Introduction to Information Security

Dr. Ashok Kumar Das

IEEE Senior Member
Associate Proofessor
Center for Security, Theory and Algorithmic Research
International Institute of Information Technology, Hyderabad

E-mail: *ashok.das@iiit.ac.in*
URL: http://www.iiit.ac.in/people/faculty/ashokkdas
https://sites.google.com/view/iitkgpakdas/

Symmetric-Key Encryption

Principle of Shannon (1945)

- **Diffusion:** The mechanism of diffusion seeks to make the statistical relationship between the plaintext and ciphertext as complex as possible in order to thwart attempts to deduce the key.
  - Diffusion can be achieved by repeatedly performing some permutation on the data followed by applying a function to that permutation.
- **Confusion:** It seeks to make the statistical relationship between the ciphertext and the value of encrypted key as complex as possible in order to thwart attempts to deduce the key.
  - Confusion can be achieved by the use of a complex substitution algorithm.

Symmetric-Key Encryption

The Fiestel Cipher

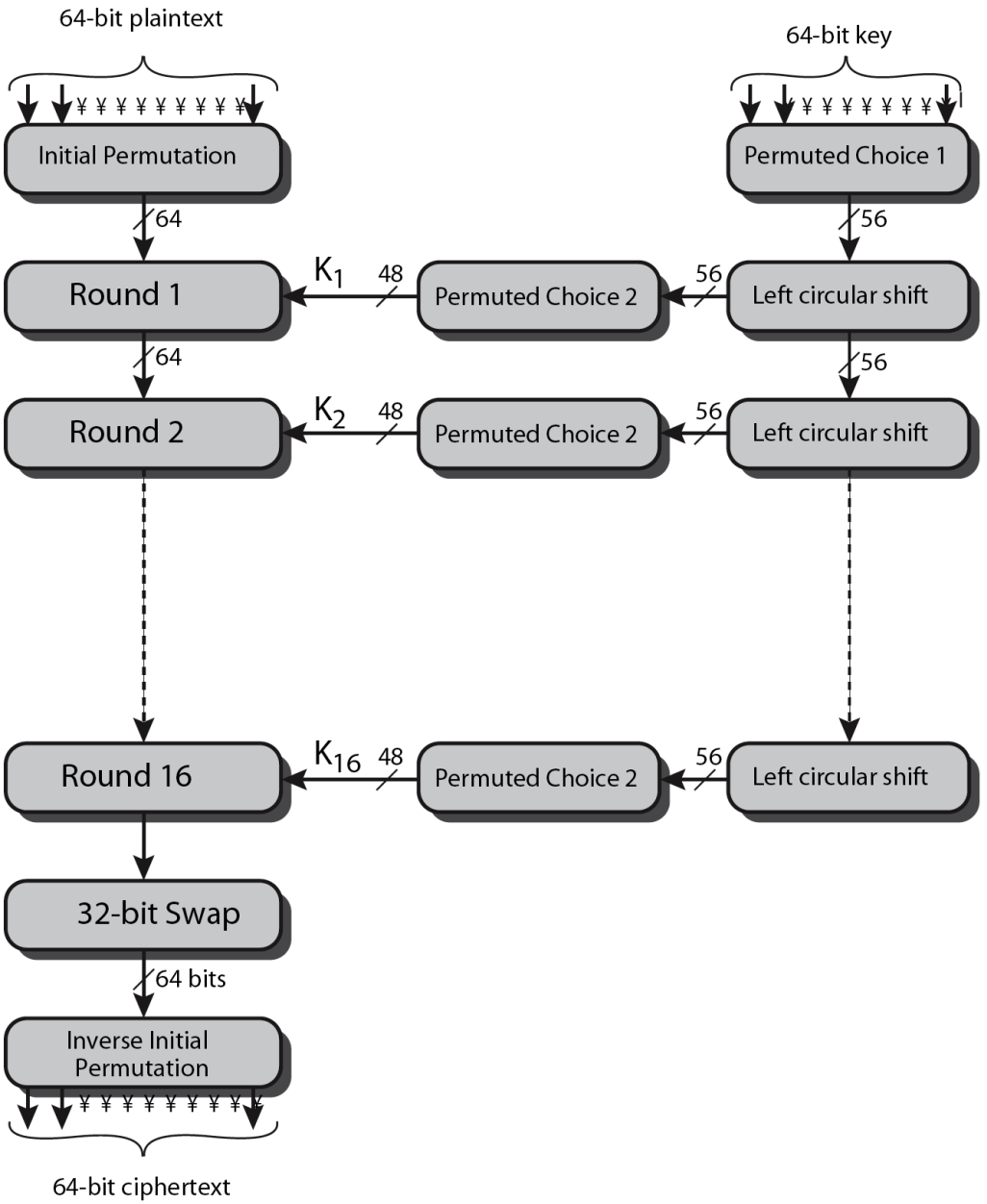
- All modern day block ciphers are based on Fiestel cipher structure.
- Fiestel structure is based on the principle of Shannon (1945): Diffusion and Confusion
- Fiestel structure is useful to construct a SPN (Substitution-Permutation Network) cipher

