Encryption

Conventional Encryption Message Confidentiality

Ola Flygt
Linnaeus University, Sweden
http://homepage.lnu.se/staff/oflmsi/
Ola.Flygt@lnu.se
+46 470 70 86 49

Outline

- Conventional Encryption Principles
- Conventional Encryption Algorithms
- Cipher Block Modes of Operation
- Location of Encryption Devices
- Key Distribution

Conventional Encryption Principles

- An encryption scheme has five ingredients:
  - Plaintext
  - Encryption algorithm
  - Secret Key
  - Ciphertext
  - Decryption algorithm

Conventional Encryption Principles

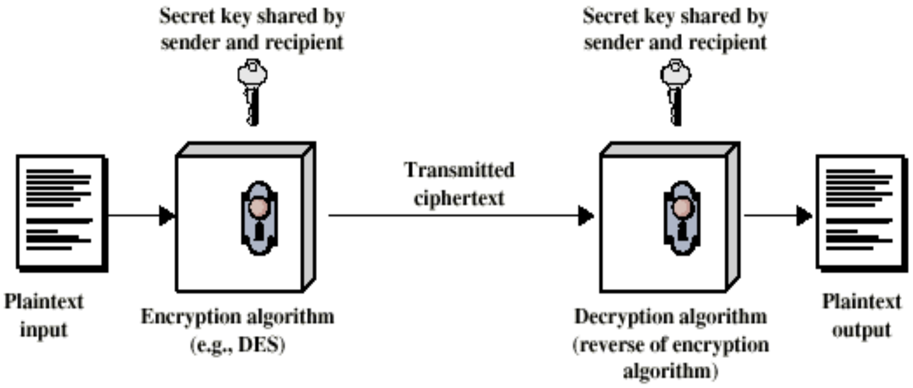


Figure 2.1 Simplified Model of Conventional Encryption

Requirements for Security

- Strong encryption algorithm
  - Even if known, should not be able to decrypt or work out key
  - Even if a number of cipher texts are available together with plain texts of them
- Sender and receiver must obtain secret key securely
- Once key is known, all communication using this key is readable

Cryptography

- Classified along three independent dimensions:
  - The type of operations used for transforming plaintext to ciphertext
  - The number of keys used
    - symmetric (single key)
    - asymmetric (two-keys, or public-key encryption)
  - The way in which the plaintext is processed

Average time required for exhaustive key search

Key Size (bits)	Number of Alternative Keys	Time required at 10^6 Decryption/µs
32	$2^{32} = 4.3 \times 10^9$	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	10 hours
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{30} years

Classical Encryption Techniques

- Substitution Techniques : plaintext are replaced by other letters or by numbers or symbols
  - Caesar Cipher
  - Monoalphabetic Cipher
  - Playfair Cipher
  - Polyalphabetic Cipher
- Transposition Techniques : some sort of permutation on the plaintext letters

Caesar Cipher

- Replacing each other letter of the alphabet with the letter standing three places further down
  - plain : meet me after the toga party
  - cipher : PHHW PH DIWHU WKH WRJD SDUWB
- Note that the alphabet is wrapped around, so that the letter following Z is A.
  - plain : abcdefghijklmnopqrstuvwxyz
  - cipher : DEFGHIJKLMNOPQRSTUVWXYZABC
- If we assign a numerical equivalent to each letter(a=1, b=2 etc)
  - $C = E(p) = (p+3) \bmod (26)$
  - $P = D(c) = (c-3) \bmod (26)$

Crypto analysis of the Caesar Cipher

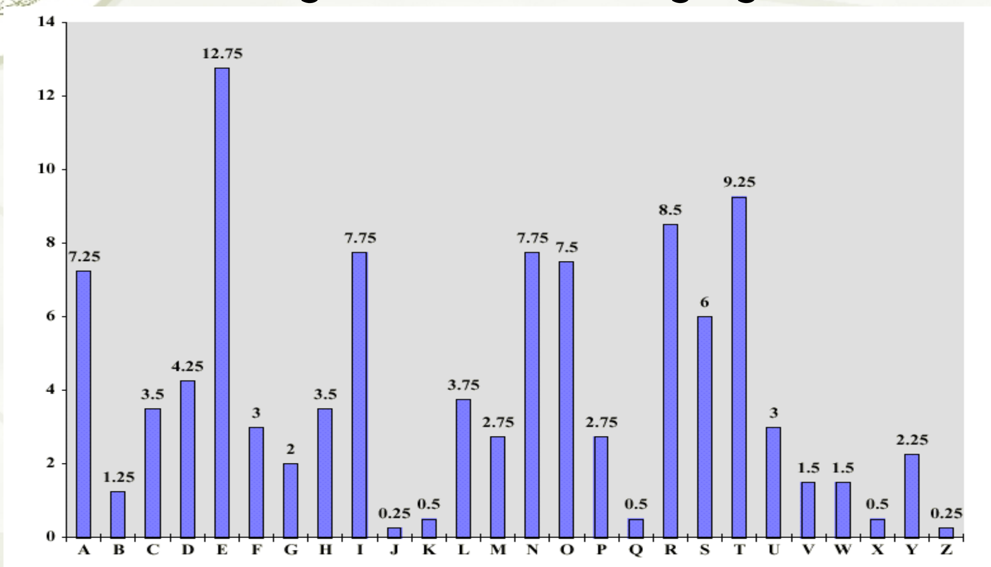
- brute-force cryptanalysis
  - Simply try all the 25 possible keys.
- Three important characteristic of this problem:
  1. The encryption/decryption algorithm are known
  2. There are only 25 keys to try
  3. The language of the plaintext is known and easily recognized

