(2 ½ Hours) **[Total Marks: 60]**

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 two* of the following. **12**

a) State the Euclidean Algorithm. Use the Euclidean algorithm to find gcd(414,662).
b) State Fermat's Little Theorem. Use it to calculate 23^{1002} mod 41.
c) What is quadratic residue? Find the quadratic residue of 7
d) State and explain the application of Congruences.

Q.2. Attempt *Any two* of the following. **12**

a) Explain Transposition Techniques with example.
b) Describe the Data Encryption Standard (DES).
c) Write a short note on Hill Cipher Technique.
d) Explain Secure Hash Algorithm (SHA) in detail.

Q.3. Attempt *Any two* of the following. **12**

a) Describe the RSA Algorithm in detail with an example.
b) What is Public Key Infrastructure? Explain PKIX Architectural Model.
c) Discuss the various attacks on RSA.
d) Explain the working of ElGamal Cryptosystem.

Q.4. Attempt *Any two* of the following. **12**

a) Describe the Diffie-Hellman Algorithm in detail.
b) Explain the simple Key Distribution Scenario with neat diagram.
c) What is Public Key Infrastructure? Explain its working.
d) Describe the X.509 Digital Certificate format.

Q.5. Attempt *Any two* of the following. **12**

a) Write a short note on: Chinese Remainder Theorem.
b) What do you mean by HMAC?
c) Describe the Public Key Cryptosystem in detail.
d) Write a short note on Pretty Good Privacy (PGP).

****