ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΚΡΥΠΤΟΓΡΑΦΙΑ

7η Διάλεξη

Κωνσταντίνου Ελισάβετ

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Άδειες Χρήσης

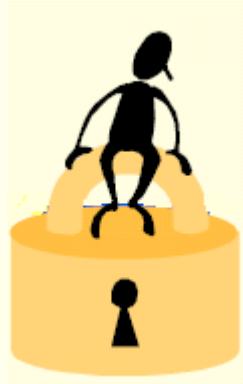
- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Αιγαίου**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

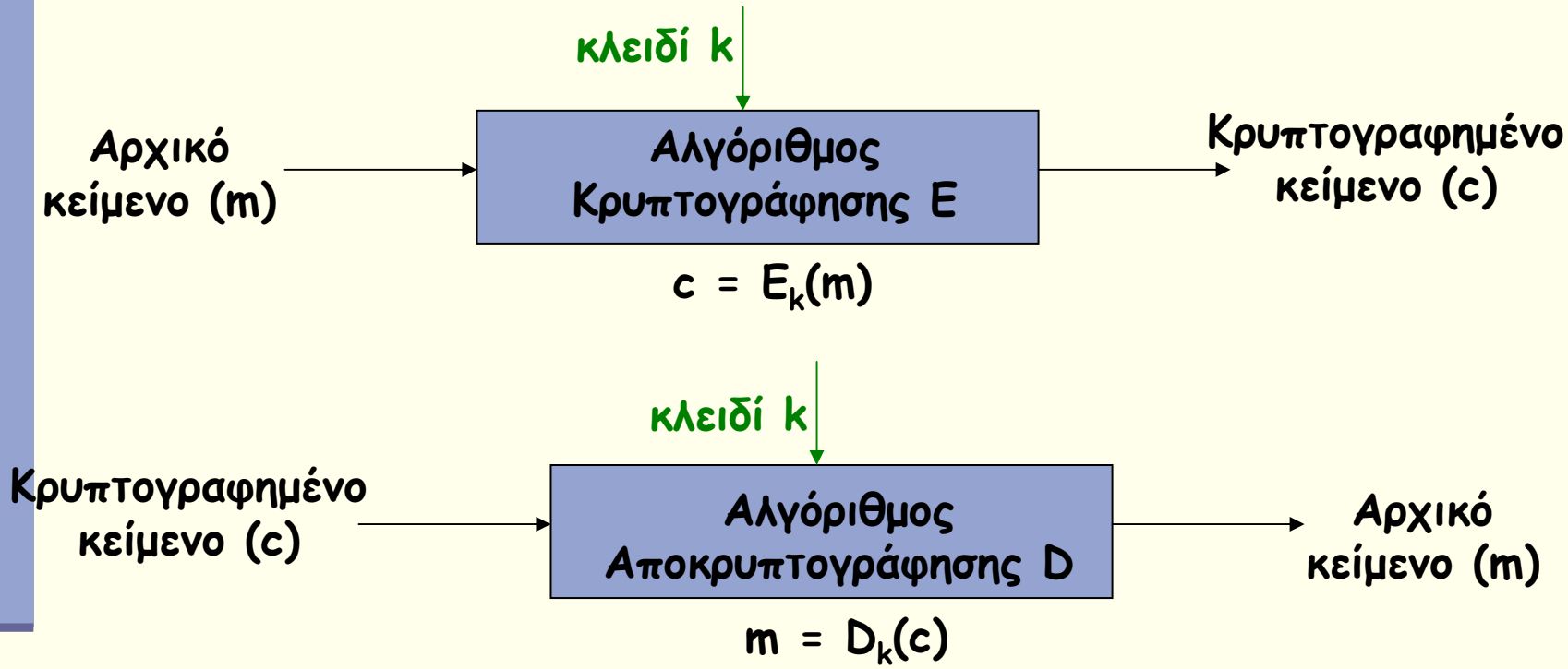
Κρυπτογραφία



Κωνσταντίνου Ελισάβετ
ekonstantinou@aegean.gr

http://www.icsd.aegean.gr/ekonstantinou

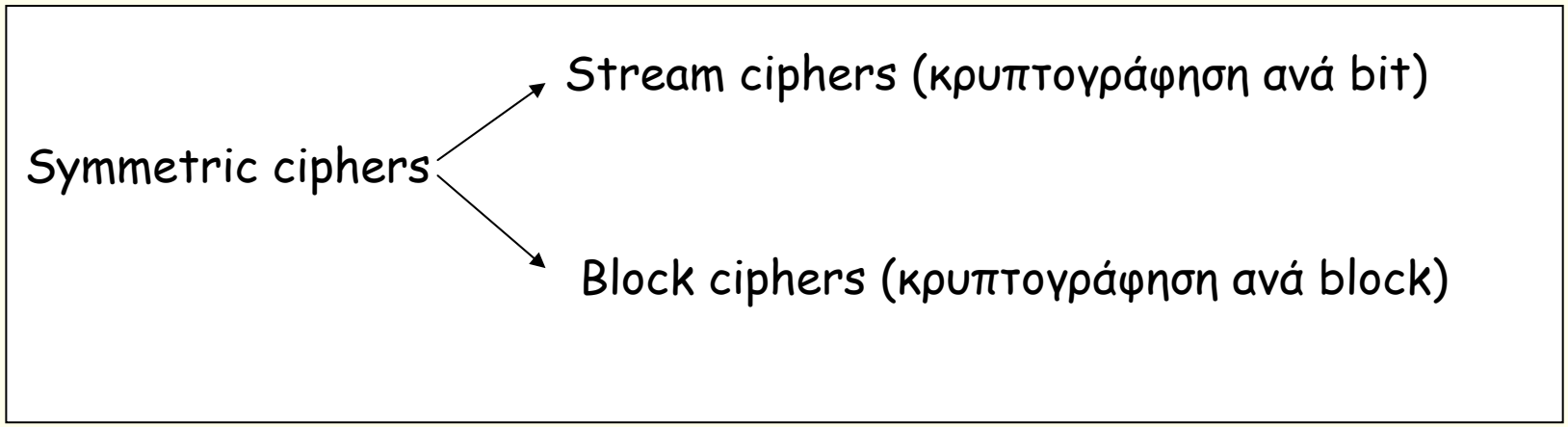
Συμμετρικά Κρυπτοσυστήματα



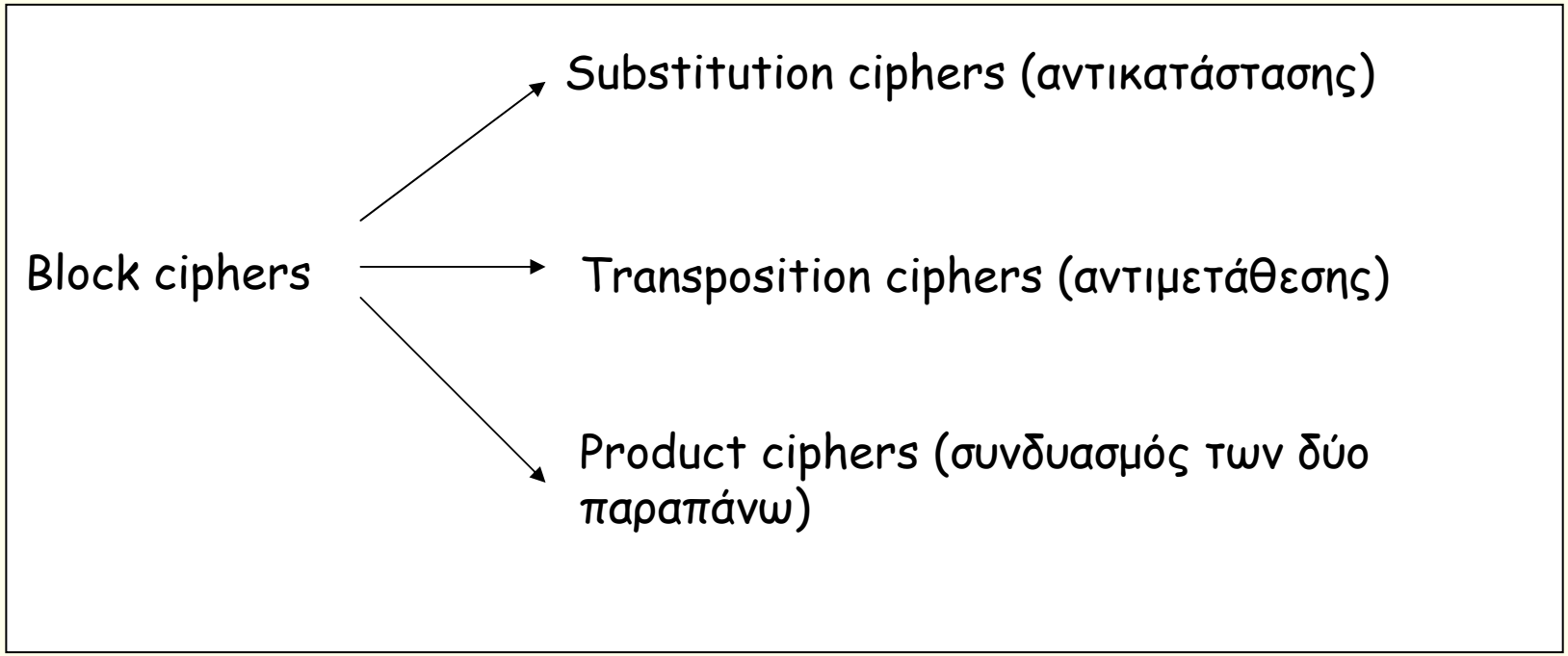
Το κλειδί αποκρυπτογράφησης μπορεί να βρεθεί εύκολα από το αντίστοιχο κλειδί κρυπτογράφησης. Στις περισσότερες περιπτώσεις είναι ακριβώς τα ίδια.

Συμμετρικά Κρυπτοσυστήματα

