PAPER M107SC: AN INTRODUCTORY COURSE ON CRYPTOGRAPHY (3Hrs./week)

Introduction- Encryption and Secrecy – The objective of Cryptography – Cryptographic protocols. **6 Hrs.**

Mathematical background- Number Theory – Introduction- Divisibility and the Euclidean algorithm. Modular Arithmetic- Integer factorization problem, Congruence's- Pollard's rho factoring- Elliptic curve factoring- Discrete logarithm problem. **11 Hrs.**

Finite fields- Basic properties- Arithmetic of polynomials- Factoring polynomials over finite fields- Square free factorization**.** **8 Hrs.**

Cryptography: Some simple cryptosystems. Enciphering matrices. Symmetric key encryption- Stream Ciphers- Block Ciphers- DES**.** **7 Hrs.**

Public Key: Public Key cryptography- Concepts of public key cryptography-Modular arithmetic- RSA- Discrete logarithm. **7 Hrs.**

TEXT BOOKS

1. Hans Delfs and Helmut Knebl, "Introduction to Cryptography", Springer Verlag, 2002.C.
2. Neal Koblitz, "A course in Number Theory and Cryptography", Springer Verlag, New York, 1987.
3. Tom M. Apostol, "Introduction to Analytic Number Theory", Springer Verlag, New York, Heidelberg Berlin, 1976.

REFERENCE BOOKS

1. William Stallings, "Cryptography and Network Security", Prentice Hall of India, 2000.
2. Alfred J. Menezes, Paul C. Van Oorchot, Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 2000.

Pattern of Question Paper: Five full questions out of eight are to be answered**.**