Conventional Encryption Message Confidentiality

What Is Cryptography?

- Cryptography -- from the Greek for "secret writing" -- is the mathematical "scrambling" of data so that only someone with the necessary ***key*** can "unscramble" it.
- Cryptography allows secure transmission of private information over insecure channels (for example packet-switched networks).
- Cryptography also allows secure storage of sensitive data on any computer.

Classical Cryptography: Secret-Key or Symmetric Cryptography

- Alice and Bob agree on an encryption method and a shared ***key***.
- Alice uses the key and the encryption method to ***encrypt*** (or ***encipher***) a message and sends it to Bob.
- Bob uses the same key and the related decryption method to ***decrypt*** (or ***decipher***) the message.

Conventional Encryption Principles

- An encryption scheme has five ingredients:
  - Plaintext
  - Encryption algorithm
  - Secret Key
  - Ciphertext
  - Decryption algorithm
- Security depends on the secrecy of the key, not the secrecy of the algorithm !

Conventional Encryption Principles

x=plain text, k= key, ciphertext y=E[k,x], decipher: x=D[k,y}

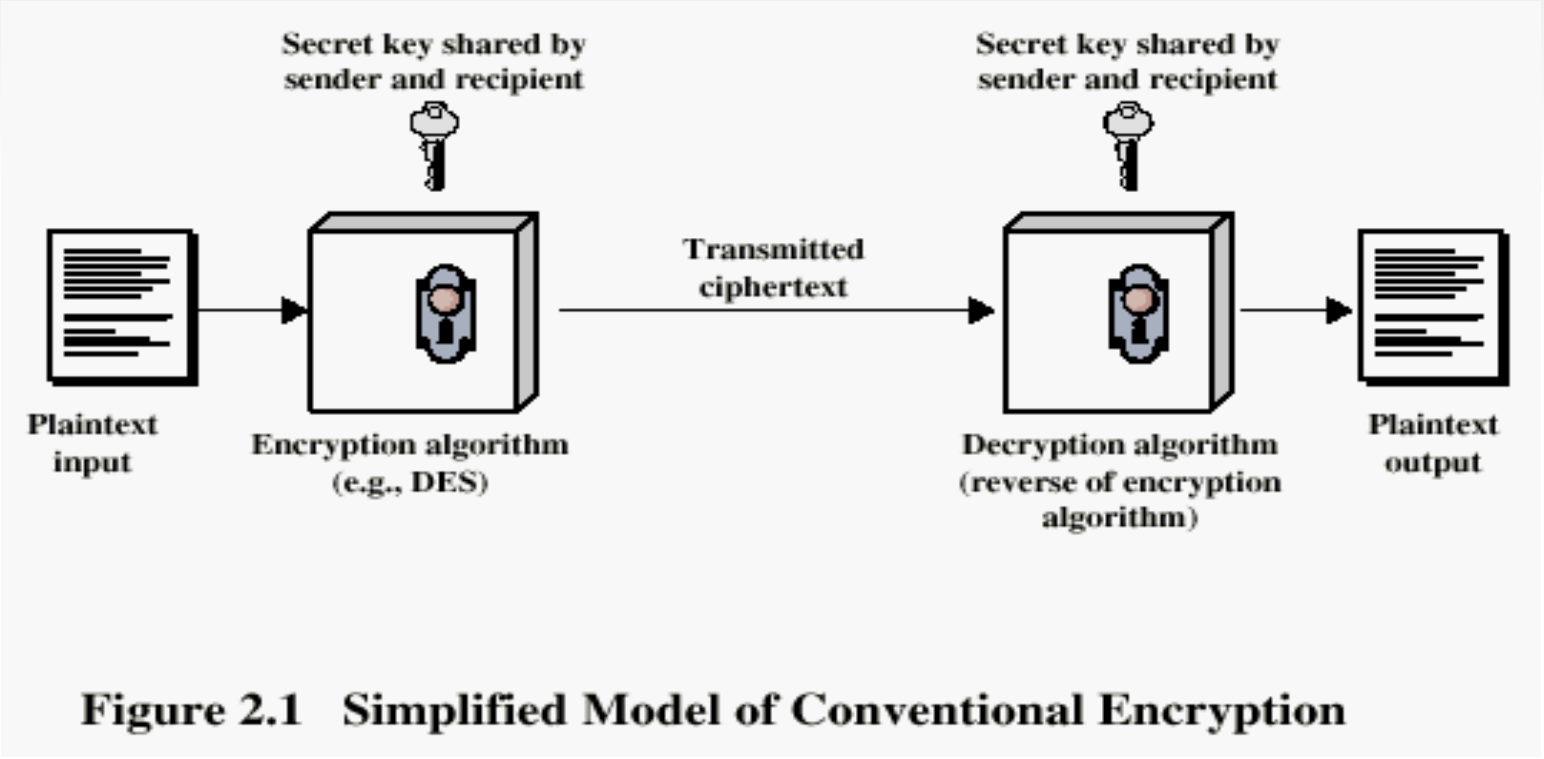
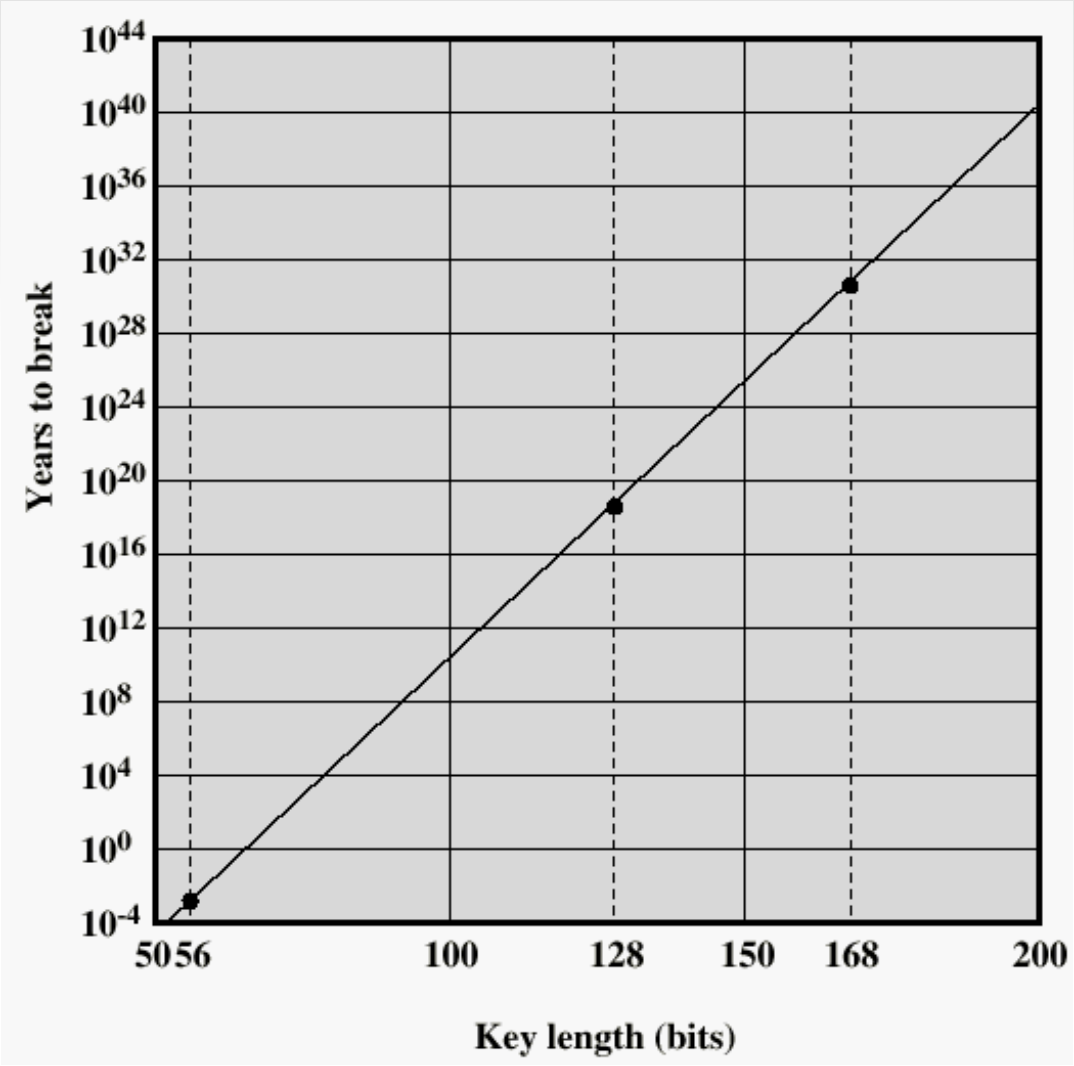


