

The image features three padlocks of different colors (two red, one blue) arranged horizontally. The background is a dark blue/black field filled with glowing green and cyan binary code (hexadecimal characters). The padlocks are stylized and appear to be floating or attached to the background. The central padlock is blue, while the two flanking ones are red. The text is overlaid on the left side of the image.

Ασφάλεια

ΛΙΑΓΚΟΥ ΒΑΣΙΛΙΚΗ
ΕΡΓΑΣΤΗΡΙΑΚΕΣ ΣΗΜΕΙΩΣΕΙΣ

Εργαστήριο

A. Block Chiphers

B. openssl

Κρυπτογραφικοί Αλγόριθμοι 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**

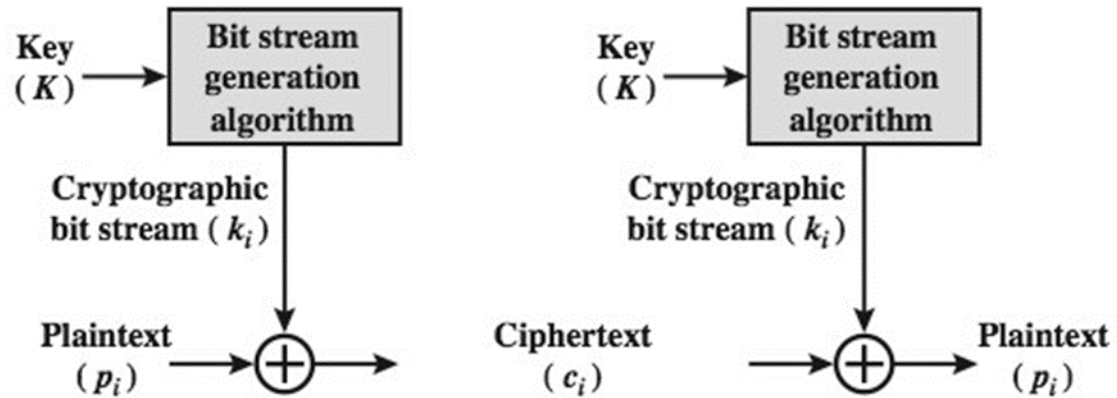
Συγχρονοι αλγοριθμοι Τμηματων

- 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 πιστοποιοησης αυθεντικοτητας
- Θα εστιασουμε στον αλγοριθμο DES (Data Encryption Standard) προκειμενου να μελετησουμε τις σχεδιαστικες αρχες των αλγοριθμων τμηματων.

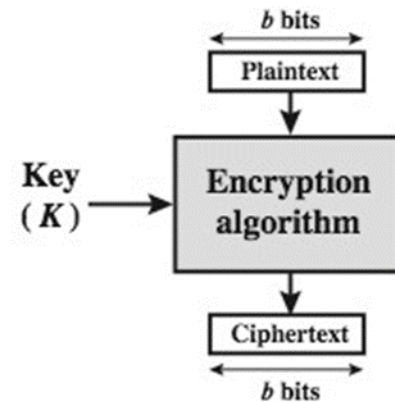
Αλγοριθμοί τμημάτων (Block Ciphers) και Αλγοριθμοί Ροής (Stream Ciphers)

- Οι αλγοριθμοί τμημάτων επεξεργάζονται τα μηνύματα κατά τμήματα το καθένα από τα οποία κρυπτογραφείται ή αποκρυπτογραφείται.
- Οι αλγοριθμοί ροής, όταν κρυπτογραφούν ή αποκρυπτογραφούν επεξεργάζονται ένα μόνο bit ή byte κάθε φορά.
- Πολλοί σύγχρονοι αλγοριθμοί κρυπτογράφησης είναι αλγοριθμοί τμημάτων.
 - Αναλύονται καλύτερα
 - Έχουν ευρύτερο πεδίο εφαρμογών

