Cryptography and Network Security Chapter 3

Fifth Edition

by William Stallings

Κρυπτογραφικοι Αλγοριθμοι Τμηματων (Block Ciphers)

All the afternoon Mungo had been working on Stern's code, principally with the aid of the latest messages which he had copied down at the Nevin Square drop. Stern was very confident. He must be well aware London Central knew about that drop. It was obvious that they didn't care how often Mungo read their messages, so confident were they in the impenetrability of the code.

***—Talking to Strange Men,* Ruth Rendell**

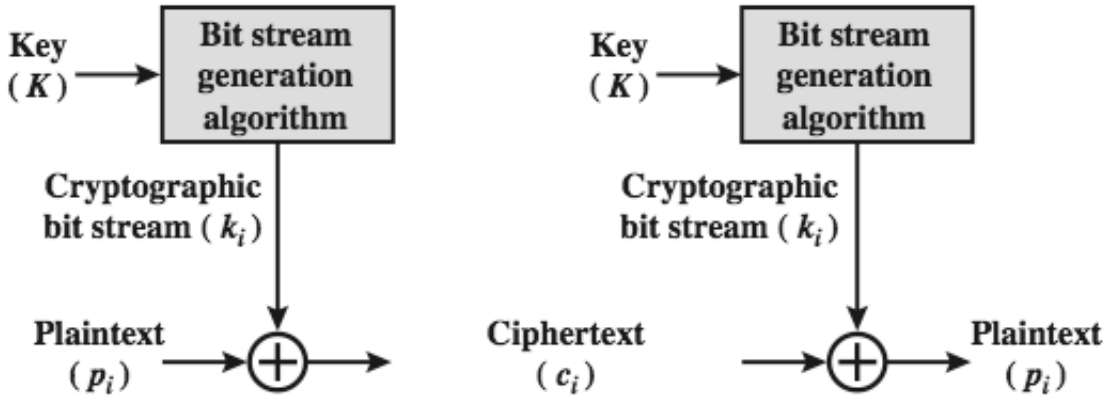
Συγχρονοι αλγοριθμοι Τμηματων

- Ας δουμε τωρα τους συγχρονους κρυπτογραφικους αλγοριθμους
- Οι αλγοριθμοι τμηματων ειναι απο τους πιο ευρεως χρησιμοποιουμενους τυπους κρυπτογραφικων αλγοριθμων.
- Χρησιμοποιουνται για τις υπηρεσιες τοσο της μυστικοτητας, οσο και της πιστοποιησης αυθεντικοτητας
- Θα εστιασουμε στον αλγοριθμο DES (Data Encryption Standard) προκειμενου να μελετησουμε τις σχεδιαστικες αρχες των αλγοριθμων τμηματων.

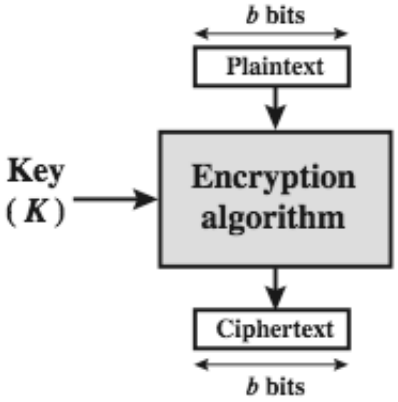
Αλγοριθμοι τμηματων (Block Ciphers) και Αλγοριθμοι Ροης (Stream Ciphers)

- Οι αλγοριθμοι τμηματων επεξεργαζονται τα μηνυματα κατα τμηματα το καθενα απο τα οποια κρυπτογραφειται ή αποκρυπτογραφειται.
- Οι αλγοριθμοι ροης, οταν κρυπτογραφουν ή αποκρυπτογραφουν επεξεργαζονται ενα μονο bit ή byte καθε φορα.
- Πολλοι συγχρονοι αλγοριθμοι κρυπτογραφησης ειναι αλγοριθμοι τμηματων.
  - Αναλυονται καλυτερα
  - Εχουν ευρυτερο πεδιο εφαρμογων

