Lecture 4.2
Symmetric Ciphers

Lecture Outline

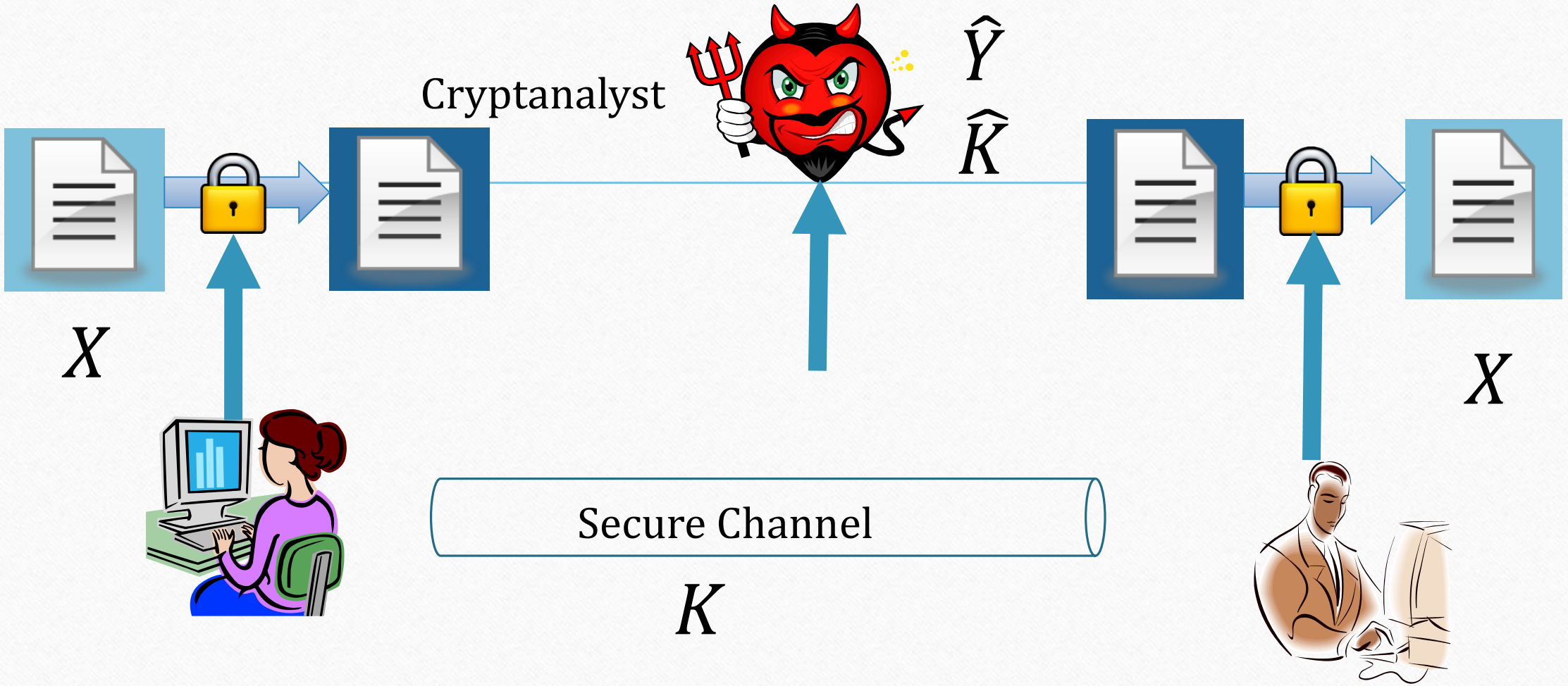
Symmetric ciphers

- Block cipher principles
- Feistel Cipher
- Data Encryption Standard (DES)
- Triple DES

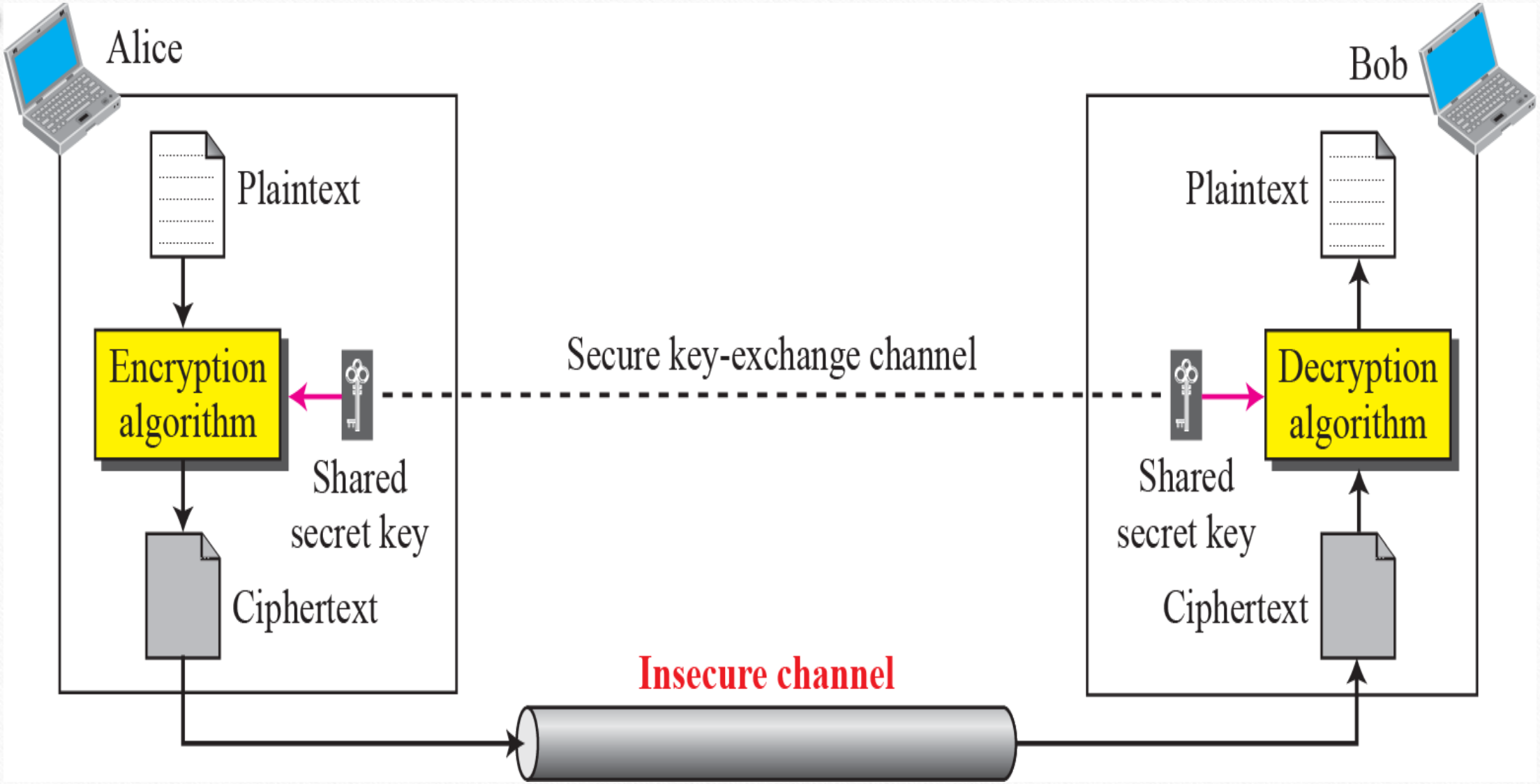
General Idea of Symmetric Ciphers

- Both sender and receiver keys are the same: $K_A = K_B$
- The keys must be kept secret and securely distributed
  - Thus, also called “Secret Key Cryptography”
- Data Encryption Standard (DES), 3DES , IDEA etc

Symmetric Cipher Model



General Idea of Symmetric Ciphers



Modern Symmetric Ciphers

- The traditional symmetric-key ciphers are character-oriented ciphers.
- Currently, bit-oriented ciphers are now more commonly used.
- This is because the information to be encrypted is not just text; it can also consist of numbers, graphics, audio, and video data.
- It is convenient to convert these types of data into a stream of bits, to encrypt the stream, and then to send the encrypted stream.
- A modern block cipher can be either a block cipher or a stream cipher.

Modern Ciphers

Stream Ciphers

- Stream ciphers, like block ciphers, break message into fixed length blocks, but use a sequence of keys to encrypt the blocks.
- The Vigenère cipher is an example of a stream cipher.
- Let E be an encipherment algorithm, and let $E_k(b)$ be the encipherment of the message b with key k.
- Let a message $m = b_1 b_2$ …where each b_i is of a fixed length, and let $k = k_1 k_2 \ldots$.
- A **stream cipher** is a cipher for which $E_k(m) = Ek_1(b_1)Ek_2(b_2)$ …

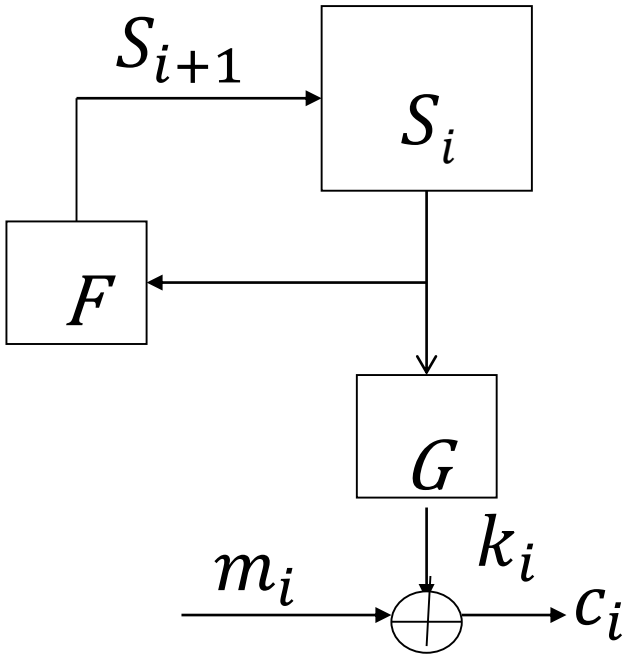
Modern Ciphers

Stream Ciphers

- Idea of a stream cipher: partition the text into small (e.g. 1 bit) blocks and let the encoding of each block depend on many previous blocks.
- For each block, a different “key” is generated.