Symmetric-Key Encryption

Data Encryption Standard (DES)

- The most widely used encryption is based on the Data Encryption Standard (DES) adopted in 1977 by the National Institute of Standards and Technology (NIST), USA.
- For DES, data are encrypted in 64-bit blocks using a 56-bit key.
- The encryption 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 (decryption).
- Mathematically, $DES : \{0,1\}^{64} \times \{0,1\}^{56} \longrightarrow \{0,1\}^{64}$ such that the ciphertext be $C = DES_K(P)$, where $K \in \{0,1\}^{56}$ is the 56-bit key, $P \in \{0,1\}^{64}$ is the plaintext message (block) and $C \in \{0,1\}^{64}$ is the ciphertext block.

Overview of Data Encryption Standard (DES)

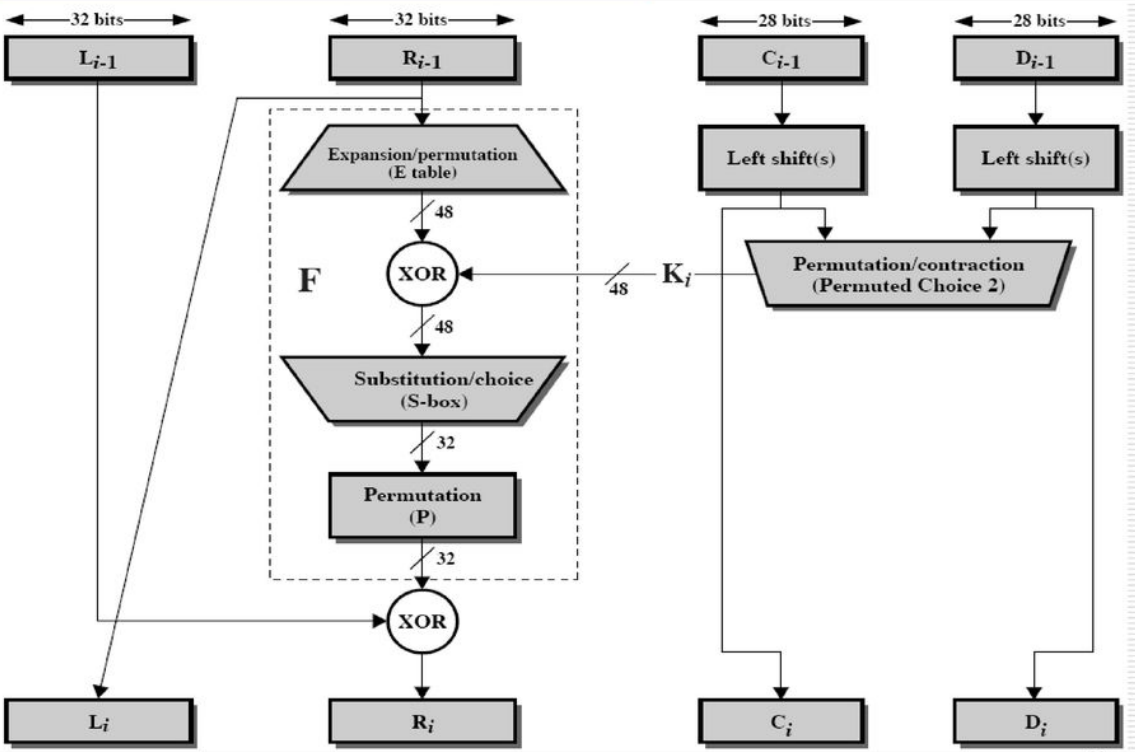


Data Encryption Standard (DES)

- K: given 56 bit key
- K is converted to 64 bit key packed with 8 bit parity: parity 8 bits at positions 8, 16, 24, 32, 40, 48, 56, and 64.
- $K_1, K_2, \cdots, K_{16}$: 16 round keys
- **Schedule of left circular shifts:**

  if (**round number = 1, 2, 9, 16**), then bits_rotated = 1
  else
  bits_rotated = 2