- Τα συμμετρικά συστήματα προϋπήρχαν των συστημάτων δημόσιου κλειδιού (τα οποία εμφανίστηκαν το 1976 με την εργασία των Diffie-Hellman).
- Βασίζονται στη μυστικότητα του κλειδιού αποκρυπτογράφησης-κρυπτογράφησης, οπότε θα πρέπει να υπάρχει ένας ασφαλής δίαυλος επικοινωνίας μεταξύ των δύο χρηστών για την εγκατάσταση του κλειδιού.
- Κάτι τέτοιο δεν χρειάζεται στα συστήματα δημόσιου κλειδιού.



Block ciphers



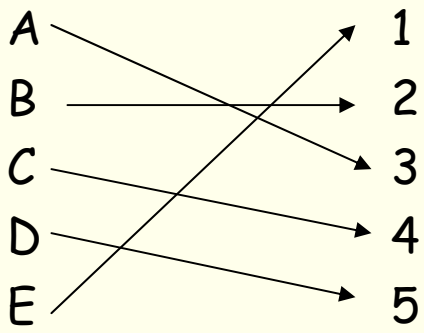
Block ciphers

Ένας block cipher είναι μια συνάρτηση που απεικονίζει blocks του plaintext μεγέθους n-bits σε blocks μεγέθους πάλι n-bits του ciphertext.

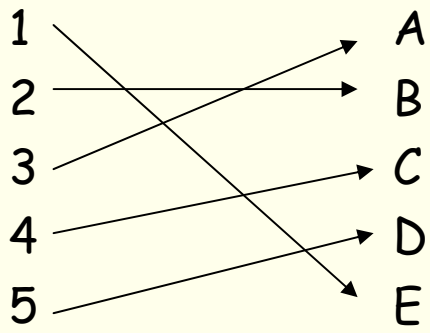
Το n καλείται blocklength.

Κανείς μπορεί να φανταστεί ότι είναι ένας απλός αλγόριθμος αντικατάστασης όπου το σύνολο των πιθανών χαρακτήρων είναι 2^n.

