Kadi Sarva Vishwavidyalaya, Gandhinagar
MCA Semester IV
MCA - 405 (C) : Information & Network Security

Rationale:

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

Prerequisites: Knowledge of Networks, OSI and TCP/IP Model

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

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

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

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
2. "Computer Networks" by Andrew Tanenbaum, Pearson Education

Other Reference Books:

1. Behrouz Forouzan, "Cryptography and Network Security", TMH Publication.
2. Nina Godbole, "Information Systems Security", Wiley Publication.
3. 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

Practical List

1. Sender/Recvr Program that converts decimal data into binary and vice versa.
2. Sender/Recvr Program appends the total count of characters in the string.
3. Sender/Recvr Program that performs byte stuffing in the data.
4. Sender/Recvr Program that performs character stuffing in the data.
5. Sender/Recvr Program to implement VRC method.
6. Sender/Recvr Program to implement LRC method.
7. Sender/Recvr Program to implement Checksum method.
8. Sender/Recvr Program to implement CRC method.
9. Sender/Recvr Program to implement Mono Alphabetic Substitution Method
10. Sender/Recvr Program to implement Caesar Method
11. Sender/Recvr Program to implement Transposition Method
12. Sender/Recvr Program to implement One time Pad Method
13. Sender/Recvr Program to implement RSA Method
14. Program to implement P-box
15. Program to implement S-box
16. Write a program of DES with Cipher Block Chaining mode.
17. Write a program of DES with Cipher Feedback mode
18. Write a program of DES with Electronic Codebook mode
19. Write a program of DES with Output Feedback mode.
20. X.509 Certificate creation