Kadi Sarva Vishwavidyalaya, Gandhinagar

MASTERS OF COMPUTER APPLICATION (MCA)

Year – II (Semester – IV) (W.E.F. January 2015)

Subject Name: Network Security (NS) – MCA-405(C)

Sub Total Credit	Teaching scheme		Examination scheme				
	(per week)		MID	CEC	External		Total Marks
	Th	Pr	Th	Th	Th.	Pr.	
5	3	4	25	25	50	50	150

Objectives:

1. To give the understanding of the different type of security mechanism performed in Internet.
2. To describe mechanism of firewall and Intruders
3. To give the understanding of the functionality symmetric and asymmetric Encryption Method.
4. To describe the working of routing algorithms and its techniques.

Learning Outcomes:

At the end of the course, student will be able to:

1. Describe and analyze the software, components of a network and the interrelations.
2. Explain networking protocols and their hierarchical relationship.
3. Compare protocol models and select appropriate protocols for a particular design.

Course Contents:

UNIT – I **Network Security and Symmetric Encryption** **[20 %]**

Security Trends, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanism, A Model for Internetwork Security, Internet Standards the Internet Society, Symmetric Encryption Principles, Symmetric Block Encryption Algorithms, Stream Ciphers and RC4, Cipher Block Modes of Operation

UNIT – II **Asymmetric key Encryption Techniques** **[20%]**

Location of Encryption Devices, Approaches to Message Authentication, Secure Hash Functions, Message Authentication Codes, Public-Key Cryptography Principles, Public-Key Cryptography Algorithms, Digital Signatures

UNIT – III **Authetication Mechanism and Virus Protection** **[20%]**

Key Management. Kerberos, X.509 Directory Authentication Service, Public Key Infrastructure, Malicious Software: Types of Malicious Software, Viruses, Virus Countermeasures, Worms, Distributed Denial of Service Attacks

UNIT – IV **Web Security and Intrusion** **[20%]**

Web Security Considerations, Secure Sockets Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET), Intruders, Intrusion Detection.

UNIT – V Passwords and Firewalls [20%]

Password Management. Firewall Design Principles, Trusted Systems, Common Criteria for Information Technology Security Evaluation.

Text Book(s):

1. William Stallings, "Network Security Essentials: Applications and Standards", 3rd Edition, Pearson Education

Other Reference Books:

A. Behrouz Forouzan, "Cryptography and Network Security", TMH Publication.

B. Nina Godbole, "Information Systems Security", Wiley Publication.

William Stallings, "Cryptography and Network Security", Pearson Education

Unit wise coverage from above Text books:

Unit No.	**Chapter**	**Description**
Unit - I	Chapter – 1	All
	Chapter – 2	All
Unit – II	Chapter – 3	All
Unit – III	Chapter – 4	All
	Chapter – 10	All
Unit – IV	Chapter – 5	All
Unit –V	Chapter – 9	All
	Chapter – 11	All

Practical Programs

Note: - Develop a JAVA program to simulate a Client – Server scenario fulfilling the following conditions

Sr.	Definition
1.	The client should encrypt the input string (plain text) and get cipher text using Transposition cipher. The sender then should send the encrypted text and the key to the server.
2.	The client should encrypt the input string (plain text) and get cipher text using Caesar cipher. The client then should send the encrypted text and the key to the server.
3.	The client should encrypt the input string (plain text) and get cipher text using Mono alphabetic substitution cipher. The client then should send the encrypted text, the plain pattern and the substitution pattern to the server.
4	The client should encrypt the input string (plain text) and get cipher text using DES. The sender then should send the cipher text and the key used, both to the receiver.
5	Write a programs to simulate encryption and decryption technique using One Time Pad, algorithm development and Communication between client and server should be done using Java server socket programming.
6	The client should encrypt the input string (plain text) and get cipher text using DES. The sender then should send the cipher text and the key used, both to the receiver.
7	Write a programs to simulate encryption and decryption technique using AES, algorithm development and Communication between client and server should be done using Java server socket programming.
8	The client should encrypt the input string (plain text) and get cipher text using Triple DES with CFM mode. The sender then should send the cipher text and the key used, both to the receiver.