Block vs Stream Ciphers



(a) Stream Cipher Using Algorithmic Bit Stream Generator

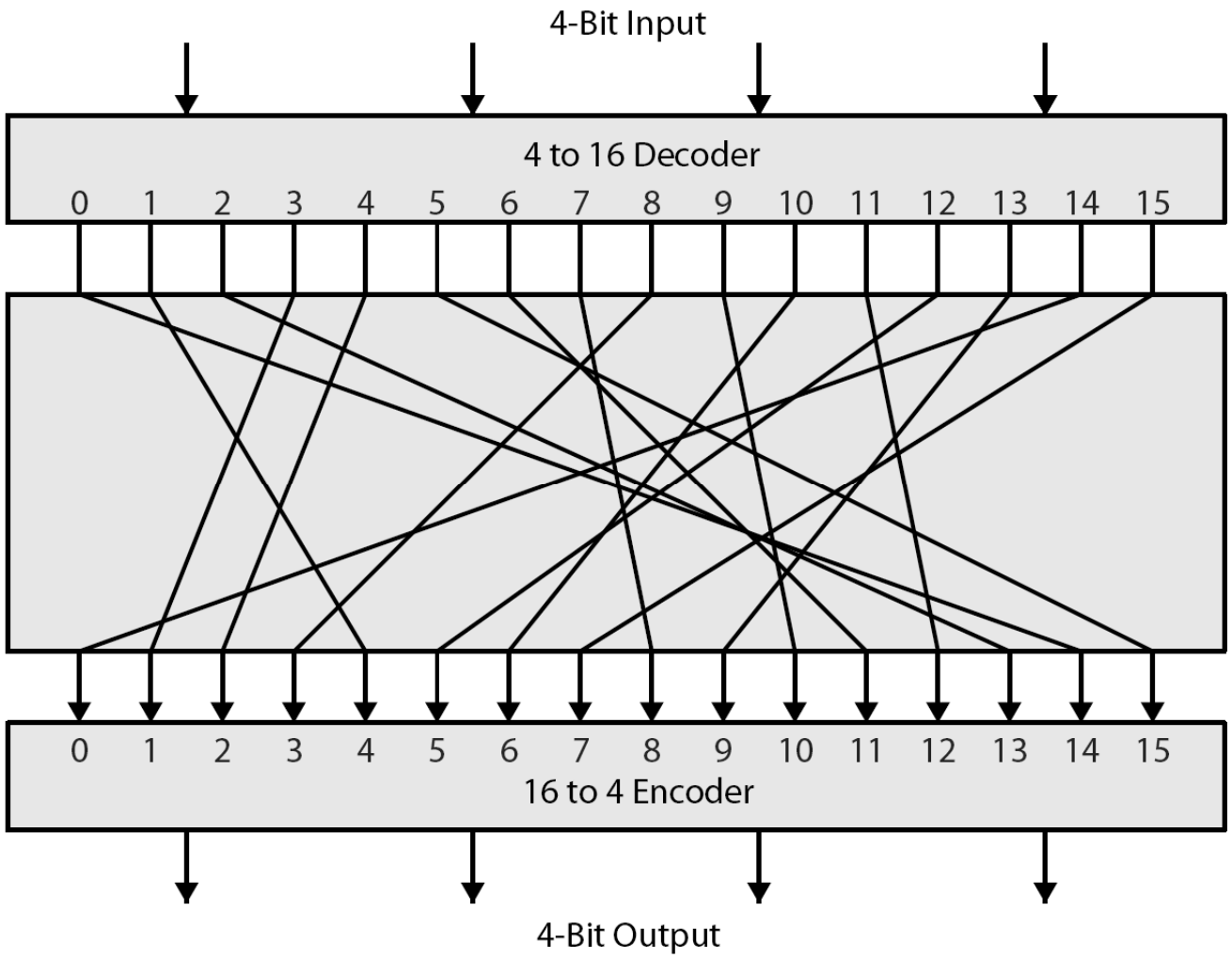


(b) Block Cipher

Αρχες των Αλγοριθμων Τμηματων

- Οι περισσοτεροι συμμετρικοι αλγοριθμοι τμηματων βασιζονται σε δομη **Feistel Cipher**
- Αποκρυπτογραφουν το ciphertext αποδοτικα
- Μπορουν να ειδωθουν ως μια εξαιρετικα μεγαλη αντικατασταση.
- Θα χρειαζονταν ομως εναν πινακα με 2^{64} entries για μια δεσμη των 64-bits
- Αποτελουνται απο μικροτερα δομικα στοιχεια και χρησιμοποιουν την ιδεα του product cipher

Ideal Block Cipher



Ο Claude Shannon και οι Κρυπτογραφικοι Αλγοριθμοι Αντικαταστασης-Μεταθεσης (Substitution-Permutation Ciphers)

- Ο Shannon εισήγαγε την ιδεα των δικτυων Αντικαταστασης-Μεταθεσης [substitution-permutation (S-P nets)] το 1949.
- Αποτελουν τη βαση των συγχρονων αλγοριθμων τμηματων
- Τα S-P nets βασιζονται σε δυο βασικες κρυπτογραφικες λειτουργιες:
  - *Αντικατασταση (substitution,* S-box)
  - *Μεταθεση (permutation,* P-box)
- Παρεχουν συγχυση και διαχυση του μηνυματος και του κλειδιου.