Monoalphabetic Cipher

- Cipher line can be any permutation of the 26 alphabetic characters
  - 26! Or greater than $4*10^{26}$ possible keys
  - If an enemy agent could check one of these possible keys every second, it would take roughly one billion times the lifetime of the universe to check all of them and find the correct one. This simple brute force approach clearly will not work.

Crypto analysis of the Monoalphabetic Cipher

- Attack : regularities of the language



Polyalphabetic Cipher

- Instead of having one key (table) that is used to encrypt each block of plaintext, we use several different keys.
- The Vigenère cipher is the classical example.

One time pad

- Messages
  - n-bit strings $[b_1,\ldots,b_n]$
- Keys
  - Random n-bit strings $[k_1,\ldots,k_n]$
- Encryption/Decryption
  - $c = E(b, k) = b \oplus k = [b_1 \oplus k_1, \ldots, b_n \oplus k_n]$
    - $\oplus$ denotes exclusive or
  - $b = D(b, k) = c \oplus k = b \oplus k \oplus k = b \oplus [1, \ldots, 1] = b$

One time pad (cont.)

- Properties
  - Provably unbreakable if used properly
  - Keys must be truly random
  - ***Must not*** be used more than once
  - Key same size as message

Transposition ciphers

- An alternative to substitution ciphers
- Instead of changing the coding of the characters (blocks) in the plaintext, we rearrange the text.
- The effect is that the cipher text and the plaintext contains the same symbols.

Simple permutation

- Algorithm
  - Divide to plaintext into blocks
  - Decide on a permutation order
  - Rearrange the blocks according to this
- Example:
  - Plaintext: We a|re t|he b|est!
  - Key: 1 4 2 3
  - Cipher text: Wae |rte |hbe |e!st

Transposition ciphers

- A more complex transposition cipher is to write the message in a rectangle, row by row, and read the message off, column by column but permute the order of the columns
  - Key: 4 3 1 2 5 6 7
    Input : t h e e x a m
    p l e j u s t
    g i v e n s u
    g g e s t s t
    h a t m u l t
  - Ciphertext EEVETEJESMHLIGATPGGHXUNTUASSSLMTUTT

Problems with classical ciphers

- Neither substitution nor transposition ciphers are secure enough today.
- They also often have problems with complex keys that are hard to remember.
- Solution?

Product ciphers

- Combine both methods!
- Simple ciphers can be implemented in hardware
  - S-box = substitution cipher
  - P-box = transposition cipher

Feistel Cipher Structure

- Virtually all conventional block encryption algorithms, including DES have a structure first described by Horst Feistel of IBM in 1973
- The realization of a Feistel Network depends on the choice of the following parameters and design features (see next slide):

Feistel Cipher Structure

- **Block size:** larger block sizes mean greater security
- **Key Size:** larger key size means greater security
- **Number of rounds:** multiple rounds offer increasing security
- **Subkey generation algorithm:** greater complexity will lead to greater difficulty of cryptanalysis.
- **Fast software encryption/decryption:** the speed of execution of the algorithm becomes a concern