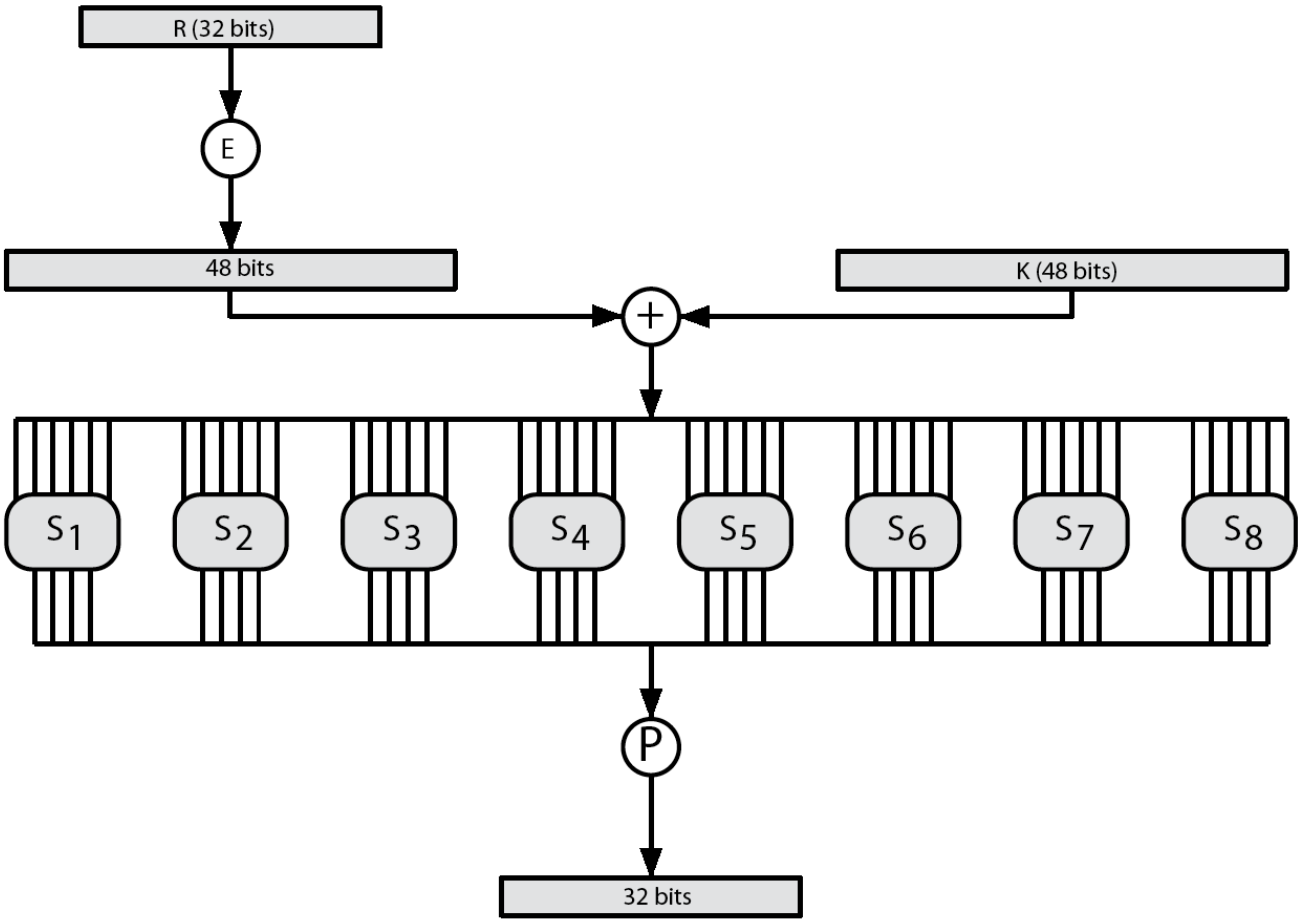
Single Round of DES



$L_i = R_{i-1}$; $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$, $\forall i = 1, 2, \cdots 16$

E: Expansion/permutation; S-Box (S_i)**: Substitution/choice; P: permutation;** L_i **: left half (32 bits) of message;** R_i **: right half (32 bits) of message;** C_i **: left half (28 bits) of key;** D_i **: left half (28 bits) of key.**

Calculation of function $F(R_i, K_i)$ in DES



$F(R_i, K_i) = P(S(E(R_i) \oplus K_i))$

E: Expansion/permutation; S: S-Box; L_i : left half (32 bits) of message; R_i : right half (32 bits) of message; K_i: i^{th} round key.