Modern Ciphers

Stream Cipher Model



S_i : state of the cipher
at time $t = i$.

F : state function.

G : output function.

- Initial state, output and state functions are controlled by the secret key.

Stream Ciphers

Encrypts a digital data stream one bit or one byte at a time

Examples:

- Autokeyed Vigenère cipher
- Vernam cipher

In the ideal case a one-time pad version of the Vernam cipher would be used, in which the keystream is as long as the plaintext bit stream

If the cryptographic keystream is random, then this cipher is unbreakable by any means other than acquiring the keystream

- Keystream must be provided to both users in advance via some independent and secure channel
- This introduces insurmountable logistical problems if the intended data traffic is very large

Stream Ciphers

For practical reasons the bit-stream generator must be implemented as an algorithmic procedure so that the cryptographic bit stream can be produced by both users

It must be computationally impractical to predict future portions of the bit stream based on previous portions of the bit stream

The two users need only share the generating key and each can produce the keystream

Modern Ciphers

Block Ciphers

- A **block cipher** is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.
- Typically, a block size of 64 , 128, 256 bits is used. As with a stream cipher, the two users share a symmetric encryption key. A block cipher can be used to achieve the same effect as a stream cipher.
- Far more effort has gone into analyzing block ciphers. In general, they seem applicable to a broader range of applications than stream ciphers. The vast majority of network-based symmetric cryptographic applications make use of block ciphers.

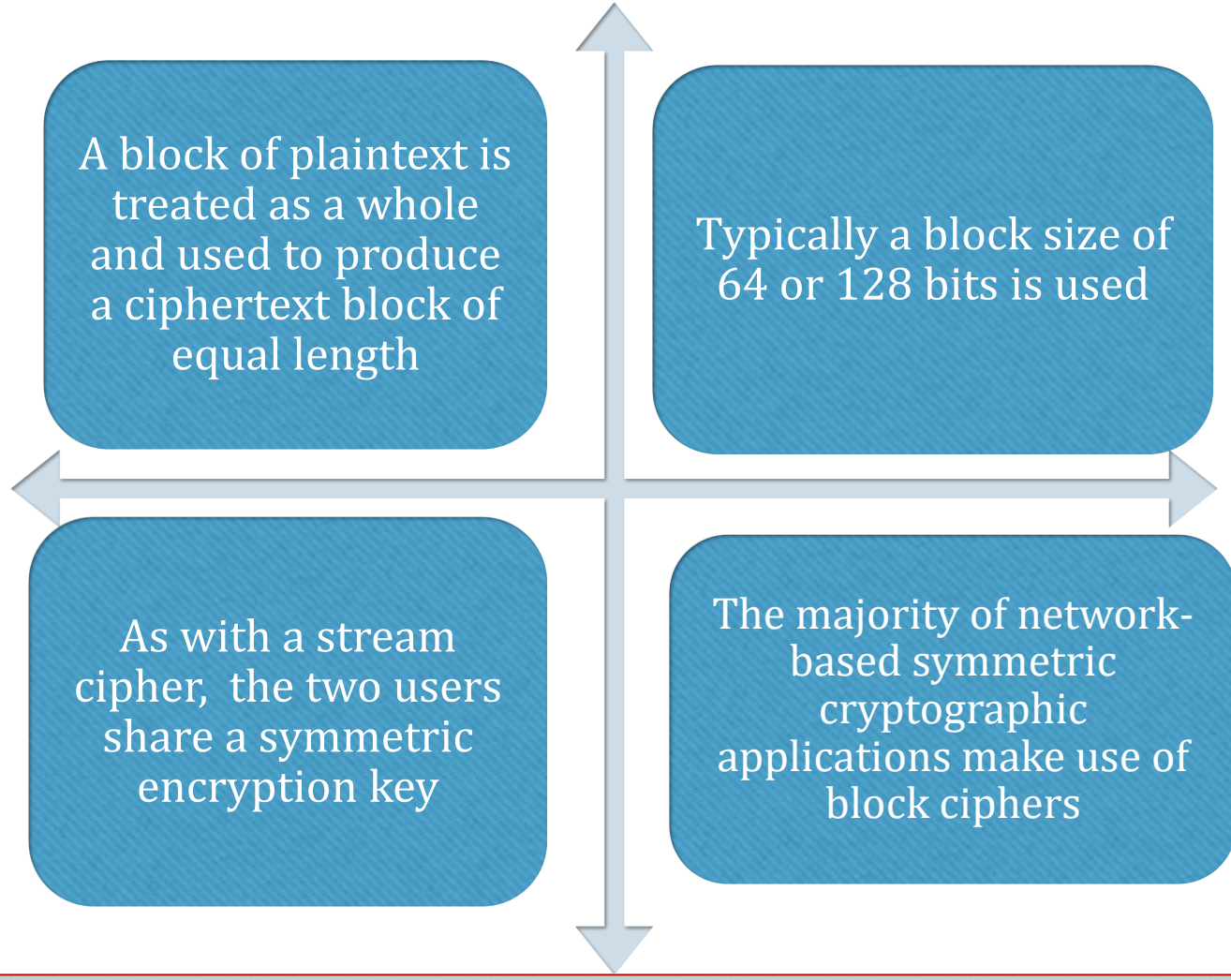
Modern Ciphers

Block Ciphers

- Idea of a block cipher: partition the text into relatively large (e.g. 128 bits) blocks and encode each block separately.
- The encoding of each block generally depends on at most one of the previous blocks.
- The same “key” is used at each block.

Modern Ciphers

Block Ciphers



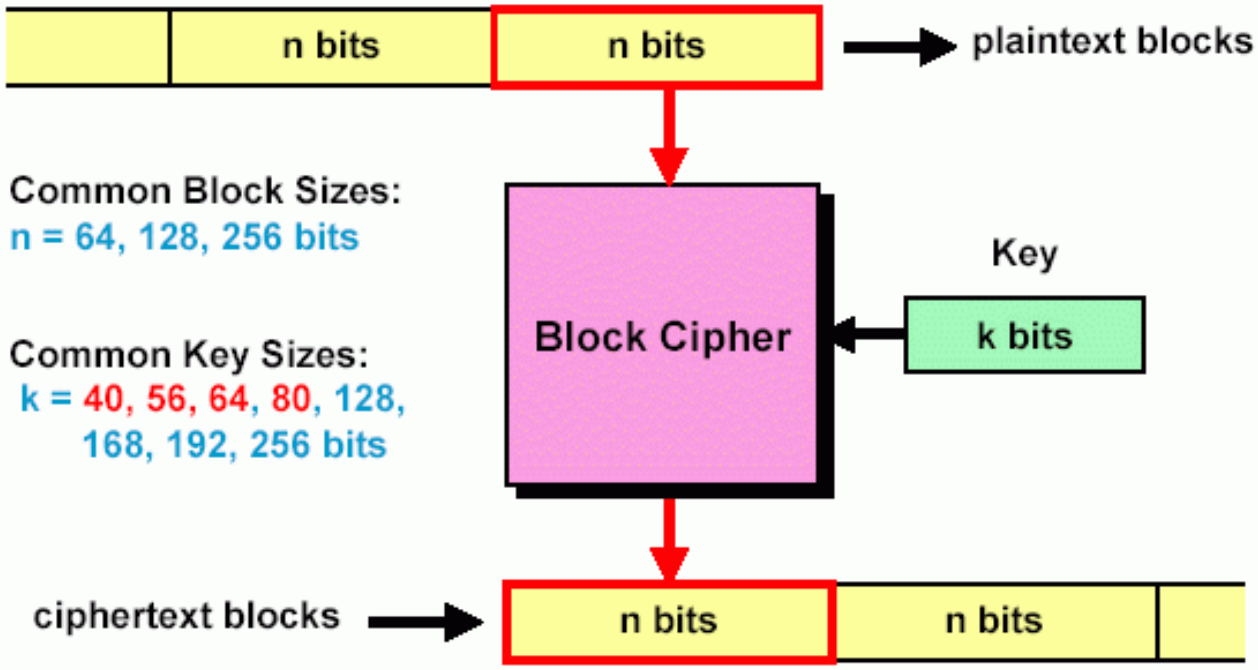
Modern Ciphers

Block Ciphers: Formal Definition

- Let E be an encipherment algorithm, and let $E_k(b)$ be the encipherment of the message b with key k.
- Let a message $m = b_1 b_2$ …where each b_i is of a fixed length.
- A **block cipher** is a cipher for which $E_k(m) = E_k(b_1)E_k(b_2)$ …

