Course Code	Course Title	L	T	P	C
1152EC126	NETWORK SECURITY	3	0	0	3

a) Course Category

Program Elective

b) Preamble

The course deals with the underlying principles of cryptography and network security. It develops the mathematical tools required to understand the topic of cryptography. It aims to introduce students to the fundamental techniques used in implementing secure network communications, and to give them an understanding of common threats and attacks.

c) Prerequisite

Data Communication Networks

d) Related Courses

None

e) Course Outcomes

Upon the successful completion of the course, student will be able to:

CO Nos.	Course Outcomes	Knowledge Level (Based on Revised Bloom's Taxonomy)
CO1	Explain about the OSI Security architecture and various Crytographic techniques	K2
CO2	Describe about the data encryption standard, block ciphers and block ciphers mode of operation.	K2
CO3	Describe the principles of various public key cryptosystems	K2
CO4	Explain the need for authentication and various authentication system methods	K2
CO5	Illustrate the different types of threats and attacks in data networks and explain about Internet and Mobile security	K2

f) Correlation of COs with POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	M	-	L	-	-	L	-	-	-	-	-	-	-	-
CO2	M	-	M	-	M	-	-	L	-	-	-	-	-	-
CO3	M	-	M	-	M	-	M	-	-	-	-	L	-	-
CO4	M	-	M	-	M	L	M	-	-	-	-	-	-	-
CO5	M	-	-	-	-	-	-	-	-	-	-	L	-	-

g) Course Content

UNIT I BASIC CIPHERS 9

Services, Mechanisms and Attacks-The OSI Security Architecture – Network Security Model – Classical Encryption Techniques, Symmetric Cipher Model, Substitution Techniques, Transposition Techniques, Steganography.

UNIT II BLOCK CIPHERS 9

Block Ciphers- Simplified Data Encryption Standard -Data Encryption Standard– Block cipher principlesblock cipher modes of operation – Triple DES-Simplified Advanced Encryption Standard-Advanced Encryption Standard (AES)

UNIT III PUBLIC KEY SYSTEM 9

Public key cryptography: Principles of public key cryptosystems – The RSA algorithm-Key management – Diffie Hellman Key exchange - Elliptic curve arithmetic – Elliptic curve cryptography- Elliptic curve digital signature algorithm.

UNIT IV AUTHENTICATION SYSTEM 9

Authentication requirement – Authentication function – MAC – Hash function – Security of hash function and MAC –MD5 – SHA– HMAC – CMAC – Digital signature and authentication protocols – DSS – EI Gamal – Schnorr – Authentication applications – Kerberos– X.509 Authentication services

UNIT V INTERNET AND MOBILE SECURITY 9

Internet Firewalls for Trusted System: Roles of Firewalls – Firewall related terminology – Types of Firewalls-Intrusion detection system – Virus and related threats – Countermeasures -Trusted systems, Email Security: Security Services for E-mail – attacks possible through E-mail – establishing keys privacyauthentication of the source – Message Integrity – Non-repudiation , mobile device security.

Total 45 Hrs

h) Learning Resources

Text Books

1. William Stallings, Cryptography and Network Security, 7th edition, Pearson Education
2. Charlie Kaufman, Radia Perlman, Mike Speciner, Network Security, Prentice Hall of India -2002

Reference Books

1. Behrouz A Ferouzan, Cryptography & Network Security, Tata McGraw Hill-2007
2. Man Young Rhee, Internet Security: Cryptographic Principles", "Algorithms and Protocols, Wiley Publications-2003
3. Charles Pfleeger, Security in Computing, Prentice Hall of India -2006
4. Ulysess Black, Internet Security Protocols, Pearson Education Asia -2000

Online Resources

1. http://www.herongyang.com/crypto/
2. http://www.cryptographyworld.com/what.htm
3. http://www.cryptography-tutorial.com
4. http://www.sans.org/reading-room/whitepapers/modeling/network-security-model-32843
5. http://searchsecurity.techtarget.com/definition/Diffie-Hellman-key-exchange
6. https://www.paloaltonetworks.com/resources/learning-center/what-is-an-intrusiondetectionsystem-ids.html
7. https://lyle.smu.edu/~nair/courses/7349/SET.ppt

Practical Aspects

1. The students shall practice the different attacks in virtual environment using kali Linux