Figure 2.1 Simplified Model of Conventional Encryption

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

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



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 Fesitel 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

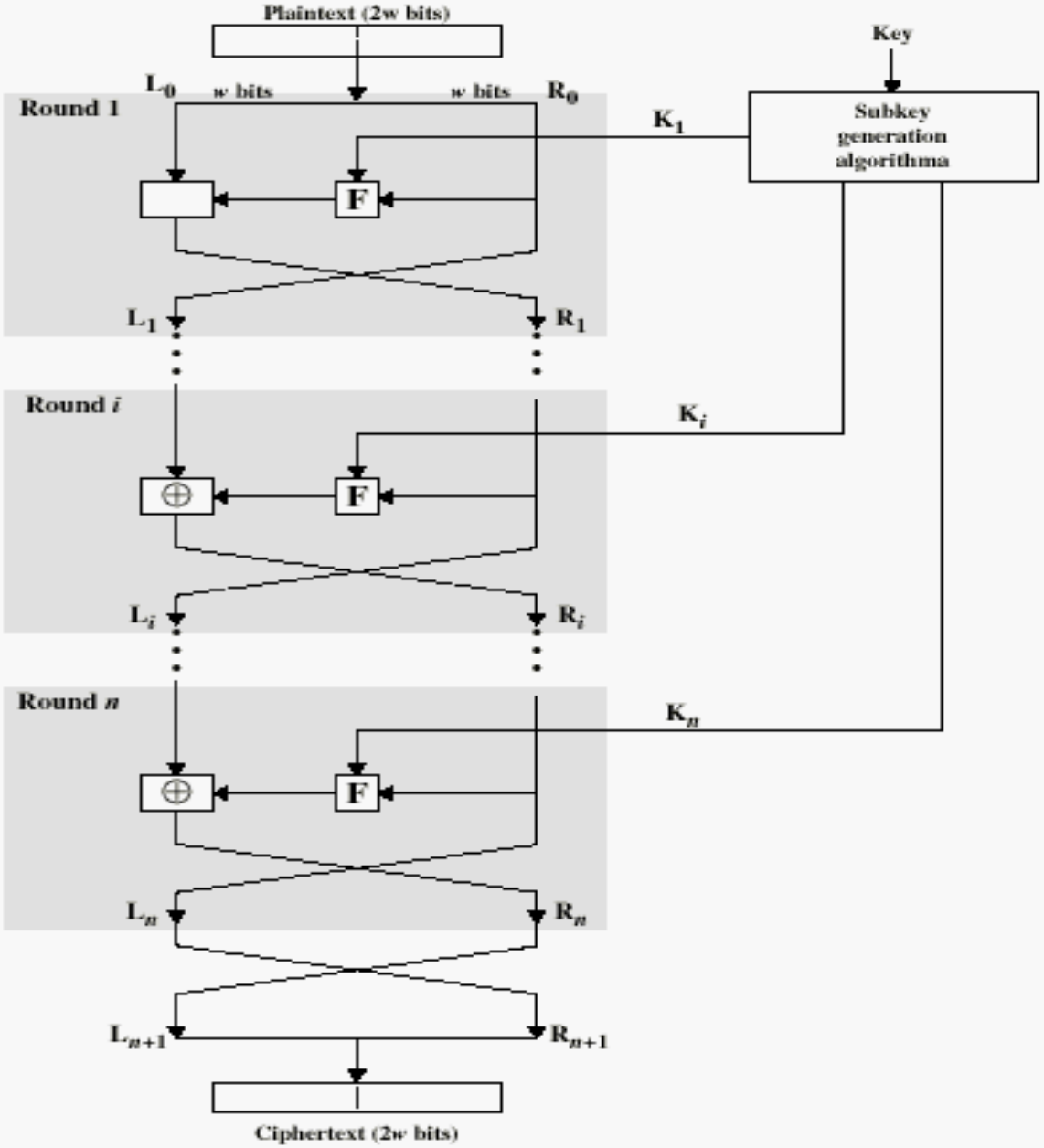


Figure 2.2 Classical Feistel Network

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:
  - The algorithm and the key length (56-bits)