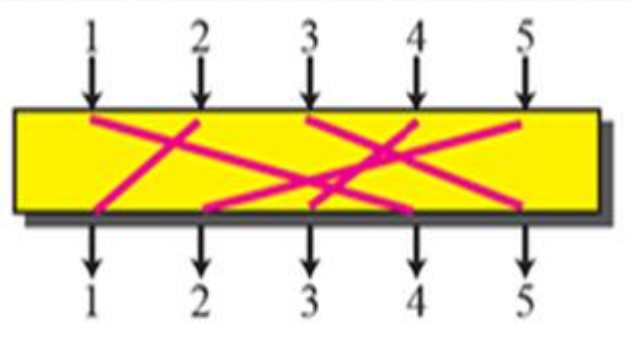
A Modern Block Cipher

Divide input bit stream into n-bit sections, encrypt only that section, no dependency/history between sections

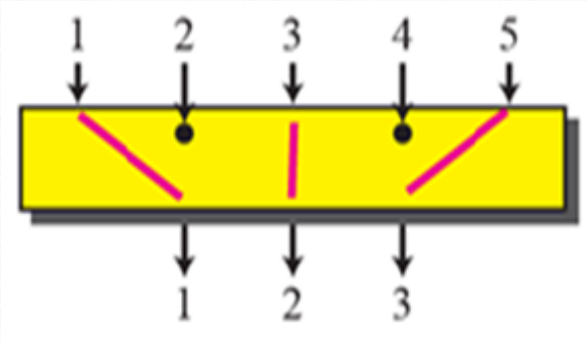


In a good block cipher, each output bit is a function of all n input bits and all k key bits

