3. Describe the ElGamal cryptosystem, including its key generation, encryption, and decryption steps. [14

OR

What is the Digital Signature Algorithm (DSA) ? Explain its structure and use cases. [2+12

4. What is an elliptic curve over the reals ? Discuss the process of computing point multiples on elliptic curves and its importance in ECC. [2+12

OR

What is point compression on an elliptic curve ? Explain how elliptic curve primality testing works and its significance in cryptographic key generation. [2+12

5. What is Public Key Infrastructure (PKI) ? Explain the working of Kerberos and its components, such as the Key Distribution Center (KDC). [2+12

OR

What is the primary purpose of Pretty Good Privacy (PGP) ? Explain how SSL/TLS provides end-to-end security in web communication.[2+12

2024

Full Marks - 70

Time - As in the Programme

Each question carries equal mark.
Answer ALL questions.

1. Differentiate between cryptography and cryptanalysis. Explain the working of the affine cipher and its cryptanalysis techniques with suitable example. [2+12

OR

Explain the Data Encryption Standard (DES), highlighting its key size, block size, and number of rounds. [14

2. Differentiate between symmetric and asymmetric key. Describe the RSA algorithm, including key generation, encryption, and decryption steps with suitable example. [2+12

OR

Explain the Diffie-Hellman key exchange algorithm with an example. [14