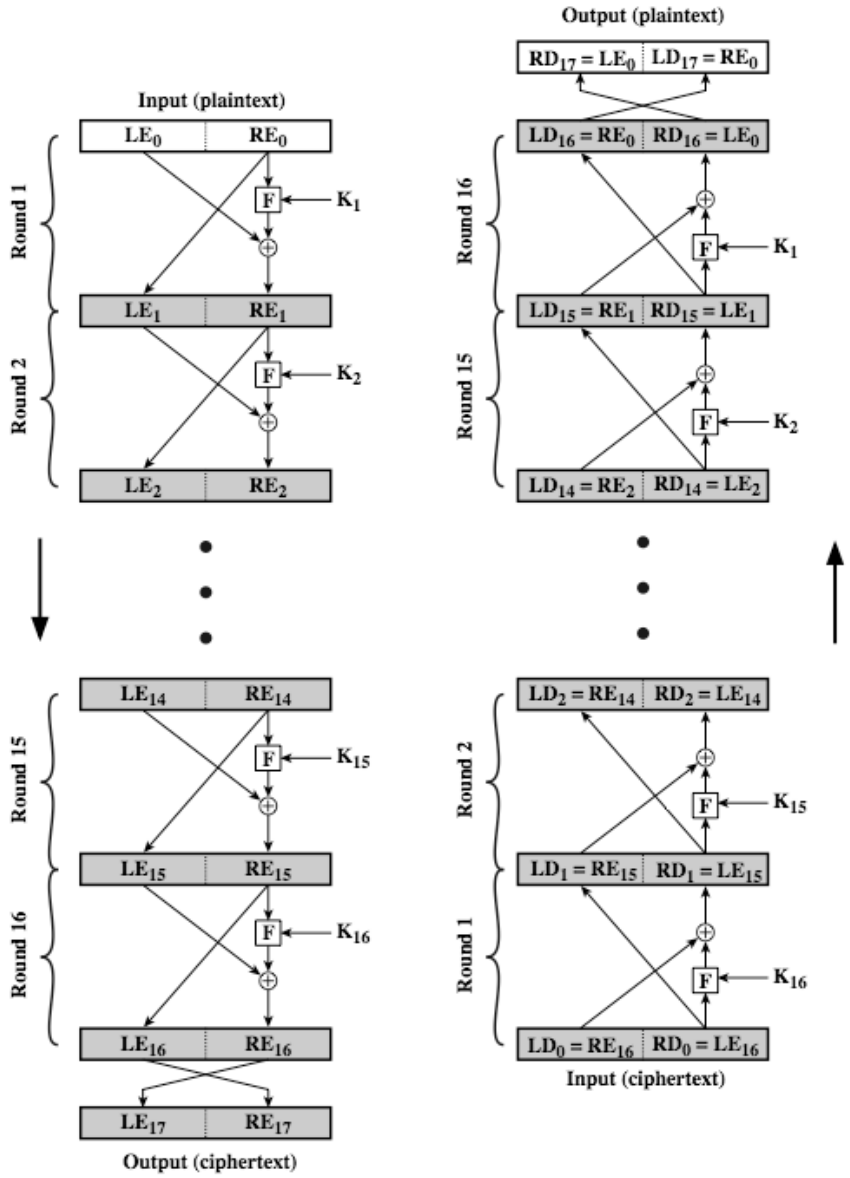
Συγχυση και Διαχυση (Confusion and Diffusion)

- Ο κρυπτογραφικος αλγοριθμος πρεπει να συσκοτιζει τελειως τις στατιστικες ιδιοτητες του αρχικου μηνυματος
- Αυτο το επιτυγχανει ενα κλειδι μιας χρησης (one-time pad)
- Ο Shannon προτεινε το συνδυασμο στοιχειων S & P (αντικαταστασης και μεταθεσης) για να επιτυχει:
- **Διαχυση (diffusion)** – δυαλυει τη στατιστικη δομη του plaintext.
- **Συγχυση (confusion)** – κανει τη σχεση μεταξυ του ciphertext και του κλειδιου οσο το δυνατον πιο πολυπλοκη

Η Δομη Feistel Cipher

- Ο Horst Feistel επινοησε τον **feistel cipher**
  - Βασιζεται στις ιδεες του Shannon
- Χωριζει το input block σε δυο ισα κομματια.
  - Τα επεξεργαζεται μεσω πολλαπλων γυρων οι οποιοι
  - Εκτελουν μια αντικατασταση στο αριστερο μισο των δεδομενων
  - Βασιζεται σε μια συναρτηση γυρου (round function) του δεξιου μισου και του υποκλειδιου.
  - Στη συνεχεια πραγματοποιει αντιμεταθεση μεταξυ των δυο μισων
- Εφαρμοζει την ιδεα των S-P nets του Shannon

Δομή Feistel Cipher



Σχεδιαστικα στοιχεια του Feistel Cipher

- Το μεγεθος των τμηματων (block size)
- Το μεγεθος του κλειδιου (key size)
- Ο αριθμος των γυρων (number of rounds)
- Ο αλγοριθμος δημιουργιας των υποκλειδιων (subkey generation algorithm)
- Η συναρτηση του γυρου (round function)
- Η δυνατοτητα για γρηγορη κρυπτογραφηση/αποκρυπτογραφηση μεσω λογισμικου (fast software en/decryption)
- Η ευκολια στην αναλυση