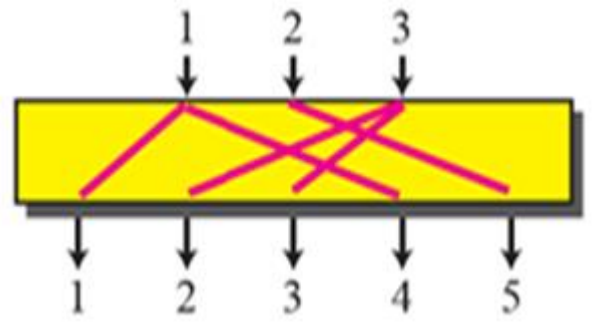
Components of a modern block cipher



Straight Permutation

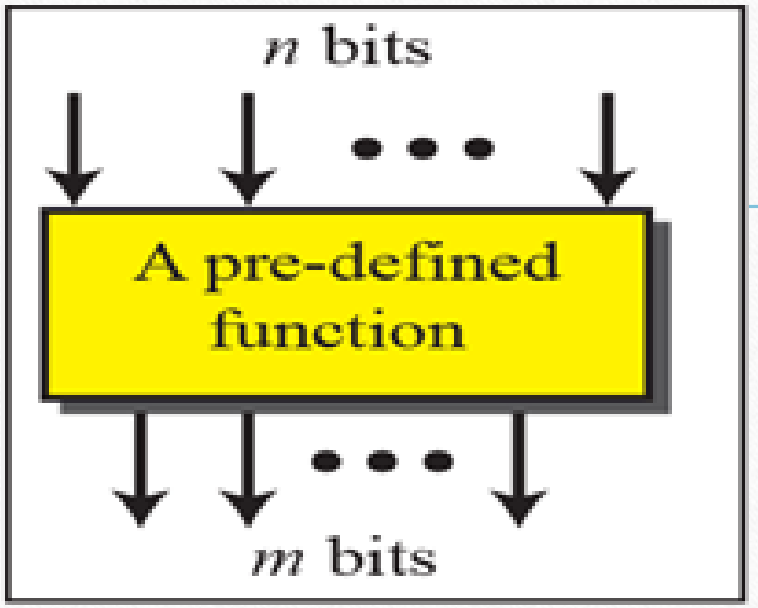


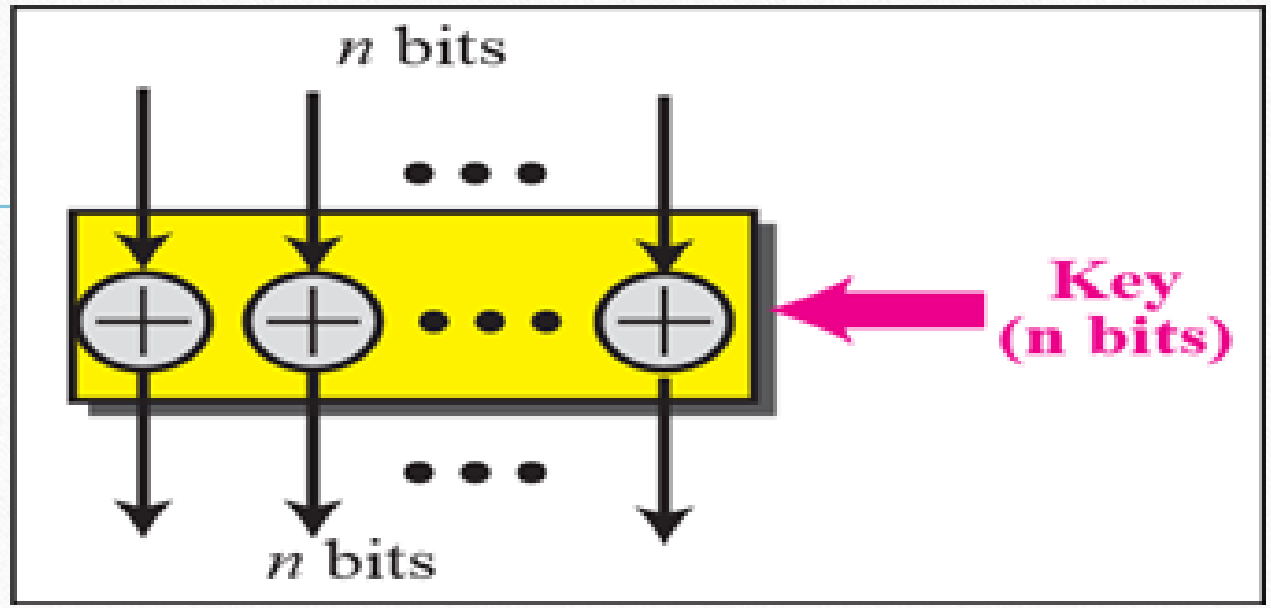
Compression Permutation



Expansion Permutation

Components of a modern block cipher

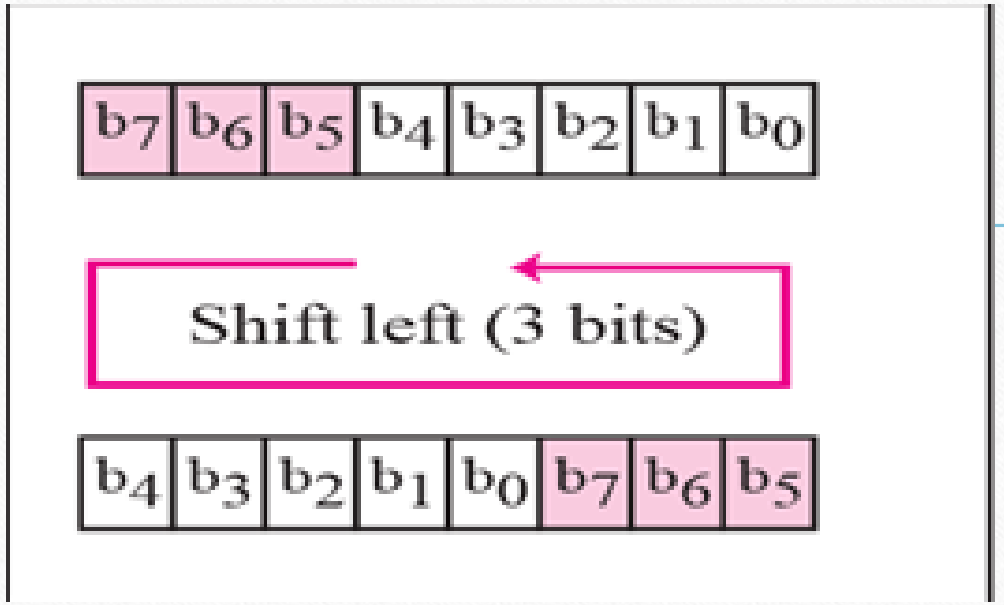




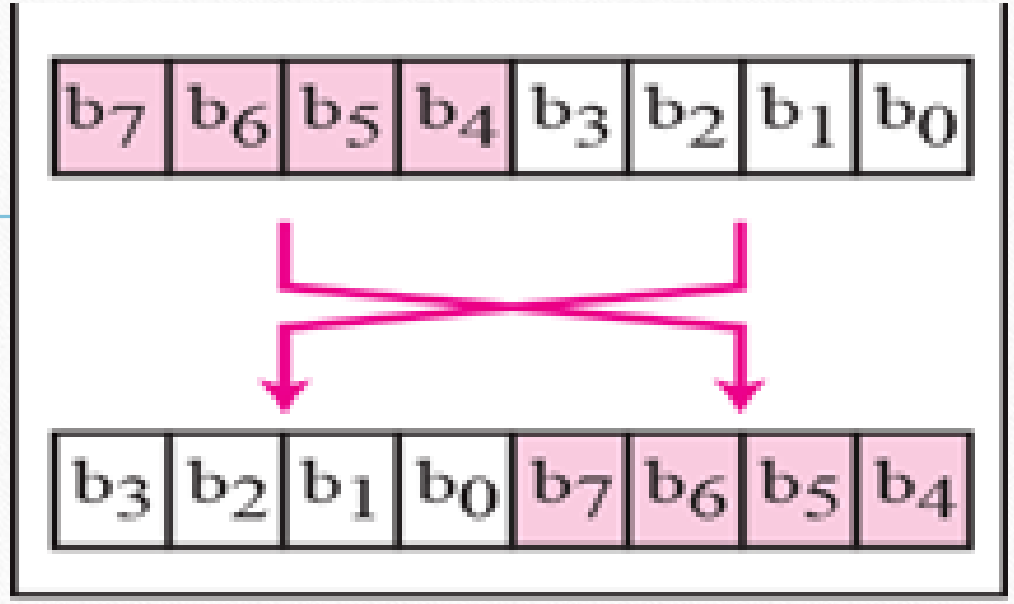
Substitution

Exclusive OR

Components of a modern block cipher

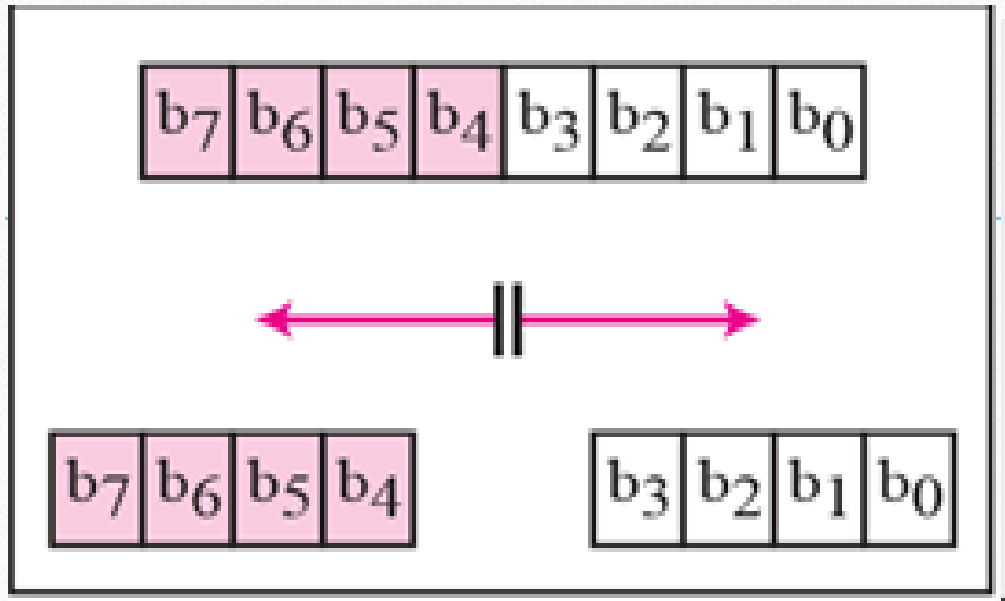


Shift

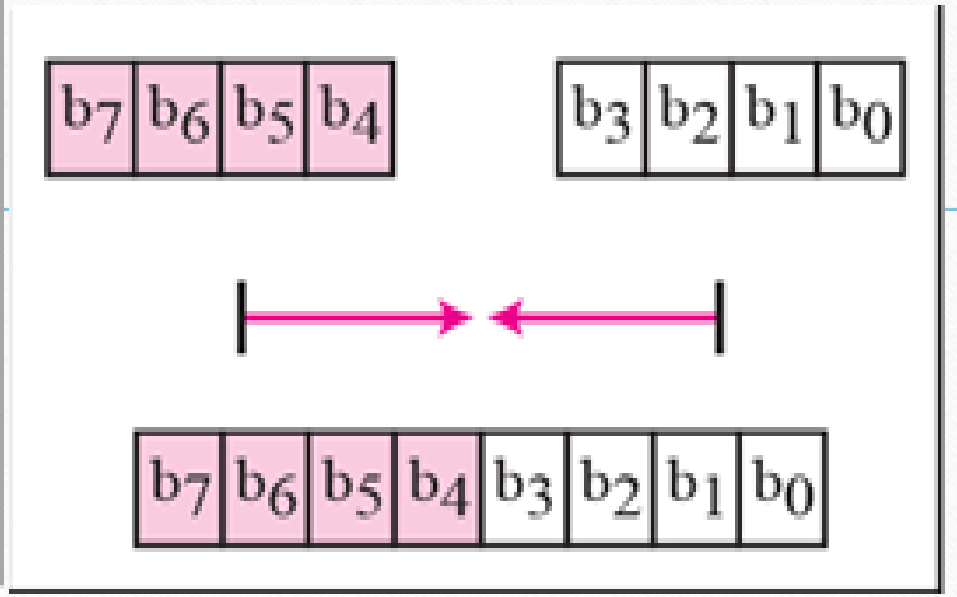


Swap

Components of a modern block cipher



Split



Combine

Lecture Outline

Symmetric ciphers

- Block cipher principles
- Feistel Cipher
- Data Encryption Standard (DES)
- Triple DES

Feistel Cipher

- Fiestal proposed the use of a cipher that alternates substitutions and permutations

Substitutions

- Each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements

Permutation

- No elements are added or deleted or replaced in the sequence, rather the order in which the elements appear in the sequence is changed

- Is a practical application of a proposal by Claude Shannon to develop a product cipher that alternates confusion and diffusion functions

- This structure used by some significant symmetric block ciphers currently in use

Feistel Cipher

- Terms introduced by Claude Shannon to capture the two basic building blocks for any cryptographic system
  - Shannon's concern was to thwart cryptanalysis based on statistical analysis

Diffusion

- The statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext
- This is achieved by having each plaintext digit affect the value of many ciphertext digits

Confusion

- Seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible
- Even if the attacker can get some handle on the statistics of the ciphertext, the way in which the key was used to produce that ciphertext is so complex as to make it difficult to deduce the key

Feistel Cipher

Feistel Cipher Design Features

- The exact realization of a Feistel network depends on the choice of certain parameters and design features:

1. Block size: Larger block sizes mean greater security but reduce encryption/decryption speed for a given algorithm. Greater security is achieved by greater diffusion. Traditionally, a block size of 64 bits has been considered a reasonable tradeoff and was nearly universal in block cipher design. However, the new AES uses a 128-bit block size.
2. Key size: Larger key size mean greater security but may decrease encryption/decryption speed. Greater security is achieved by greater resistance to brute-force attacks and greater confusion. Key sizes of 64 bits or less are now widely considered to be inadequate, and 128 bits has become a common size.

Feistel Cipher

Feistel Cipher Design Features

- The exact realization of a Feistel network depends on the choice of the following parameters and design features:

3. Number of rounds: The essence of the Feistel cipher is that a single round offers inadequate security but that multiple rounds offer increasing security. A typical size is 16 rounds.
4. Subkey generation algorithm: Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis.
5. Round function F: Again, greater complexity generally means greater resistance to cryptanalysis.

Feistel Cipher

Feistel Cipher Design Features

There are two other considerations in the design of a Feistel cipher:

i. Fast software encryption/decryption: In many cases, encryption is embedded in applications or utility functions. Accordingly, the speed of execution of the algorithm becomes a concern.

ii. Ease of analysis: Although we would like to make our algorithm as difficult as possible to cryptanalyze, there is great benefit in making the algorithm easy to analyze. That is, if the algorithm can be concisely and clearly explained, it is easier to analyze that algorithm for cryptanalytic vulnerabilities and therefore develop a higher level of assurance as to its strength. DES, for example, does not have an easily analyzed functionality

Lecture Outline

Symmetric ciphers

- Block cipher principles
- Feistel Cipher
- Data Encryption Standard (DES)
- Triple DES

Data Encryption Standard (DES)

- DES is a block cipher; it encrypts data in 64-bit blocks.
- The fundamental building block of DES is called a round and it (DES) has 16 rounds
- The same algorithm and key are used for encryption and decryption (except for minor differences in key schedule).

$$\mathcal{M} = \mathsf{C} = \{0,1\}^{64}$$

- The key length is 56 bits. $k = \{0,1\}^{56}$

(The key is usually expressed as a 64-bit number, but every eight bit is used for parity checking and ignored.)

- A handful of numbers are considered weak keys, e.g.,

$$E_k\big(E_k(\mathcal{M})\big) = \mathcal{M}$$

$$E_{k_1}(E_{k_2}(\mathcal{M}) = \mathcal{M}$$

Data Encryption Standard (DES)

- Encodes plaintext in 64-bit chunks using a 64-bit key (56 bits + 8 bits parity)
- Uses a combination of diffusion and confusion to achieve security
- Was cracked in 1997
  - Parallel attack – exhaustively search key space
- Decryption in DES – it's symmetric! Use K_A again as input and then the same keys except in reverse order

Data Encryption Standard (DES)

1. 64-bit input is permuted
2. 16 stages of identical operation
   - Differ in the 48-bit key extracted from 56-bit key - complex
   - $R_I = R_{I-1}$ encrypted with K_I and XOR'd with L_{I-1}
3. Final inverse permutation stage

Data Encryption Standard (DES)

1. First, the 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the *permuted input.*

2. This is followed by a phase consisting of sixteen rounds of the same function, which involves both permutation and substitution functions.

