19UCS122

PAGE NO.:

Tutorial 3

Q.1. Explain encryption and decryption in DES.

Ans: DES Encryption:

- 64 bit plaintext pass through initial permutation rearrange bit to produce permuted input.
- Followed by 16 rounds of same function which involves permutation and substitution functions.
- The output of last ~~four~~ round swapped to produce pre-output.
- Preoutput pass through a permutation (IP^{-1})

DES Decryption:

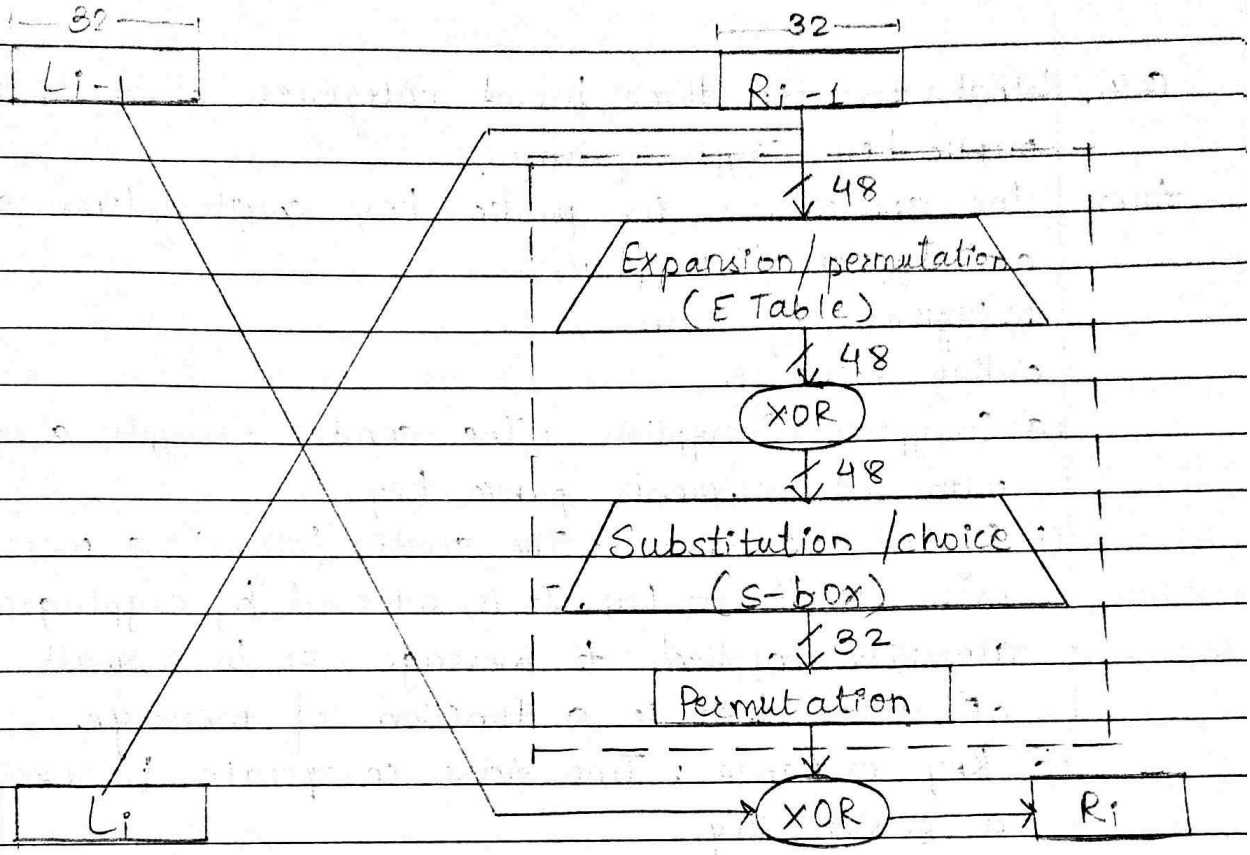
- As with any Fiestel cipher, decryption uses the same algorithm as encryption
- The subkeys are reversed.

Q.2. Explain single round in DES.

Ans:

- Left and right halves of 64 bits are separated into 2*32 bit parts $L_i R_i$
- $L_i = R_i$
- $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$
- R is expanded to 48 bits using permutation E
- Resulting 48 bits are ~~XORED~~ XORed with K_i.
- 48 bit result passes thru substitution function f (8-S-boxes) producing 32-bit output.
- Output is permutted using permutation function.

PAGE NO.:



Q.3. What are the principle elements of public key cryptosystems?

Ans: a) Plaintext: The data to be protected.

b) Encryption Algorithm: It takes plaintext and encryption key as input and produces ciphertext.

c) Ciphertext: The coded message produced by encryption algorithm using the encryption key.

d) Decryption Algorithm: It produces a unique plaintext for any given ciphertext and decryption key.

e) Encryption key: It is a value known to the sender. The sender uses it to compute ciphertext.

f) Decryption key: It is a value known to the receiver. The receiver uses it with ciphertext to compute plaintext.