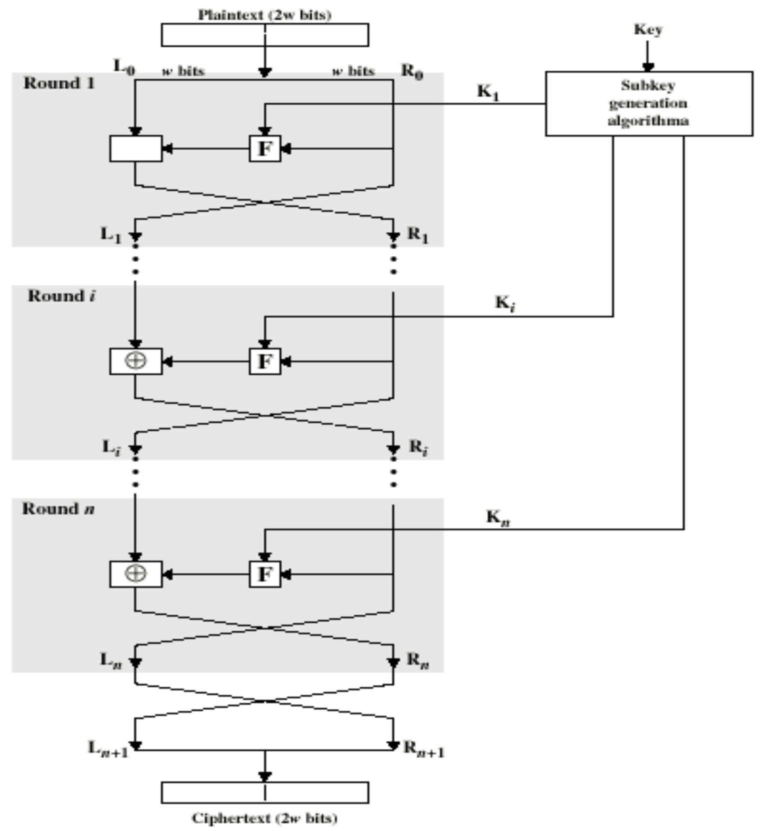
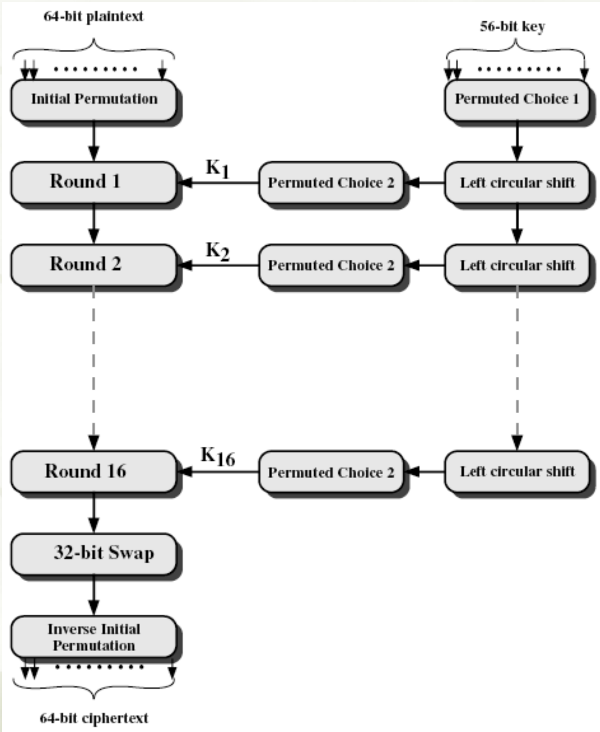


Figure 2.2 Classical Feistel Network

Conventional Encryption Algorithms

- Data Encryption Standard (DES)
  - Was for a long time the most widely used encryption scheme
  - The algorithm is referred to the Data Encryption Algorithm (DEA)
  - DES is a block cipher
  - The plaintext is processed in 64-bit blocks
  - The key is 56-bits in length

