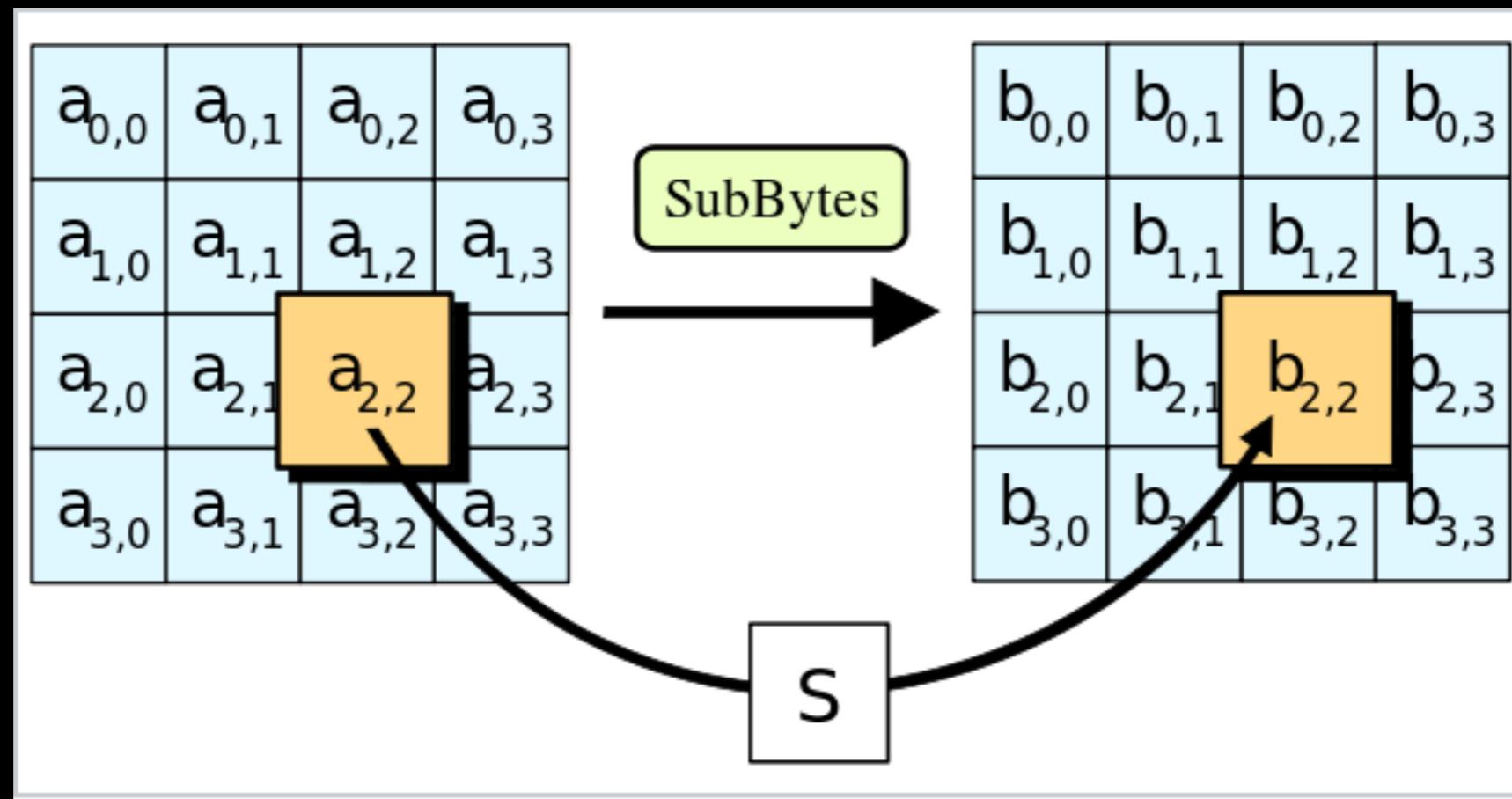
Linear Transformation