Block vs Stream Ciphers



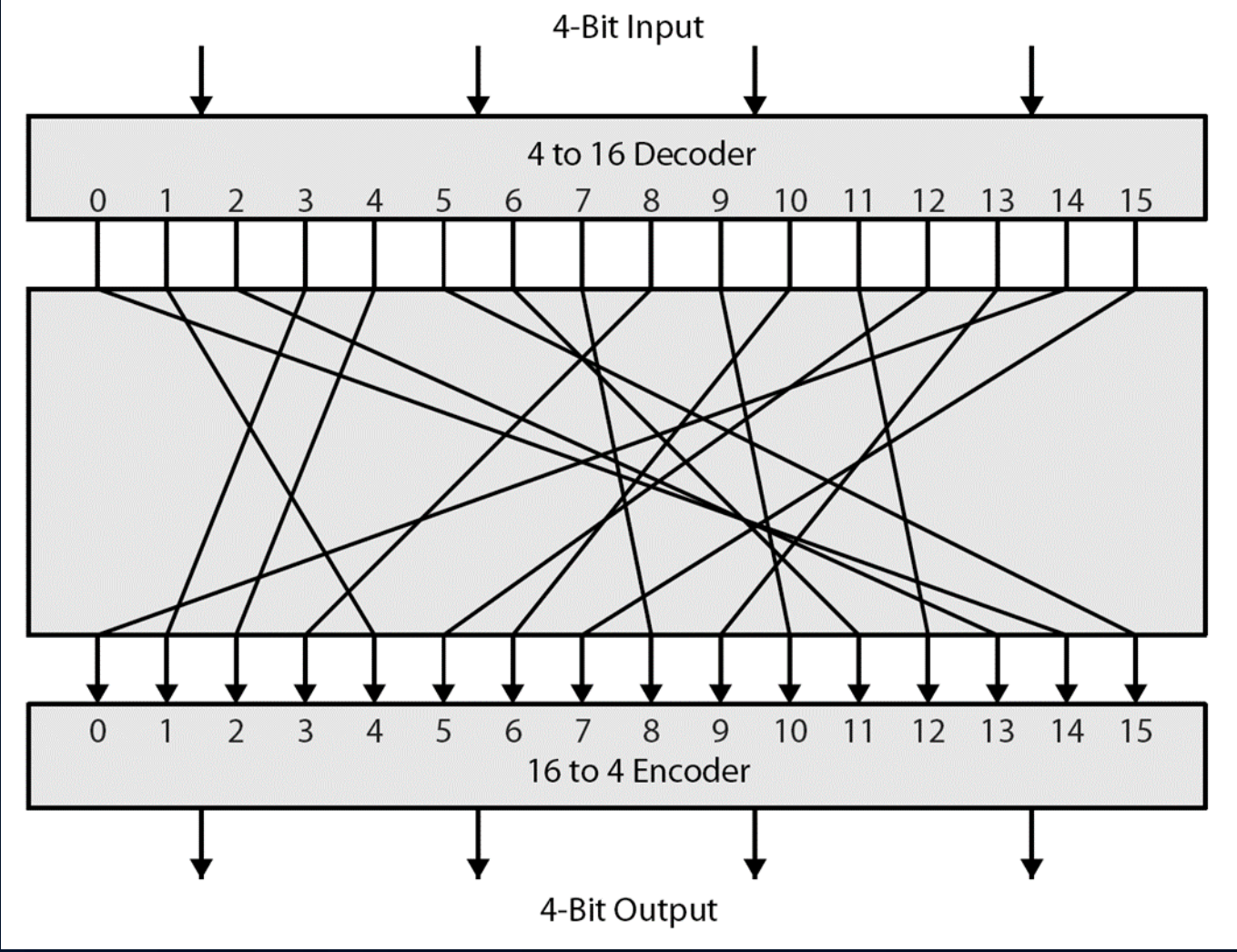
(a) Stream Cipher Using Algorithmic Bit Stream Generator



(b) Block Cipher

Αρχες των Αλγοριθμων Τμηματων

- Οι περισσότεροι 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



Ο Claude Shannon και οι Κρυπτογραφικοί Αλγόριθμοι Αντικατάστασης-Μεταθεσης (Substitution-Permutation Ciphers)

- Ο Shannon εισήγαγε την ιδέα των δικτυων Αντικατάστασης-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.

