	L	T	P	C
IV Year – I Semester	**4**	**0**	**0**	**3**

CRYPTOGRAPHY AND NETWORK SECURITY

OBJECTIVES:

- In this course the following principles and practice of cryptography and network security are covered:
- Classical systems, symmetric block ciphers (DES, AES, other contemporary symmetric ciphers)
- Public-key cryptography (RSA, discrete logarithms),
- Algorithms for factoring and discrete logarithms, cryptographic protocols, hash functions, authentication, key management, key exchange, signature schemes,
- Email and web security, viruses, firewalls, digital right management, and other topics.

UNIT- I:
Basic Principles
Security Goals, Cryptographic Attacks, Services and Mechanisms, Mathematics of Cryptography

UNIT- II:
Symmetric Encryption
Mathematics of Symmetric Key Cryptography, Introduction to Modern Symmetric Key Ciphers, Data Encryption Standard, Advanced Encryption Standard.

UNIT- III:
Asymmetric Encryption
Mathematics of Asymmetric Key Cryptography, Asymmetric Key Cryptography

UNIT- IV:
Data Integrity, Digital Signature Schemes & Key Management
Message Integrity and Message Authentication, Cryptographic Hash Functions, Digital Signature, Key Management.

UNIT -V:
Network Security-I
Security at application layer: PGP and S/MIME, Security at the Transport Layer: SSL and TLS

UNIT -VI:
Network Security-II
Security at the Network Layer: IPSec, System Security

OUTCOMES:

- To be familiarity with information security awareness and a clear understanding of its importance.
- To master fundamentals of secret and public cryptography
- To master protocols for security services
- To be familiar with network security threats and countermeasures
- To be familiar with network security designs using available secure solutions (such asPGP,
- SSL, IPSec, etc)

TEXT BOOKS:

1) Cryptography and Network Security, Behrouz A Forouzan, DebdeepMukhopadhyay, (3e) Mc Graw Hill.
2) Cryptography and Network Security, William Stallings, (6e) Pearson.
3) Everyday Cryptography, Keith M.Martin, Oxford.

REFERENCE BOOKS:

1) Network Security and Cryptography, Bernard Meneges, Cengage Learning.