Bijection: f: X -> Y



η συνάρτηση f^{-1} είναι επίσης bijection



Block ciphers

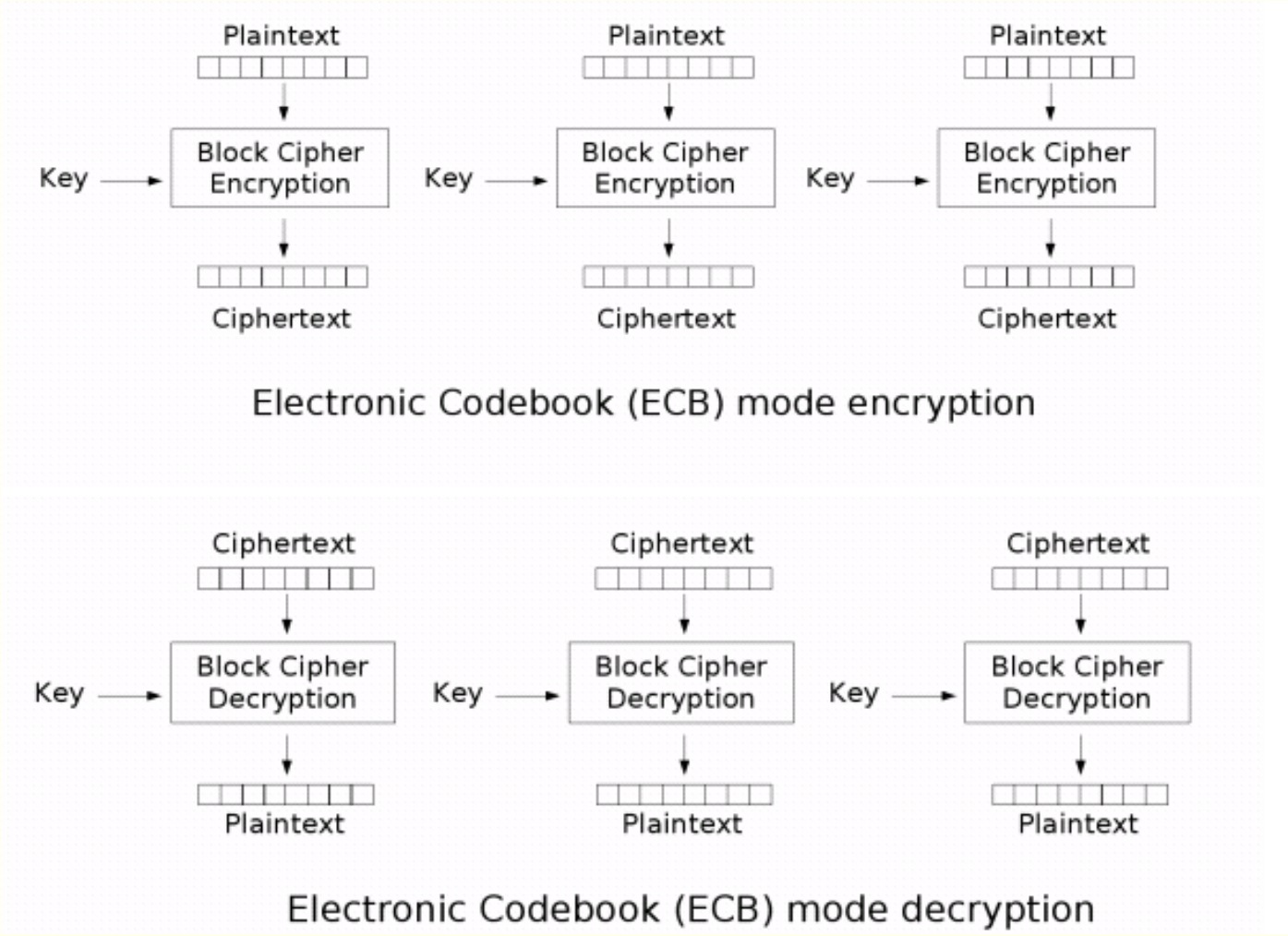
Ορισμός: Ένας πραγματικά τυχαίος cipher (true random cipher) είναι ένας n-bit block cipher που υλοποιεί όλα τα $2^n!$ bijections των 2^n στοιχείων.

Κάθε block έχει συνήθως 64 bits. Αν ένα μήνυμα ξεπερνά τα 64 bits, τότε το χωρίζουμε σε τμήματα των 64 bits.

Αν έχουμε πολλά blocks, πως τα κρυπτογραφούμε και αποκρυπτογραφούμε?

⇒ Υπάρχουν 4 βασικοί τρόποι για το σκοπό αυτό που καλούνται modes of operation: ECB, CBC, CFB, OFB.

ECB mode

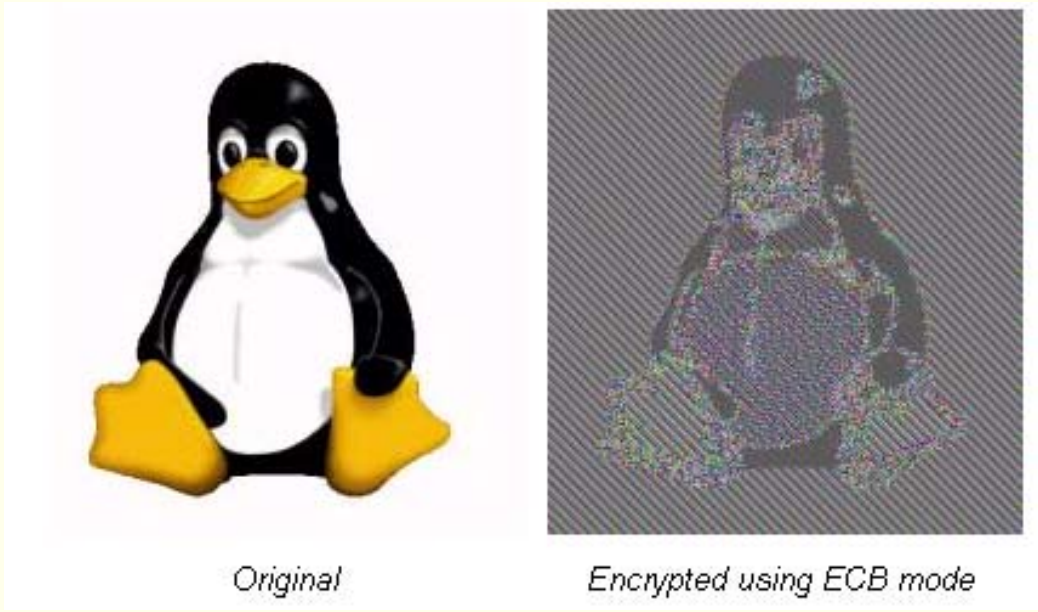

Plaintext
Key
Block Cipher Encryption
Ciphertext
Plaintext
Key
Block Cipher Encryption
Ciphertext
Plaintext
Key
Block Cipher Encryption
Ciphertext
Electronic Codebook (ECB) mode encryption
Ciphertext
Key
Block Cipher Decryption
Plaintext
Ciphertext
Key
Block Cipher Decryption
Plaintext
Ciphertext
Key
Block Cipher Decryption
Plaintext
Electronic Codebook (ECB) mode decryption

ECB mode

1) Ίδια plaintext blocks οδηγούν σε ίδια ciphertext blocks (προφανώς όταν χρησιμοποιείται το ίδιο κλειδί).
2) Η κρυπτογράφηση και η αποκρυπτογράφηση μπορούν να γίνουν παράλληλα για όλα τα blocks.
3) Error propagation: 1 ή περισσότερα λάθη στα bits ενός ciphertext block, επηρεάζουν την αποκρυπτογράφηση μόνο αυτού του block.

Λόγω της 1ης ιδιότητας, το ECB δεν προτείνεται για μηνύματα που ξεπερνούν το ένα block ή αν το ίδιο κλειδί χρησιμοποιείται για πολλά blocks.

