Cryptographic System

Symmetric cryptography

- In this type, the encryption and decryption process uses the same key. It is also called as **secret key cryptography**.
- The main features of symmetric cryptography are as follows –
  - It is simpler and faster.
  - The two parties exchange the key in a secure way.

Drawback

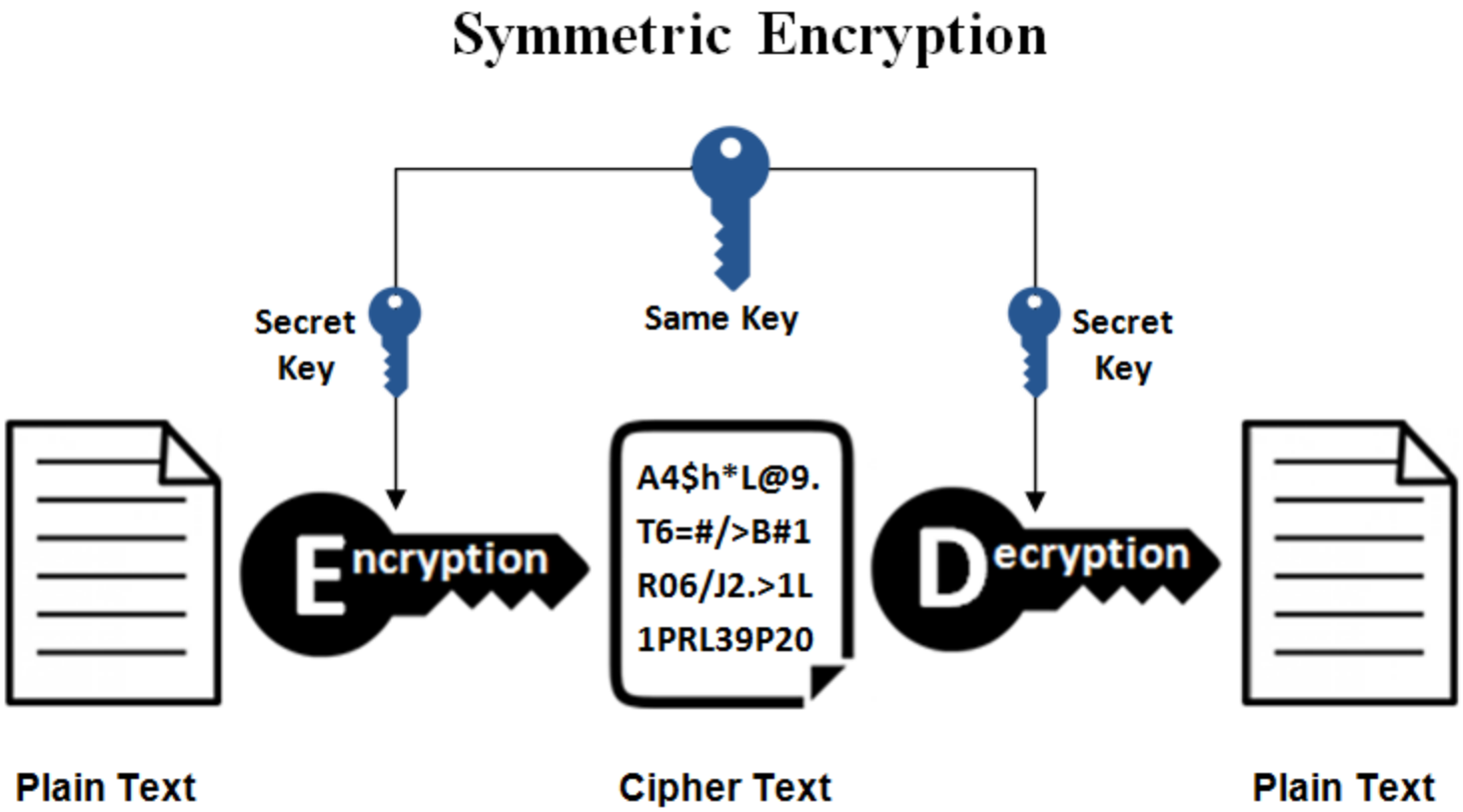
- The major drawback of symmetric cryptography is that if the key is leaked to the intruder, the message can be easily changed and this is considered as a risk factor.