XOR



AES

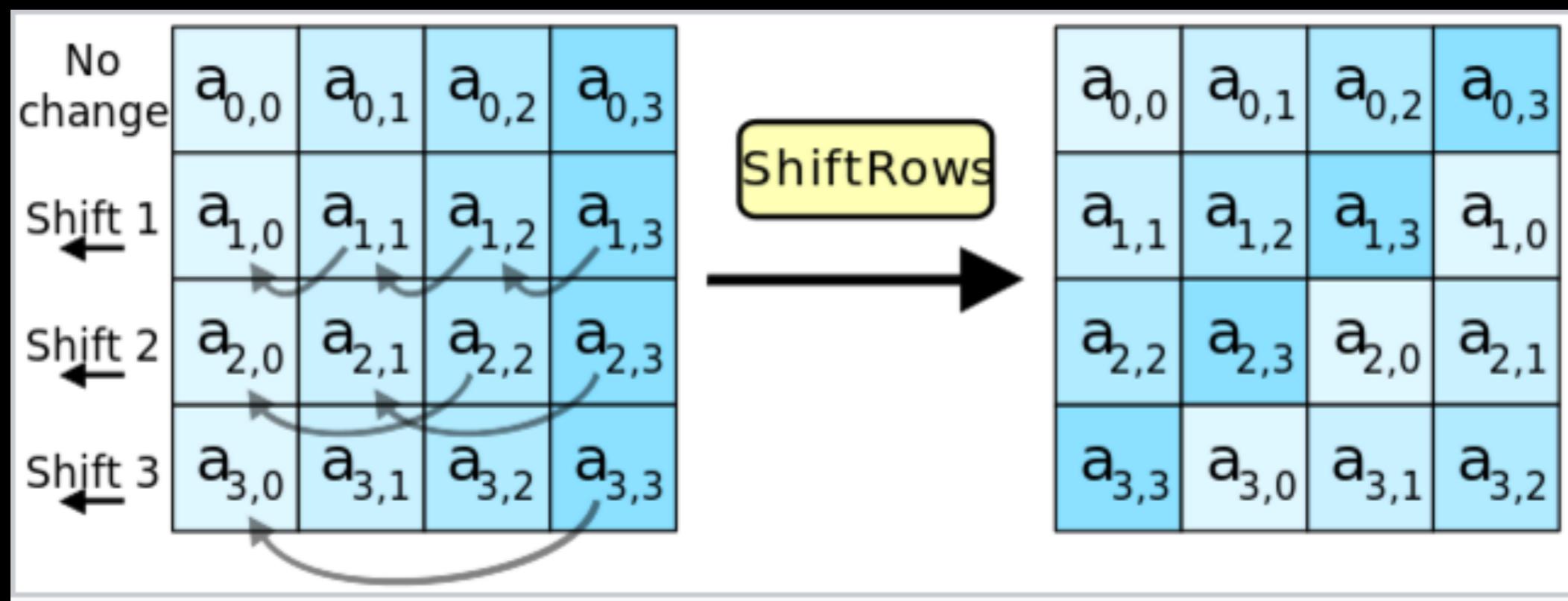
(SubBytes)