General description of DES



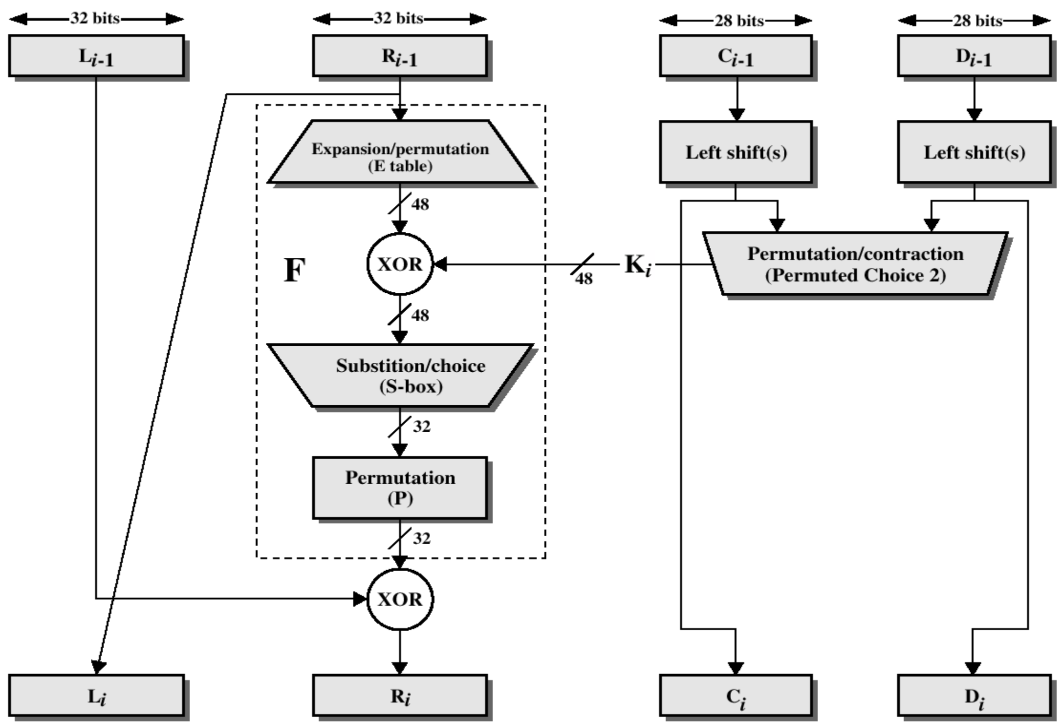
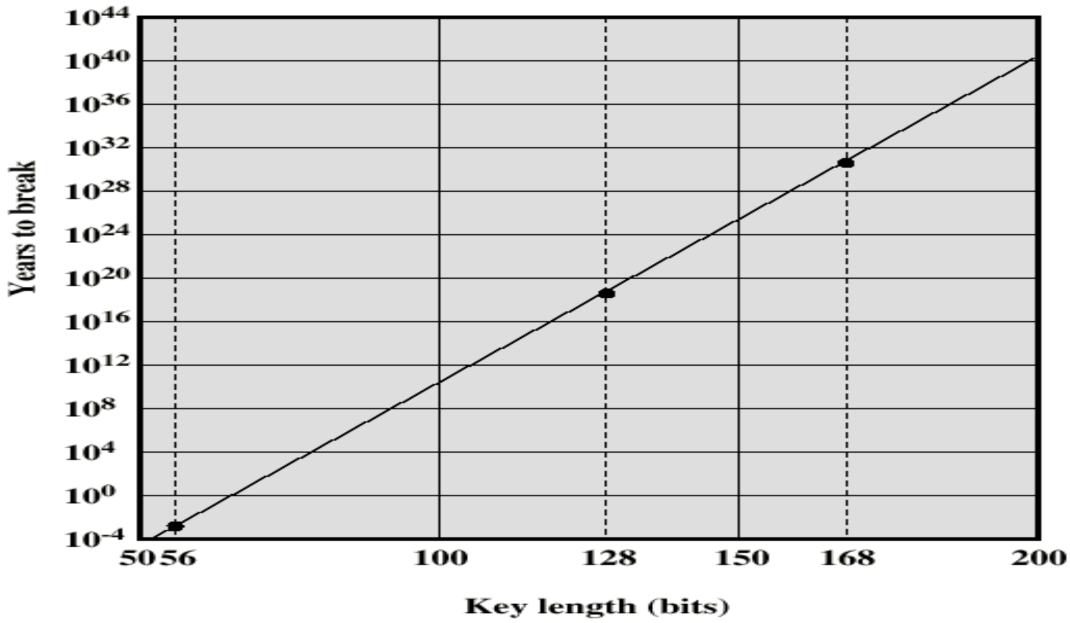


Figure 2.4 Single Round of DES Algorithm

DES

- **The overall processing at each iteration:**
  - $L_i = R_{i-1}$
  - $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$
- Concerns about DES:
  - The algorithm itself
  - The key length (56-bits)

Time to break a code
(10^6 decryptions/μs)



Problem with DES

- Broken in 1998 by Electronic Frontier Foundation
  - Used special purpose machine - $250,000
  - Took less than three days
  - Today it takes much shorter time than that
  - Still, DES is NOT worthless!!!!

Triple DEA

- Use three keys and three executions of the DES algorithm (encrypt-decrypt-encrypt)

$$C = E_{K3}[D_{K2}[E_{K1}[P]]]$$

  - C = ciphertext
  - P = Plaintext
  - EK[X] = encryption of X using key K
  - DK[Y] = decryption of Y using key K
- Effective key length of 168 bits

Triple DEA

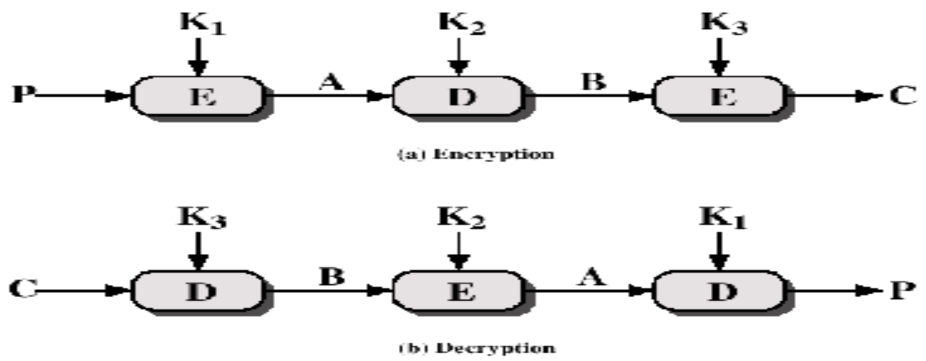


Figure 2.6 Triple DEA

Other Symmetric Block Ciphers

- **International Data Encryption Algorithm (IDEA)**
  - 128-bit key
  - Used in PGP
- **Blowfish**
  - Easy to implement
  - High execution speed
  - Run in less than 5K of memory