3. The output of the last (sixteenth) round consists of 64 bits that are a function of the input plaintext and the key. The left and right halves of the output are swapped to produce the pre-output.

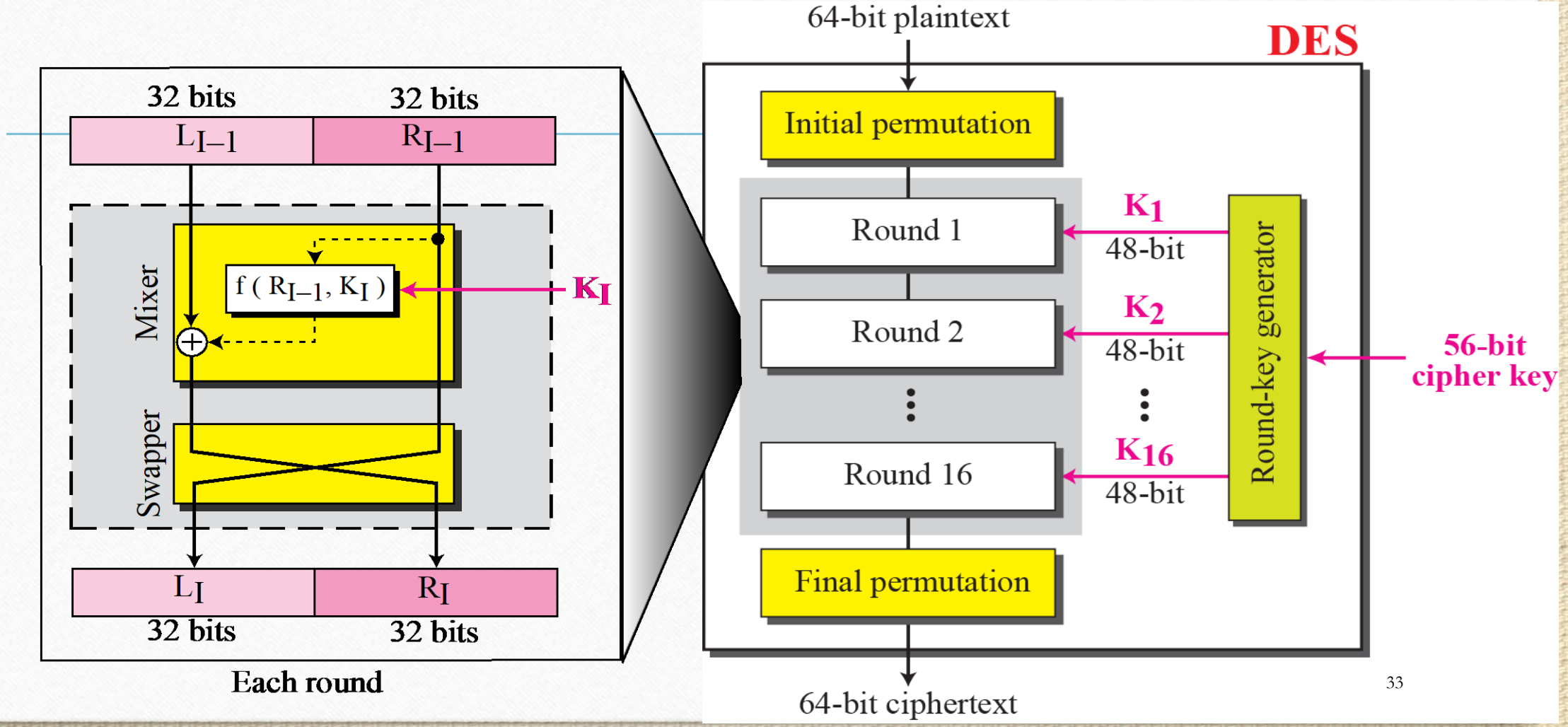
Data Encryption Standard (DES)

4. Finally, the pre-output is passed through a permutation that is the inverse of the initial permutation function, to produce the 64-bit ciphertext.

5. With the exception of the initial and final permutations, DES has the exact structure of a Feistel cipher.

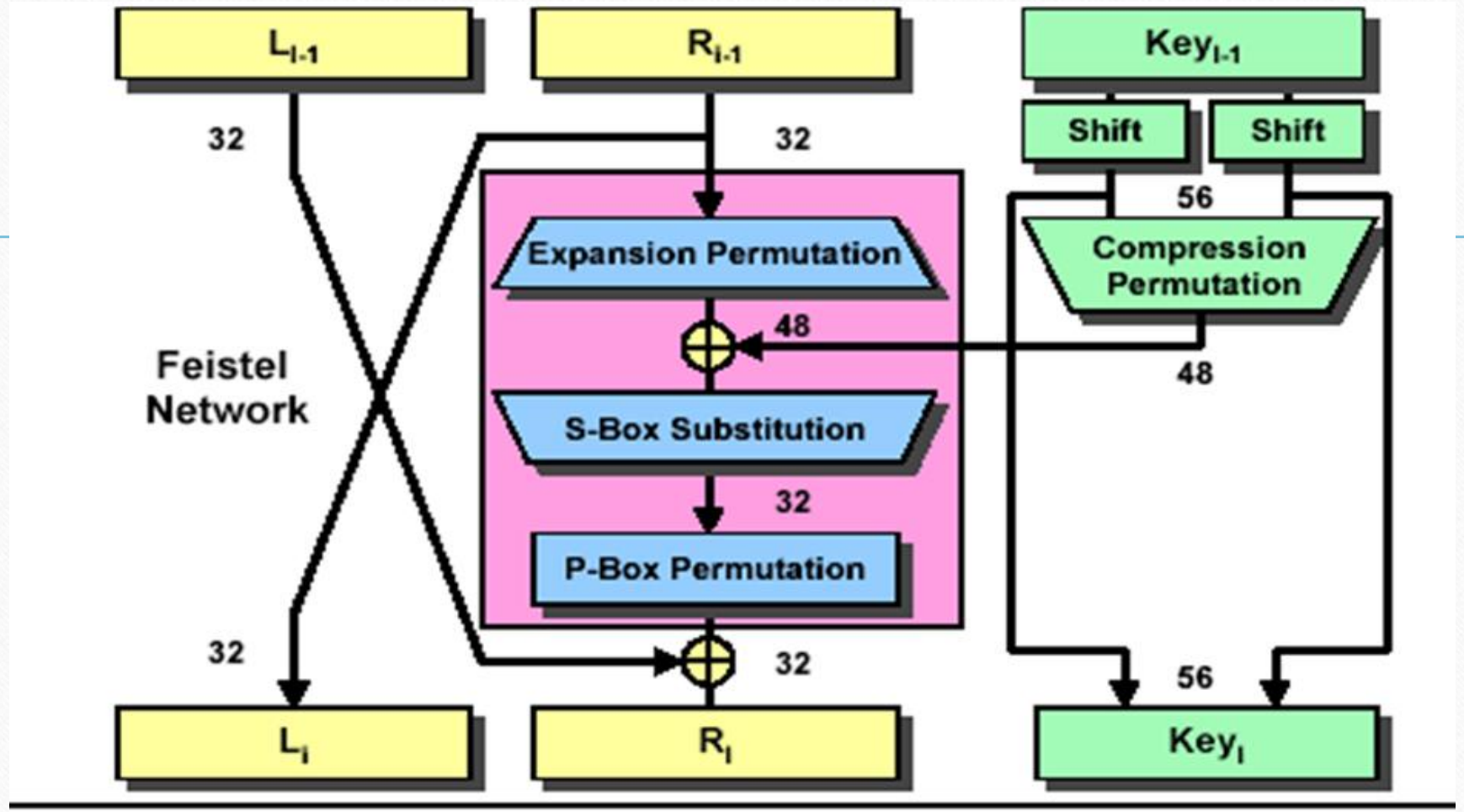
DES Inner Working

General Structure of DES



Data Encryption Standard (DES)

General Structure of DES



Data Encryption Standard (DES)

Feistel Network

- The network has the F-functions as the main component

The F-functions' (Feistel Function) basic operation

- It operates on half a block (32-bit)at a time and consists of 4 stages:-

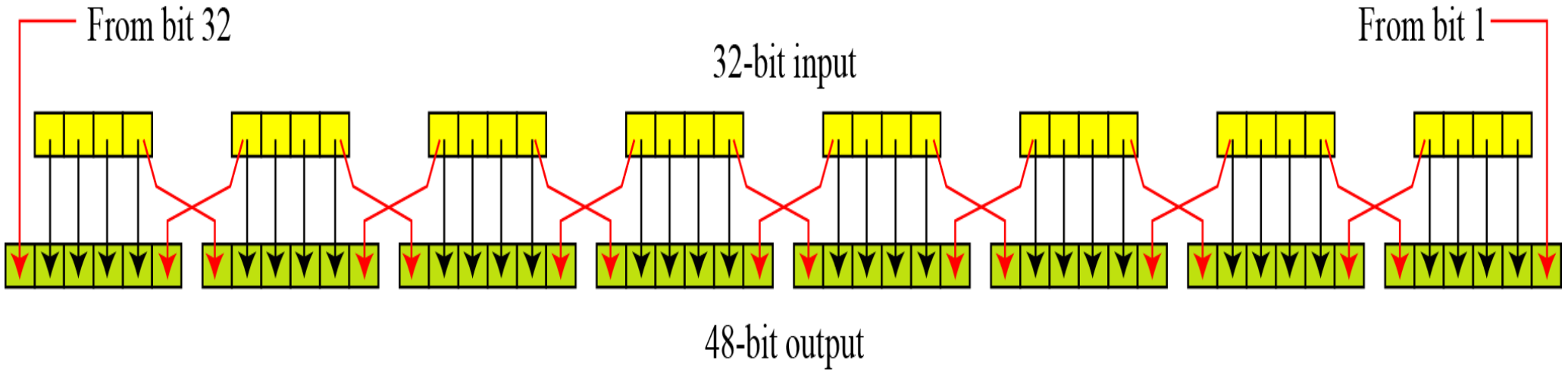
1. Expansion: The 32-bit block is expanded to 48 bits using the expansion permutation, by duplicating half of the bits. The o/p consists of eight 6-bit (8*6 = 48-bits) pieces, each containing a copy of 4 corresponding input bits, plus a copy of the immediately adjacent bit from each of the input pieces to either side.

