P → Plain Text

k → secret key

$Enc(P,k) = P \oplus k = C$

$Dec(C,k) = C \oplus k = P$

Week 03

16/01/2023.

OTP One Time Padding :-

$Pr[message | ciphertext] = Pr[message]$

⇒ OTP on one bit encryption :-

message ← $m \in \{0,1\}$

key ↓ $k \in \{0,1\}$

$Pr[m=0] = P$

$Pr[m=1] = 1-P$

$Pr[k=0] = 1/2$

$Pr[k=1] = 1/2$

Encryption $c = m \oplus k$

$c=0 \Rightarrow \{m=0, k=0\} \cup \{m=1, k=1\}$

$Pr[c=0] = Pr[m=0, k=0] + Pr[m=1, k=1]$

$= P \times 1/2 + (1-P) \times \frac{1}{2}$

$= \frac{P+1-P}{2} = \frac{1}{2}$

$Pr[c=01] = 1 - Pr[c=0]$

$= 1 - 1/2$

$= 1/2$

$Pr[M=m \mid c=c] \stackrel{?}{=} Pr[M=m]$

$\rightarrow Pr(A/B) = \frac{Pr(A \cap B)}{Pr(B)}$

$\rightarrow Pr(A \cap B) = Pr(B/A) \cdot P(A)$

$\Rightarrow Pr[M=0 \mid c=0]$

$= \frac{Pr[M=0 \cap c=0]}{Pr[c=0]}$

$= \frac{Pr[c=0 \mid M=0] \times Pr[M=0]}{1/2}$

$= \frac{\frac{1}{2} \times Pr[M=0]}{1/2}$

$= Pr[M=0]$

- $Pr[M=0 \mid c=0] = Pr[M=0]$

  Thus it provides perfect

Conditions

1) $M_1 \oplus K = C_1$
   $M_2 \oplus K = C_2$
   } this will reveal information on messages.

$C_1 \oplus C_2 = (M_1 \oplus K) \oplus (M_2 \oplus K)$

$= M_1 \oplus M_2$

Cipher text difference will give you message differenace

iii) Len(k) < Len(P)

$$C = P \oplus k$$

Ex: 32-bit message P
16-bit key k

$$P \oplus k = P \oplus \underbrace{0 \ldots 0 k}_{16 \text{ bits}}$$

$$P = P_1 \ldots P_L \quad P_n$$
$$\oplus k = k_1 \ldots k_L k_1 \ldots k_t$$

$$C = \underbrace{(P_1 \oplus k_1)}_{C_1} (P_2 \oplus k_2) \ldots (P_L \oplus k_L) \underbrace{(P_{L+1} \oplus k_L)}_{C_{L+1}} \ldots (P_n \oplus k_t)$$

$$C_1 \oplus C_{L+1} = (P_1 \oplus k_1) \oplus (P_{L+1} \oplus k_1)$$
$$= P_1 \oplus P_{L+1}$$

Information about message is revealed

* OTP is not usable in real life.

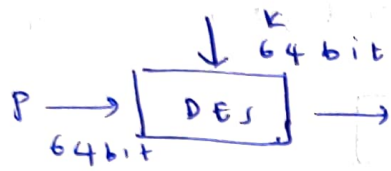
VA Data Encryption standard (DES)

→ It is a block cipher.
→ Designed by IBM

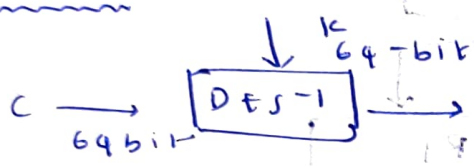
i) Block size = 64 bit
ii) Number of rounds = 16
iii) secret key size = 64 bit with 8 parity check bits.

iv) It is based on Feistel Network.

Encryption



Decryption



☑ Secret key is 64 bit with 8 parity check bits.

0 1 1 0 1 0 1 0 1 1 0 1 0 0 0 1 ... 0 1

Parity check bits (8)

☑ In DES, we have 16 round key

$K_1, K_2, \ldots, K_{16}$

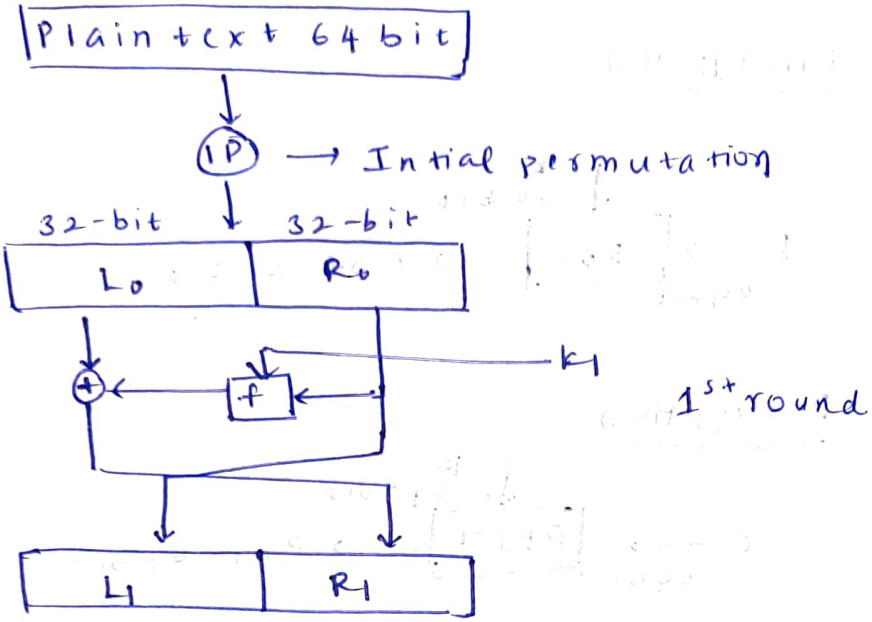
Which are generated using key scheduling algorithm

key scheduling algo will take the secret key as a input

len (k_i) = 48 bit. $\quad g(k) \rightarrow k_1 \ldots k_{16}$

Structure of DES

Encryption



$$f : \{0,1\}^{32} \times \{0,1\}^{48} \longrightarrow \{0,1\}^{32}$$

$$L_{i+1} = R_i$$

$$R_{i+1} = L_i \oplus f(R_i, K_{i+1})$$

We have to learn the following.

