NAME :- KRUNAL RANK

ROLL NO :- U18CO081

CLASS :- BTECH 4TH YEAR

SEMESTER :- 7

DIVISION :- B

Cryptography and Network Security
Tutorial 7

Ans 1:

Symmetric Key Encryption	Assymetric Key Encryption
• It only requires a single key for encryption as well as decryption.	• It requires two keys seperate for encryption and decryption.
• Very fast encryption process.	• Very slow encryption process.
• Used when large amount of data is transferred since cipher text is usually smaller than plain text.	• Used to transfer small amount of data since cipher text is usually larger than plain text.
• Provides confidentiality.	• Provides confidentiality, authentication and non-repudiation.
• Examples: 3DES, AES, DES, etc..	• Examples:- Diffie-Hellman, RSA etc..

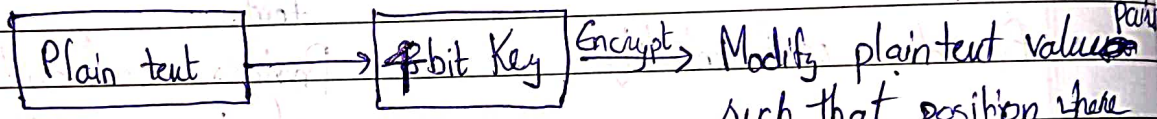
Ans 2: Public Key Cryptography uses two different keys. One key is used to encrypt the information and shared publically. The other key is used to decrypt the information and kept secured with user. This kind of encryption is also known as assymmetric key encryption.

Ans 3: • Diffie Hellman key exchange establishes a shared secret between two parties that can be used for secret communication for exchanging data over public channel.
• The process begins by having two parties, say Alice and Bob, publically agreeing on ~~the~~ an arbitrary starting value that does not need to be kept secret.

- Each person also select a secret value with themselves.
- The crucial part of the process is that Alice and Bob combine their secret with the publically shared value.
- Finally, they combine their own private value with the public value.

The Diffie Hellman key exchange is vulnerable to :-
- man in the middle attack
- Logjam attack

Ans 4:
i)



Example:-
Plain text :- 10100101
Key :- 1001
Make plain text pairs and assign key values :- $\frac{10}{1}$ $\frac{10}{0}$ $\frac{01}{0}$ $\frac{01}{1}$

Modify plain text so that pairs assigned 0 come before pairs assigned 1 :- (in stable) $\frac{10}{0}$ $\frac{01}{0}$ $\frac{10}{1}$ $\frac{01}{1}$

Cipher text :- 10011001

Decrypt in the same way. Assign number of 0's in key to the first number of 0's pairs. Then place those pairs in same location as keys.

ii) Plain text → 4 Bit Key → Encrypt → If Key value is 1, swap pairs values in that pair → Cipher text.

Example:-
Plain text:- 10100110
Key:- 1001
Assign pairs:- 10 10 01 10
values 1 0 0 1
Swap pairs with assigned value :- 01 10 01 01
1 0 0 1

Cipher text:- 01100101

iii) Plain text → 4 bit Key → Encrypt → Shift right by Key times → Cipher text.

Plain text:- 10100100
Key:- 0010 (2)
Cipher text:- 00101001

Sol → Generating Public Key
- Choose 2 large prime numbers P and Q.
- First part of public key $n = P \times Q$
- Choose randomly e such that $1 < e < \phi(n)$ $[\phi(n) = (P-1)(Q-1)]$ and $\gcd(e, n) = 1$.
- Public key :- (n, e)

→ Generating Private Key :-
- Choose d such that d is inverse of e using mod $(\phi(n))$
- ~~Public~~ Private key :- (P, Q, e)

Encryption :- $C = P^e \bmod n$
Decryption :- $P = C^d \bmod n$