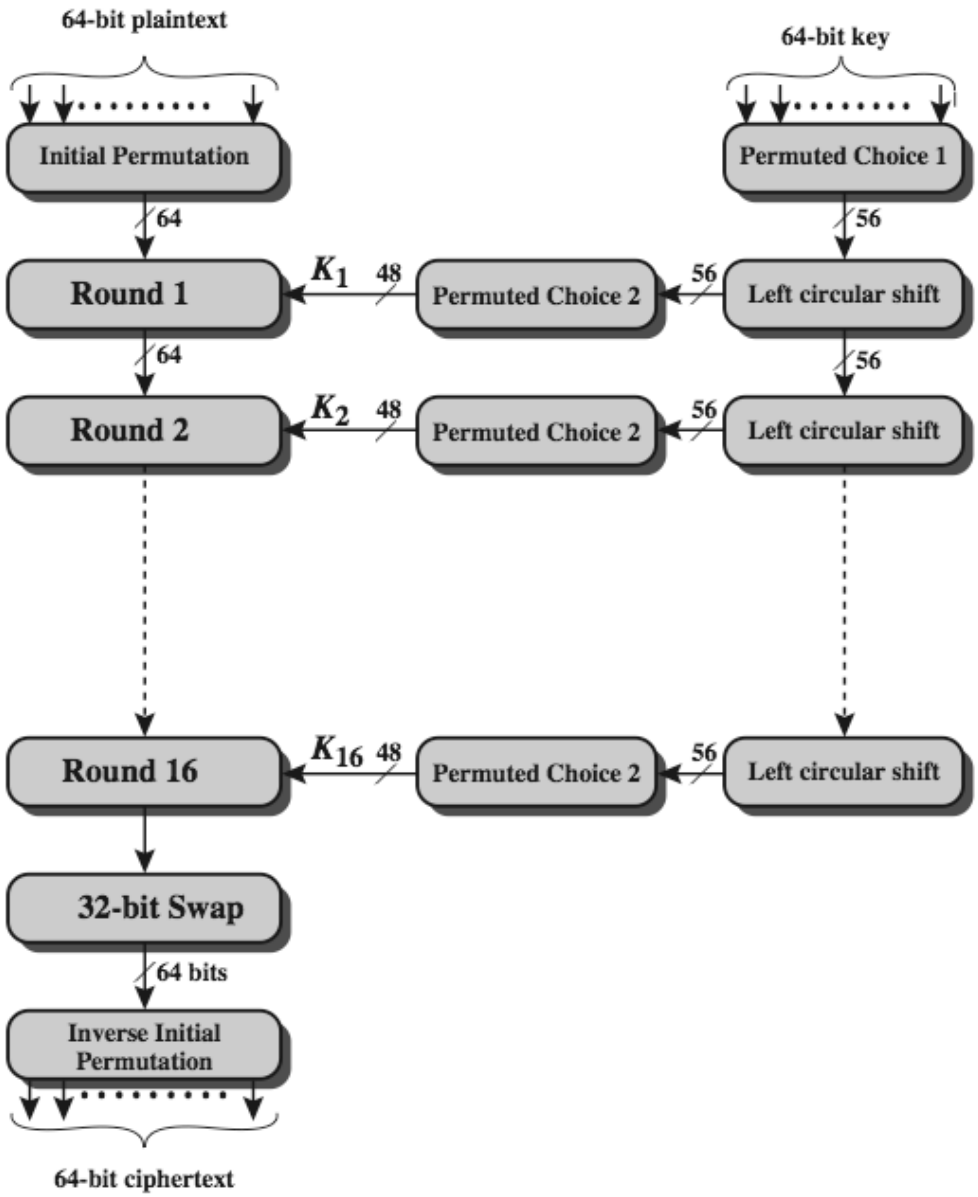
Data Encryption Standard (DES)

- Ο πιο ευρεως διαδεδομενος κρυπτογραφικος αλγοριθμος τμηματων στον κοσμο.
- Κρυπτογραφει δεδομενα των 64-bit χρησιμοποιωντας κλειδι των 56-bits
- Η ασφαλεια του εχει αμφισβητηθει

Αμφισβητηση του σχεδιασμου του DES

- Αν και το DES standard ειναι πασιγνωστο υπαρχει σημαντικη αμφισβητηση για το σχεδιασμο του.
  - Για την επιλογη κλειδιου των 56-bit (εναντι 128-bit αλλων αλγοριθμων)
  - Για το γεγονος οτι τα σχεδιαστικα του κριτηρια ειναι διαβαθμισμενα
- Ωστοσο μεταγενεστερα γεγονοτα και αναλυσεις δειχνουν οτι τελικα ο σχεδιασμος του DES ηταν σωστος

Κρυπτογραφηση DES



Δομη του γυρου DES

- Χρησιμοποιει δυο μισα (Left & Right, L&R) των 32-bits.
- Οποιοσδηποτε Feistel cipher μπορει να περιγραφει ως εξης:

  $L_i = R_{i-1}$

  $R_i = L_{i-1} \oplus \mathrm{F}(R_{i-1}, K_i)$
- Η F παιρνει το δεξι μισο των 32-bits (R) και το υποκλειδι των 48-bits:
  - Επεκτεινεται το R στα 48-bits χρησιμοποιωντας τη μεταθεση E
  - Στη συνεχεια γινεται XOR με το υποκλειδι
  - Οτι προκυπτει περναει μεσα απο 8 S-boxes και προκυπτει αποτελεσμα των 32-bits
  - Τελικα πραγματοποιειται μεταθεση, χρησιμοποιωντας την 32-bit μεταθεση P