- The security offered by this operation comes from one bit affecting two substitutions in the S-boxes.
- This causes the dependency of the output bits on the input bits to spread faster, creating what is called the avalanche affect.

Data Encryption Standard (DES)

Feistel Network

- Expansion permutation



Data Encryption Standard (DES)

Feistel Network

- The network has the F-functions as the main component

The F-functions' (Feistel Function) basic operation

- It operates on half a block (32-bit)at a time and consists of 4 stages:-

2. Key Mixing: The result is combined with a subkey using an XOR operation. Sixteen 48-bits subkeys, one for each round, are derived from the main key using the key schedule.

Data Encryption Standard (DES)

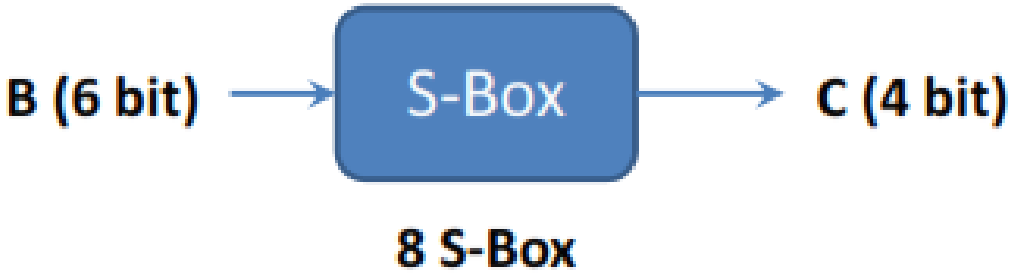
- Feistel Network

3. Substitution: The above block (48-bits) is then divided to eight 6-bit pieces before processing by the S-boxes (substitution boxes).

- Each of the eight S-boxes replaces its 6 input bits with 4 output bits according to a non linear transformation, provided in the form of a lookup table.
- The S-boxes provide the core of the security of DES, without them the cipher would be linear and trivially breakable.

Data Encryption Standard (DES)

- Feistel Network



S= matrix 4×16, values form 0 to 15

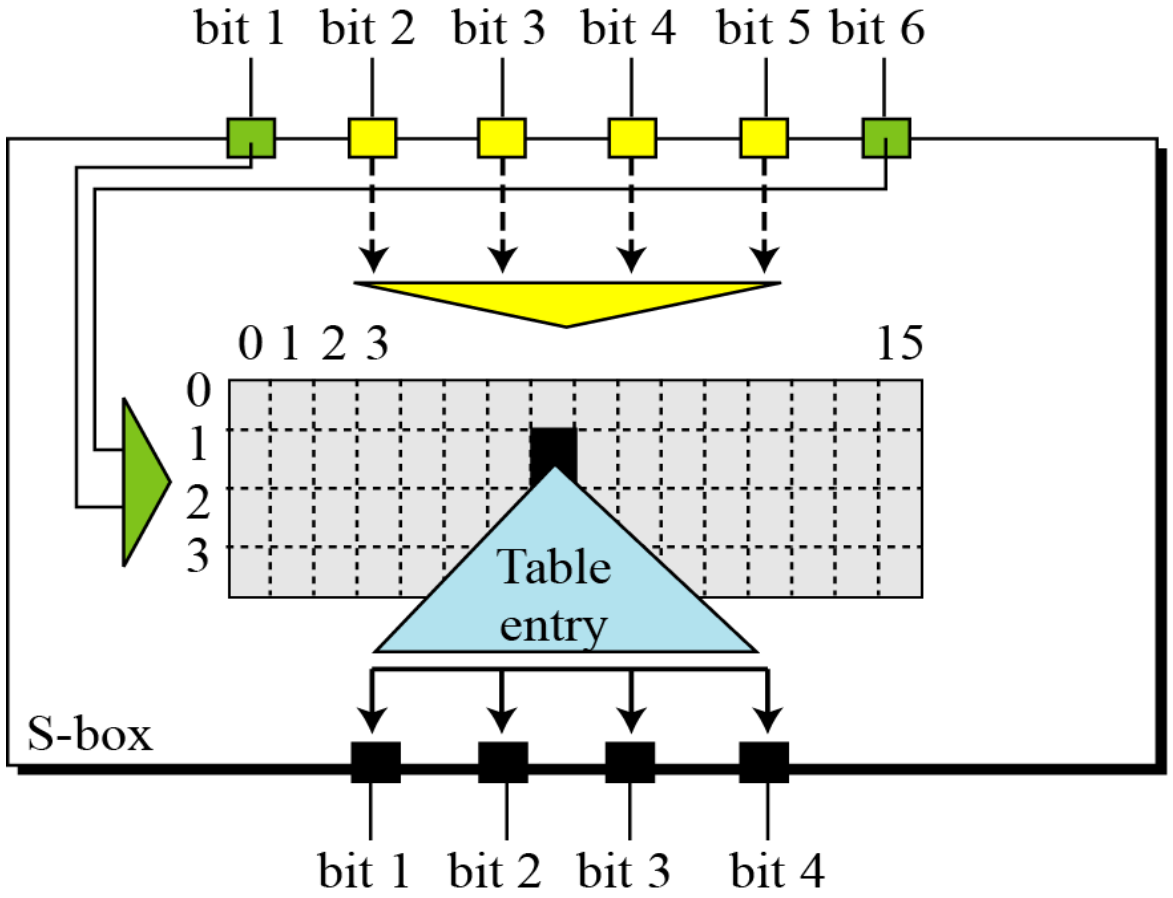
B(6 bit long)= $b_1 b_2 b_3 b_4 b_5 b_6$

$b_1 b_6 \implies r$ =row of the matrix (2 bits: 0,1,2,3)

$b_2 b_3 b_4 b_5 \implies c$= column of the matrix (4 bits: 0,1,2,3,…,15)

C(4 bit long)= Binary representation of S(r,c)

Data Encryption Standard (DES)



Data Encryption Standard (DES)

- Example

Row #	S_1	1	2	3	...	7							15	Column #
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S(i, j) <16, can be represented with 4 bits

Example 1: B=10111

$b_1 b_6 = 11$ =row 3

$b_2 b_3 b_4 b_5$= 0111=column 7

C(4 bit long)= Binary representation of S(r,c)=0111

Example 2: B=011011 ?

Data Encryption Standard (DES)

Feistel Network

S_5	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

Data Encryption Standard (DES)

