DSE-1C	BCS-E501C	CRYPTOGRAPHY	L	C	CIA	ESE	Time for ESE
			4	4	30	70	3Hrs.

PREREQUISITES	:	Knowledge of Data Structure
COURSE OBJECTIVES/ LEARNING OUTCOMES	:	• To impart an essential study of computer security issues • To develop basic knowledge on cryptography • To impart an essential study of various security mechanisms

NOTE: The question paper shall consist of three sections (Sec.-A, Sec.-B and Sec.-C). **Sec.-A** shall contain 10 objective type questions of one mark each and student shall be required to attempt all questions. **Sec.-B** shall contain 10 short answer type questions of four marks each and student shall be required to attempt any five questions. **Sec.-C** shall contain 8 descriptive type questions of ten marks each and student shall be required to attempt any four questions. Questions shall be uniformly distributed from the entire syllabus. The previous year paper/model paper can be used as a guideline and the following syllabus should be strictly followed while setting the question paper.

Elementary number theory: Prime numbers, Fermat's and Euler's theorems, Testing for primality, Chinese remainder theorem, discrete logarithms. **10L**

Finite fields: Review of groups, rings and fields; Modular Arithmetic, Euclidean Algorithms, Finite fields of the form GF(p), Polynomial Arithmetic, Finite fields of the form GF(2). **12L**

Data Encryption Techniques: Algorithms for block and stream ciphers, private key encryption – DES, AES, RC4; **12L**

Algorithms for public key encryption – RSA, DH Key exchange, KERBEROS, elliptic curve cryptosystems. **12L**

Message authentication and hash functions, Digital Signatures and authentication protocols, Public key infrastructure, Cryptanalysis of block and stream ciphers. **14L**

BOOKS RECOMMENDED

1 W. Stallings, Cryptography and Network Security Principles and Practices, 4th Ed., Prentice-Hall of India, 2006.

2 C. Pfleeger and S.L. Pfleeger, Security in Computing, 3rd Ed., Prentice-Hall of India, 2007.

3 M.Y. Rhee, Network Security, John Wiley and Sons, NY, 2002.