Q.4. What are the three broad categories of application of public key crypto systems?

Ans: The applications for public-key cryptosystems are-

a) Encryption / Decryption.

b) Digital Signature

c) Key exchange.

(a) Encryption / Decryption : The sender encrypts a message with the recipients public key.

(b) Digital Signature : The sender 'signs' a message with its private key. It is achieved by cryptographics algorithm applied to message or to a small block of data that is a function of message.

(c) Key exchange : Two sides co-operate to exchange a session key.

Q.5. Explain RSA algorithm.

Ans:
- Plaintext is encrypted in blocks
- Block's binary value $2^k < n$
- Equivalently, block size $k \leq \log 2(n)$
- Encryption (plaintext block M, ciphertext C)
  $C = M^e \bmod n$
- Decryption.
  $M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$
- To encrypt a message M the sender:
  - obtains public key of recipient $KU = \{e, N\}$
  - computes: $C = M^e \bmod N$, where $0 \leq M < N$
- To decrypt the ciphertext C the owner:
  - uses their private key $KR = \{d, p, q\}$
  - computes: $M = C^d \bmod N$
- The message M must be smaller than modulus N.

19UCS122

PAGE NO.:

Q.6. Perform encryption and decryption using the RSA algorithm for the following.

a. $p=3, q=11, e=7, M=5$

Ans: $n = p \times q$

$= 3 \times 11 = 33$

$\phi(N) = (p-1)(q-1) = 20$

$d = e^{-1} \bmod \phi(N)$

$= 1/7 \bmod 20 = 3$

$C = M^e \bmod n = 5^7 \bmod 33 = 14 \longrightarrow$ Encryption

$M = C^d \bmod n = 14^3 \bmod 33 = 5 \longrightarrow$ Decryption.

b. $p=5, q=11, e=3, m=9$

Ans: $n = p \times q = 55$

$\phi(N) = (p-1)(q-1) = 4 \times 10 = 40$

$d = e^{-1} \bmod \phi(N) = 27$

$C = M^e \bmod n = 9^3 \bmod 55 = 14 \longrightarrow$ Encryption.

$M = C^d \bmod n = 14^{27} \bmod 55 = 9 \longrightarrow$ Decryption.

c. $p=11, q=13, e=11, M=7$

Ans: $n = p \times q = 143$

$\phi(N) = (p-1)(q-1) = 120$

$d = e^{-1} \bmod \phi(N) = 1/11 \bmod 120 = 11$

public key, $KPU = \{e, n\} = \{11, 143\}$

private key, $KPR = \{d, n\} = \{11, 143\}$

$C = M^e \bmod n = 7^{11} \bmod 143 = 106 \longrightarrow$ Encryption.

$M = C^d \bmod n = 106^{11} \bmod 143 = 7 \longrightarrow$ Decryption.

d. $p=17, q=31, e=7, M=2$.

Ans: $n = p \times q = 17 \times 31 = 527$.

$\phi(N) = (p-1)(q-1) = 480$

$d = e^{-1} \bmod \phi(N)$

$= 1/7 \bmod 480$

$= 343$

$C = M^e \bmod n = 2^7 \bmod 527 = 128 \longrightarrow$ Encryption

$M = C^d \bmod n = 128^{343} \bmod 527 = 2 \longrightarrow$ Decryption

Q.7. In a public key system using RSA you intercept the ciphertext $C = 10$ sent to a user whose public key is $e = 5$, $n = 35$. What is M?

Ans: $C = M^e \bmod n$

$10 = M^5 \bmod 35$

Let $p = 5, q = 7$ then

$n = p \times q = 5 \times 7 = 35$

$\phi(N) = (p-1)(q-1) = 24$

$\gcd(\phi(N), e) = \gcd(24, 5)$

$= 1$ and $1 < e < \phi(N)$

Now $d = e^{-1} \bmod \phi(N)$

$ed = \bmod \phi(N)$

$e = 5, \quad \phi(N) = 24$

$\therefore d = 5$

$KR = \{d, n\} = \{5, 35\}$

RSA : $M = C^d \bmod n$

$= 10^5 \bmod 35 = 5$

To verify correctness,

$C = M^e \bmod n = 5^5 \bmod 35$

$\therefore C = 10$

$\therefore$ Plaintext $M = 5$

PAGE NO.:

Q.8. In RSA, system the public key of given user is $e = 31$, $n = 3599$. What is private key of the user?

Ans: $n = 3599 = 3600 - 1$

$= (60)^2 - 1^2$

$= (60-1)(60+1)$

i.e. 59, 61

$p = 59$, $q = 61$ and $e = 31$

$\phi(N) = (p-1)(q-1)$

$= 58 \times 60$

$= 3480$

$d = e^{-1} \bmod \phi(n)$

$ed = \bmod \phi(n)$

$ed \equiv (\bmod \phi(N)) = 1$

$e = 31$, $\phi(N) = 3480$

So,

$31 \cdot d \cdot \bmod 3480 = 1$

$\therefore d = 3031$

Private key $KR = \{d, n\} = \{3031, 3599\}$