SVKM's Mithibai College of Arts, Chauhan Institute of Science & Amrutben Jivanlal College of Commerce & Economics (AUTONOMOUS)

Program: Bachelor of Science (Computer Science)		**Semester: V**	
Course: Information and Network Security		**Course Code: USMACS503**	
Teaching Scheme		**Evaluation Scheme**	
Lecture (Hours per week)	**Credit**	**Continuous Assessment**	**Semester End Examinations (SEE) (Marks-75 in Question Paper)**
04	4	25%	75%

Learning Objectives:

- To provide students with knowledge of basic concepts of computer security includingnetwork security and cryptography.

Course Outcomes:

After completion of the course, learners would be able to:

CO1: Identify risk related to information and network security
CO2: Recommend various security techniques, applications and intrusion detection methods.
CO3: Apply cryptographic algorithms to maintain information security.
CO4: Differentiate between the use of cryptography and Hashing
CO5: Apply measures to prevent attacks on networks using firewall.
CO6: Formulate hash function for authentication

Outline of Syllabus: (per session plan)

Module	**Description**	**No of hours**
1	Introduction, Classical Encryption Techniques, Cryptography and RSA	15
2	Program Security	15
3	Digital Signatures and Authentication	15
4	Electronic Mail Security, Web Security, Intrusion, Firewalls	15
	Total	**60**

SVKM's Mithibai College of Arts, Chauhan Institute of Science & Amrutben Jivanlal College of Commerce & Economics (AUTONOMOUS)

Module	Information and Network Security	No. of Hours/Credits 60/4
1	**Introduction, Classical Encryption Techniques, Cryptography and RSA**	**15**
	Introduction: Security Trends, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms	**3**
	Classical Encryption Techniques: Symmetric Cipher Model, Substitution Techniques, Transposition Techniques Steganography	**7**
	Block Cipher Principles, The Data Encryption Standard, The Strength of DES, AES (round details not expected), Multiple Encryption and Triple DES, Block Cipher Modes of Operation, Stream Ciphers	**4**
	Public-Key Cryptography and RSA: Principles of Public-Key Cryptosystems, The RSA Algorithm, Key Management: Public-Key Cryptosystems, Key Management, Diffie-Hellman Key Exchange	**2**
2	**Program Security**	**15**
	Program Security: Secure programs: Fixing Faults, Unexpected Behavior, Types of Flaws. Non-malicious program errors: Buffer overflows, Incomplete Mediation.	**4**
	Viruses and other malicious code: Why worry about Malicious Code, Kinds of malicious code, how viruses attach, how viruses gain control, Prevention,	**4**
	Control Example: The Brain virus, The Internet Worm, Web bugs. Targeted malicious code- Trapdoors, Salami Attack.	**4**
	Controls against program threats- Development Controls, Peer reviews, Hazard Analysis.	**3**
3	**Digital Signatures and Authentication**	**15**
	Message Authentication and Hash Functions: Authentication Requirements, Authentication Functions, Message Authentication Codes, Hash Functions, Security of Hash Functions and Macs, Secure Hash Algorithm, HMAC	**6**
	Digital Signatures and Authentication: Digital Signatures, Authentication Protocols, Digital Signature Standard Authentication Applications:	**4**
	Kerberos, X.509 Authentication, Public-Key Infrastructure	**2**
	Network Access Control: Network Access Control, Extensible Authentication Protocol, IEEE 802.1X Port-Based Network Access Control.	**2**
	Wireless Network Security: Mobile Device Security, Wireless LAN Security	**1**

4	**Electronic Mail Security, Web Security, Intrusion, Firewalls, Biometric security**	**15**
	Electronic Mail Security: Pretty Good Privacy, S/MIME, DomainKeys Identified Mail.	**3**
	IP Security: Overview, Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations, Key Management	**3**
	Web Security: Web Security Considerations, Secure Socket Layer and Transport Layer Security, HTTPS standard , Secure Socket Shell	**3**
	Intrusion: Intruders, Intrusion Techniques, Intrusion Detection,	**2**
	Firewalls: Firewall Design Principles, Types of Firewalls Security in Online transactions	**2**

RECOMMENDED READING:

ESSENTIAL READING:

1. Cryptography and Network Security: Principles and Practice 5th Edition, William Stallings, Pearson, 2010.
2. Cryptography and Network Security, Atul Kahate, Tata McGraw-Hill, 2013.

SUPPLEMENTARY READING:

1. Cryptography and Network, Behrouz A Fourouzan, Debdeep Mukhopadhyay, 2ndEdition, TMH, 2011.
2. Information Security Principles and Practice By Mark Stamp, Willy India Edition.