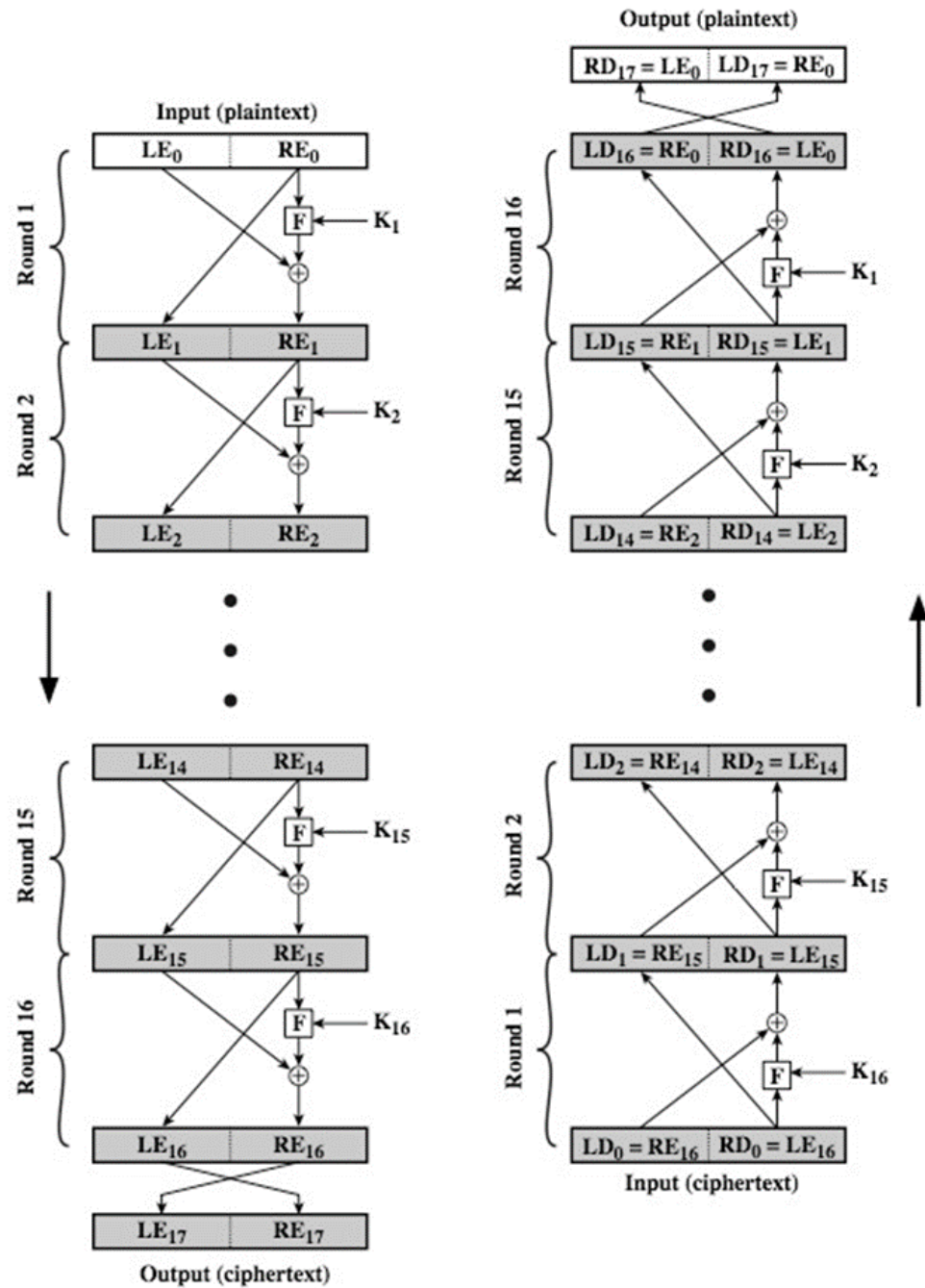
Συγχυση και Διαχυση (Confusion and Diffusion)

- Ο κρυπτογραφικός αλγόριθμος πρέπει να συσκοτίζει 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 Δομή Feistel Cipher

- Ο Horst Feistel επινόησε τον **feistel cipher**
 - Βασίζεται στις ιδέες του Shannon
- Χωρίζει το input block σε δυο ίσα κομμάτια.
 - Τα επεξεργάζεται μέσω πολλαπλών γυρών οι οποίοι
 - Εκτελούν μια αντικατάσταση στο αριστερό μισό των δεδομένων
 - Βασίζεται σε μια συνάρτηση γύρου (round function) του δεξιού μισού και του υποκλειδίου.
 - Στη συνέχεια πραγματοποιεί αντιμετάθεση μεταξύ των δυο μισών
- Εφαρμόζει την ιδέα των S-P nets του Shannon

Δομή Feistel Cipher



Σχεδιαστικά στοιχεία του Feistel Cipher

- Το μέγεθος των τμημάτων (block size)
- Το μέγεθος του κλειδίου (key size)
- Ο αριθμός των γυρών (number of rounds)
- Ο αλγόριθμος δημιουργίας των υποκλειδίων (subkey generation algorithm)
- Η συνάρτηση του γύρου (round function)
- Η δυνατότητα για γρήγορη κρυπτογράφηση/αποκρυπτογράφηση μέσω λογισμικού (fast software en/decryption)
- Η ευκολία στην ανάλυση