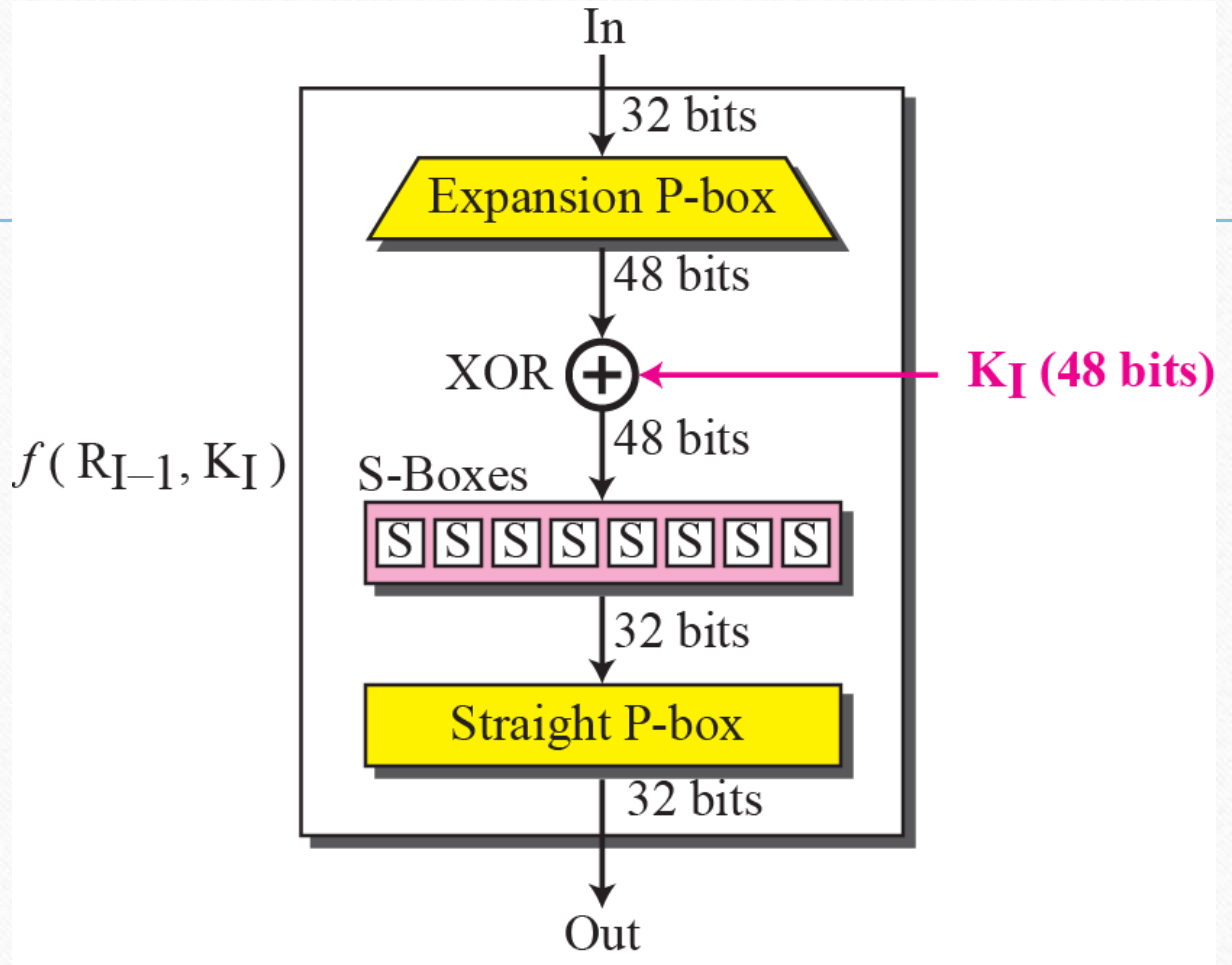
- Feistel Network

4. Permutation: Finally, the 32 outputs from the S-boxes are rearranged according to a fixed permutation, the P-box.

- This is designed so that after expansion, each S-box's output bits are spread across 6 different S-box in the next round.

Data Encryption Standard (DES)

DES Function



Data Encryption Standard (DES)

Key Generation

- How the 56-bit key is used.
- Initially, the key is passed through a permutation function.
- Then, for each of the sixteen rounds, a *subkey* (K_i) *is produced by the combination of a left* circular shift and a permutation.
- The permutation function is the same for each round, but a different subkey is produced because of the repeated shifts of the key bits.

Data Encryption Standard (DES)

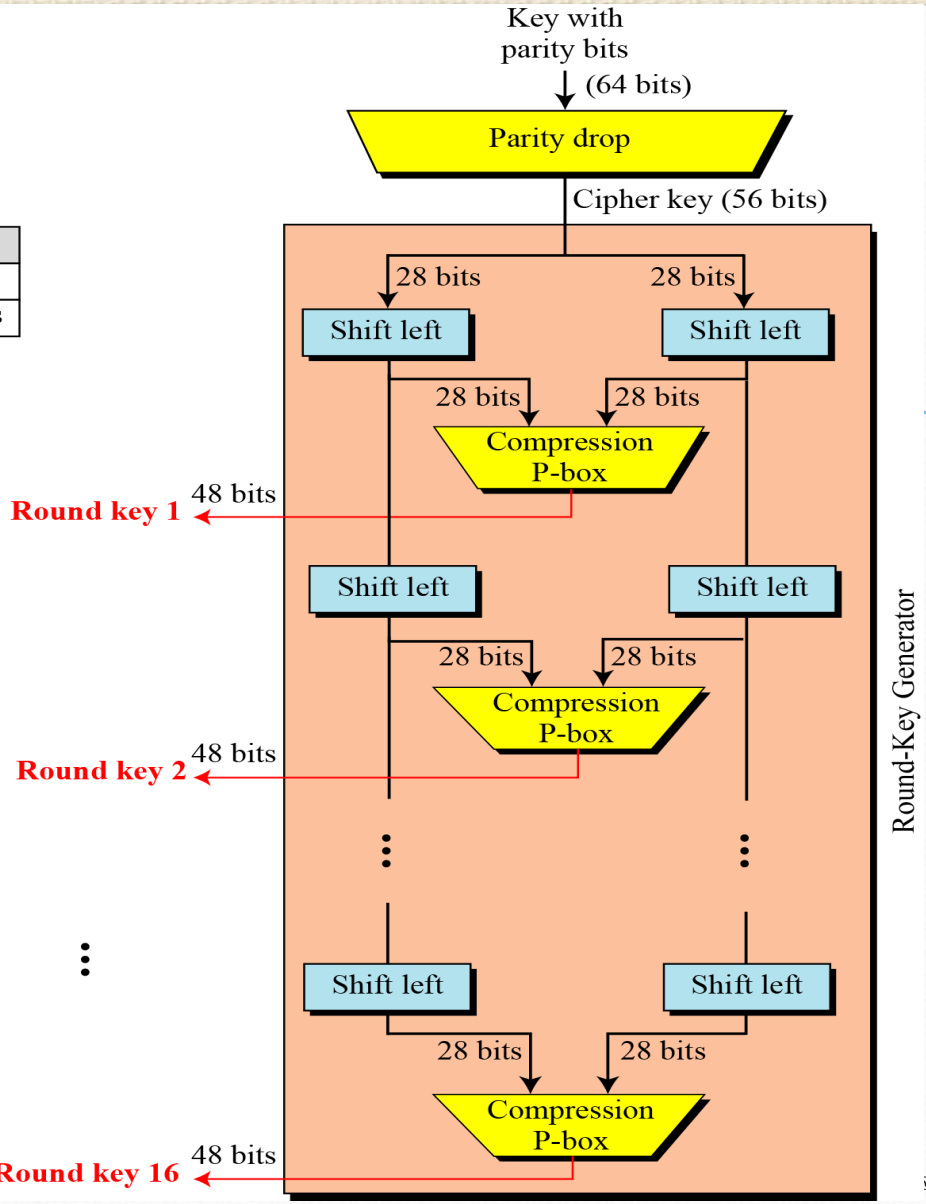
Key Generation

- The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key.

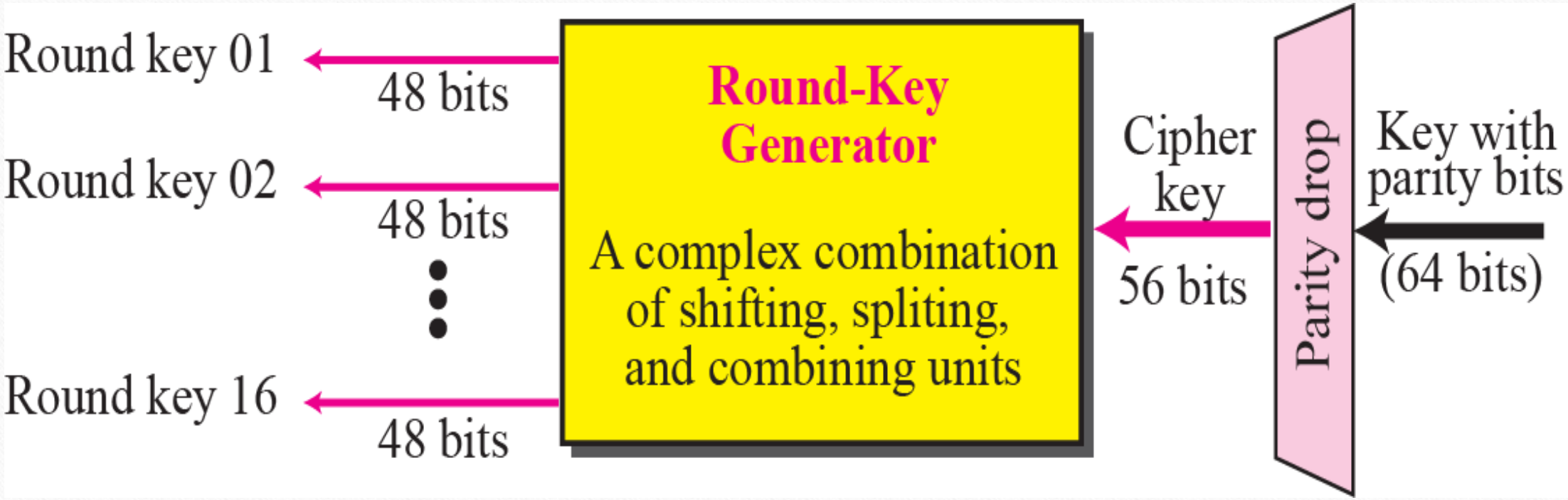
DES Key Generation

Shifting

Rounds	Shift
1, 2, 9, 16	one bit
Others	two bits



Data Encryption Standard (DES)