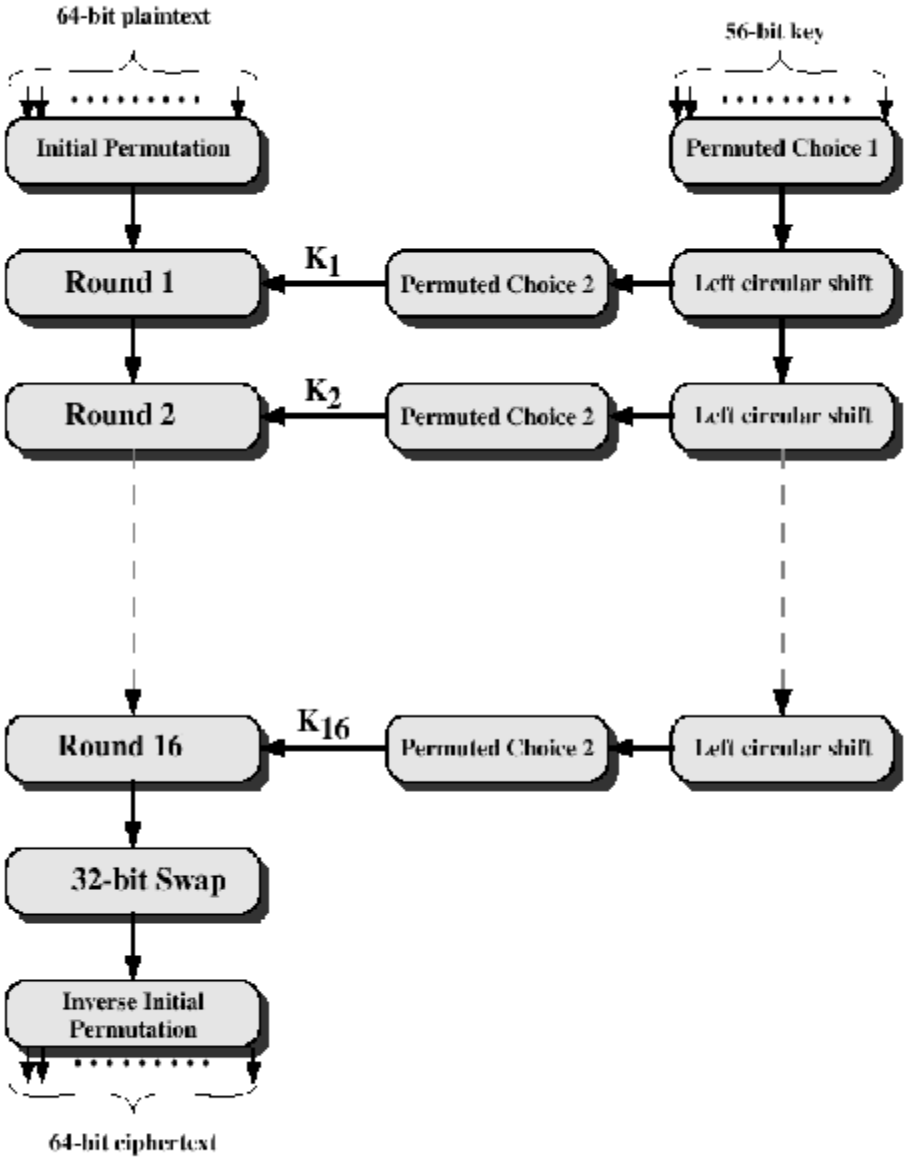


Figure 2.3 General Depiction of DES Encryption Algorithm