Initial Permutation (IP) and IP^{-1}

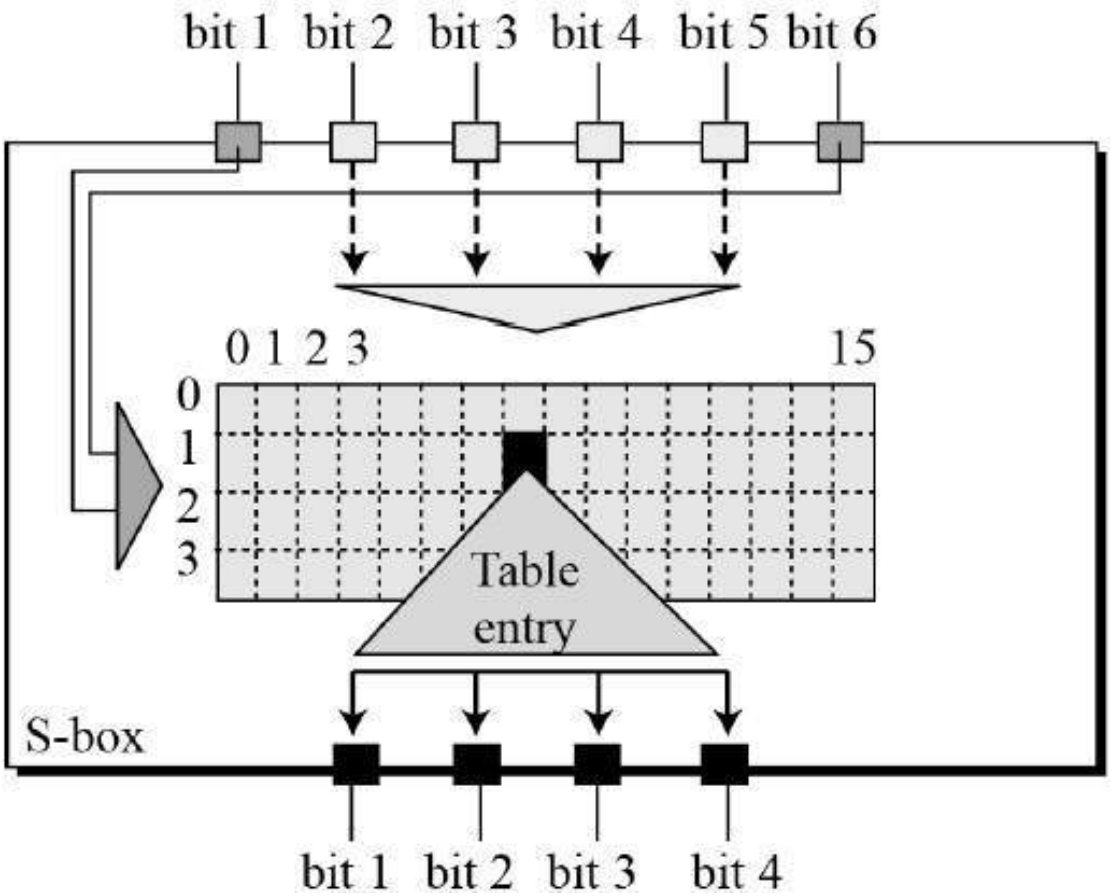
IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

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

E: Expansion/permutation

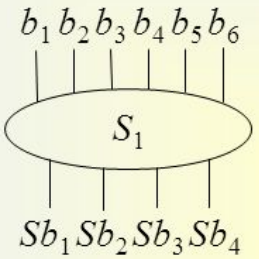
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	28
24	25	26	27	28	29
28	29	30	31	32	1

S-Box Rule


bit 1 bit 2 bit 3 bit 4 bit 5 bit 6
0 1 2 3
15
0
1
2
3
Table entry
S-box
bit 1 bit 2 bit 3 bit 4

S-Box (S_1) Example

S-box (substitution box)



Look-up a value from the table using
$b_1\,b_6$: row
$b_2\,b_3\,b_4\,b_5$: column

$b_1\,b_6$: row — S_1-box table

	Sb_1															
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
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

$b_2\,b_3\,b_4\,b_5$: column

8

Example: Input (6 bits) = 1 1 1 0 0 1; row-index $= b_1\,b_6 =$ **(1 1)**$_2 = 3$;
col-index $= b_2\,b_3\,b_4\,b_5 =$ **(1 1 0 0)**$_2 = 12$;
output = S_1**[row-index][col-index]** $= 10 =$ **(1 0 1 0)**$_2$

DES S-Box Tables

Substitution Boxes S-Boxes

Box	Row	Column 0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1																	
	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_2																	
	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3																	
	0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4																	
	0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5																	
	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
S_6																	
	0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7																	
	0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8																	
	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Data Encryption Standard (DES)

Theorem

Let $DES_{K_1 K_2 \cdots K_{16}}$ denote the DES encryption function, where $K_1, K_2, \ldots, K_{16}$ be the 16 round keys of a given 56-bit input key K. Then, for all plaintext messages $x \in \{0,1\}^{64}$, $DES_{K_{16} K_{15} \cdots K_1}(DES_{K_1 K_2 \cdots K_{16}}(x)) = x$, that is, $DES_{K_{16} K_{15} \cdots K_1}$ becomes the DES decryption function.