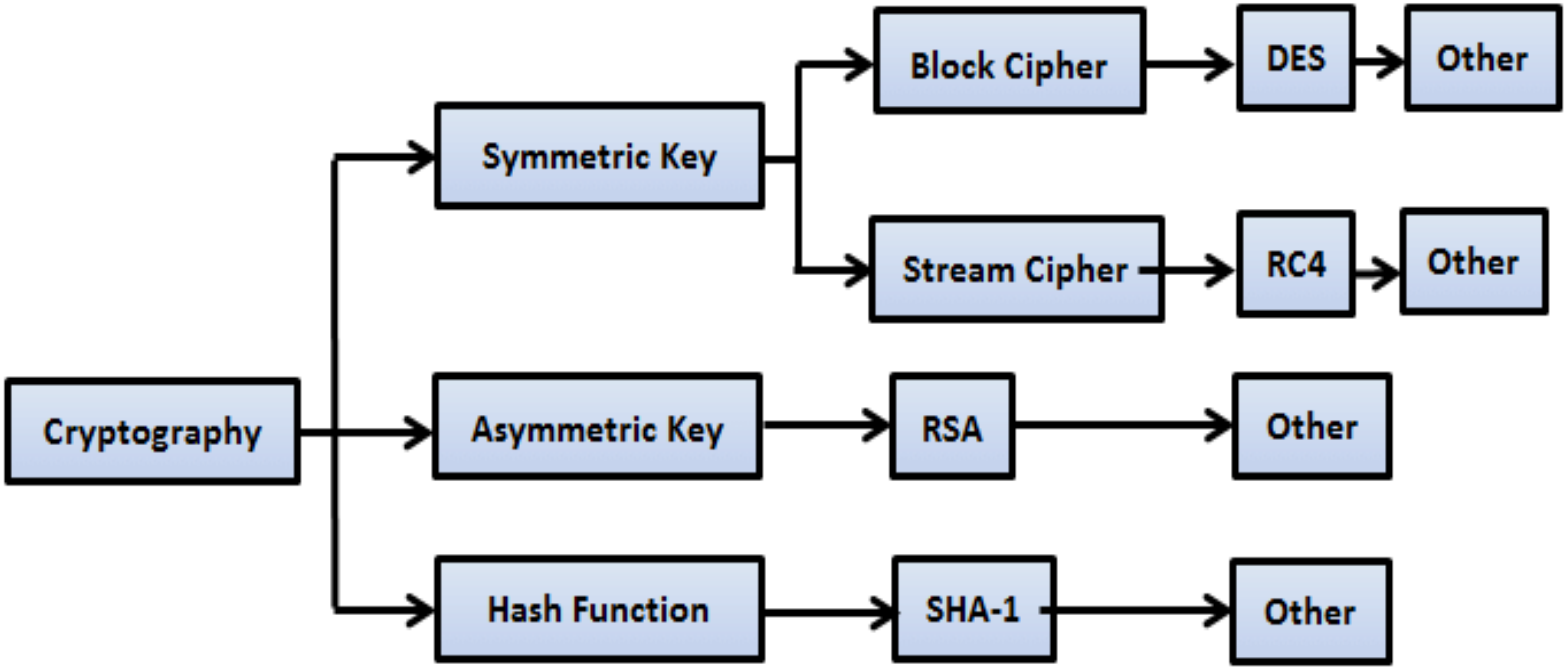
Symmetric encryption is also referred to as *private-key* encryption and *secure-key* encryption.

symmetric encryption algorithms include:

- AES (Advanced Encryption Standard)
- **DES** (**Data Encryption Standard**)
- IDEA (International Data Encryption Algorithm)
- **Blowfish** (Drop-in replacement for **DES** or IDEA)
- RC5 (Rivest Cipher 5)
- RC6 (Rivest Cipher 6)