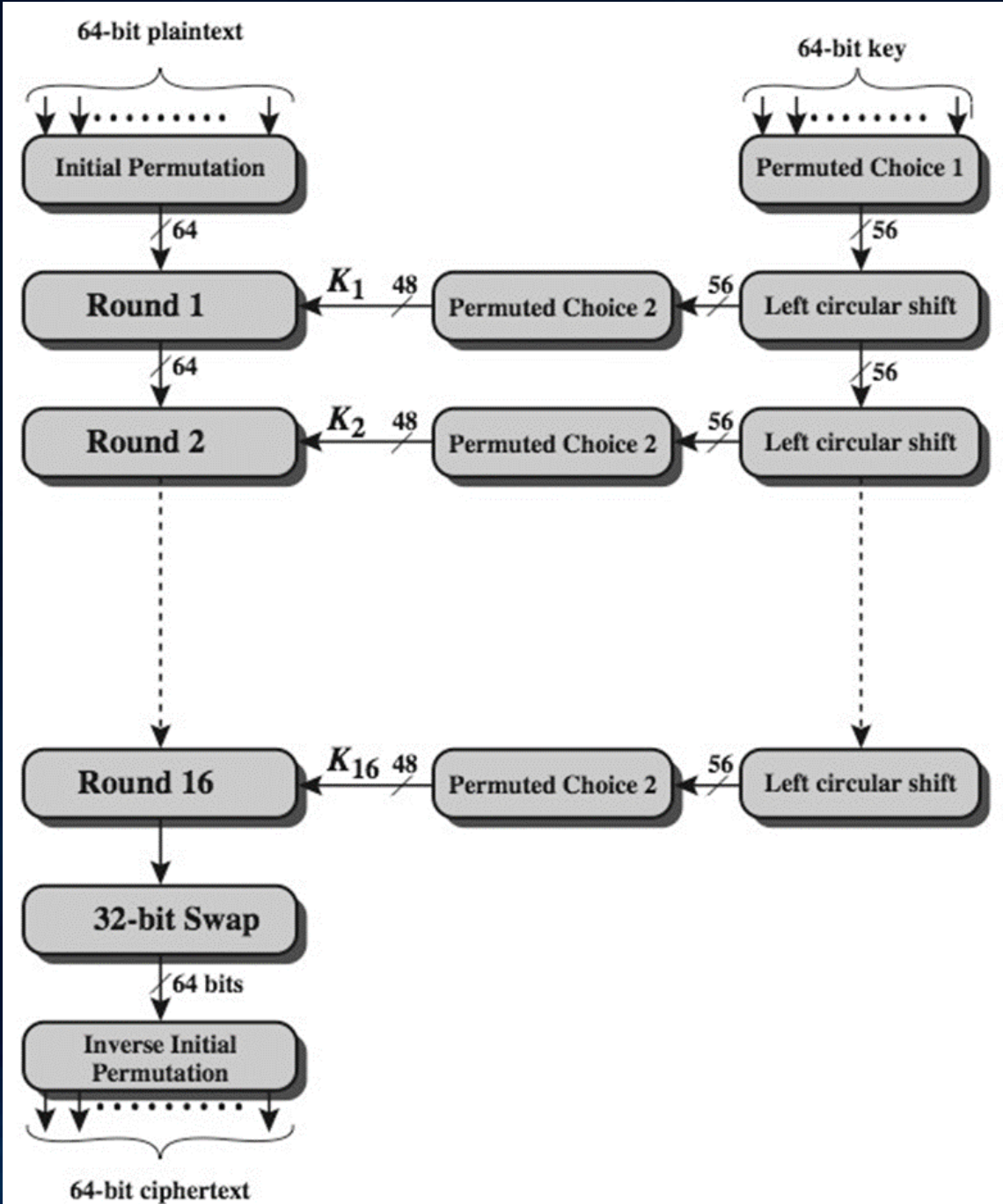
Data Encryption Standard (DES)

- Ο πιο ευρέως διαδεδομένος κρυπτογραφικός αλγόριθμος τμημάτων στον κόσμο.
- Κρυπτογραφεί δεδομένα των 64-bit χρησιμοποιώντας κλειδί των 56-bits
- Η ασφάλεια του έχει αμφισβητηθεί

Αμφισβήτηση του σχεδιασμού του DES

- Αν και το DES standard είναι πασιγνώστο υπάρχει σημαντική αμφισβήτηση για το σχεδιασμό του.
 - Για την επιλογή κλειδίου των 56-bit (εναντι 128-bit άλλων αλγορίθμων)
 - Για το γεγονός ότι τα σχεδιαστικά του κριτήρια είναι διαβαθμισμένα
- Ωστόσο μεταγενέστερα γεγονότα και αναλύσεις δείχνουν ότι τελικά ο σχεδιασμός του DES ήταν σωστός