Πηγή εικόνων: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

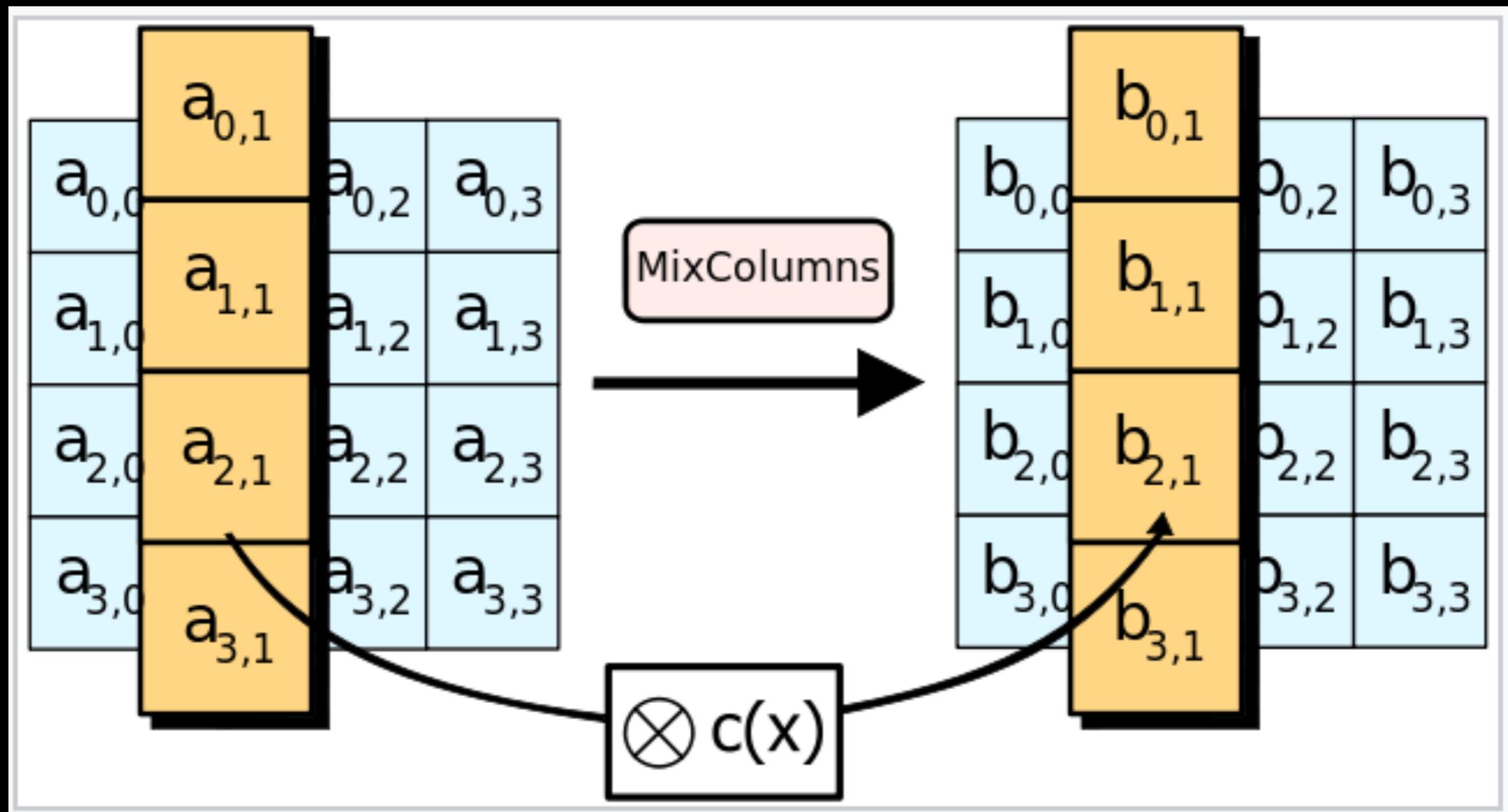
AES

(ShiftRows)