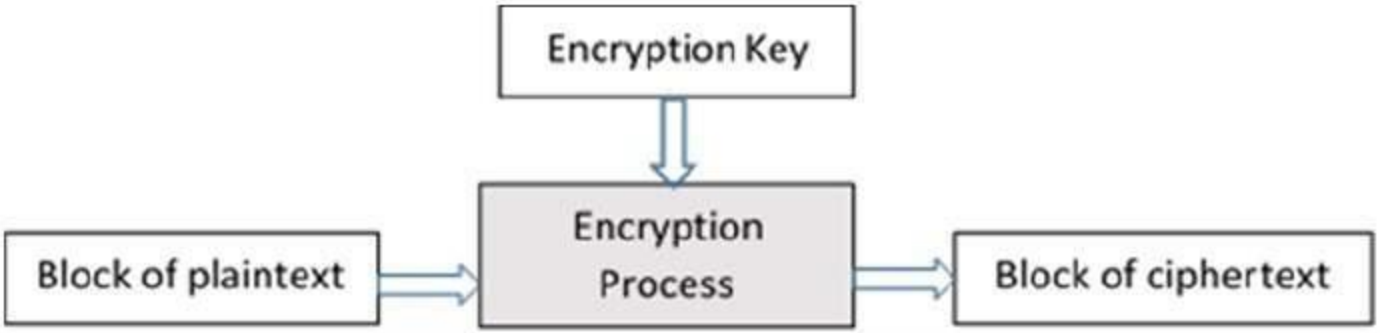
- There are two types of symmetric encryption algorithms:
- **Block algorithms** are used to encrypt blocks of electronic data. Specified set lengths of bits are altered, while continuing to use the designated private key. This key is then used for each block.
- As the data is being encrypted, the system holds the data in its memory as it waits for complete blocks.
- **Stream algorithms.** Data is encrypted as it streams instead of being retained in the system's memory.


Symmetric Encryption
Secret Key
Same Key
Secret Key
Encryption
A4$h*L@9.
T6=#/>B#1
R06/J2.>1L
1PRL39P20
Decryption
Plain Text
Cipher Text
Plain Text


Cryptography
Symmetric Key
Block Cipher
DES
Other
Stream Cipher
RC4
Other
Asymmetric Key
RSA
Other
Hash Function
SHA-1
Other

Block Cipher

A block cipher takes a block of plaintext bits and generates a block of ciphertext bits, generally of same size. The size of block is fixed in the given scheme. The choice of block size does not directly affect to the strength of encryption scheme. The strength of cipher depends up on the key length.



