Unit-4

1) In RSA algorithm find private key if the public key is (e, n) where p & q are primes with $1<e<\phi(n)$.

2) Using Diffie-Hellman key exchange find the common key 'k' with p=353, α=3, a=97 & b=233.

3) Using RSA algorithm, find the public key if the private key is (7,33) for p=3 and q=11.

4) Define one-way function.

5) Write applications of public key cryptosystems.

6) Define Probabilistic encryption.

7) Using Diffie-Hellman key exchange find the common key 'k' with p=7, α=5, X_A=3 & X_B=4.

8) Define Public-key cryptography.

9) What are the two basic principles of public-key cryptosystem?

10) Define trap-door one-way function.

11) Explain about Public Key Cryptography.

12) Explain about RSA Algorithm.

13) Explain about Diffie-Hellman Key Exchange Algorithm.

14) Explain about Elliptic Curve Cryptosystem.

15) Alice and Bob use the Diffie–Hellman key exchange technique with a common prime q= 17 and a primitive root α = 5.

   a. If Alice has a private key X_A = 9, find her public key *YA*.

   b. If Bob has a private key X_B= = 8, find his public key *YB*.

   c. What is the shared secret key between Alice and Bob?

16) Write Diffie-Hellman Key exchange algorithm. Using Diffie-Hellman key exchange algorithm, find the common key 'k' with p=29, α=2, X_A=11 & X_B=19.

17) Write RSA Algorithm. In RSA algorithm find private key if the public key is (7, 187) where p =17 and q=11.

18) Perform encryption and decryption using RSA algorithm for the plain text 'NO' with encipher key (public key) (n,e) = (77, 19) where p=11 and q=7.

19) What is Elliptic Curve Cryptography? Explain in detail about encryption and decryption in ECC.

20) Write and explain five possible approaches to attack the RSA algorithm.