3.	Geir Agnarsson and R. Gveenlaw, Graph theory: Modeling applications and Algorithms, Pearson edu., Inc.	2009
4.	L.R. Foulds, Graph theory applications, Narosa Pub. House	1992
5.	Corman, Leiserson and Rivest, Introduction to Algorithms, PHI	1998

1. Subject Code: **MC-407** Course Title: **CRYPTOGRAPHY AND NETWORK SECURITY**

2. Contact Hours L-3 T-1 P-0

3. Examination Duration (Hrs.) : Theory: 3 Practical: Nil

4. Relative Weightage : CWS: 25 PRS: 0 MTE: 25 ETE: 50 PRE: 0

5. Credits : 4

6. Semester : VII

7. Subject Area : DCC

8. Pre-requisite : NIL

9. Objective : To study various cryptographic techniques, mathematics related to cryptography and some network security protocols.

10. Details of Course

S. No.	Contents	Contact Hours
1.	Introduction: Introduction to security attacks, services and mechanism, introduction to cryptography, classical encryption techniques- substitution ciphers and transposition ciphers, cryptanalysis, steganography, stream and block ciphers, Intruders, Viruses and related threads.	6

2.	Modern Block Ciphers: Block ciphers principles, Shannon’s theory of confusion and diffusion, fiestal, Data ciphers encryption standard(DES), strength of DES, crypt analysis of DES, triple DES, IDEA encryption and decryption, strength of IDEA, key distribution algorithm.	6
3.	Introduction to graph, ring and field, prime and relative prime numbers, modular arithmetic, Fermat’s and Euler’s theorem, primarily testing, Euclid’s Algorithm, Chinese Remainder theorem, discrete logarithms, Principals of public key crypto systems, RSA algorithm, security of RSA, key management, Diffle-Hellman key exchange algorithm, introductory idea of Elliptic curve cryptography, Elganel encryption.	8
4.	Message Authentication and Hash Function: Authentication requirements, authentication functions, message authentication code (MAC), hash functions, message digest algorithm(MD5), Secure hash algorithm(SHA), Public Key Infrastructure(PKI): Digital Certificate, private key management, Digital Signatures: Digital Signatures, authentication protocols, digital signature standards (DSS), proof of digital signature algorithm.	6
5.	Authentication Applications: Kerberos and X.509, directory authentication service, password, challenge-response, biometric authentication, electronic mail security-pretty good privacy (PGP), S/MIME.	8
6.	IP Security: Architecture, Authentication header, Encapsulating security payloads, combining security associations, key management. Web Security: Secure Socket Layer(SSL) and transport layer security, TSP, Secure Electronic Transaction (SET), Electronic money, WAP security, firewall design principals, Virtual Private Network (VPN) security.	8

11. Suggested Books

S. No.	Name of Books/Authors/Publishers	Year of Publication/ Reprint
Text Books:		
1.	William Stallings, "Cryptography and Network Security: Principals and Practice", Prentice Hall, New Jersy.	1997
2.	AtulKahate, "Cryptography and Network Security", TMH.	2003
3.	Behrouz A. Forouzan, "Cryptography and Network Security", TMH.	2003
Reference Books:		
1.	Johannes A. Buchmann, "Introduction to Cryptography", Springer-Verlag.	2001
2.	Bruce Schiener, "Applied Cryptography".	1994

1. Subject Code: **MC-409** Course Title: **Mathematical modeling and simulation**

2. Contact Hours : L-3 T-0 P-2

3. Examination Duration (Hrs.) : Theory: 3 Practical: Nil

4. Relative Weightage : CWS: 15 PRS: 15 MTE :30 ETE: 40 PRE:

5. Credits : 4

6. Semester : VII

7. Subject Area : DCC

8. Pre-requisite : Basic knowledge of differential equations and statistics

9. Objective : To learn how to model and solve real life problems

10. Details of Course