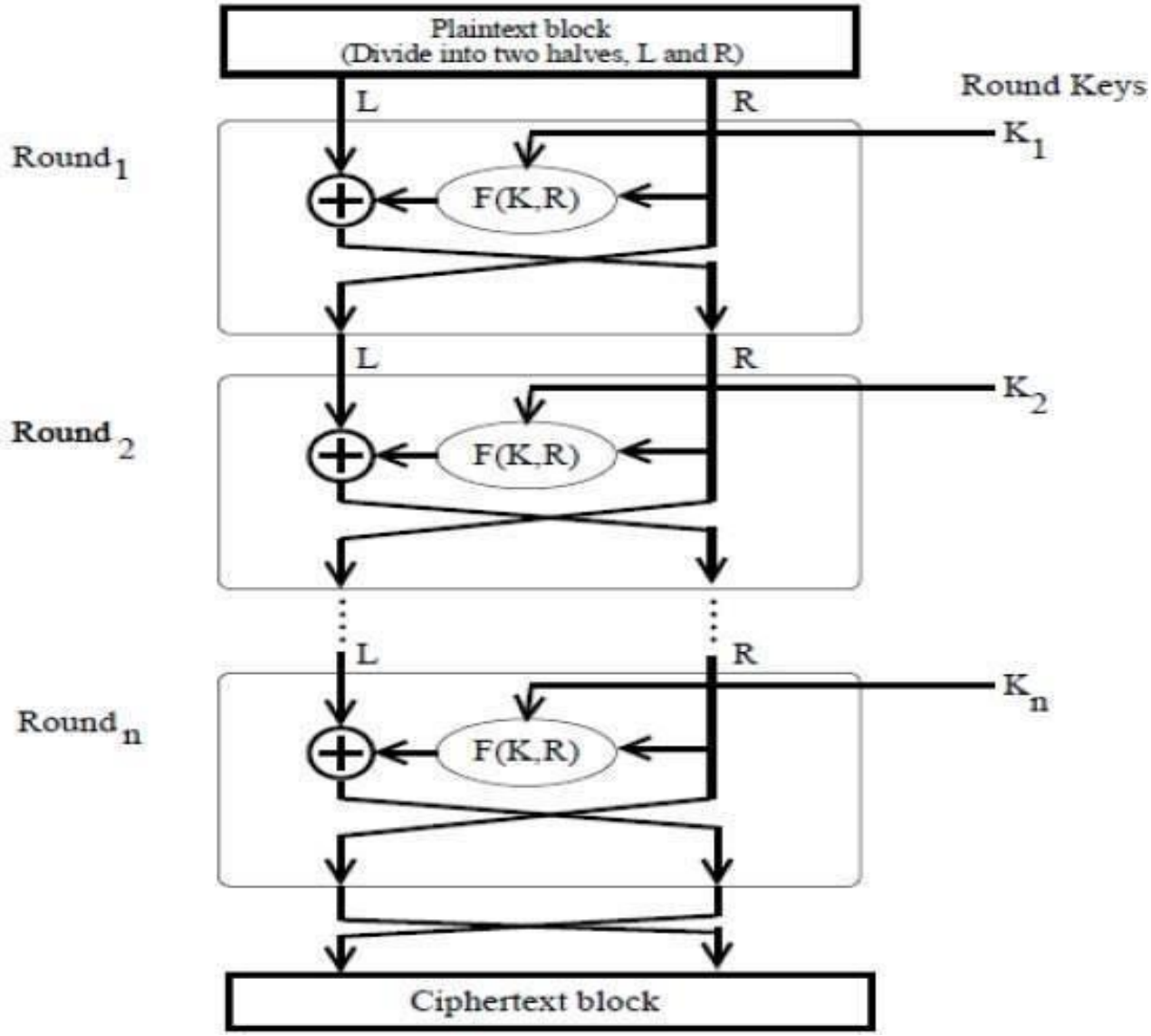
Block Cipher Schemes

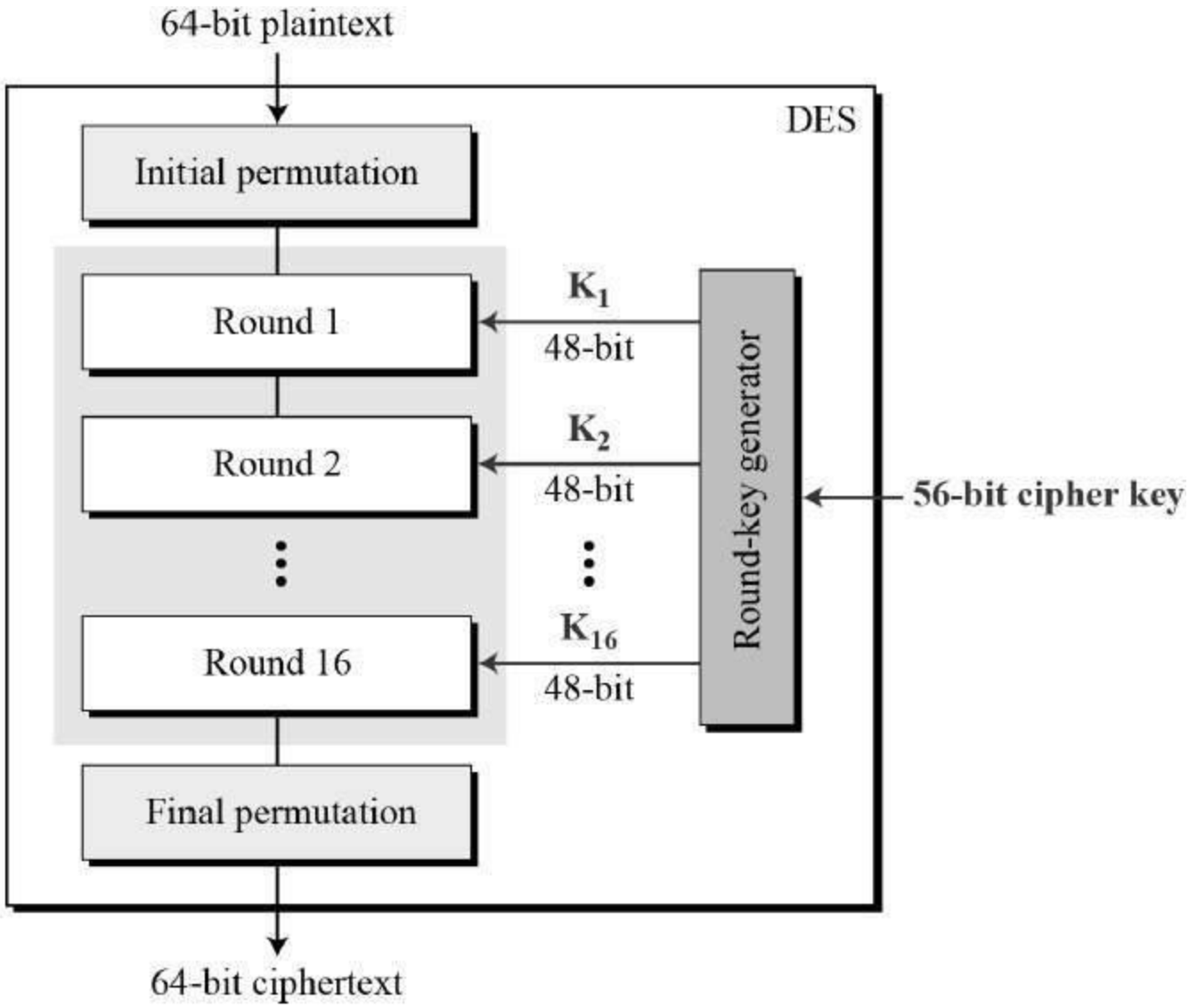
- There is a vast number of block ciphers schemes that are in use. Many of them are publically known. Most popular and prominent block ciphers are listed below.