Κρυπτογραφηση DES



Δομη του γυρου DES

- Χρησιμοποιει δυο μισα (Left & Right, L&R) των 32-bits.
- Οποιοσδηποτε Feistel cipher μπορεί να περιγραφει ως εξης:
$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$
- 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 περναι μεσα απο 8 S-boxes και προκυπτει αποτελεσμα των 32-bits
 - Τελικα πραγματοποιοιεται μεταθεση, χρησιμοποιωντας την 32-bit μεταθεση P

Δομή του γύρου DES (DES Round Structure)

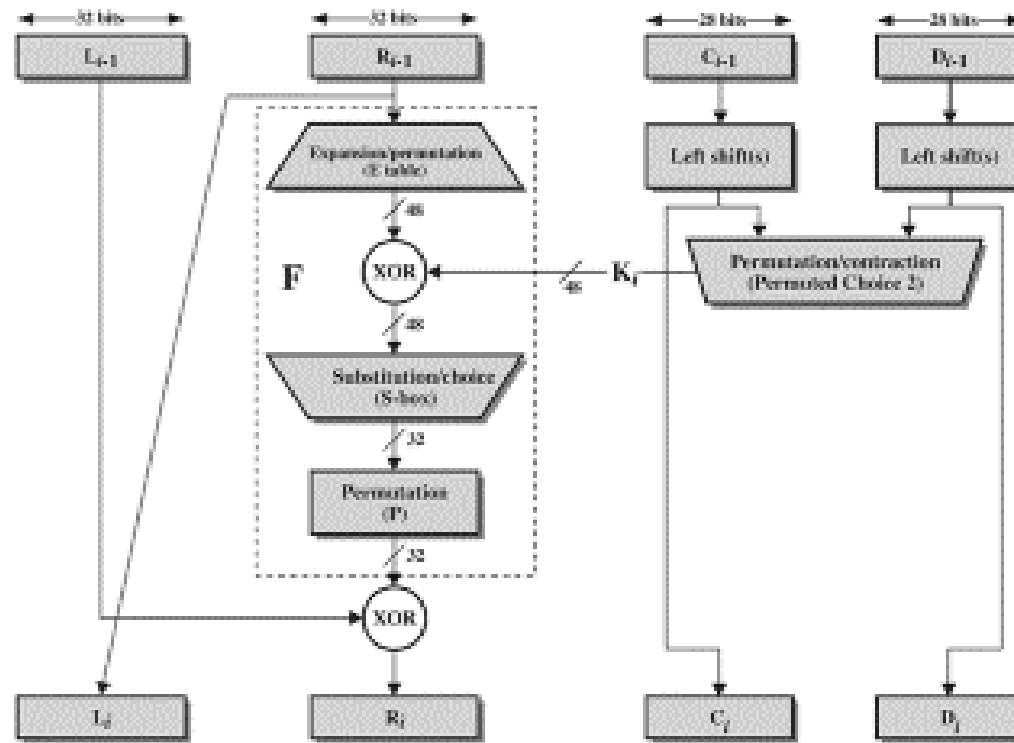
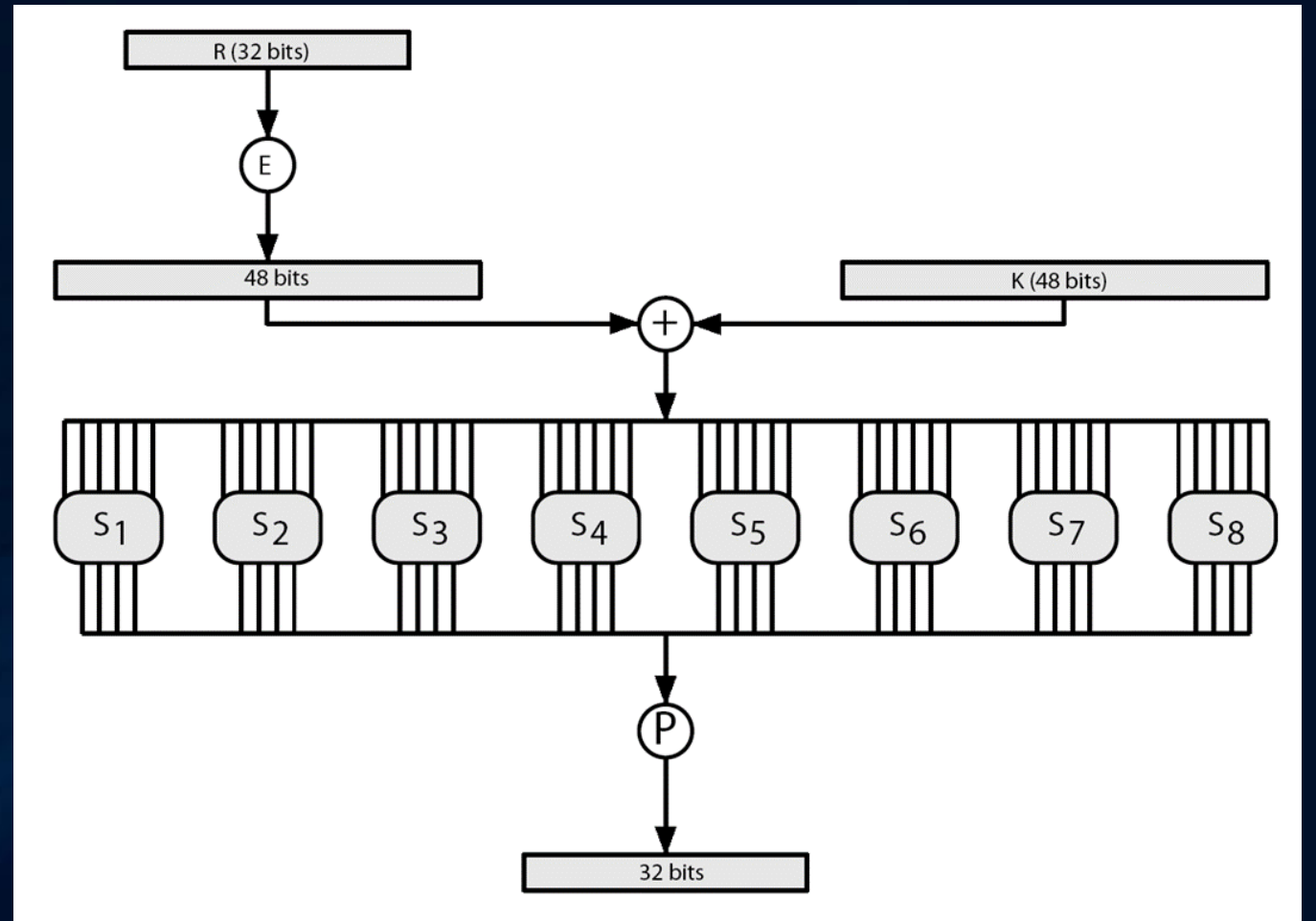


