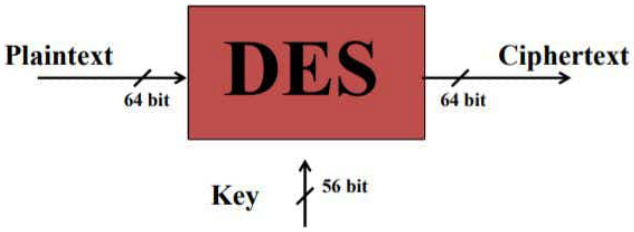
Data Encryption Standard (DES)

- The most widely used encryption scheme is based on the Data Encryption Standard (DES) adopted in 1977 by the National Bureau of Standards, now the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46)
- The algorithm itself is referred to as the Data Encryption Algorithm (DEA)
- For DES, data are encrypted in **64-bit blocks using a 56-bit key**
- The algorithm transforms 64-bit input in a series of steps into a 64-bit output
- The same steps, with the same key, are used to reverse the encryption

DES Features

- Features:
  - Block size = 64 bits
  - Key size = 56 bits (in reality, 64 bits, but 8 are used as parity-check bits for error control, see next slide)
  - Number of rounds = 16
  - 16 intermediary keys, each 48 bits



DES Encryption

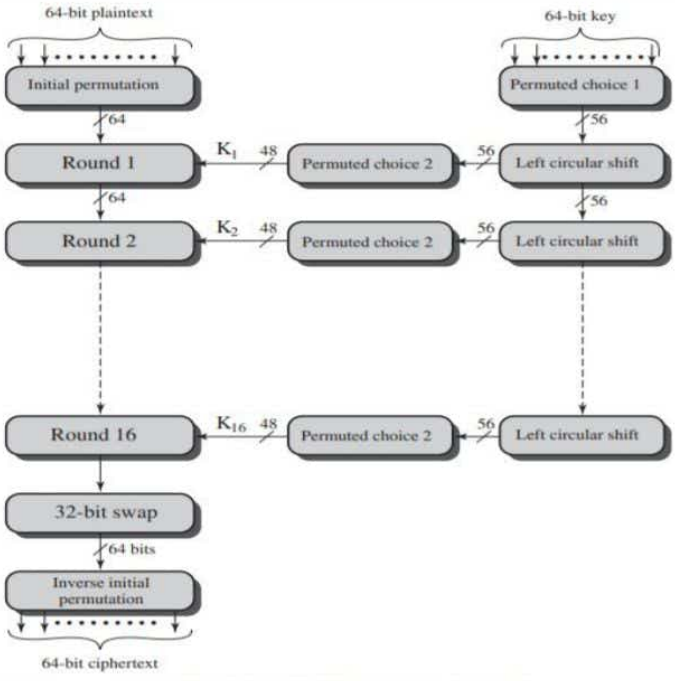
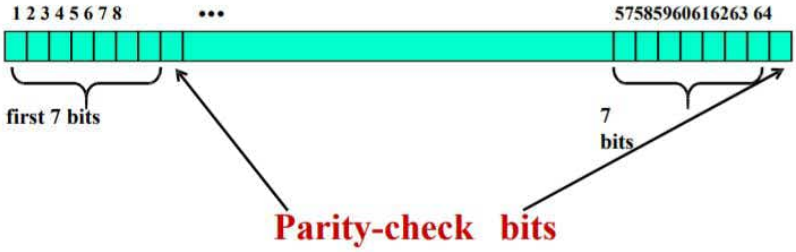


Figure General Depiction of DES Encryption Algorithm

Key length in DES

- 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

(a) Initial Permutation (IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

(b) Inverse Initial Permutation (IP^{-1})

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

(c) Expansion Permutation (E)

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

(d) Permutation Function (P)

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

DETAILS OF SINGLE ROUND

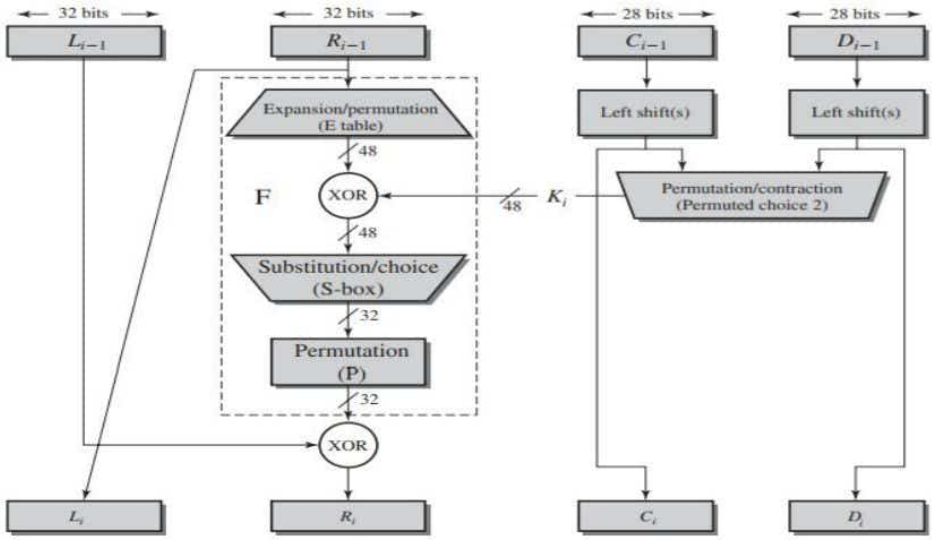


Figure Single Round of DES Algorithm

DES Decryption

- A change in one bit of the plaintext or one bit of the key should produce a change in many bits of the cipher text is known as the **Avalanche Effect**

- The statistical structure of the plaintext is dissipated into long-range statistics of the cipher text is called **Diffusion**

Strength of DES

- **The Use of 56-Bit Keys - With a key length of 56 bits, there are 256** possible keys, which is approximately 7.2 * 1016 keys. Thus a brute-force attack appears impractical.
- DES finally and definitively proved insecure in July 1998, when the Electronic Frontier Foundation (EFF) announced that it had broken a DES encryption using a special-purpose "DES cracker" machine that was built for less than $250,000.

The attack took less than three days.

- The Nature of the DES Algorithm - cryptanalysis is possible by exploiting the characteristics of the DES algorithm.
- A timing attack is one in which information about the key or the plaintext is obtained by observing how long it takes a given implementation to perform decryptions on various ciphertexts.
- A timing attack exploits the fact that an encryption or decryption algorithm often takes slightly different amounts of time on different inputs.