Other Symmetric Block Ciphers

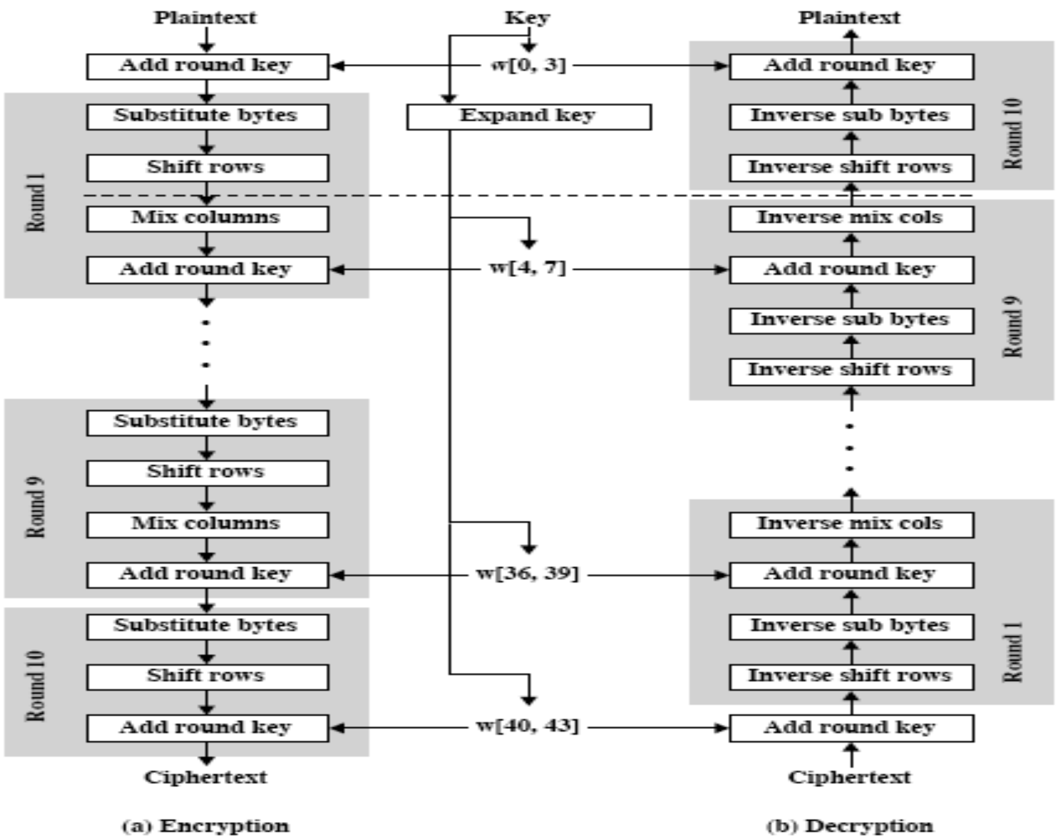
- **RC5 (Rivest Cipher)**
  - Suitable for hardware and software
  - Fast, simple
  - Adaptable to processors of different word lengths
  - Variable number of rounds (0 to 255)
  - Variable-length key (0 to 2040 bits)
  - Low memory requirement
  - High security
  - Data-dependent rotations
- **Cast-128**
  - Key size from 40 to 128 bits
  - The round function differs from round to round

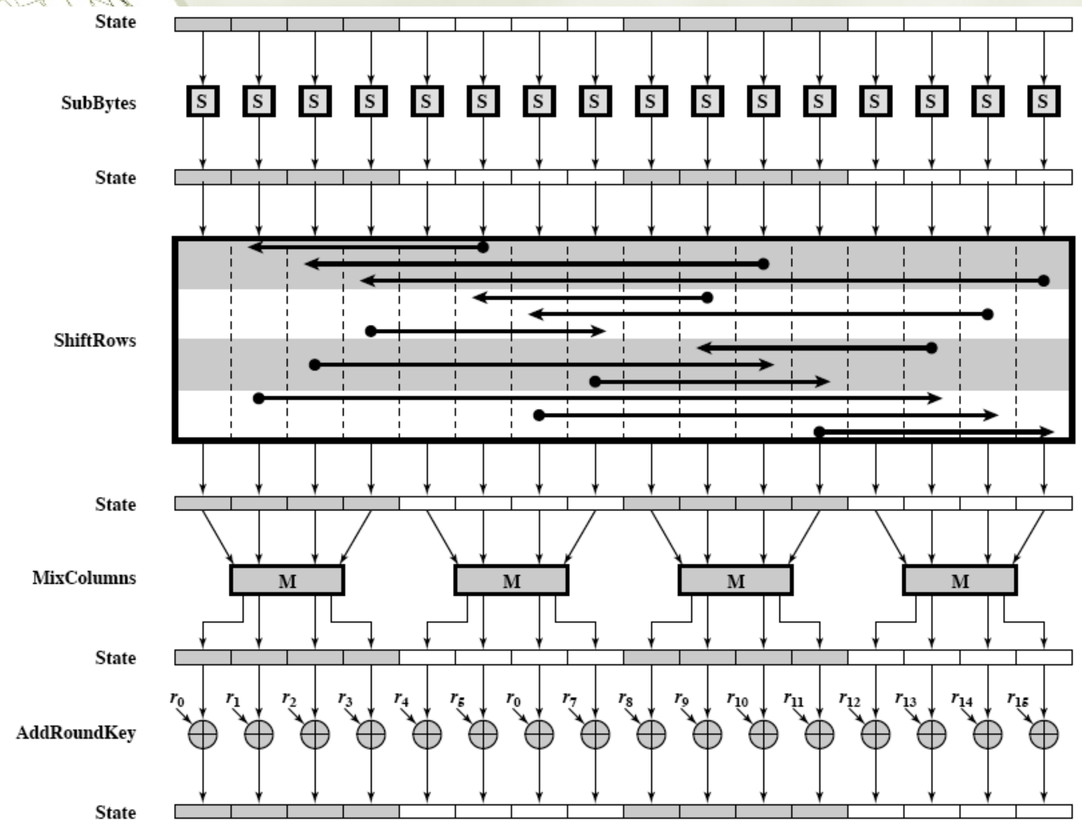
Advanced Encryption Standard (AES)