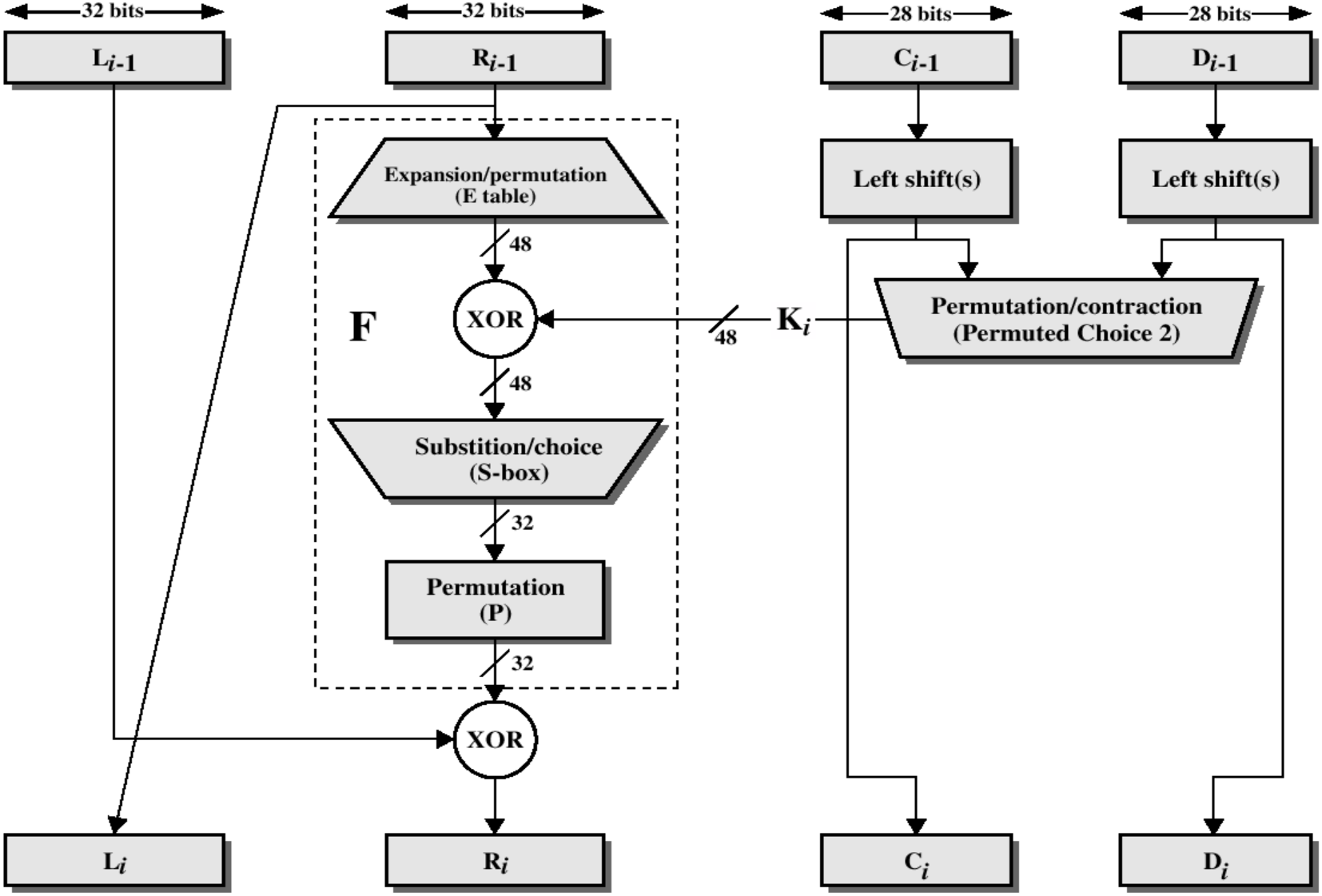
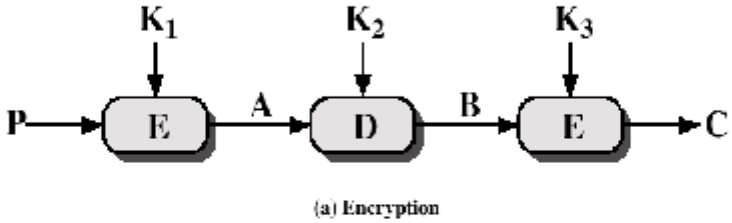
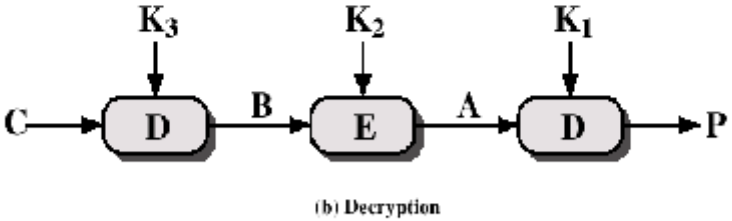