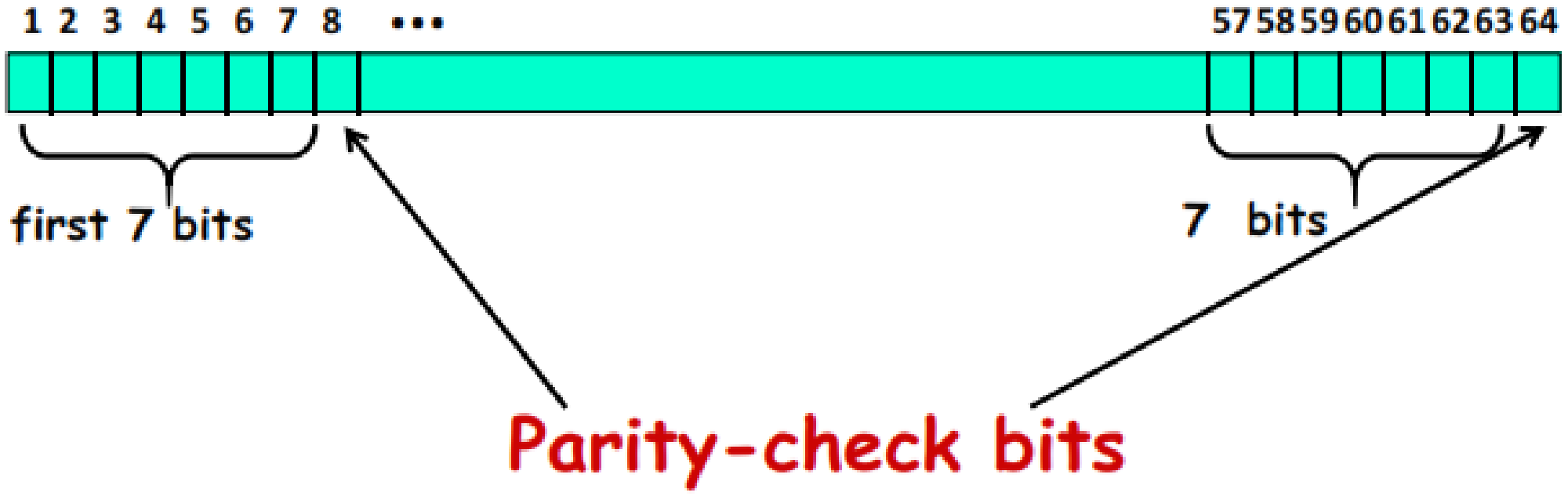


Key Generation

Key Generation

In the DES specification, the key length is 64 bit:

- 8 bytes; in each byte, the 8th bit is a parity-check bit



Each parity-check bit is the XOR of the previous 7 bits

DES Decryption

The decryption process with DES is essentially the same as the encryption process and is as follows:

- Use the ciphertext as the input to the DES algorithm but use the keys K_i in reverse order. That is, use K_{16} on the first iteration, K_{15} on the second until K_1 which is used on the 16th and last iteration.

Data Encryption Standard (DES)

Summary

- The basic operation is as follows:
- Split the plaintext block into two equal pieces, (L_0, R_0)

1. Apply a fixed Initial permutation "IP" to the input block

$$(L_0, R_0) \leftarrow IP(Input\ block)$$

2. Iterate the following 16 rounds

$$L_i \leftarrow R_{i-1}$$

$$\mathrm{R_i} \leftarrow L_{i-1} \oplus f(R_{i-1}, k_i)$$

3. The results from round 16 (L_{16}, R_{16}) is input into the inverse of IP to cancel the effects of the IP. The o/p from this step is the o/p of the DES algorithm i.e.

$$Output\ block \leftarrow IP^{-1}(L_{16}, R_{16})$$

Avalanche Effect

- Desirable property of any encryption algorithm is that a small change in either plaintext or key should produce significant changes in the ciphertext.
- DES exhibits a strong avalanche effect.

Avalanche Effect

(a) Change in Plaintext		(b) Change in Key	
Round	Number of bits that differ	Round	Number of bits that differ
0	1	0	0
1	6	1	2
2	21	2	14
3	35	3	28
4	39	4	32
5	34	5	30
6	32	6	32
7	31	7	35
8	29	8	34
9	42	9	40
10	44	10	38
11	32	11	31
12	30	12	33
13	30	13	28
14	26	14	26
15	29	15	34
16	34	16	35

Lecture Outline

Symmetric ciphers

- Block cipher principles
- Feistel Cipher
- Data Encryption Standard (DES)
- Triple DES

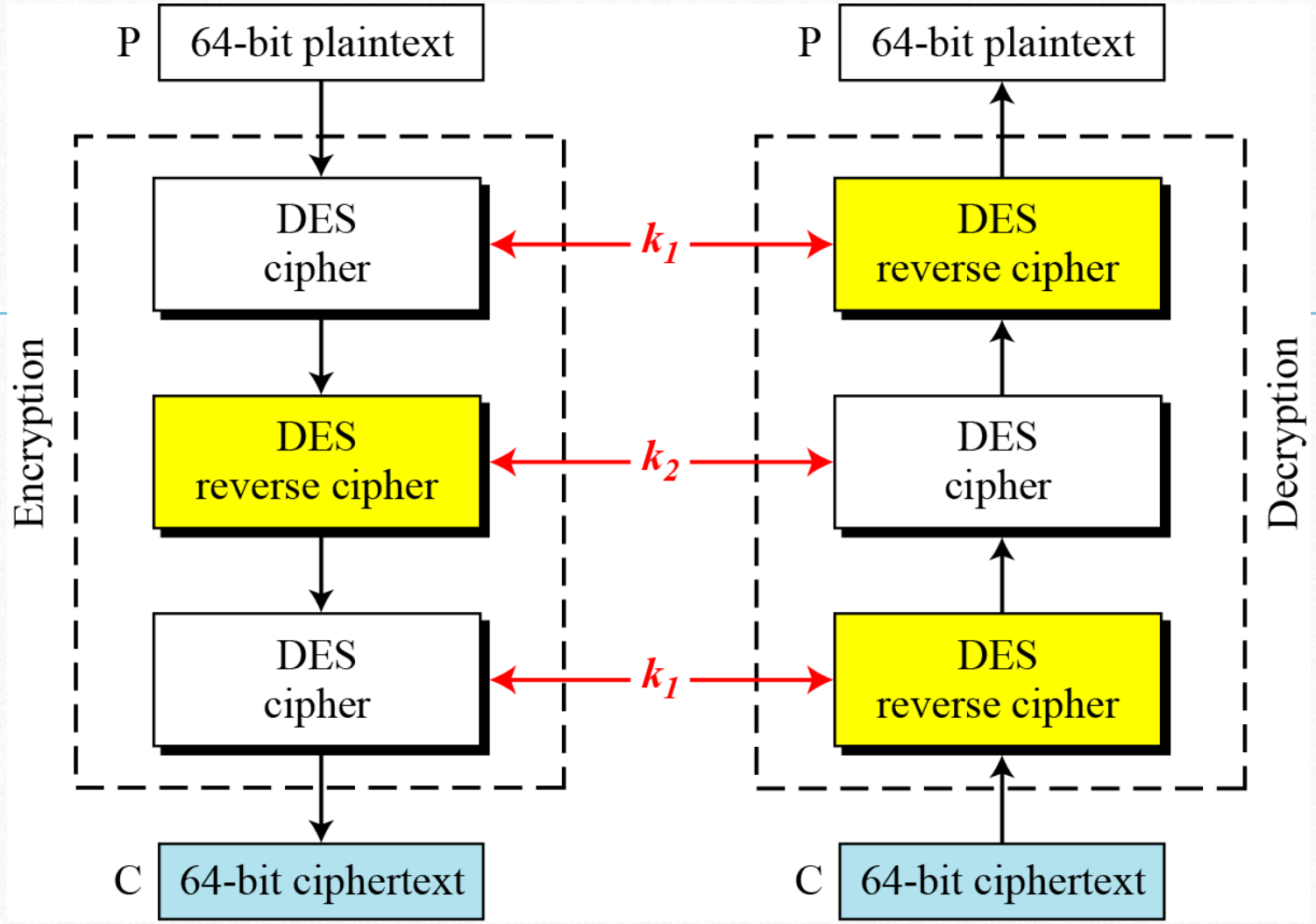
Triple DES

- The main disadvantage of DES is that it has a short key making it more prone to brute force attack.
- A soln. to overcoming this limitation is to run the DES algorithm a multiple number of times using different keys in a proposal called triple DES (encryption –decryption-encryption)

$$C \leftarrow E_{k_1}(D_{k_2}\left(E_{k_1}(m)\right))$$

$$m \leftarrow D_{k_1}\left(E_{k_2}\left(D_{k_1}(c)\right)\right)$$

Triple DES


P
64-bit plaintext
DES cipher
DES reverse cipher
DES cipher
C
64-bit ciphertext
Encryption
k_1
k_2
k_1
P
64-bit plaintext
DES reverse cipher
DES cipher
DES reverse cipher
C
64-bit ciphertext
Decryption

Triple DES

Result:

- Achieves the effect of enlarging the key space.
- The scheme also achieves easy compatibility with single DES if $k_1 = k_2$ is used.
- It can also use three different keys but this way is not compatible with single key DES.

Assignment

1. Discuss in detail the major concerns/weaknesses of DES that may make it unsuitable for cryptography (10 marks)
2. Describe RC5 in terms of (20 marks)
   - History
   - Working Principles
   - Key scheduling algorithm
   - Pseudo-random key generation algorithm
   - Encryption and decryption
   - Advantages and disadvantages


BREAK