- **Data Encryption Standard (DES)** – The popular block cipher of the 1990s. It is now considered as a 'broken' block cipher, due primarily to its small key size.
- **Triple DES** – It is a variant scheme based on repeated DES applications. It is still a respected block ciphers but inefficient compared to the new faster block ciphers available.
- **Advanced Encryption Standard (AES)** – It is a relatively new block cipher based on the encryption algorithm **Rijndael** that won the AES design competition.
- **IDEA** – It is a sufficiently strong block cipher with a block size of 64 and a key size of 128 bits. A number of applications use IDEA encryption, including early versions of Pretty Good Privacy (PGP) protocol. The use of IDEA scheme has a restricted adoption due to patent issues.
- **Twofish** – This scheme of block cipher uses block size of 128 bits and a key of variable length. It was one of the AES finalists. It is based on the earlier block cipher Blowfish with a block size of 64 bits.

Data Encryption Standard

- The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).
- DES is an implementation of a Feistel Cipher.
- It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).
- General Structure of DES is depicted in the following illustration –


Plaintext block
(Divide into two halves, L and R)
Round Keys
L
R
Round 1
K1
F(K,R)
L
R
Round 2
K2
F(K,R)
L
R
Round n
Kn
F(K,R)
Ciphertext block

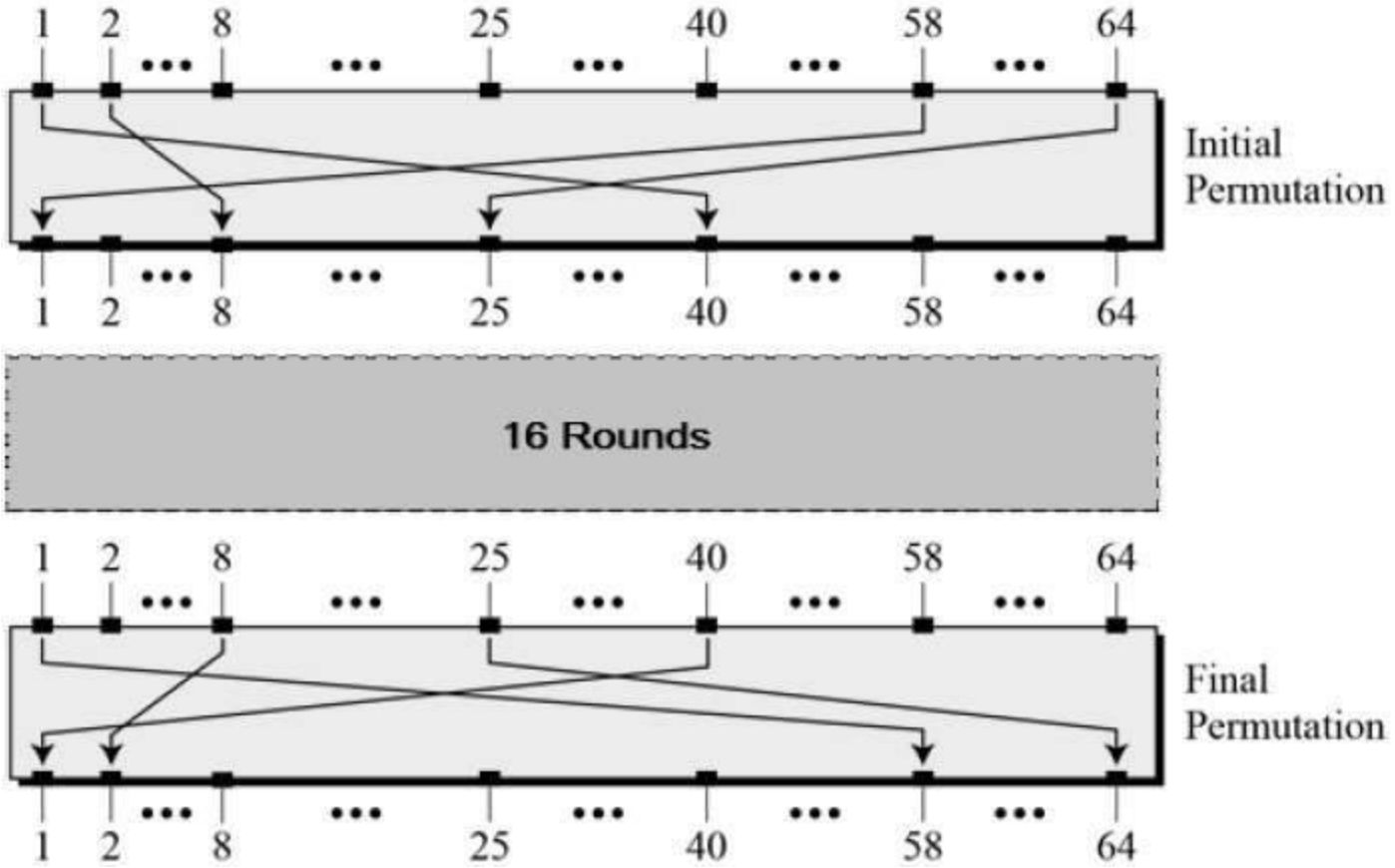

64-bit plaintext
DES
Initial permutation
Round 1
Round 2
Round 16
Final permutation
K_1
48-bit
K_2
48-bit
K_{16}
48-bit
Round-key generator
56-bit cipher key
64-bit ciphertext

Since DES is based on the Feistel Cipher, all that is required to specify DES is −

- Round function
- Key schedule
- Any additional processing − Initial and final permutation

