CRYPTOGRAPHY & NETWORK SECURITY

Paper Code: ETIT-403	**L**	**T/P**	**C**
Paper: Cryptography & Network Security	**3**	**0**	**3**

INSTRUCTIONS TO PAPER SETTERS: **MAXIMUM MARKS: 75**

1. Question No. 1 should be compulsory and cover the entire syllabus. This question should have objective or short answer type questions. It should be of 25 marks.
2. Apart from Question No. 1, rest of the paper shall consist of four units as per the syllabus. Every unit should have two questions. However, student may be asked to attempt only 1 question from each unit. Each question should be of 12.5 marks.

Objectives: Syllabus should be proposed so as to be covered in 42 to 45 lectures (assuming 14 or 15 weeks session). Syllabus should be evenly divided into 4 Units only.

UNIT- I:

Basic Cryptographic Techniques, Computational Complexity, Finite Fields, Number Theory, DES and AES, Public Key Cryptosystems, Traffic Confidentiality ,Cryptanalysis, Intractable (Hard) Problems, Hash Functions, OSI Security Architecture Privacy of Data.

[T1, T2][No. of Hrs: 11]

UNIT- II:

Linear Cryptanalysis, Differential Cryptanalysis, DES, Triple DES, Message Authentication and Digital Signatures, Attacks on Protocols, Elliptic Curve Architecture and Cryptography, Public Key Cryptography and RSA, , Evaluation criteria for AES, Key Management, Authentication requirements Digital forensics including digital evidence handling: Media forensics, Cyber forensics, Software forensics, Mobile forensics.

[T1, T2][No. of Hrs: 11]

UNIT- III:

Buffer Flow attack, Distributed Denial of service attack, Weak authentication, Design of Substitution Boxes (S-Boxes), Hash Functions , Security of Hash Functions, Secure Hash Algorithm, Authentication applications, Kerberos, IP security, Pretty Good Privacy (PGP), Web Security Light weight cryptography for mobile devices, Side channel attacks.

[T1, T2][No. of Hrs: 11]

UNIT- IV:

System security, Security Standards, Intruders, and Viruses, Firewalls, Malicious software, Intrusion Detection System, Intrusion Prevention System, Trusted Systems, Virus Counter measures, Authentication Strategies.

[T1, T2][No. of Hrs: 11]

Text Book:

[T1] William Stallings, "Cryptography And Network Security - Principles and Practices", Prentice Hall of India, Third Edition, 2003.

[T2] Wade Trappe, Lawrence C Washington, " Introduction to Cryptography with coding theory", 2nd ed, Pearson, 2007.

Reference Book:

[R1] R.Rajaram, "Network Security and Cryptography" SciTech Publication, First Edition, 2013.

[R2] Atul Kahate, "Cryptography and Network Security", Tata McGraw-Hill, 2003

[R3] Bruce Schneier, "Applied Cryptography", John Wiley & Sons Inc, 2001.

[R4] http://www.iiitd.edu.in/~gauravg/