Δομη του γύρου DES
(DES Round Structure)

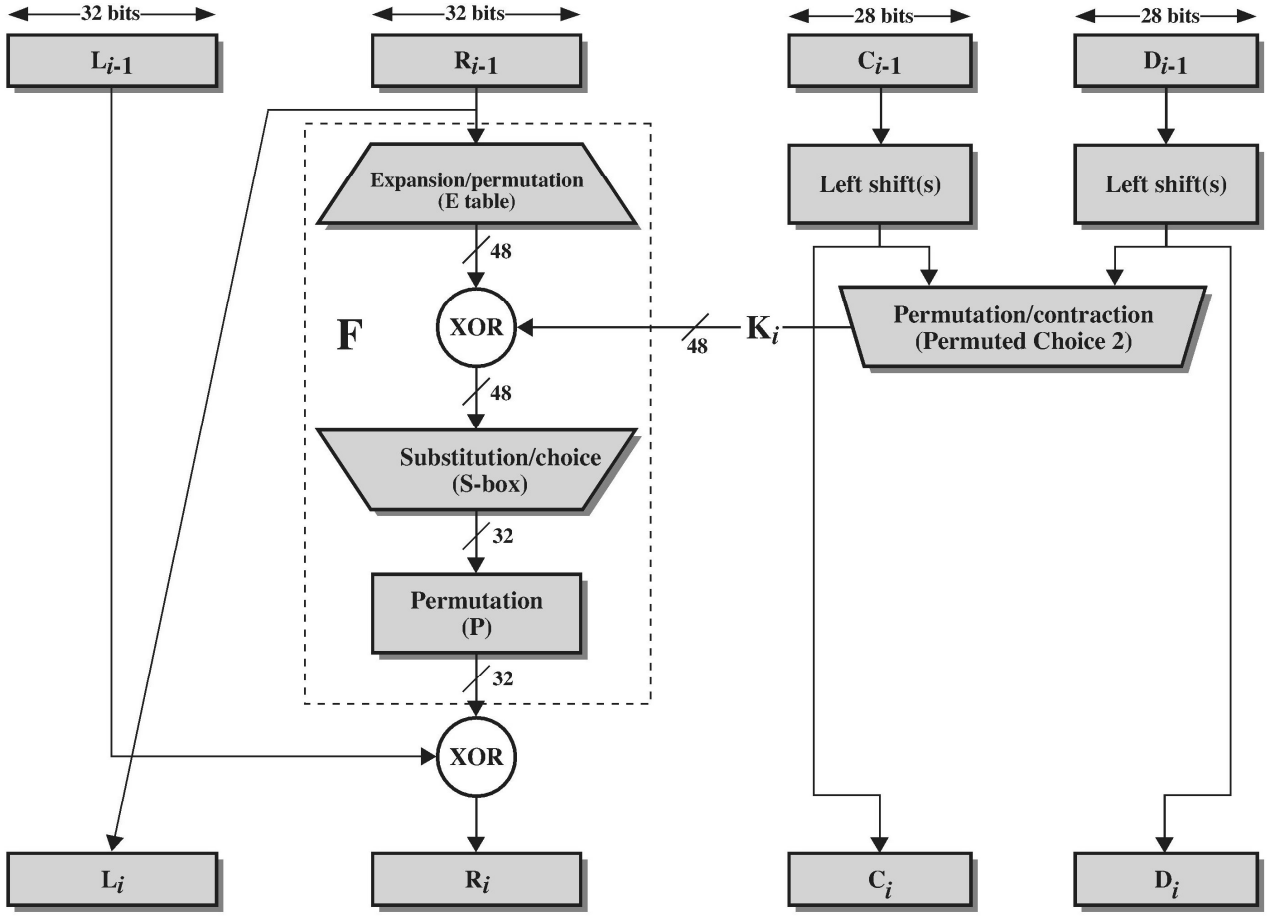
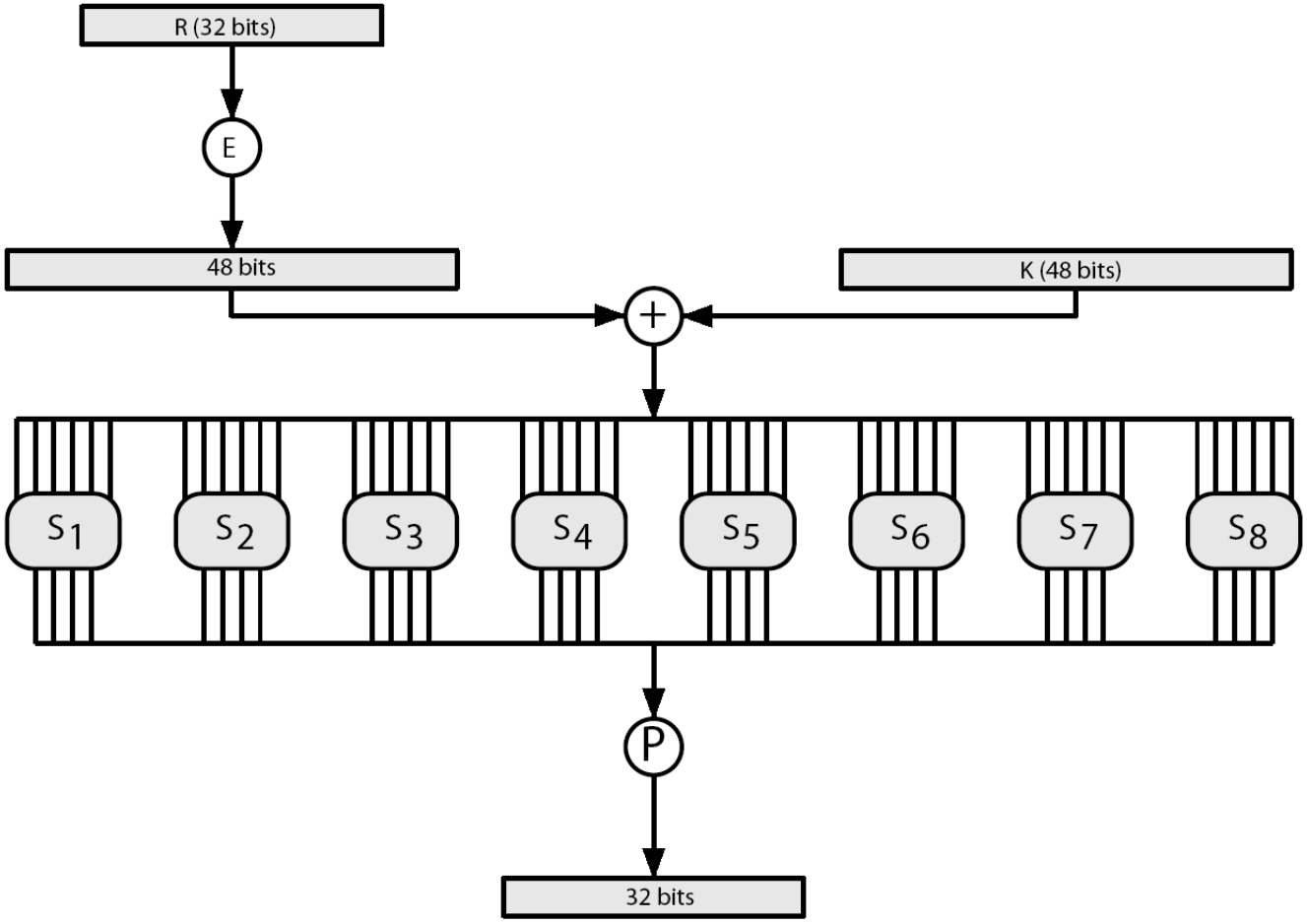