ECB mode

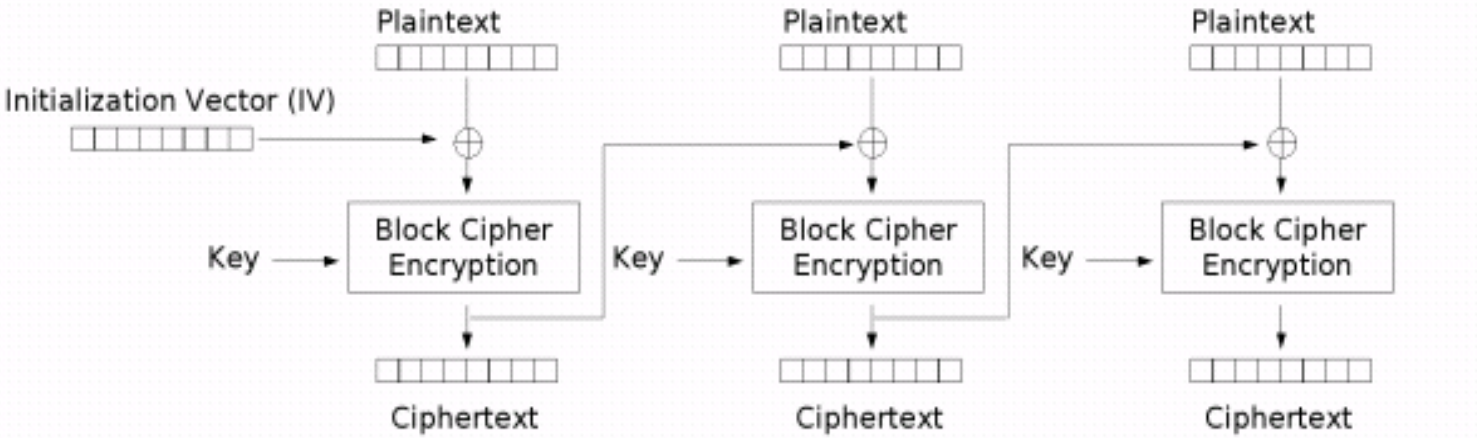


Original

Encrypted using ECB mode

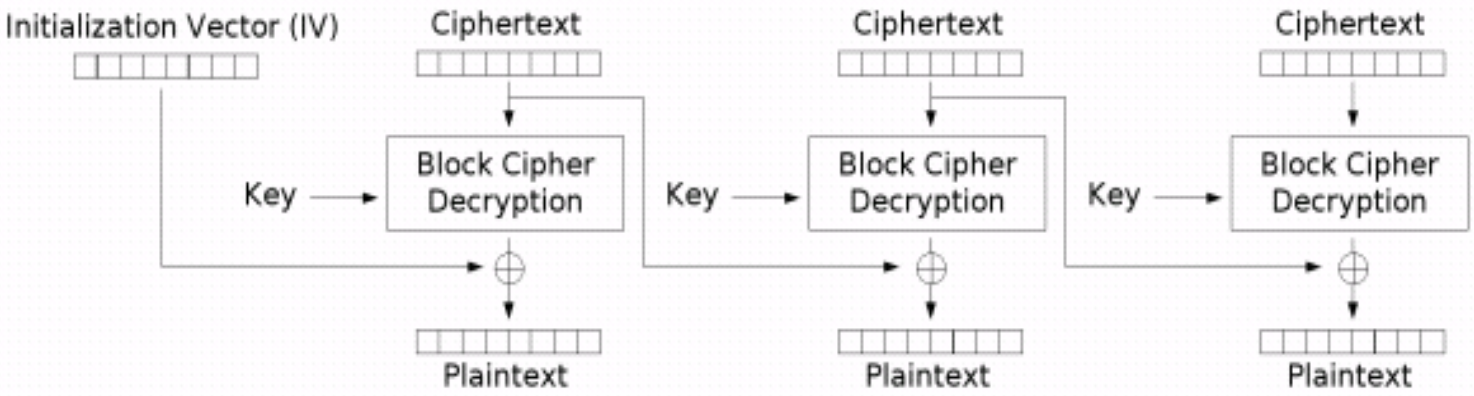
Αντιμετώπιση: Προσθήκη τυχαίων bits στο τέλος κάθε block.

CBC mode



Cipher Block Chaining (CBC) mode encryption

CBC mode



Cipher Block Chaining (CBC) mode decryption

CBC mode

1) Ίδια plaintext blocks οδηγούν σε ίδια ciphertext blocks μόνο αν κρυπτογραφούνται με το ίδιο κλειδί και το ίδιο IV.

2) Κάθε ciphertext c_j εξαρτάται από το αντίστοιχο plaintext x_j και όλα τα προηγούμενα plaintexts. Αν αλλάξουμε τη σειρά των ciphertexts χαλάει η διαδικασία της αποκρυπτογράφησης. Για να αποκρυπτογραφήσουμε σωστά ένα block πρέπει να έχουμε αποκρυπτογραφήσει σωστά και το προηγούμενο.

3) Error propagation: 1 bit λάθους στο ciphertext c_j, επηρεάζει την αποκρυπτογράφηση του block c_j και του c_{j+1}. Το block x_j που θα λάβουμε θα είναι τελείως τυχαίο, ενώ το x_{j+1} θα έχει λάθος ακριβώς στο ίδιο bit που έχει λάθος το c_j. Κάποιος που θέλει να επιτεθεί στο σύστημα μπορεί να κάνει όποιες αλλαγές θέλει στο x_{j+1} αλλάζοντας τα αντίστοιχα bits του c_j.