Figure 3.6 Single Round of DES Algorithm

Δομη του γύρου
DES
Υπολογισμος
του F



Κουτια Αντικατάστασης 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:
 - $s(18\ 09\ 12\ 3d\ 11\ 17\ 38\ 39) = 5fd25e03$

Αποκρυπτογράφηση DES (DES Decryption)

- Ακολουθείται ακριβώς η αντιστροφή πορεία με τα βήματα της κρυπτογράφησης χρησιμοποιώντας τα υποκλειδιά με αντιστροφή σειρά (SK16 ... SK1)
 - Η αρχική μεταθεση (IP) αναιρεί το τελευταίο βήμα (FP) της κρυπτογράφησης.
 - Ο πρώτος γυρος με το υποκλειδί SK16 αναιρεί τον 16^ο γυρο της κρυπτογράφησης
 -
 - Ο 16ος γυρος με το υποκλειδί SK1 αναιρεί τον πρώτο γυρο της κρυπτογράφησης
 - Τέλος το τελικό βήμα FP αναιρεί το αρχικό βήμα IP της κρυπτογράφησης
 - Κι έτσι καταλήγουμε στα αρχικά δεδομένα.

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 ωρες!
- Ωστοσο πρεπει παντα να εχει τη δυνατοτητα ο επιτιθεμενος να αναγνωριζει το plaintext

Ισχύς του DES – Αναλυτικές Επιθέσεις

- Υπάρχουν αρκετές αναλυτικές επιθέσεις για τον DES
- Χρησιμοποιούν τη βαθια δομή του DES
 - Συγκεντρώνοντας πληροφορίες για τις κρυπτογραφησεις μπορεί κανείς να ανακαλύψει όλα τα μερικά η και όλα τα υποκλειδιά
 - Αν χρειάζεται, μπορεί να ψάξει εξαντλητικά για τα υπολοιπα
- Γενικά αυτές είναι στατιστικές επιθέσεις.
 - Διαφορική Κρυπταναλυση (differential cryptanalysis)
 - Γραμμική Κρυπταναλυση (linear cryptanalysis)
 - Επιθέσεις σχετιζομενου κλειδιου (related key attacks)