Figure 3.6 Single Round of DES Algorithm

Δομη του γύρου DES
Υπολογισμος του F



Κουτια Αντικαταστασης S (Substitution Boxes S)

- Εχουμε 8 S-boxes που αντιστοιχουν καθε 6αδα bits σε μια 4αδα
- Καθε S-box ειναι στην πραγματικοτητα 4 μικρα boxes των 4 bits.
  - Τα εξωτερικα bits 1 & 6 (**row** bits) επιλεγουν μια γραμμη των 4
  - Τα εσωτερικα bits 2-5 (**col** bits) αντικαθιστανται
  - Το αποτελεσμα ειναι 8 ομαδες των 4 bits, ή 32 bits
- Η επιλογη γραμμης εξαρταται τοσο απο τα δεδομενα, οσο και απο το κλειδι
  - Το χαρακτηριστικο αυτο ονομαζεται autoclaving (autokeying)
- Παραδειγμα:
  - `S(18 09 12 3d 11 17 38 39) = 5fd25e03`

Αποκρυπτογραφηση DES (DES Decryption)

- Ακολουθειται ακριβως η αντιστροφη πορεια με τα βηματα της κρυπτογραφησης χρησιμοποιωντας τα υποκλειδια με αντιστροφη σειρα (SK16 … SK1)
  - Η αρχικη μεταθεση (IP) αναιρει το τελευταιο βημα (FP) της κρυπτογραφησης.
  - Ο πρωτος γυρος με το υποκειδι SK16 αναιρει τον 16^{ο} γυρο της κρυπτογραφησης
  - ….
  - Ο 16ος γυρος με το υποκλειδι SK1 αναιρει τον πρωτο γυρο της κρυπτογραφησης
  - Τελος το τελικο βημα FP αναιρει το αρχικο βημα IP της κρυπτογραφησης
  - Κι ετσι καταληγουμε στα αρχικα δεδομενα.