- National Institute of Standards and Technology (NIST) in 1997 issued call for Advanced Encryption Standard (AES)
  - Security strength equal to or better than 3DES
  - Improved efficiency
  - Symmetric block cipher
  - Block length 128 bits
  - Key lengths 128, 192, and 256 bits

AES

- Evaluation included security, computational efficiency, memory requirements, hardware and software suitability, and flexibility
- The selected cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, and submitted to the AES selection process under the name "Rijndael"
- 2001, AES issued as federal information processing standard (FIPS 197)





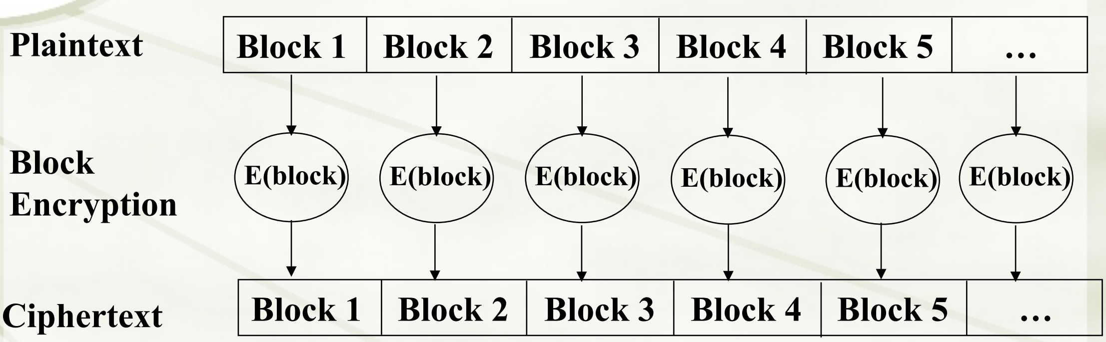
Comparison table

Algorithm	Key Size (bits)	Block Size (bits)	Number of Rounds	Applications
DES	56	64	16	SET, Kerberos
Triple DES	112 or 168	64	48	Financial key management, PGP, S/MIME
AES	128, 192, or 256	128	10, 12, or 14	Intended to replace DES and 3DES
IDEA	128	64	8	PGP
Blowfish	variable to 448	64	16	Various software packages
RC5	variable to 2048	64	variable to 255	Various software packages

Cipher Block Modes of Operation

- Electronic Code Book (ECB) Mode
- Cipher Block Chaining (CBC) Mode
- Cipher Feedback (CFB) Mode