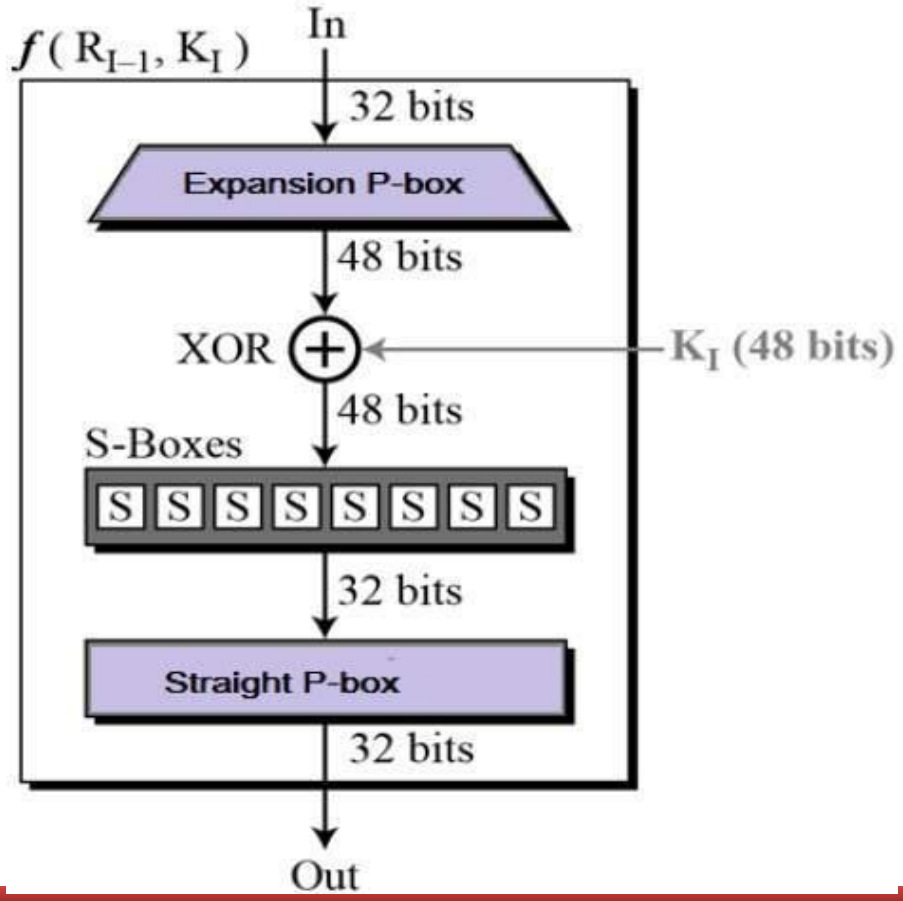
Initial and Final Permutation

- The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other.
- They have no cryptography significance in DES. The initial and final permutations are shown as follows −


1 2 8 25 40 58 64
Initial Permutation
1 2 8 25 40 58 64
16 Rounds
1 2 8 25 40 58 64
Final Permutation
1 2 8 25 40 58 64

Round Function

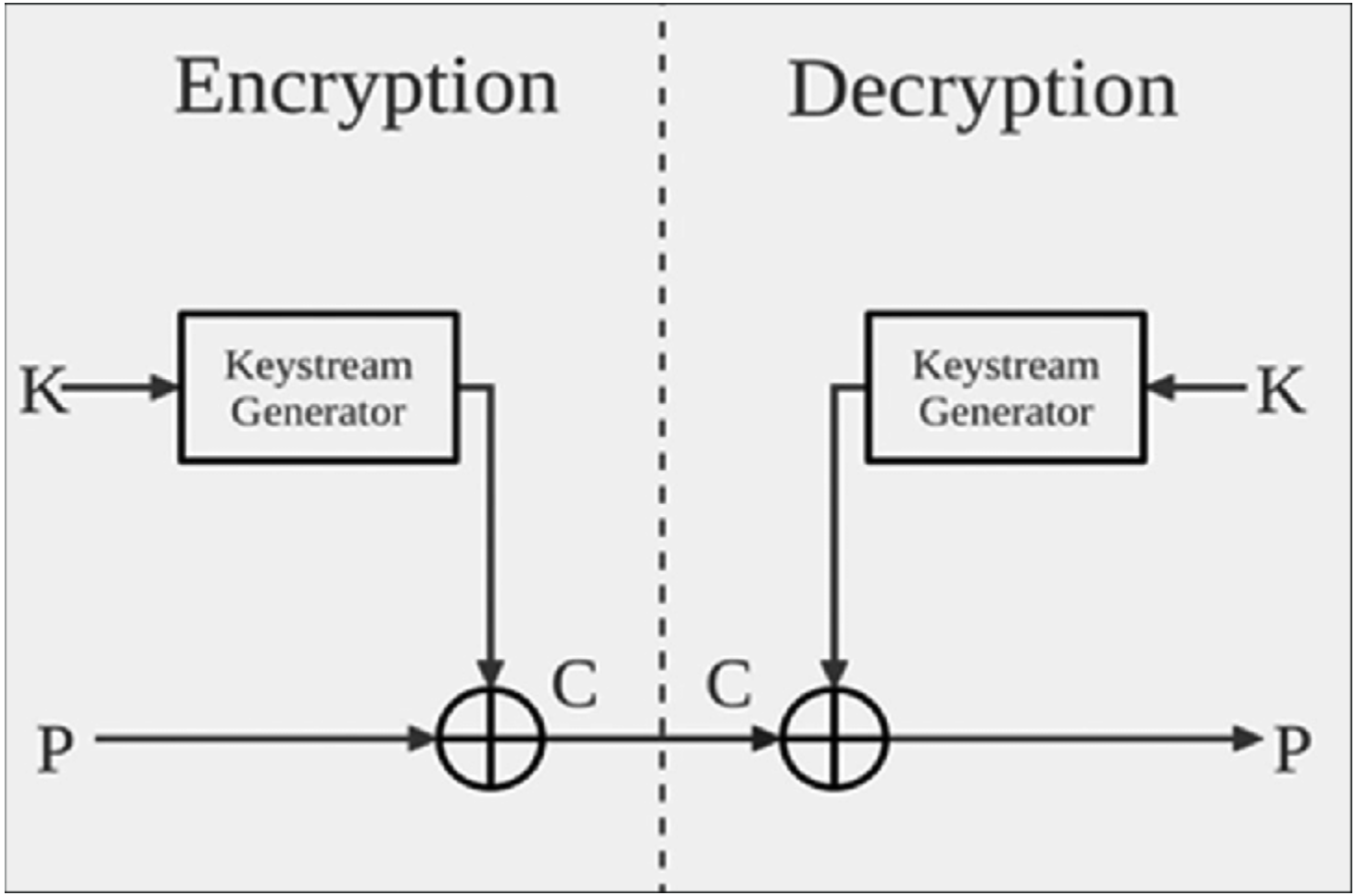
– The heart of this cipher is the DES function, *f*. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output