Ισχυς του DES – Μεγεθος Κλειδιου

- Τα κλειδια των 56-bit εχουν $2^{56} = 7.2 \times 10^{16}$ τιμες
- Δυσκολο να σαρωθουν με επιθεση brute force
- Οι σχετικα προσφατες εξελιξεις ομως, δειχνουν οτι αυτο ειναι δυνατο.
  - Το 1997 με χρηση του Internet σε λιγους μηνες
  - Το 1998 με χρηση ειδικα σχεδιασμενου hardware μεσα σε λιγες μερες.
  - Το 1999 με συνδυασμο των παραπανω μεσα σε 22 ώρες!
- Ωστοσο πρεπει παντα να εχει τη δυνατοτητα ο επιτιθεμενος να αναγνωριζει το plaintext

Ισχυς του DES – Αναλυτικες Επιθεσεις

- Υπαρχουν αρκετες αναλυτικες επιθεσεις για τον DES
- Χρησιμοποιουν τη βαθεια δομη του DES
  - Συγκεντρωνοντας πληροφοριες για τις κρυπτογραφησεις μπορει κανεις να ανακαλυψει ολα τα μερικα η και ολα τα υποκλειδια
  - Αν χρειαζεται, μπορει να ψαξει εξαντλητικα για τα υπολοιπα
- Γενικα αυτες ειναι στατιστικες επιθεσεις.
  - Διαφορική Κρυπταναλυση (differential cryptanalysis)
  - Γραμμικη Κρυπταναλυση (linear cryptanalysis)
  - Επιθεσεις σχετιζομενου κλειδιου (related key attacks)

Ισχυς του DES – Επιθεσεις Χρονισμου

- Επιτιθεται στην υλοποιηση του αλγοριθμου
- Χρησιμοποιει γνωση των συνεπειων της υλοποιησης για να εξαγει πληροφοριες για μερικα ή ολα τα υποκλειδια
- Συγκεκριμενα, χρησιμοποιει το γεγονος οτι οι υπολογισμοι μπορουν να εχουν διαφορετικους χρονους εκτελεσης αναλογα με το σε τι input εκτελουνται

Κρυπτανάλυση στον DES

- Όντας πρότυπο για πολλά χρόνια, ο DES κίνησε το ενδιαφέρον πολλών κρυπταναλυτών για την εύρεση μεθόδων που θα μπορούσαν να τον «σπάσουν»
- Βασικοί αλγόριθμοι κρυπτανάλυσης
  - **Διαφορική κρυπτανάλυση** [differential cryptanalysis – Biham and Shamir (1990)]
  - **Γραμμική κρυπτανάλυση** [linear cryptanalysis – Matsui (1993)]

  Συλλογή στοιχείων με τις δύο αυτές μεθόδους υπάρχουν στη διεύθυνση:

  http://www.tcs.hut.fi/~helger/crypto/link/block/dc.html

- Οι μέθοδοι αυτές εφαρμόζονται σε κάθε νέο αλγόριθμο που προτείνεται, για τον έλεγχο της ασφάλειάς του

Διαφορική Κρυπτανάλυση

- Εξεταζει ζευγη κρυπτογραμματων, των οποιων τα αρχικα μηνυματα διαφερουν σε συγκεκριμενες θέσεις (chosen-plaintext attack)
- Προσομοιωνοντας τον αλγοριθμο, καποια κλειδια είναι πιο πιθανα από καποια άλλα, με δεδομενη την παραπάνω συνθηκη
- Οσο πιο πολλα κρυπτογραφηματα αναλυονται, τοσο πιο πολλα κλειδιά «απορριπτονται» ως λιγοτερο πιθανα
- Οι λεπτομερειες της μεθοδου εινα πολυ συνθετες
- Οι 8 γυροι του DES «σπανε» με γνωστα 2^{14} επιλεγμενα αρχικα μηνυματα (chosen plaintexts). Ολοι οι 16 γύροι του DES ομως χρειαζονται 2^{47} επιλεγμένα αρχικα μηνυματα

Αναφορά: «Differential Cryptanalysis of DES-like cryptosystems», E. Biham, A. Shamir, Crypto 1990

Γραμμική Κρυπτανάλυση

- Αναζητειται γραμμικοτητα στο συστημα
- Εστω οτι γινονται XOR τα bits ενός αρχικου μηνυματος, XOR τα bits του αντιστοιχου κρυπτογραμματος και XOR τα δυο αποτελεσματα. Ιδανικα, η πιθανοτητα αυτου του bit αποτελεσματος να είναι 1 ή 0 θα έπρεπε να είναι ½. Οταν δεν ισχυει, μπορεί να εξαχθει καποια πληροφορια για το κλειδι
- Η παραπάνω πιθανοτητα εξαρταται κυριως από τη γραμμικοτητα των S-boxes
- Οι λεπτομερειες της μεθοδου ειναι επισης συνθετες
- Καλα αποτελεσματα για λιγους γυρους του DES, οχι ομως για το συνολο του (οπου χρειαζονται 2^{43} επιλεγμενα γνωστα αρχικα μηνυματα)