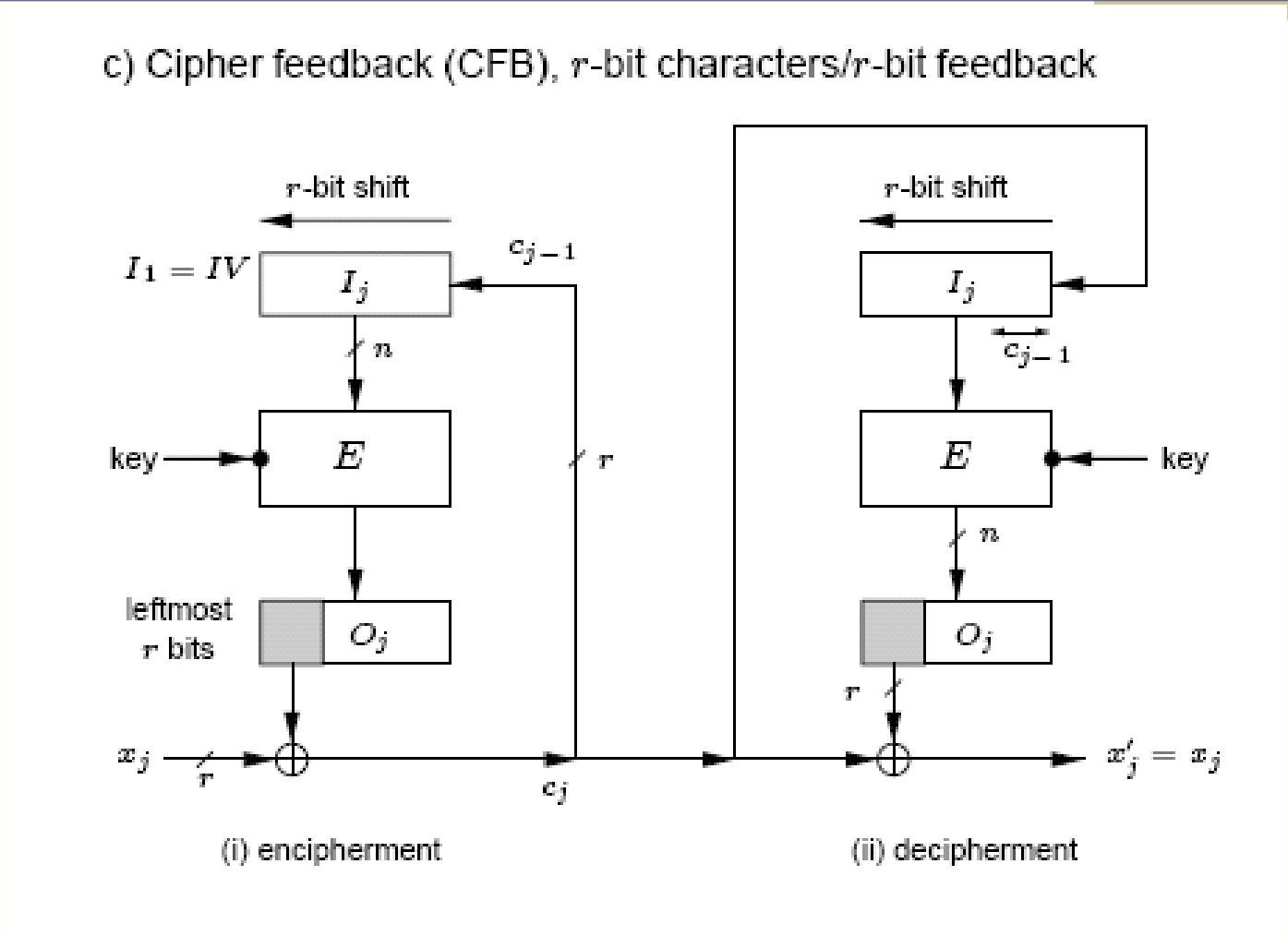
CBC mode

4) Error recovery: αν συμβεί ένα λάθος στο block c_j, αλλά όχι στο c_{j+1}, τότε το c_{j+2} αποκρυπτογραφείται σωστά.

Σημειώνεται ότι παρόλο που ένα λάθος σε ένα ciphertext block δεν επηρεάζει πολύ την αποκρυπτογράφηση, ένα λάθος σε ένα plaintext block επηρεάζει όλα τα ciphertext blocks που δημιουργούνται μετά.

Επίσης, το IV δεν χρειάζεται να είναι μυστικό. Πρέπει όμως να προστατεύεται η ακεραιότητά του. Ο λόγος είναι ότι προβλέψιμες αλλαγές στο IV προκαλούν προβλέψιμες αλλαγές στο πρώτο plaintext block.

CFB mode


c) Cipher feedback (CFB), r-bit characters/r-bit feedback
r-bit shift
$I_1 = IV$
I_j
c_{j-1}
n
key
E
r
leftmost
r bits
O_j
x_j
r
c_j
(i) encipherment
r-bit shift
I_j
c_{j-1}
E
key
n
O_j
r
$x'_j = x_j$
(ii) decipherment

CFB mode

1) Ίδια plaintext blocks οδηγούν σε ίδια ciphertext blocks μόνο αν χρησιμοποιείται το ίδιο IV.
2) Κάθε ciphertext c_j εξαρτάται από το αντίστοιχο plaintext x_j και όλα τα προηγούμενα plaintexts. Αν αλλάξουμε τη σειρά των ciphertexts χαλάει η διαδικασία της αποκρυπτογράφησης. Για να αποκρυπτογραφήσουμε σωστά ένα block πρέπει τα προηγούμενα $\left\lceil \frac{n}{r} \right\rceil$ ciphertext blocks να είναι σωστά.
3) Error propagation: 1 ή παραπάνω bits λάθους στο ciphertext c_j, επηρεάζει την αποκρυπτογράφηση και των υπολοίπων $\left\lceil \frac{n}{r} \right\rceil$ ciphertext blocks.

   Το block x_j που θα λάβουμε θα έχει λάθος ακριβώς στα ίδια bits που έχει λάθος το c_j, κάτι που μπορεί να εκμεταλλευτεί ένας επιτιθέμενος στο σύστημα.

CFB mode

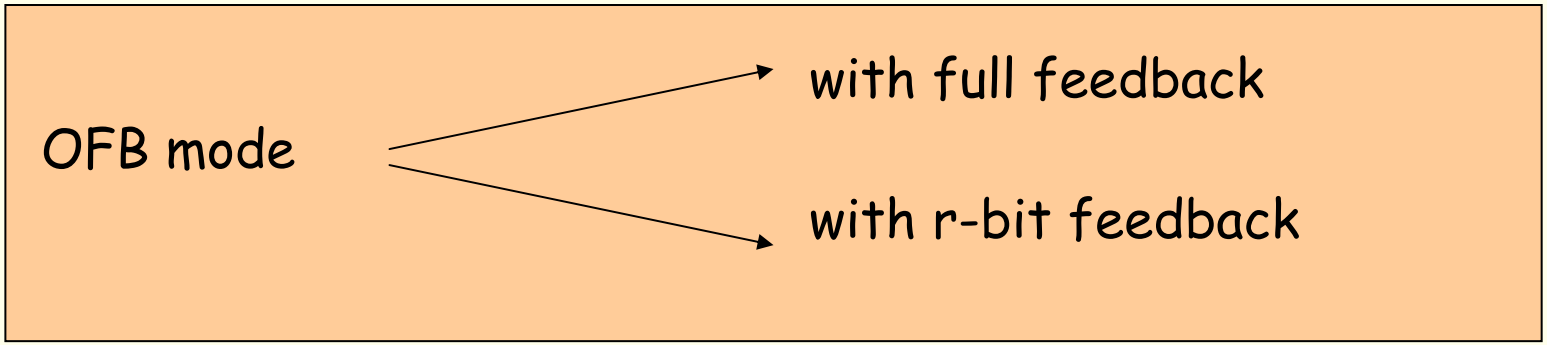
4) Error recovery: αν συμβεί ένα λάθος στο block c_j, αλλά όχι στο c_{j+1}, τότε το σύστημα ανακάμπτει μετά από $\left\lceil \frac{n}{r} \right\rceil$ ciphertext blocks.

Το CFB (όπως και το OFB) χρησιμοποιούν **μόνο** τον αλγόριθμο κρυπτογράφησης. Αυτό σημαίνει ότι μπορούν να χρησιμοποιηθούν για την δημιουργία του keystream ενός stream cipher.

