

(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

- a) Explain Fermat's Little Theorem. Use it to calculate $23^{1002} \bmod 41$.
- b) Define quadratic residue. Find the quadratic residue of 7.
- c) State the Euclidean Algorithm. Use the Euclidean algorithm to find gcd (414,662).
- d) Explain with example the Chinese Remainder Theorem.
- e) What are the different types of modular arithmetic operations?
- f) State and explain the application of Congruences.

Q.2. Attempt any three of the following.

15

- a) Explain Transposition Techniques with example.
- b) What is IDEA algorithm? Explain the encryption process used by IDEA Algorithm.
- c) What are the components of public Cryptosystem?
- d) Describe the Data Encryption Standard (DES).
- e) Write a short note on Hill Cipher Technique.
- f) Explain Secure Hash Algorithm (SHA) in detail.

Q.3. Attempt any three of the following.

15

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

Q.4. Attempt any three of the following.

15

- a) Describe the Diffie-Hellman Algorithm in detail.
- b) Explain Station to Station protocol.
- c) Write a brief note on Secure Socket Layer.
- d) Explain the simple Key Distribution Scenario with neat diagram.
- e) What is Public Key Infrastructure? Explain its working.
- f) Describe the X.509 Digital Certificate format.

Q.5. Attempt any three of the following.

15

- a) What do you mean by HMAC?
- b) Explain Rabin cryptosystem.
- c) What is MTI Key Agreement?
- d) Explain the working of triple DES.
- e) Write a short note on Pretty Good Privacy (PGP).
- f) Explain difference between AES and DES algorithm.
