IMPORTANT QUESTION FOR CT2

1. Explain Shannon Confusion and Diffusion technique.

2. Explain Difference between AES and DES.

3. Define **"BLOWFISH"** Algorithm.

4. Short note on **"PLAYFAIR"** Cipher. Use the playfair cipher to encipher the message **"THE KEY IS HIDDEN THE DOOR PAD"**. The Secret key is **"GUIDANCE".**

5. Explain "**Euler's totient function and solve ϕ(7), ϕ(21), ϕ(49), ϕ(1000**).

6. Find the primitive roots of **19.**

7. Compute **GCD(24120, 1640)** using Euclid's algorithm.

8. Explain Modular Algebraic structure **(Group, Field, and Ring)**.

9. Define Extended Euclidean Algorithm for Multiplicate inverse. Compute **MI of (50, 71)**

10. Explain Chinese Remainder Theorem (CRT) and find X for the given set of congruent equations using Chinese Remainder Theorem

    X = 1 mod 5
    X = 2 mod 7
    X = 3 mod 9
    X = 4 mod 11

11. Describe RSA algorithm in Detail. Calculate the private key of A wherein RSA cryptosystem a particular A uses tow prime numbers p = 13 and q = 17 to generate her public and private keys. Let the public key of A is 35.

12. What is DSS? Explain DSA algorithm for Digital Signature.

13. What basic arithmetical and logical functions are used in MD5? Explain SHA-I logic, give comparison of SHA1 and MD5.

14. Illustrate the working of SHA-1 algorithm with diagram.

15. What is Digital Certificate? Give the format of X.509 certificate showing the important elements of the certificate. How is an X.509 certificate revoked?

16. Define Diffie-Hellman Algorithm. In a Diffie-Hellman Key exchange algorithm, let the prime number be 353 and one of its primitive roots be 3. Let A and B select their Secret Keys Xa = 97 and Xb=233 so compute public keys of A & B & Common secret key.

17. Define Kerberos and explain its working with the help of diagram.

18. Explain Birthday Attack.