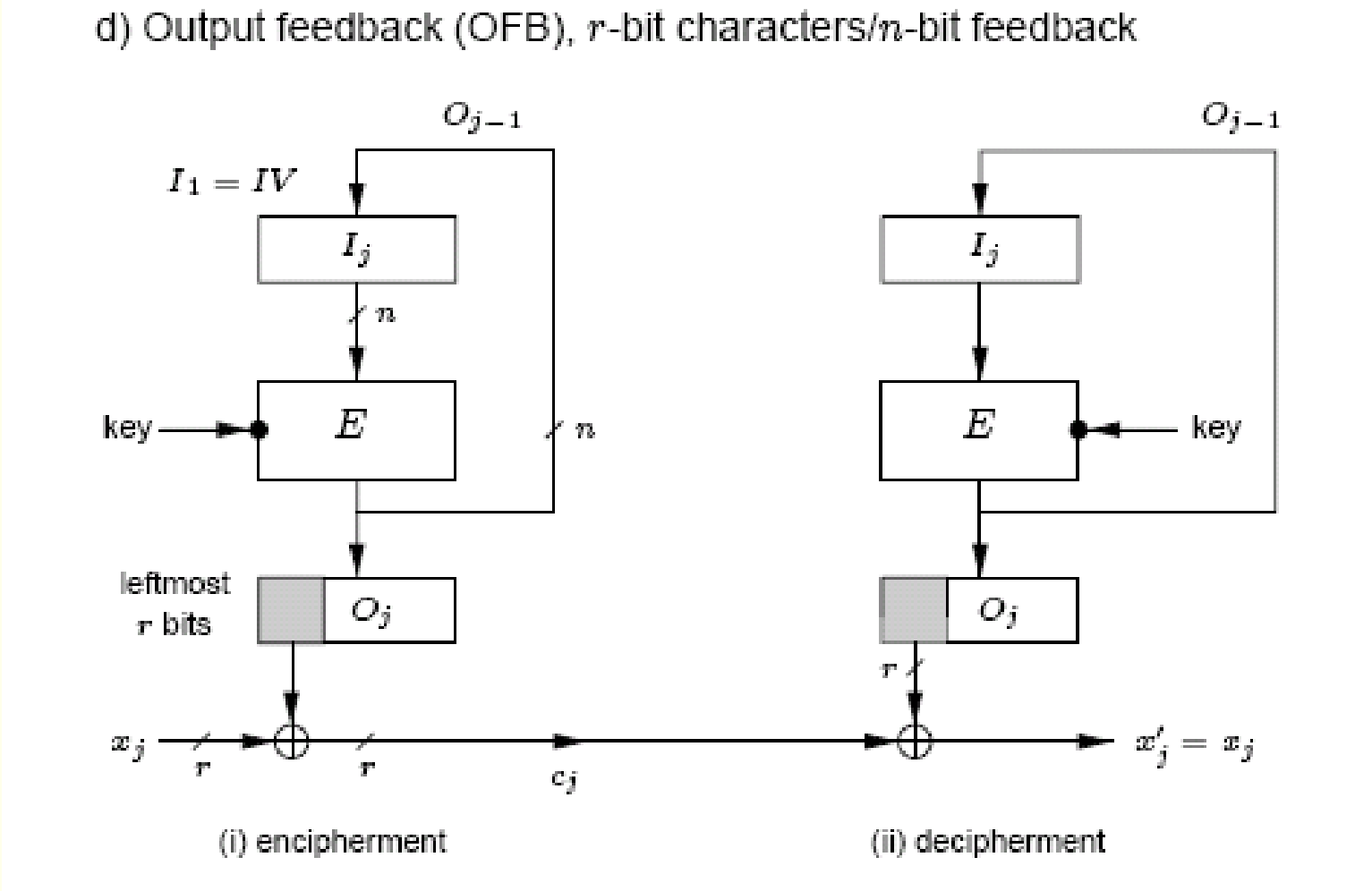
OFB mode

- Είναι παρόμοιο με το CFB και χρησιμοποιείται σε εφαρμογές όπου κάθε error propagation πρέπει να αποφεύγεται.

- Χρησιμοποιεί επίσης μόνο τον αλγόριθμο κρυπτογράφησης και μπορεί να χρησιμοποιηθεί ως stream cipher.



OFB mode


d) Output feedback (OFB), r-bit characters/n-bit feedback
O_{j-1}
$I_1 = IV$
I_j
n
key
E
n
leftmost
r bits
O_j
x_j
r
r
c_j
O_{j-1}
I_j
E
key
O_j
r
$x'_j = x_j$
(i) encipherment
(ii) decipherment

OFB mode

1) Ίδια plaintext blocks οδηγούν σε ίδια ciphertext blocks μόνο αν χρησιμοποιείται το ίδιο IV.

2) Η τιμή του IV παρόλο που δεν χρειάζεται να είναι μυστική, θα πρέπει να αλλάζει αν το ίδιο κλειδί K χρησιμοποιείται. Αν δεν αλλάζει ούτε το IV, ούτε το K, τότε προκύπτει το ίδιο keystream.

3) Error propagation: 1 ή παραπάνω bits λάθους στο ciphertext c_j, προκαλεί λάθη στο αντίστοιχο μόνο plaintext block x_j, ακριβώς στις ίδιες θέσεις.

OFB mode

4) Error recovery: τα λάθη που μπορεί να υπάρχουν σε μερικά bits ενός ciphertext block, επηρεάζουν το αντίστοιχο plaintext block στην αποκρυπτογράφηση.

5) Τα blocks του keystream μπορούν να υπολογιστούν πριν την διαδικασία της κρυπτογράφησης αφού οι τιμές τους δεν εξαρτώνται από τα plaintext-ciphertext blocks. Αυτό επιταχύνει πολύ την όλη διαδικασία.

Block ciphers

Για έναν n-bit block cipher με k-bit μεγέθους κλειδί K, γνωρίζοντας κανείς έστω και ένα ζευγάρι plaintext-ciphertext, το K μπορεί να βρεθεί με exhaustive key search. Κατά μέσο όρο μετά από 2^{k-1} υπολογισμούς το κλειδί θα έχει βρεθεί.

Για παράδειγμα στον DES όπου k=56, n=64 το κλειδί βρίσκεται μετά από 2^{55} βήματα.

Οι επιθέσεις στον DES εκμεταλλεύτηκαν το μικρό μήκος κλειδιού και όχι κάποια τρύπα στον αλγόριθμο.