Electronic Code Book (ECB) Mode

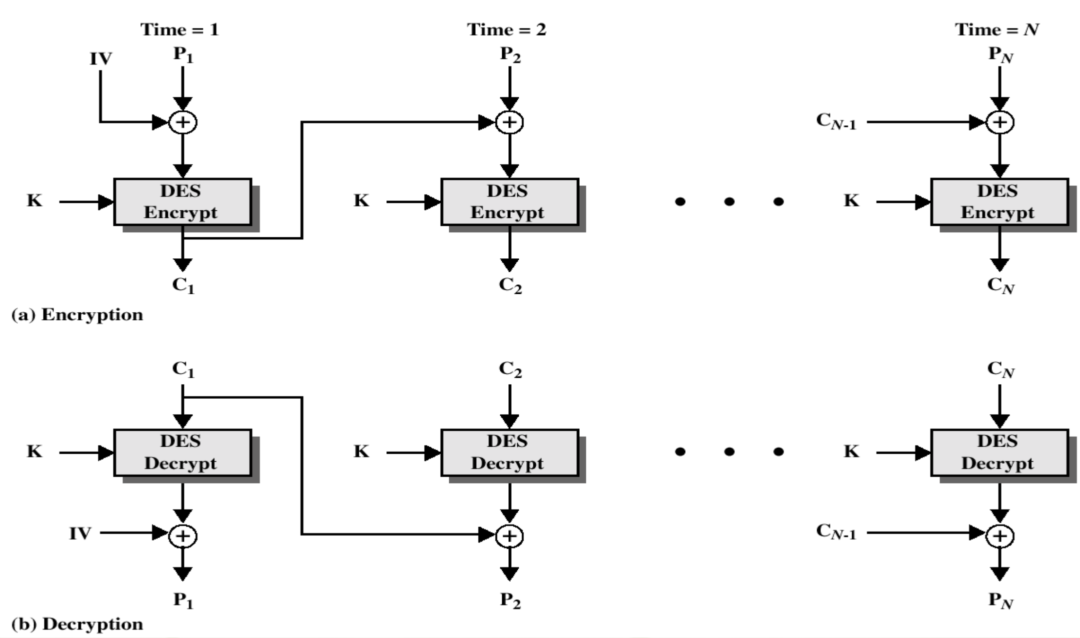


- **Pad last block, if necessary**

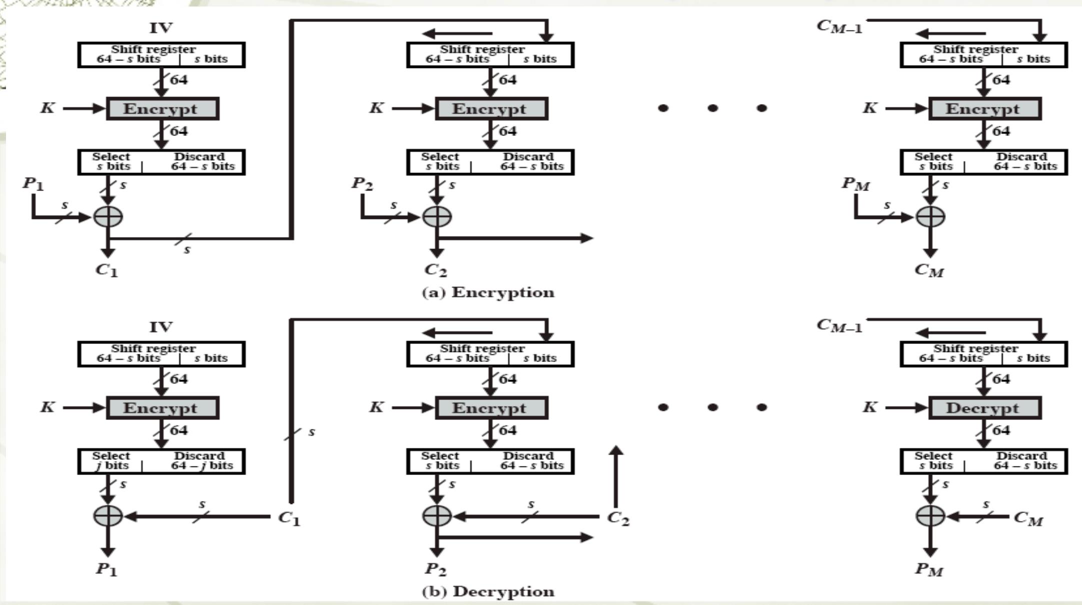
Cipher Block Chaining (CBC) Mode

- The input to the encryption algorithm is the XOR of the current plaintext block and the preceding cipher text block.
- Repeating pattern of 64-bits are not exposed

Cipher Block Chaining Mode



Cipher Feedback (CFB) Mode



Location of Encryption Device

- **Link encryption:**
  - A lot of encryption devices
  - High level of security
  - Decrypt each packet at every switch
- **End-to-end encryption**
  - The source encrypt and the receiver decrypts
  - Payload encrypted
  - Header in the clear
- **High Security:** Both link and end-to-end encryption are needed