Ισχύς του DES – Επιθεσεις Χρονισμού

- 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

- Εξετάζει ζευγη κρυπτογραμμάτων, των οποίων τα αρχικά μηνύματα διαφέρουν σε συγκεκριμένες θέσεις (chosen-plaintext attack)
- Προσομοιώνοντας τον αλγόριθμο, κάποια κλειδιά είναι πιο πιθανά από κάποια άλλα, με δεδομένη την παραπάνω συνθήκη
- Όσο πιο πολλά κρυπτογραφήματα αναλύονται, τόσο πιο πολλά κλειδιά «απορριπτονται» ως λιγότερο πιθανά
- Οι λεπτομερείς της μεθοδου είναι πολύ σύνθετες
- Οι 8 γύροι του DES «σπανε» με γνωστά 2^{14} επιλεγμένα αρχικά μηνύματα (chosen plaintexts). Όλοι οι 16 γύροι του DES όμως χρειάζονται 2^{47} επιλεγμένα αρχικά μηνύματα

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

Γραμμική Κρυπτανάλυση

- Αναζητείται γραμμικότητα στο σύστημα
- Εστω ότι γίνονται XOR τα bits ενός αρχικού 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 $\frac{1}{2}$. Όταν 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)

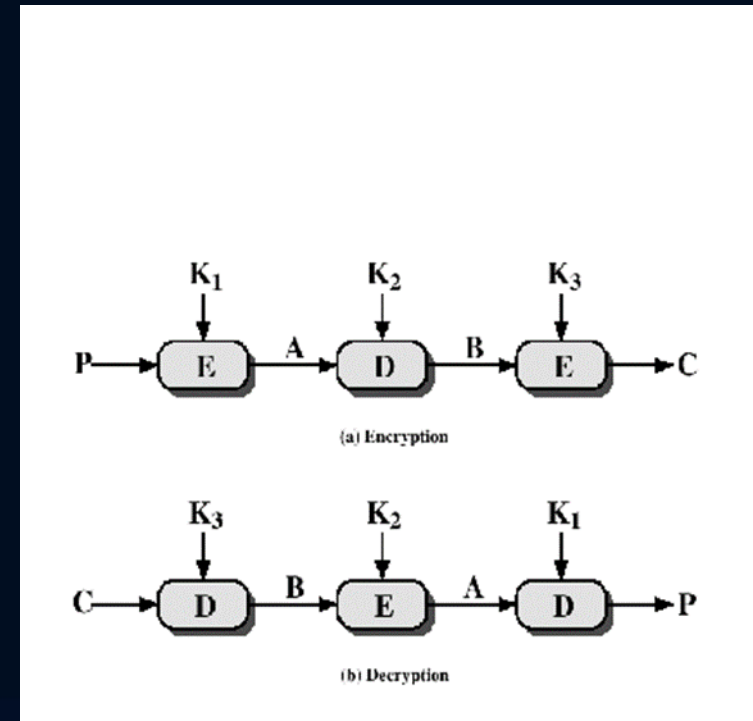
Αναφορα: «Linear Cryptanalysis Method for DES Cipher», Matsui M., *Advances in Cryptology -- EUROCRYPT '93*. 386-397.

Σχεδιαστικά Κριτηρια του DES (DES Design Criteria)

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

Triple DES (3DES)

- Παραλλαγή του DES, η οποία παρέχει περισσότερη ασφάλεια
- Ο 3DES χρησιμοποιεί τρία κλειδιά των 56-bit
 - $C = E_{k_3}(D_{k_2}(E_{k_1}(P)))$
 - $P = D_{k_1}(E_{k_2}(D_{k_3}(C)))$
- Σημείωση: αν $K_1 = K_2$, 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, ανακοινώθηκε ως νικητής αλγορίθμος 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/>)

OpenSSL

- Το OpenSSL είναι μια βιβλιοθήκη κρυπτογράφησης για την υλοποίηση των πρωτοκόλλων
- SSL (Secure Sockets Layer) και TLS (Transport Layer Security). Το πρόγραμμα openssl
- χρησιμοποιεί συναρτήσεις της βιβλιοθήκης OpenSSL για τη δημιουργία κλειδιών τόσο
- συμμετρικής όσο και ασύμμετρης κρυπτογράφησης, για την υλοποίηση διαδικασιών
- κρυπτογράφησης και αποκρυπτογράφησης καθώς και για τις διαδικασίες υπογραφής και
- επαλήθευσης.

