Course Number and Name

BEC012- CRYPTOGRAPHY AND NETWORK SECURITY

Credits and Contact Hours

3 and 45

Course Coordinator's Name

Ms S.Pothumani

Text Books and References

Text Books:

1. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013.
2. Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security", Prentice Hall of India,2002.

References:

1. Behrouz A. Ferouzan, "Cryptography & Network Security", Tata Mc Graw Hill, 2007.
2. Charles Pfleeger, "Security in Computing", 4th Edition, Prentice Hall of India, 2006.
3. Ulysess Black, "Internet Security Protocols", Pearson Education Asia, 2000.
4. Charlie Kaufman and Radia Perlman, Mike Speciner, "Network Security, Second Edition, Private Communication in Public World", PHI 2002.
5. Bruce Schneier and Neils Ferguson, "Practical Cryptography", First Edition, Wiley Dream tech India Pvt Ltd, 2003.
6. www.ics.uci.edu/~stasio/spring04/ics180.html

Course Description

- To know about various encryption techniques.
- To understand the concept of Public key cryptography.
- To study about message authentication and hash functions
- To impart knowledge on Network security

Prerequisites	Co-requisites
Communication Engineering - I	Computer Communication and Networks

required, elective, or selected elective (as per Table 5-1)

Selected Elective

Course Outcomes (COs)

CO1: classify the symmetric encryption techniques
CO2 : Illustrate various Public key cryptographic techniques
CO3 : Evaluate the authentication and hash algorithms.
CO4 : Discuss authentication applications
CO5: Summarize the intrusion detection and its solutions to overcome the attacks.
CO6 : Basic concepts of system level security

Student Outcomes (SOs) from Criterion 3 covered by this Course

COs/SOs	a	b	c	d	e	f	g	h	i	j	k
CO1	H		M		M	M	M	H	M		L
CO2	M	L	H				H		L	H	
CO3	M	H	M	M			M	M	M		H
CO4	M	H	H		M				M		M
CO5		M			M	M	M		M		
CO6				M	M	H	M				

List of Topics Covered

UNIT I INTRODUCTION 9

OSI Security Architecture - Classical Encryption techniques – Cipher Principles – Data Encryption Standard – Block Cipher Design Principles and Modes of Operation - Evaluation criteria for AES – AES Cipher – Triple DES – Placement of Encryption Function – Traffic Confidentiality

UNIT II PUBLIC KEY CRYPTOGRAPHY 9

Key Management - Diffie-Hellman key Exchange – Elliptic Curve Architecture and Cryptography - Introduction to Number Theory – Confidentiality using Symmetric Encryption – Public Key Cryptography and RSA.

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 – RIPEMD – 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 9

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