Figure 2.4 Single Round of DES Algorithm

Triple DEA



(a) Encryption



(b) Decryption

Figure 2.6 Triple DEA

Cipher Block Modes of Operation

- Cipher Block Chaining Mode (CBC)
  - The input to the encryption algorithm is the XOR of the current plaintext block and the preceding ciphertext block.
  - Repeating pattern of 64-bits are not exposed

$$C_i = E_k[C_{i-1} \oplus P_i]$$

$$D_K[C_i] = D_K[E_K(C_{i-1} \oplus P_i)]$$

$$D_K[C_i] = (C_{i-1} \oplus P_i)$$

$$C_{i-1} \oplus D_K[C_i] = C_{i-1} \oplus C_{i-1} \oplus P_i = P_i$$

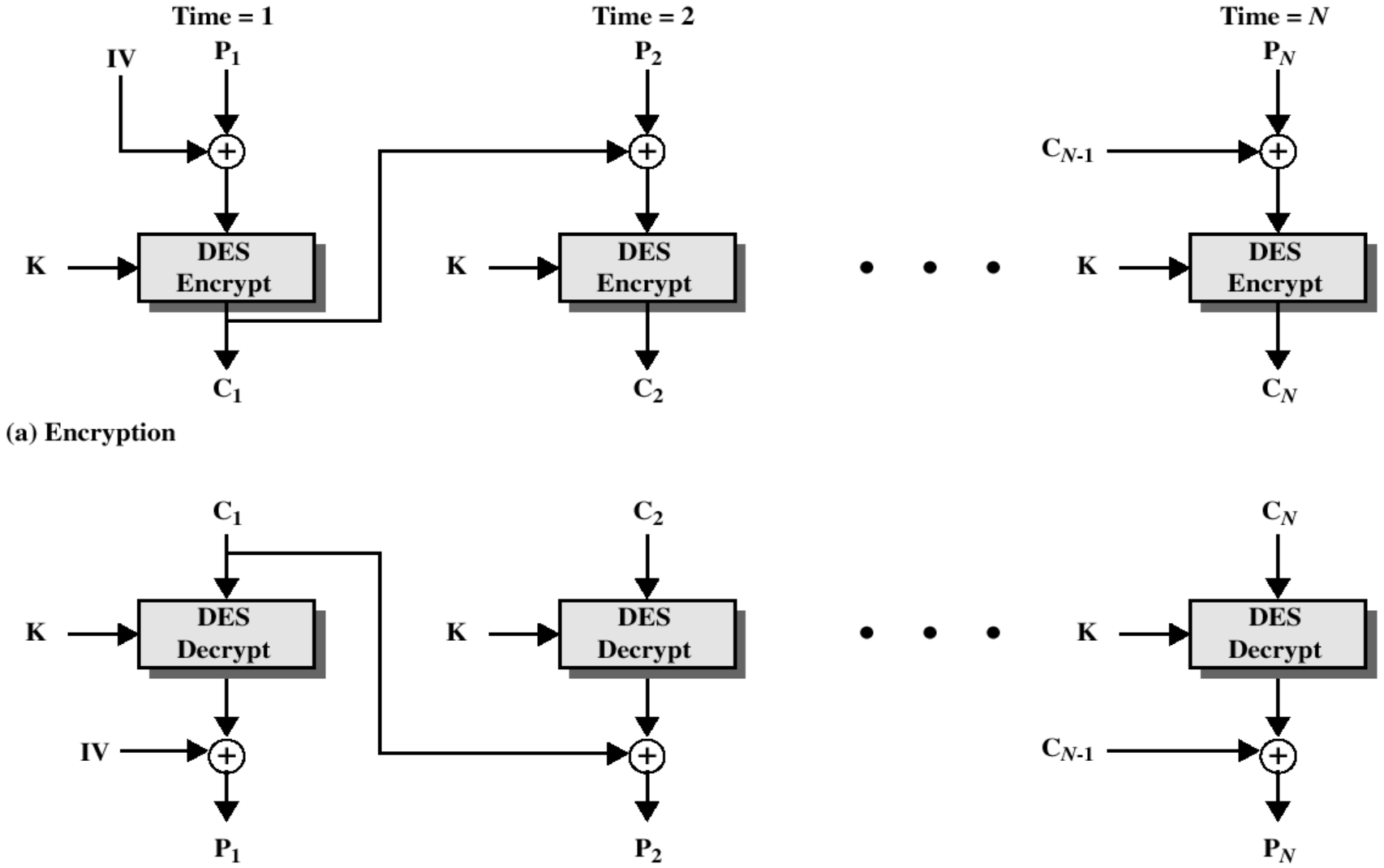


Figure 2.7 Cipher Block Chaining (CBC) Mode

Advantages of Classical Cryptography

- There are some very fast classical encryption (and decryption) algorithms
- Since the speed of a method varies with the length of the key, faster algorithms allow one to use longer key values.
- Larger key values make it harder to guess the key value -- and break the code -- by brute force.

Disadvantages of Classical Cryptography

- *Requires secure transmission of key value*
- Requires a separate key for each group of people that wishes to exchange encrypted messages (readable by any group member)
- For example, to have a separate key for each pair of people, 100 people would need 4950 different keys n(n-1).

Clasification of Cryptography

- The number of keys used
  - symmetric (single key)
  - asymmetric (two-keys, or public-key encryption)

Conventional Encryption Algorithms

- Data Encryption Standard (DES)
  - The most widely used encryption scheme
  - The algorithm is reffered 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

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

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

Secret key Distribution:

- The two parties must share they secret key

1. generated by one party and manualy deleivered
2. generated by one and delivered using shared secret
3. created by thid party and deliver through secured channel

1-2: for small organizations

- number of pairs for n users: n*(n-1)/2
- KDC can play the role of key distribution

Algorithms:

1. U_A issues req. to kdc for session key for session with user U_B

.

req. =identity of U_A, identity of connection ID_A (=time stamp, counter or rand. no., protocol ref.)

2. kdc creates session key(Ks), responds with msg ecrypted using a pre-established secret key K_A between U_A and kdc.

msg = session key Ks + original req copy + sub msg. encrypted using preshared key K_B between kdc and U_B (sub msg=Ks, id. of U_A)

Now U_A can verify that original req. was not altered.

3. U_A sends msg to U_B.

msg = its identity, session id ID_A, encrypted sub message of kdc to be relayed to U_B, encryption of ID_A

4. On arrival U_B can chekc identity of U_A, and integrity of Ks.

(At this point one can deduce that secret key has been securely delivered to U_A and U_B.)

Now the message transfer can go on between U_A and U_B.