- Γενική μορφή σύνταξης:
- `openssl command <command_options> <command_args>`

cat > <αρχείο>

- Η εντολή cat σε συνδυασμό με την ανακατεύθυνση εξόδου (>) δημιουργεί νέα αρχεία
 - Το αρχείο δημιουργείται στον κατάλογο που ορίζει το όνομα διαδρομής <αρχείο>, στο τέλος του οποίου τοποθετούμε το όνομα του νέου αρχείου
 - Όταν εκτελέσουμε την παραπάνω εντολή, ο υπολογιστής αναμένει να εισάγουμε περιεχόμενα στο αρχείο
 - Για να ολοκληρώσουμε την εισαγωγή, αφήνουμε μία κενή γραμμή και πληκτρολογούμε ctrl+d
 - Αν τυχόν το αρχείο προϋπάρχει, τότε καταστρέφεται και τη θέση του παίρνει το καινούριο
- **Στον παραπάνω φάκελο δημιουργείστε το αρχείο lab1.txt στο οποίο θα γράψετε**
- **μέσα το όνομα, το επίθετο και το ID σας (π.χ. Pavlos Antoniou 817651).**
- **Αποθηκεύστε και κλείστε το αρχείο.**

Κρυπτογράφηση DES

- Στο terminal πληκτρολογήστε την εντολή:
- `openssl des -e -in lab1.txt -out testDES.txt`
- Θα σας ζητηθεί συνθηματικό και επιβεβαίωσή του (επιλέγετε κατά βούληση).
- Η παραπάνω εντολή χρησιμοποιεί το συμμετρικό αλγόριθμο κρυπτογράφησης DES (des) προκειμένου να κρυπτογραφήσει (-e) το αρχείο που δηλώνετε ως είσοδος (-in lab1.txt) και να παράγει έξοδο το αρχείο testDES.txt (-out testDES.txt).

- Ανοίξτε το αρχείο testDES.txt με ένα editor
- Για την αποκρυπτογράφηση (-d) του testDES1.txt στο testDES1Dec.txt
- πληκτρολογήστε την εντολή:
- `openssl des -d -in testDES.txt -out testDES1Dec.txt`
- Το αρχείο testDES1Dec.txt θα πρέπει να περιέχει ότι και το αρχείο lab1.txt.

- Δοκιμάστε τις εντολές:
- `openssl des -e -a -in lab1.txt -out testDESb.txt` και
- `openssl des -d -a -in testDESb.txt -out testDESbDec.txt`
- και συγκρίνετε τα αρχεία `testDES.txt` και `testDESb.txt`.
- Το αρχείο `testDESbDec.txt` θα πρέπει να περιέχει ότι και το αρχείο `lab1.txt`.
- Η επιλογή της παραμέτρου `-a` μαζί με το `-e` επιτρέπει την κωδικοποίηση του περιεχομένου του
- `lab1.txt` σε `base64 encoding` (χρησιμοποιείται για κωδικοποίηση δυαδικών αρχείων – binary files – που πρέπει να σταλούν πάνω από μέσα τα οποία είναι σχεδιασμένα να επεξεργάζονται αρχεία κειμένου – `textual data` – βλέπε μεταφορά εικόνων σαν attachments μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου).

Το κλειδί

- Ενώ βρίσκεστε στον οικείο κατάλόγο σας, δημιουργήστε ένα αρχείο που περιέχει ψευδοτυχαίο αριθμό 56 bytes long. Αργότερα, θα χρησιμοποιήσετε αυτόν τον αριθμό ως το κλειδί DES. Σε μια ανοιχτή κονσόλα παράθυρο, πληκτρολογήστε:
- `openssl rand -out des_keyXX 56`
- `cat des_keyXX`

Κρυπτογράφηση με αρχείο

- `openssl des -e -a -kfile des_keyXX -in lab1.txt -out rfc3766XX.enc`
- Δείτε το κρυπτογραφημένο αρχείο
- `cat rfc3766XX.enc`
- Ή με editor

- Τώρα για να εξασφαλίσετε ότι η διαδικασία λειτουργεί με δύο τρόπους, θα πρέπει να αποκρυπτογραφήσετε το .enc αρχείο που μόλις δημιουργήσατε.
- Αφού αποκρυπτογραφήσετε το αρχείο, δείτε αν είναι το αρχικό
- `openssl des -d -a -kfile des_keyXX -in rfc3766XX.enc -out rfc3766XX.dec`
- `cat rfc3766XX.dec`

- Αναμένετε ότι το αρχείο rfc3766XX.dec θα είναι ίδιο με το αρχείο που κατεβάσατε rfc3766XX.txt.
- Δεδομένου ότι τα πανομοιότυπα αρχεία θα έχουν ταυτόσημα μηνύματα, μπορείτε να αποδείξετε ότι τα αρχεία είναι πανομοιότυπα, δημιουργώντας και συγκρίνοντας τα αρχεία κάθε αρχείου.
- Εισάγετε το ακολουθώντας τις γραμμές εντολών. Στη συνέχεια, συγκρίνετε τα παραγόμενα (hashes).

- openssl md5 rfc3766XX.txt
- openssl md5 rfc3766XX.dec