Block ciphers

Για να αποφευχθούν οι επιθέσεις τύπου exhaustive search, συχνά το ίδιο block κρυπτογραφείται πολλές φορές με διαφορετικά κλειδιά. Π.χ.:

$$C = E_{kn}(E_{kn-1} \dots E_{k1}(m))$$

Αν τα κλειδιά είναι ανεξάρτητα μεταξύ τους, ο αλγόριθμος καλείται cascade cipher. Διαφορετικά, αν (μερικά από) τα κλειδιά είναι ίδια, τότε έχουμε multiple encryption.

Σε ένα σύστημα double encryption $E(m) = E_{k2}(E_{k1}(m))$ με κλειδιά k1, k2, μεγέθους k-bits θα πρέπει κανείς να κάνει 2^{2k} υπολογισμούς μέχρι να σπάσει το σύστημα. Εναλλακτικά, μπορεί να μειώσει το χρόνο σε 2^k αν χρησιμοποιήσει χώρο αποθήκευσης 2^k. Πως??

Σύγχρονοι Συμμετρικοί Αλγόριθμοι

1971: Horst Feistel (IBM) – Αλγόριθμος Lucifer

1973: Η NIST (National Institute of Standards and Technology) απευθύνει κάλεσμα για υποβολή προτάσεων με σκοπό τη δημιουργία ενός νέου αλγορίθμου κρυπτογράφησης.

1974: Η IBM υποβάλλει ως πρόταση έναν αλγόριθμο βασισμένο στον Lucifer.

1977: Data Encryption Standard (DES) γίνεται πρότυπο FIPS PUB 46.

1997: Η NIST απευθύνει κάλεσμα για νέο πρότυπο.

1999: Ο DES σπάει σε 22 ώρες.

2000: Η NIST επιλέγει τον Rijndael ή AES (Advanced Encryption Standard).

DES

Η σχεδίαση του DES σχετίζεται με δύο ciphers: τους product ciphers και τους Feistel ciphers.

Ορισμός: Ένα δίκτυο αντικατάστασης – αντιμετάθεσης (substitution – permutation or SP network) είναι ένας product cipher που αποτελείται από διάφορα στάδια, το καθένα από τα οποία περιλαμβάνει αντικαταστάσεις και αντιμεταθέσεις.

Δίκτυο Αντικατάστασης - Αντιμετάθεσης

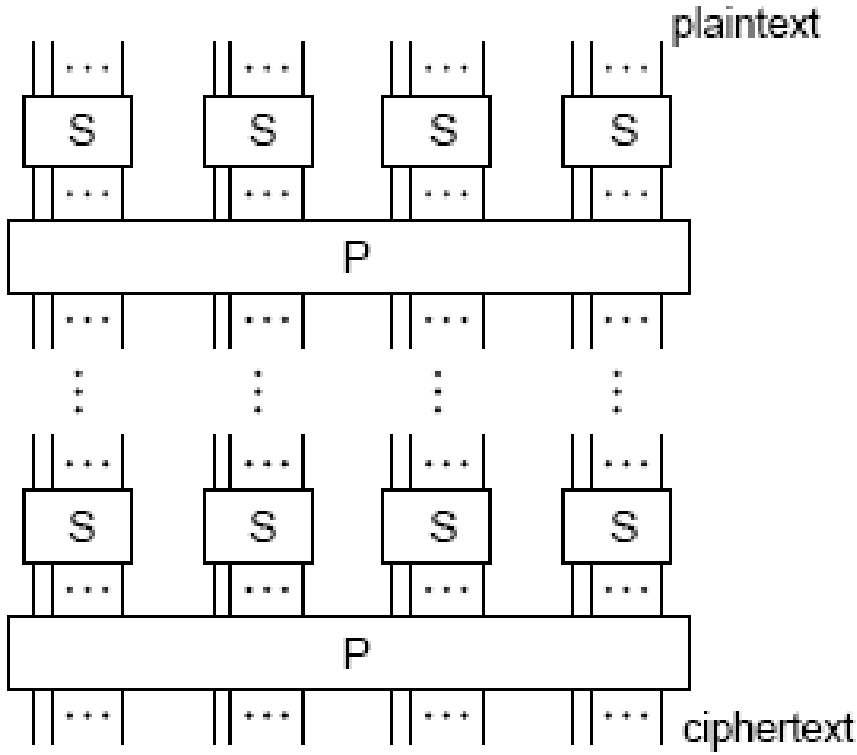


Figure 7.7: *Substitution-permutation (SP) network.*

Γενικοί Ορισμοί

Ορισμός: Ένας επαναληπτικός block cipher αποτελείται από διαδοχικές επαναλήψεις μιας συνάρτησης που καλείται round function. Παράμετροι σε έναν τέτοιο cipher είναι ο αριθμός των γύρων (rounds) r, το μέγεθος του block n και το μέγεθος σε bits k του κλειδιού εισόδου K από το οποίο παράγονται r υποκλειδιά k_i (round keys).

Ορισμός: Ένας Feistel cipher είναι ένας επαναληπτικός cipher που απεικονίζει ένα 2t μεγέθους (σε bits) plaintext (L_0, R_0), για δύο t-bits blocks L_0 και R_0, σε ένα ciphertext (R_r, L_r) μέσω μιας διαδικασίας που αποτελείται από r rounds. Για κάθε i, ο γύρος i αντιστοιχίζει το ζευγάρι (L_{i-1}, R_{i-1}) στο ζευγάρι (L_i, R_i) με τον εξής τρόπο: $L_i = R_{i-1}$ και $R_i = L_{i-1}$ XOR $f(R_{i-1}, k_i)$ όπου f() είναι η round function και κάθε k_i παράγεται από ένα αρχικό κλειδί K.

Η αποκρυπτογράφηση γίνεται με τον ίδιο τρόπο, αλλά τα κλειδιά k_i χρησιμοποιούνται με την αντίστροφη σειρά. Η συνάρτηση f() είναι συνήθως ένας product cipher.

DES

Ουσιαστικά ο DES είναι ένας Feistel cipher ο οποίος επεξεργάζεται blocks μεγέθους n = 64 bits και παράγει ciphertext blocks των 64 bits επίσης.

Το μέγεθος του κλειδιού που χρησιμοποιείται είναι K = 56 bits.

Η κρυπτογράφηση γίνεται σε 16 γύρους (rounds). Από το αρχικό κλειδί K παράγονται 16 κλειδιά των 48-bits (καθένα από αυτά χρησιμοποιείται σε κάθε γύρο).