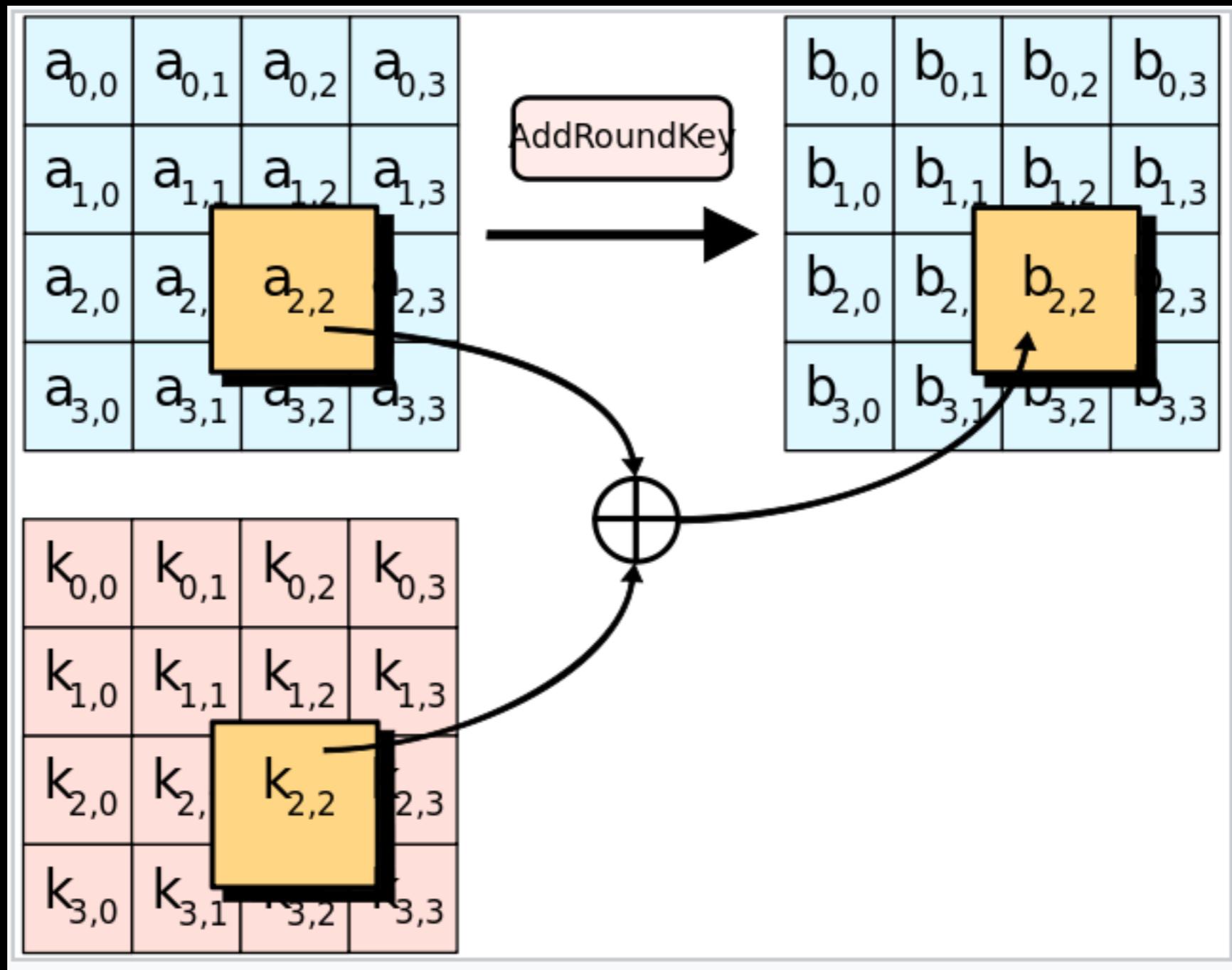
AES

(MixColumns)



