COURSE CODE	COURSE TITLE	L	T	P	C
1153IT103	CRYPTOGRAPHY AND NETWORK SECURITY	3	0	0	3

Course Category:

~~Foundation (0)/ Program Core (1)~~ **/ Program Elective (2)** / Allied Elective (3) / ~~University Elective (4) / Value Education Elective (5) / Independent Learning (6) / Industry - Higher Learning Institute Interaction (7)~~

a. Preamble:

This course describes the explosive growth in computer systems and their interconnections

via networks, has increased the dependence of both organizations and individuals on the information stored and communicated using these systems. This, in turn, has led to a heightened awareness of the need to protect data and resources from disclosure, to guarantee the authenticity of data and messages, and to protect systems from network-based attacks and the disciplines of cryptography and network security have matured, leading to the development of practical, readily available applications to enforce network security.

b. Pre-requisites:

Sl. No	Course Code	Course Name
1		Data Communication and Computer Networks

c. Related Courses:

Sl. No	Course Code	Course Name
1		Forensics and Cyber Applications
2		Information Security
3		Project Work

d. Course Educational Objectives:

Students undergoing this course are expected to

- Learn fundamentals of cryptography and its application to network security.
- Understand network security threats, security services, and countermeasures.
- Acquire background on well known network security protocols such as IPSec, SSL, and WEP.
- Understand vulnerability analysis of network security.
- Acquire background on hash functions; authentication; firewalls; intrusion detection techniques.

E. Course Outcomes:

CO Nos	Course Outcomes	Level of learning domain (Based on revised Bloom's taxonomy)
CO1	Compare various Cryptographic Techniques	K3
CO2	Demonstrate various data encryption techniques.	K3
CO3	Implement Hashing and Digital Signature techniques	K3
CO4	Explain the various Security Application	K2
CO5	Design and implement Secure applications	K3

f. Correlation of COs with Program Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	**H**	**M**	**L**	**L**								
CO2			**M**	**L**	**L**							
CO3		**M**	**M**	**M**		**L**						
CO4		**M**	**M**	**M**	**L**	**H**						
CO5			**M**	**L**	**M**		**L**					

H- High; M-Medium; L-Low

g. Course Content:

UNIT I FOUNDATIONS OF CRYPTOGRAPHY AND SECURITY 10

OSI Security Architecture - Security Attacks and Services. Mathematical Tools for Cryptography: Substitutions and Permutations, Modular Arithmetic, Euclid's Algorithm, Finite Fields, Polynomial Arithmetic.. Design Principle of Block ciphers: DES and Triple DES, Modes of Operation (ECB, CBC, OFB, CFB)

UNIT II BLOCK CIPHER ALGORITHMS AND PUBLIC KEY CRYPTOGRAPHY 9

AES- RC5- Introduction to Number Theory : Prime numbers- Chinese remainder theorem-Fermat and Euler's theorem –RSA- Public Key Management - Diffie-Hellman key Exchange - Elliptic Curve Cryptography.

UNIT III AUTHENTICATION AND HASH FUNCTION 9

Authentication requirements - Authentication functions - Message Authentication Codes - Hash Functions - Security of Hash Functions and MACs - MD5 message Digest algorithm - Secure Hash Algorithm -SHA 512 – HMAC- Digital Signatures - Authentication Protocols - Digital Signature Standard

UNIT IV NETWORK SECURITY 9

Authentication Applications: Kerberos - X.509 Authentication Service - Electronic Mail Security

- PGP - S/MIME - IP Security - Web Security.

UNIT V SYSTEM LEVEL SECURITY 8

Intrusion detection - password management - Viruses and related Threats - Virus Counter measures - Firewall Design Principles - Trusted Systems.

TOTAL: 45 Periods

h. Learning Resources

i. Text Books:

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

2. William Stallings, "Cryptography and Network security Principles and Practices", Pearson/PHI, 4th ed, 2006.

ii. Reference Books:

1. W. Mao, "Modern Cryptography – Theory and Practice", Pearson Education, Second Edition, 2007.

2. Charles P. Pfleeger, Shari Lawrence Pfleeger – Security in computing Third Edition - Prentice Hall of India, 2006.

iii. Online Resources:

1. williamstallings.com/Extras/Security-Notes/