COURSE TITLE : INFORMATION AND NETWORK SECURITY
COURSE CODE : 6262
COURSE CATEGORY : A
PERIODS/WEEK : 4
PERIODS/SEMESTER : 60
CREDITS : 4

TIME SCHEDULE

MODULE	TOPICS	PERIODS
1	**Introduction to Cryptography**	15
2	**Symmetric and Asymmetric Ciphers**	15
3	**Cryptographic Data Integrity Algorithms**	15
4	**Network Security**	15

COURSE GENERAL OUTCOMES:

Sl.	G.O	On completion of this course the student will be able to :
1	1	**Understand Computer and Data Security concepts**
2	1	**Comprehend Symmetric Ciphers**
	2	**Comprehend Asymmetric Ciphers**
3	1	**Understand the Data Integrity algorithms**
	2	**Understand the concept of Digital Signatures**
4	1	**Understand the various Network Security concepts**
	2	**Recognize the Wireless LAN security issues**

SPECIFIC OUTCOMES:

MODULE – I: Introduction to Cryptography

1.1 Understand Computer and Data Security concepts

1.1.1 Define Confidentiality, Integrity and availability.

1.1.2 Distinguish between active and passive security attacks

1.1.3 Explain the different categories of Passive attacks.

1.1.4 Explain the different types of Active attacks.

1.1.5 Explain the Network Security Model

1.1.6 Demonstrate the Model for Network Security

1.1.7 Explain the Symmetric Cipher Model

1.1.8 Explain the various substitution technique Caesar Cipher with example

1.1.9 Explain the various substitution technique Mono-alphabetic Ciphers with example

1.1.10 Explain the various substitution technique Poly-alphabetic Ciphers with example

1.1.11 Explain the various substitution technique One-Time Pad

1.1.12 Compare the Substitution techniques – Caesar Cipher, Mono-alphabetic Ciphers, Poly-alphabetic Ciphers and One-Time Pad

1.1.13 Simulate the various substitution techniques learned.

1.1.14 Describe Transposition Techniques

1.1.15 Define Stegnography

MODULE – II: Symmetric and Asymmetric Ciphers

2.1 Comprehend Symmetric Ciphers

2.1.1 Define Symmetric Cipher

2.1.2 Describe the DES method, its encryption and decryption procedures

2.1.3 Analyze the strength of DES

2.1.4 Describe the AES method of cryptography – structure and Encryption Decryption methods

2.1.5 Compare and Judge the performance of DES and AES algorithms

2.2 Comprehend Asymmetric Ciphers

2.2.1 Define Asymmetric Cipher

2.2.2 State Fermat's theorem

2.2.3 State Euler's theorem.

2.2.4 Explain the Public Key cryptosystems

2.2.5 List the essential steps in Public Key encryption

2.2.6 Describe the elements of public encryption system

2.2.7 Compare the symmetric key and public key encryption system.

2.2.8 Describe the RSA algorithm

MODULE – III: Cryptographic Data Integrity Algorithms

3.1 Understand the Data Integrity algorithms

3.1.1 Describe the applications of Cryptographic Hash functions

3.1.2 Describe message authentication

3.1.3 Explain the logic of SHA 1 algorithm

3.1.4 Describe the different types of attacks in the context of communications across a network

3.1.5 Summarize the Message Authentication Requirements

3.1.6 Summarize Message Authentication Functions

3.1.7 Describe the basic idea of Message Authentication Code

3.2 Understand the concept of Digital Signatures

3.2.1 Define Digital Signature

3.2.2 Explain the properties of Digital Signature

3.2.3 Identify the Digital Signature Requirements

3.2.4 Explain the Digital Signature Algorithm

3.2.5 Describe techniques for the distribution of public keys

3.2.5.1 Public announcement

3.2.5.2 Publicly available directory

3.2.5.3 Public-key authority

3.2.5.4 Public-key certificates

3.2.6 Recognize the importance of X.509 Certificates

3.2.7 Illustrate the Public-Key Certificate Use with figure

MODULE – IV: Network Security

4.1 Understand the various Network Security concepts

4.1.1 List the web security considerations

4.1.2 Explain the SSL architecture

4.1.3 Define the SSL concepts Connection and Session.

4.1.4 Write the parameters that defines a session state.

4.1.5 Write the parameters that defines a Connection state.

4.1.6 Define HTTPS

4.1.7 Describe HTTPS

4.1.8 Describe the importance of HTTPS in web

4.1.9 Describe SSH Protocol Stack

4.2 Recognize the Wireless LAN security issues

4.2.1 Write a short description on Wireless LAN Security

4.2.2 List down the various 802.11i services

4.2.3 Assess the different IEEE 802.11i Phases of Operation

4.2.4 Define Wireless Markup Language

4.2.5 Explain WAP Architecture

4.2.6 Explain IPsec applications

4.2.7 Discuss the benefits of IPSec

4.2.8 List down the IPSec Services

CONTENT DETAILS

MODULE – I: Introduction to Cryptography

Computer Security Concepts- Security Attacks - Security Services - A model for network Security - Classical Encryption Techniques: Symmetric Cipher Model- Substitution Technique- Caesar Cipher, Mono-alphabetic Ciphers, Poly-alphabetic Ciphers, One-Time Pad, Transposition Techniques, Stegnography.

MODULE – II: Symmetric and Assymteric Ciphers

Symmetric Ciphers: Data Encryption Standard (DES)- DES Encryption, DES Decryption, Strength of DES. AES - General Structure, Detailed Structure, AES Encryption and Decryption. Asymmetric Cyphers: Fermat's Theorem and Eulers's Theorem, Public-Key Cryptosystems, RSA Algorithm - Description of the Algorithm.

MODULE – III: Cryptographic Data Integrity Algorithms

Applications of Cryptographic Hash functions - SHA 1 - Logic, Message Authentication Codes: Message Authentication Requirements, Message Authentication Functions, Digital Signatures: Properties, Attacks and Forgeries, Digital Signature Requirements, DSS Approach, Digital Signature Algorithm, Distribution of Public Keys, X.509 Certificate.

MODULE – IV: Network Security

Web Security Considerations, SSL Architecture, HTTPS, SSH Protocol Stack, Wireless LAN Security - IEEE 802.11i Services, IEEE 802.11i Phases of Operation, Wireless Application ProtocolOverview, IP Security overview.

TEXT BOOK(S)

1. Cryptography and Network Security- Principles and Practice, William Stallings, 5th Edition, Pearson.

REFFERENCE

1. Network Security: Private Communication in a Public World - Charlie Kaufman, Radia

Perlman, Mike Speciner, Prentice Hall Publication, Second Edition.

2. Network Security and Cryptography- Bernard L. Menezes, Cengage Learning 2011.
3. Behrouz A. Frouzan, Cryptography and Network Security, TMH Publication, third edition, 2004.