AES

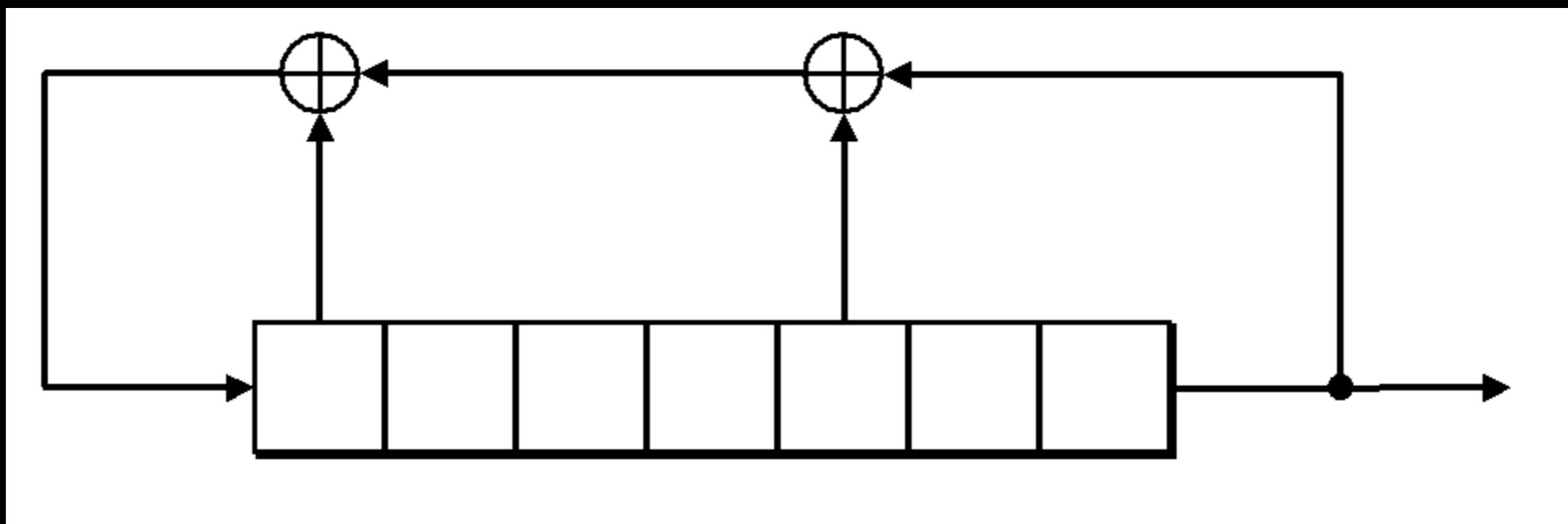
(AddRoundKey)



Stream Ciphers

- Η κρυπτογράφηση των ψηφίων του plaintext γίνεται με βάση με ένα “ψευδοτυχαίο ρεύμα” (**pseudorandom stream**) από ψηφία (**keystream**).
- Κάθε ψηφίο του plaintext κρυπτογραφείται κάθε φορά με ένα αντίστοιχο του keystream.
- Πολύ κοντά στην προσέγγιση του “**one-time pad**”.

Linear Feedback Shift Register (LFSR)



LFSR-based Stream Ciphers

$$e_{i+n+1} = a_1 e_{i+1} + a_2 e_{i+2} + \dots + a_n e_{i+n} \bmod 26$$

Βιβλιογραφία

Jonathan Katz and Yehuda Lindell. Introduction to Modern *Cryptography*. Chapman and Hall/CRC; 1 edition (August 31, 2007). ISBN-10: 1584885513.

R. J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley & Sons, Inc., New York, NY, USA, 2001. ISBN 0471389226.

N. Ferguson and B. Schneier, "Practical Cryptography", John Wiley & Sons, 1st edition, 2003

Στέφανος Γκρίτζαλης, Σωκράτης Κάτσικας, Δημήτρης Γκρίτζαλης. Ασφάλεια Δικτύων Υπολογιστών. Εκδόσεις Παπασωτηρίου (Νοέμβριος 2004). ISBN:13 9789607530455

Auguste Kerckhoffs, La cryptographie militaire, *Journal des sciences militaires*, vol. IX, pp. 5-38, Jan. 1883, pp. 161-191, Feb. 1883.

Shannon, Claude (1949). "Communication Theory of Secrecy Systems". *Bell System Technical Journal*. 28 (4): 656–715.

Bill Poser. Language Log: The Provezano Code. 2006. [Online] Available: <http://itre.cis.upenn.edu/myl/languagelog/archives/003049.html>.

The Principle of the Enigma. 2017. [Online] Available: <https://www.codesandciphers.org.uk/enigma>.

The ECB Penguin. 2017. [Online] Available: <https://blog.filippo.io/the-ecb-penguin/>.

Joan Daemen, Vincent Rijmen, "The Design of Rijndael: AES – The Advanced Encryption Standard." Springer, 2002. ISBN 3-540-42580-2.

Matsui M. (1994) Linear Cryptanalysis Method for DES Cipher. In: Helleseth T. (eds) *Advances in Cryptology — EUROCRYPT '93. EUROCRYPT 1993*. Lecture Notes in Computer Science, vol 765. Springer, Berlin, Heidelberg

Daniel Rees. Stream Ciphers - Encryption / Decryption. [Online] Available: <https://www.youtube.com/watch?v=3uJI2zutyO4>.