Stream cipher

- A **stream cipher** is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (key stream).
- In a stream cipher, each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the ciphertext stream.
- Since encryption of each digit is dependent on the current state of the cipher, it is also known as ***state cipher***.

Stream cipher structure



S.NO	BLOCK CIPHER	STREAM CIPHER
1.	Block Cipher Converts the plain text into cipher text by taking plain text's block at a time.	Stream Cipher Converts the plain text into cipher text by taking 1 byte of plain text at a time.
2.	Block cipher uses either 64 bits or more than 64 bits.	While stream cipher uses 8 bits.
3.	The complexity of block cipher is simple.	While stream cipher is more complex.
4.	Block cipher Uses confusion as well as diffusion.	While stream cipher uses only confusion.

5.	In block cipher, reverse encrypted text is hard.	While in stream cipher, reverse encrypted text is easy.
6.	The algorithm modes which are used in block cipher are: ECB (Electronic Code Book) and CBC (Cipher Block Chaining).	The algorithm modes which are used in stream cipher are: CFB (Cipher Feedback) and OFB (Output Feedback).
7.	Block cipher works on transposition techniques like Caesar cipher, polygram substitution cipher, etc.	While stream cipher works on substitution techniques like rail-fence technique, columnar transposition technique, etc.
8.	Block cipher is slow as compared to stream cipher.	While stream cipher is fast in comparison to block cipher.

Block Cipher modes of Operation

Encryption algorithms are divided into two categories based on input type, as block cipher and stream cipher.

Block cipher is an encryption algorithm which takes fixed size of input say *b* bits and produces a ciphertext of *b* bits again.

If input is larger than *b* bits it can be divided further. For different applications and uses, there are several modes of operations for a block cipher.

Table 6.1 Block Cipher Modes of Operation

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of 64 plaintext bits is encoded independently using the same key.	• Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext.	• General-purpose block-oriented transmission • Authentication
Cipher Feedback (CFB)	Input is processed *s* bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	• General-purpose stream-oriented transmission • Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding encryption output, and full blocks are used.	• Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	• General-purpose block-oriented transmission • Useful for high-speed requirements

Table 1. Comparison between different modes of operation

Evaluation criteria	ECB	CBC	CTR	CCM	CC
Chain dependency	No	Yes	No	No	Yes
Error propagation	No	One block	No	No	One block
Authentication code	No	Yes	No	Yes	Yes
Confidentiality	Yes	Yes	Yes	Yes	Yes
Number of passes	One	One	One	Two	Two
Parallelism	Yes	No	Yes	No	Yes
implementing nonce	No	No	Could be	Yes	No, but could be in the counter
Message size	Any	Any	Any	Fixed	Any
Block cipher algorithm	Any	Any	Any	only with 128-bit block size algorithms	Any

ECB=electronic code book, CBC=cipher block chaining, CTR=counter, CCM=counter mode with the CBC-MAC mode, CC=counter chain.


Thank You