

(2 ½ Hours)

[Total Marks: 75]

- N.B. (1) All questions are compulsory.
(2) Figures to the right indicate full marks.
(3) Assume additional data if necessary but state the same clearly.
(4) Symbols have their usual meanings and tables have their usual standard design unless stated otherwise.
(5) Use of calculators and statistical tables are allowed.

Q.1. Attempt any three of the following.

15

- Define Fermat's Little Theorem. Use it to calculate $23^{1002} \bmod 41$.
- Discuss different types of modular arithmetic operations.
- Describe the Euclidean Algorithm. explain with an example.
- What is a Linear Congruence? Use the Chinese Remainder Theorem to solve the following system of congruence's: $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 2 \pmod{7}$.
- Define quadratic residue. Find the quadratic residue of 7.
- State and explain the application of Congruences.

Q.2. Attempt any three of the following.

15

- Explain Substitution Cipher Technique with example.
- What is IDEA algorithm? Explain the encryption process used by IDEA Algorithm.
- What are the components of public Cryptosystem?
- Describe the Advanced Encryption Standard (AES).
- Write a short note on Hill Cipher Technique.
- Write a short note on Message Authentication Code (MAC).

Q.3. Attempt any three of the following.

15

- Explain the working of ElGamal Cryptosystem.
- Discuss various possible attacks on RSA.
- What is Public Key Infrastructure? Explain PKIX Architectural Model.
- Describe the concept of public key Cryptography.
- Explain the RSA Algorithm in detail with an example.
- Explain the purpose of Diffie-Hellman Key Agreement Algorithm.

Q.4. Attempt any three of the following.

15

- Describe the X.509 Digital Certificate format.
- Explain Station to Station protocol.
- Write a short note on Pretty Good Privacy (PGP).
- Explain the simple Key Distribution Scenario with neat diagram.
- Describe the Diffie-Hellman Algorithm in detail.
- Explain different PKIX Services.

Q.5. Attempt any three of the following.

15

- Write a brief note on Secure Socket Layer.
- Explain Rabin cryptosystem.
- What is MTI Key Agreement?
- Write a brief note on Secure Hash Algorithm (SHA).
- Describe the working of triple DES.
- Differentiate between AES and DES algorithm.