i) IP, IP^{-1}

ii) what is f (round function)

iii) How $K_1, \ldots K_{16}$

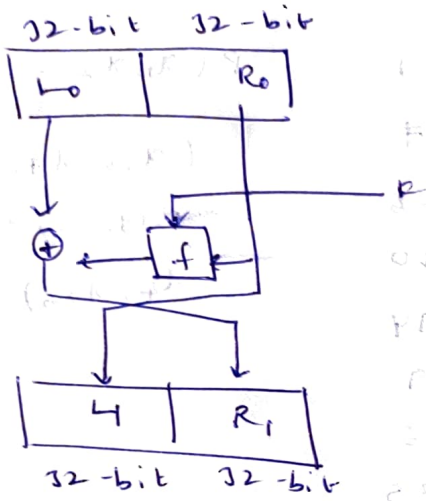
i) IP Intial permutation

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

$IP(m_1, m_2, m_3, \ldots m_{64}) = (m_{58}, m_{50}, m_{42}, \ldots, m_4)$

Round Function of DES :-



$f : \{0,1\}^{32} \times \{0,1\}^{48} \rightarrow \{0,1\}^{32}$

$f(R_i, K_i) = X_i$

where, R_i is 32 bit, K_i is 48 bit, X_i is 32 bit

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

Expansion function...

$$E : \{0,1\}^{32} \longrightarrow \{0,1\}^{48}$$

Substitution function :-

$$S : \{0,1\}^{48} \longrightarrow \{0,1\}^{32}$$

$X : B_1 B_2 \ldots B_8$

$B_i \rightarrow 6$ bit

$S_i : \{0,1\}^6 \longrightarrow \{0,1\}^4 \quad \forall\ i \in (1, 8)$

$S(B_i) = C_i$, $B_i = b_1 b_2 b_3 b_4 b_5 b_6$

$r = (2 * b_1 + b_6)$ $\quad c = (b_2 b_3 b_4 b_5)$

$S_i(B_i) = a_{r,c} \longrightarrow 4$ bit

☑ Permutation P

$$P: \{0,1\}^{32} \rightarrow \{0,1\}^{32}$$

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

$P(x_1, x_2, \ldots, x_{32}) =$

$(x_{16}, x_7, x_{20}, x_{21}, \ldots$
$x_{17}, \ldots, x_{26}, \ldots, x_{22}, x_{11},$
$x_4, x_{25})$

☑ We have to understand the key scheduling Algorithm.

Input: 64 bit key k

Output: 16 round key k_i, $1 \le i \le 16$

$len(k_i) = 48$ bit.

i) v_i, $1 \le i \le 16$ where $v_i = 1$

if $i \in \{1, 2, 9, 16\}$ else $v_i = 2$

ii) Delete the parity check bit. Now key k is 56 bit.

iii) $T = PC1(\tilde{k})$; $PC1: \{0,1\}^{56} \rightarrow \{0,1\}^{56}$

iv) $(C_0, D_0) = T$ where C_0 is of 28 bit,
D_0 is of 28 bit.

v) for $i = 1$ to 16

$C_i = (C_{i-1} \circlearrowleft v_i)$
$D_i = (D_{i-1} \circlearrowleft v_i)$

$\circlearrowleft$ left circular shift.

$K_i = PC2(C_i, D_i)$

$PC2 : \{0,1\}^{56} \rightarrow \{0,1\}^{48}$.

vi) Round keys $= (K_1, K_2, \ldots, K_{16})$

PC1 : $\{0,1\}^{56} \rightarrow \{0,1\}^{56}$

PC1

c_i

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36

d_i

63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	5	28	12	4

$PC1(k_1 k_2, \ldots k_7, k_8, \ldots, k_{64})$

$= (k_{57} k_{49}, \ldots, k_9, k_1, \ldots, k_{36}, \ldots k_{55}, \ldots k_4)$

PC_2 :

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

$\Rightarrow M, \bar{M}, K, \bar{K}$

$FN(M, K) = C_1$

$FN(\bar{M}, \bar{K}) = C_2$

$E^c \oplus E(R^c) = E(R)^c \oplus K^c = E(R) \oplus K$

$P(S(K^c \oplus E(R^c))) = P(S(E(R) \oplus K))$

$L_0 \| R_0 = M \qquad \bar{L_0} \| \bar{R_0} = \bar{M}$

$L_1 = R_0$

$R_1 = L_0 \oplus f(R_0, K)$

$\bar{L_1} = \bar{R_0}$

$\bar{R_1} = \bar{L_0} \oplus f(\bar{R_0}, \bar{K}) = \bar{L_0} \oplus f(R_0, K) =$

$= (L_0 \oplus f(R_0, K))^c = R_1^c$

$C_1 = L_1 \| R_1$

$C_2 = L_1^c \| R_1^c$

$C_2 = C_1^c$