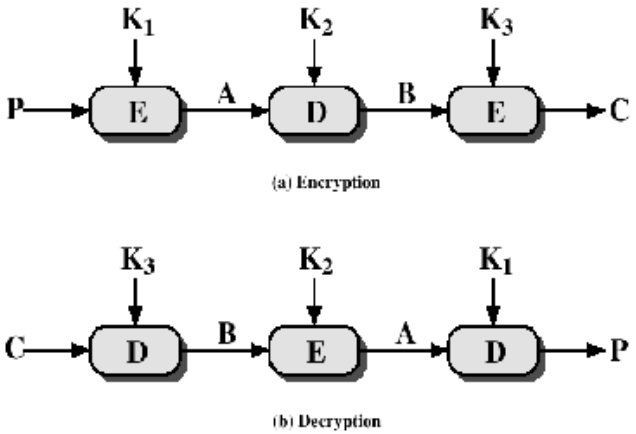
Αναφορα: «Linear Cryptanalysis Method for DES Cipher», Matsui M., *Advances in Cryptology -- EUROCRYPT '93.* 386-397.

Σχεδιαστικα Κριτηρια του DES (DES Design Criteria)

- Οπως αναφερεται απο τον Coppersmith [COPP94]
- 7 κριτηρια για τα S-boxes εξασφαλιζουν
  - Μη γραμμικότητα
  - Αντισταση στη διαφορικη κρυπταναλυση
  - Καλη συγχυση
- 3 κριτηρια για την αντιμεταθεση P εξασφαλιζουν
  - Αυξημενη διαχυση

Triple DES (3DES)

- Παραλλαγή του DES, η οποία παρέχει περισσότερη ασφάλεια
- Ο 3DES χρησιμοποιεί τρία κλειδιά των 56-bit
  - $C=E_{k3}(D_{k2}(E_{k1}(P)))$
  - $P=D_{k1}(E_{k2}(D_{k3}(C)))$
- Σημείωση: αν K1=K2, τότε 3DES=DES



AES- Advanced Encryption Standard

- Το 1997, ο NIST προσκάλεσε δημόσια για ορισμό νέου προτύπου
  - Ως ελάχιστο μήκος κλειδιού τέθηκε 128 bits
  - Δυνατότητα υλοποίησης σε επεξεργαστές 8 bit
- Το 1998, επελέχθησαν 15 επικρατέστεροι
- Αργότερα, έμειναν 5 επικρατέστεροι
    - MARS (IBM - ΗΠΑ)
    - RC6 (RSA Labs - ΗΠΑ)
    - Rijndael (Daemen and Rijmen – Βέλγιο)
    - SERPENT (Anderson, Biham, and Knudsen – Μεγάλη Βρετανία, Ισραήλ, Νορβηγία)
    - TWOFISH (Schneier, Kelsey, και άλλοι - ΗΠΑ)

Advanced Encryption Standard (AES) (II)

- Τελικοί βαθμοί των 5 επικρατέστερων αλγορίθμων:

	MARS	RC6	Rijndael	Serpent	Twofish
General Security	3	2	2	3	3
Implementation of Security	1	1	3	3	2
Software Performance	2	2	3	1	1
Smart Card Performance	1	1	3	3	2
Hardware Performance	1	2	3	3	2
Design Features	2	1	2	1	3

Το 2000, ανακοινωθηκε ως νικητης αλγοριθμος ο Rijndael.

Αλγόριθμος Rijndael

- Μήκη κλειδιού 128, 192, 256 bits
- Μήκη blocks δεδομένων 128, 192, 256 bits
- Εύκολη υλοποίηση hardware

  - 10-15 γύροι, ανάλογα με το μήκος του κλειδιού
  - Κάθε γύρος έχει 4 βήματα:
    - Αντικατάσταση byte (Byte substitution) – χρήση s-boxes με καλά χαρακτηριστικά
    - Ολίσθηση (Shift row)
    - Συνδυασμός πολλών bit (Mix Column)
    - Πρόσθεση (XOR) του κλειδιού

Σύγκριση DES, 3DES, AES

	DES	**3DES**	**AES**
Key Length (bits)	56	112 or 168	128, 192, 256
Strength	Weak	Strong	Strong
Processing Requirements	Moderate	High	Modest
RAM Requirements	Moderate	High	Modest

Άλλοι Block Ciphers

- Blowfish (Schneier) (http://www.schneier.com/blowfish.html)
- CAST (http://adonis.ee.queensu.ca:8000/cast/)
- Int'l Data Encryption Alg (IDEA), Lai and Masey (http://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm)
- Safer (Secure and Fast Encryption Routine) (http://home.ecn.ab.ca/~jsavard/crypto/co040301.htm)
- RC5 (http://www.funet.fi/pub/crypt/cryptography/papers/rc5/)

Συνοψη

- Κρυπτογραφικοι αλγοριθμοι τμηματων εναντι ροης
- Σχεδιασμος και Δομη Feistel cipher
- DES
- Διαφορικη και Γραμμικη Κρυπτανάλυση
- Triple DES
- AES

Αναφορα

Κ.Χαλατσης, «Εισαγωγη στην Κρυπτογραφια», Lecture Notes.