COURSE CODE	COURSE TITLE	L	T	P	C
1152CS101	CRYPTOGRAPHY AND NETWORK SECURITY	3	0	0	3

Course Category: Program Elective

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	1151CS111	Computer Networks

C. Related Courses:

Sl. No	Course Code	Course Name
1	1152CS128	Forensics and Cyber Applications
2	1152CS117	Information Security
3	1156CS601	Minor Project
4	1156CS701	Major Project

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:

Upon the successful completion of the course, students will be able to

CO Nos	Course Outcomes	Level of learning domain (Based on revised Bloom's taxonomy)
CO1	Understand various Cryptographic Techniques	K2
CO2	Apply various public key cryptography techniques	K3
CO3	Implement Hashing and Digital Signature techniques	K3
CO4	Understand the various Security Applications	K2
CO5	Implement system level security applications	K3

Correlation of COs with Program Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	H	M	L	L											

CO2	**M**	**M**	**M**	**L**	**L**			**L**				**L**	**H**	**L**	
CO3	**M**	**M**	**M**	**M**		**L**		**L**	**L**		**L**	**L**	**M**	**M**	**M**
CO4	**M**	**M**	**M**	**M**	**L**	**H**		**L**	**L**		**L**	**L**	**M**	**H**	
CO5	**M**		**M**	**L**	**L**			**L**				**M**	**L**	**L**	**M**

H- High; M-Medium; L-Low

F. Course Content:

UNIT I FOUNDATIONS OF CRYPTOGRAPHY AND BLOCK CIPHER TECHNIQUES 9

OSI Security Architecture - Security Attacks and Services. Mathematical Tools for Cryptography:Substitutions and Permutations,Design Principle of Block ciphers: DES and Triple DES- AES- RC5.

UNIT II SYMMETRIC / ASYMMETRIC KEY CRYPTOGRAPHY 9

Introduction to Number Theory : Prime numbers- Chinese remainder theorem- Fermat and Euler's theorem –DES – AES – IDEA – RC4- Blowfish- RSA- Public Key Management - Diffie-Hellman key Exchange- Elliptic curve Cryptography.

UNIT III AUTHENTICATION AND HASH FUNCTION 10

Authentication requirements - Authentication functions - Message Authentication Codes - Hash Functions - 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 - Firewall Design Principles - Trusted Systems.. **TOTAL: 45 Hours**

G. 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.
3. Atul Kahate, "Cryptography and Network Security", McGraw Hill, 3rd ed, 2003

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/
2. www.cs.bilkent.edu.tr/~selcuk/teaching/cs519/
3. http://freevideolectures.com/Course/3027/Cryptography-and-Network-Security
4. http://cs.brown.edu/courses/csci1510/2013_lectures.html