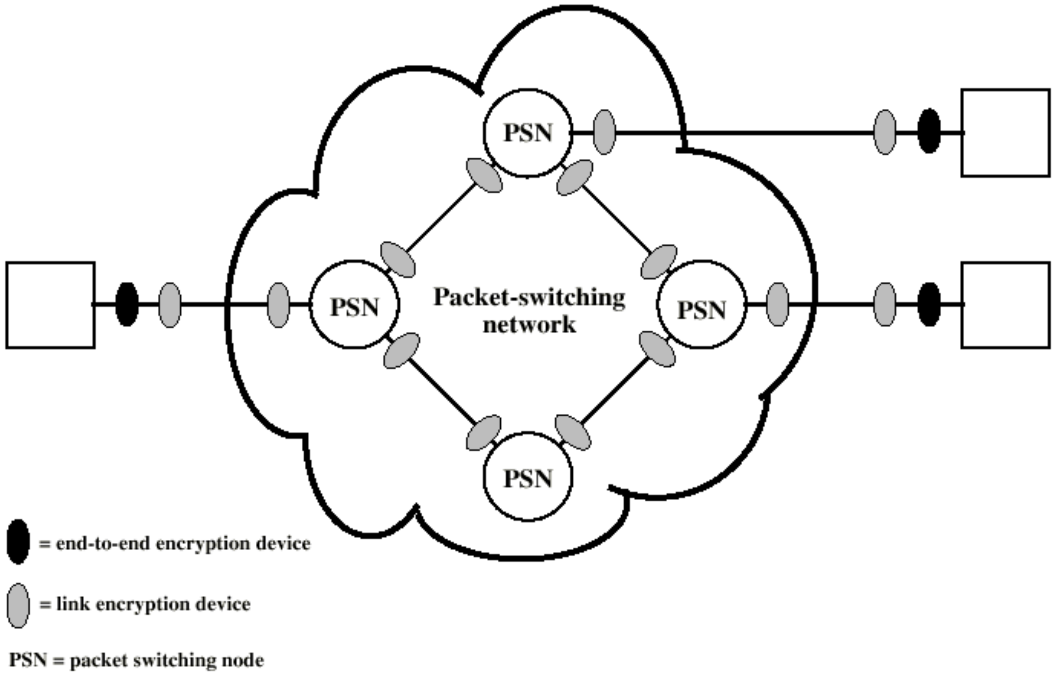


Figure 2.9 Encryption Across a Packet-Switching Network

Key Distribution

1. A key could be selected by A and physically delivered to B.
2. A third party could select the key and physically deliver it to A and B.
3. If A and B have previously used a key, one party could transmit the new key to the other, encrypted using the old key.
4. If A and B each have an encrypted connection to a third party C, C could deliver a key on the encrypted links to A and B.

Key Distribution

- **Session key:**
  - Data encrypted with a one-time session key. At the conclusion of the session the key is destroyed.
- **Permanent key:**
  - Used between entities for the purpose of distributing session keys.

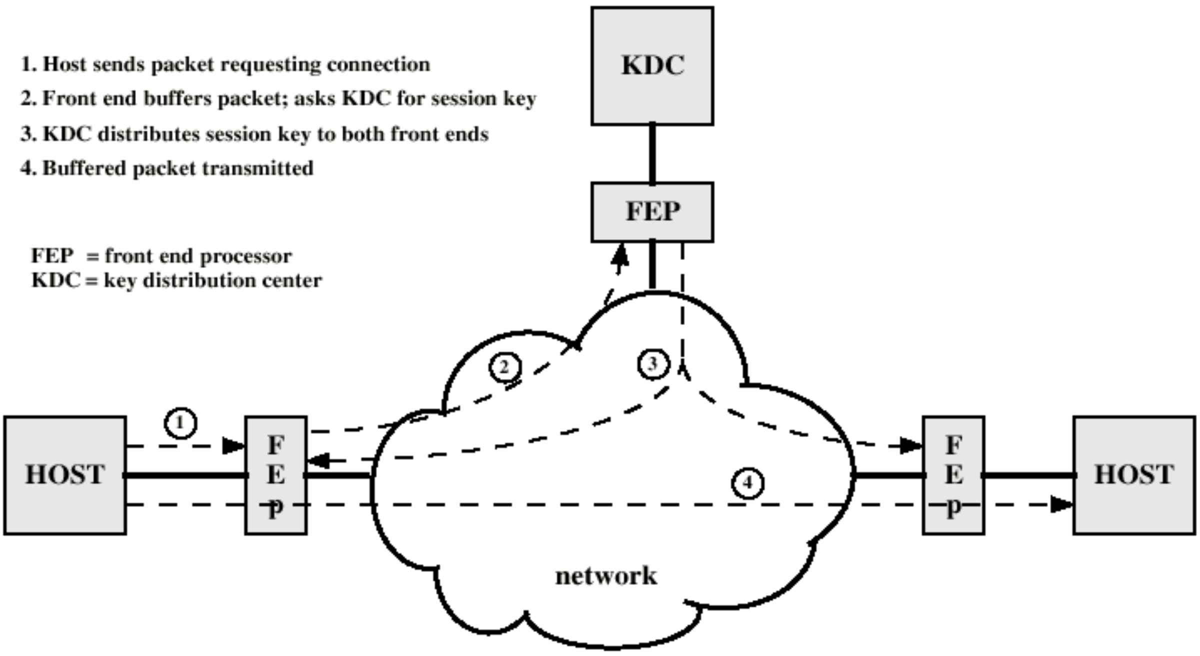


Figure 2.10 Automatic Key Distribution for Connection-Oriented Protocol

Steganography

- Security through obscurity i.e. hide information in other information
- Can be in images, in text or hidden between lines of text in a document
- Example
  - In an image you can use the last significant bit of each pixel value and distribute a message over these.