GUJARAT TECHNOLOGICAL UNIVERSITY

Master in Computer Applications (Integrated MCA)

Year IV – (Semester-VIII) (W.E.F. Dec 2016)

Subject Name: Network Security (NS)
Subject Code: 4480603

---

1. **Learning Objectives:**

After completion of this course student will be able to:

- Understand OSI security architecture, threats, vulnerabilities and various types of attacks.
- Understand and apply the various symmetric key algorithms.
- Understand and apply the various asymmetric key algorithms.
- Understand the concepts of hashing with algorithms and apply them.
- Understand and use the message authentication and its requirement.
- Understand the concepts of digital signature and digital certificates.
- Analyze the use of Authentication applications, Web, IP and Email security.
- Evaluate the need of Intrusion Detection and Firewalls.

2. **Prerequisites:**
   Fundamentals of Networking, Mathematical Concepts: Number theory, finite fields and Random number.

3. **Contents:**

Unit No.	Chapter Details	Weightage	No. of Lecture
1	**Introduction** Computer Security Concepts, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, A Model for Network Security.	05%	2
2	**Cryptography: Symmetric Encryption, Message Confidentiality, Public-Key Cryptography and Message Authentication** Symmetric Encryption Principles, Symmetric Block Encryption Algorithms, Random and Pseudorandom Numbers, Stream Ciphers and RC4,Cipher Block Modes of Operation. Approaches to Message Authentication, Secure Hash Functions,	25%	10

	Message Authentication Codes, Public-Key Cryptography Principles, Public-Key Cryptography Algorithms, Digital Signatures.		
3.	**Key Distribution and User Authentication, Transport-Level Security, HTTPS and SSH** Symmetric Key Distribution Using Symmetric Encryption, Kerberos, Key Distribution Using Asymmetric Encryption, X.509 Certificates,Public-Key Infrastructure. Web Security Considerations, Secure Socket Layer and Transport Layer Security, Transport Layer Security, HTTPS, Secure Shell (SSH) .	**25%**	**10**
4.	**Wireless Network Security** Overview of IEEE 802.11 WLAN, IEEE 802.11i Wireless LAN Security.	**10%**	**3**
5	**E-MAIL & IP** Pretty Good Privacy, S/MIME , IP Security Overview, IP Security Policy, Encapsulating Security Payload, Combining Security Associations.	**20%**	**7**
6.	**System Security and Malicious Software** Intruders, Intrusion Detection, Password Management, Types of Malicious Software, Viruses, Virus Countermeasures, Worms,Distributed Denial of Service Attacks, The Need for Firewalls, Firewall Characteristics, Types of Firewalls, Firewall Basing, Firewall Location and Configurations.	**15%**	**8**

4. Text Books:

1. William Stallings, "Network Security Essentials: Applications and Standards", 4th Edition, Pearson Education,2011.

5. Reference Books:

1. Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security: Private communication in a public world", Second Edition, Pearson India Education,2017
2. Behrouz A. Ferouzan, "Cryptography & Network Security", Tata Mc Graw Hill, 2007.
3. Nina Godbole, "Information Systems Security", Wiley Publication,2009
4. Nirbhay Chaubey, "Securing AODV Routing Protocol in Design of Mobile Ad-Hoc Networks:, LAP Lambert Academic Publishing,2015

5. Bruce Schneier "Applied Cryptography: Protocols, Algorithms, and Source Code in C", Wiley India,1996

6. Man Young Rhee, "Internet Security: Cryptographic Principles", "Algorithms and Protocols", Wiley Publications, 2003.

7. Charles P. Pfleeger, Shari Lawrence Pfleeger, "Security in Computing", 4th Edition, Prentice Hall of India, 2006.

8. Bruce Schneier and Neils Ferguson, "Practical Cryptography", First Edition, Wiley Dreamtech India Pvt Ltd, 2003.

6. Chapter Wise Coverage from Text Book:

Unit No.	Text Books	Topics/Subtopics
1	Book-1	Chapter - 1.1 to 1.6
2	Book-1	Chapter - 2.1 to 2.5, 3.1 to 3.6
3	Book-1	Chapter - 4.1 to 4.5, 5.1 to 5.5
4	Book-1	Chapter - 6.1 to 6.2
5	Book-1	Chapter - 7.1, 7.2, 8.1 to 8.4
6	Book-1	Chapter - 9.1 to 9.3, 10.1 to 10.5, 11.1 to 11.5

7. Accomplishments of the student after completing the course :

- Student will be able to understand the importance of network security in today's world and apply security services and mechanisms in evaluating networked systems and also while creating new applications.
- Analyze and use apply best suited Network Security mechanisms and standards in various applications.
- Design Secure applications

8. Suggestions for Lab Sessions :

a) Suggested Lab Activities

Sr. #	Sub Task Description
NS	Implement DES.
	Implement 3DES.
	Implement AES algorithms.
	Implement HMAC, Hashing a Session Key, Duplicating a Hash, encoding and decoding a hash message, signing a hash and verifying the hash signature.
	Implement a basic MD5 algorithms.
	Implement RC4 encryption algorithm.
	Implement Diffi-Hellmen Key exchange Method.
	Implement RSA encryption-decryption algorithm.
	Write a program to generate SHA-1 hash.
	Write a program to generate SHA-512 hash.
PS: Above are suggestive lists so student can perform on any programming language C,C++/Java available at institute.	

Additional Assignment: List of Open Source Software/learning website:

- Download Software: cryptool (www.cryptool.org) and Perform various encryption decryption techniques with cryptool.
- Download Software: Wireshark (network packet analyzer): (www.wireshark.org) to Study and use the Wireshark for the various network protocols.