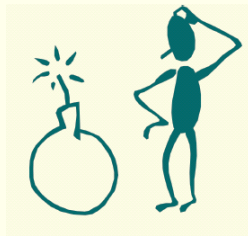
DES

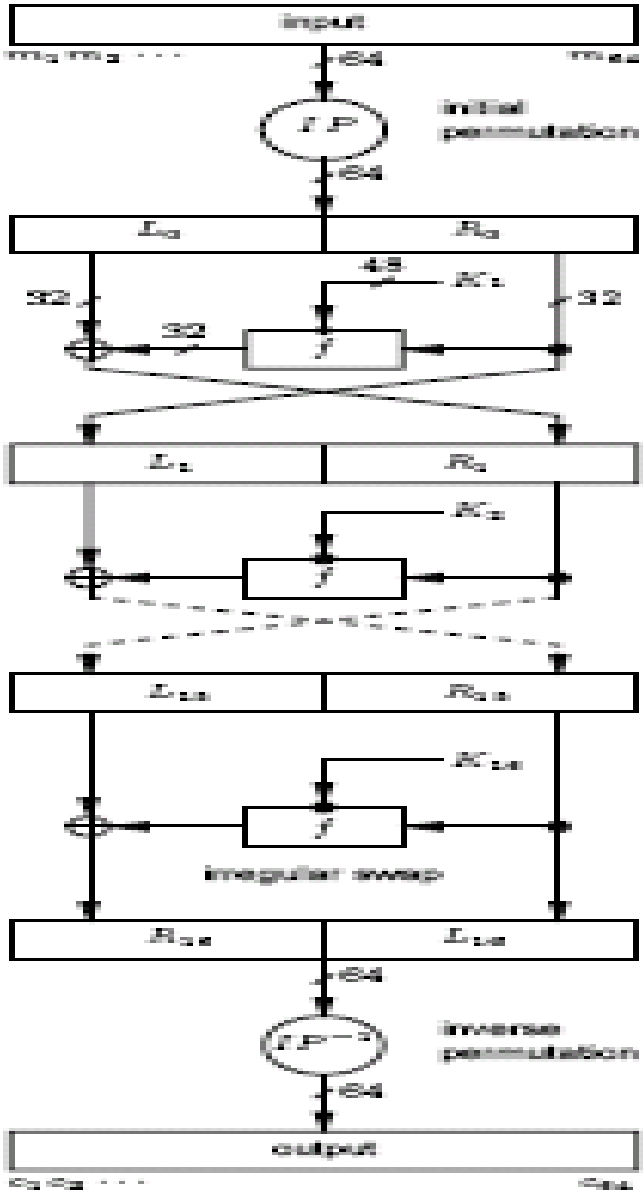
Κάθε plaintext block των 64-bits χωρίζεται σε 2 τμήματα L_0 και R_0. Στη συνέχεια εκτελείται ένας Feistel cipher από 16 γύρους, όπου η συνάρτηση f() είναι ίση με $f(R_{i-1}, k_i) = P(S(E(R_{i-1}) \text{ xor } k_i))$ όπου:

E (Expansion): προσθέτει στο R_{i-1} 16 bits (από 32 το κάνει 48)

S (Substitution): 8 S-boxes, το καθένα είναι ένας 6-to-4 bits αλγόριθμος αντικατάστασης

P (Permutation): αλγόριθμος αντιμετάθεσης




input
64
initial permutation
64
48
32
32
32
inverse permutation
64
output

DES

α) Πως υλοποιούνται τα IP και IP^{-1}?

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Table 7.2: *DES initial permutation and inverse (IP and* IP^{-1}*).*

DES

β) Πως υλοποιείται η συνάρτηση f(.)?

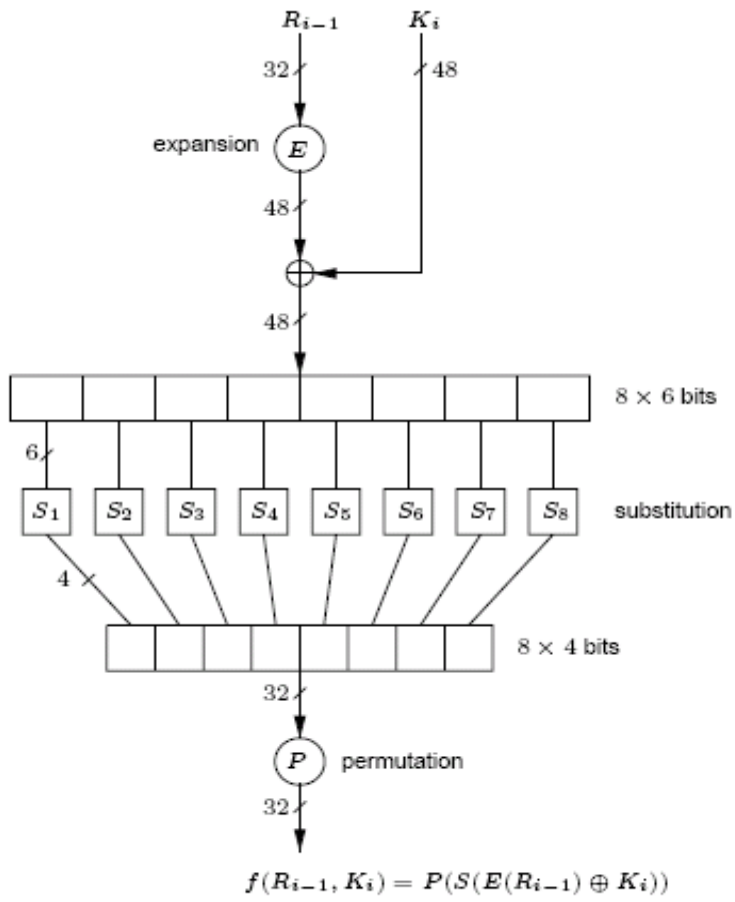


Figure 7.10: *DES inner function f.*

Ιδιότητες DES

1) Κάθε bit του ciphertext εξαρτάται από όλα τα bits του κλειδιού και όλα τα bits του plaintext.

2) Στατιστικά, τα bits των plaintext και ciphertext είναι ανεξάρτητα.

3) Η αλλαγή ενός bit του plaintext ή του κλειδιού, πρέπει να οδηγεί στην αλλαγή οποιουδήποτε bit του ciphertext με πιθανότητα $\frac{1}{2}$.

4) Η αλλαγή ενός bit του ciphertext πρέπει να οδηγεί το plaintext σε μη προβλέψιμες αλλαγές.

Ασθενή Κλειδιά του DES

Αν τα κλειδιά k1 και k16 είναι ίδια, τότε ισχύει ότι k2=k15, k3=k14 κ.ο.κ.

Δηλαδή η διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης είναι η ίδια, ή αλλιώς $E_K(E_K(m)) = m$.

Τα κλειδιά που έχουν αυτή την ιδιότητα καλούνται weak keys.

Αν για δύο κλειδιά K, K' ισχύει ότι $E_{K'}(E_K(m)) = m$, τότε αυτά καλούνται semi-weak keys.

Ο DES έχει 4 weak keys και 6 ζευγάρια από semi-weak keys.

Διάβασμα…

Κεφάλαια 7.1, 7.2 και 7.4 του
Handbook of Applied Cryptography