GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Master of Computer Applications

Level: Post Graduate

Course / Subject Code: MC03094101

Course / Subject Name : Information and Network Security

w. e. f. Academic Year:	2025-26
Semester:	3
Category of the Course:	Elective Group-1

Prerequisite:	Fundamentals of computer network **,** Mathematical concepts: Random numbers, Number theory, finite fields
Rationale:	The use of the Internet for various purpose including social, business, communication and other day to day activities has been in common place. The information exchanged through Internet plays vital role for their owners and the security of such information/data is of prime importance. Knowing the concepts, principles and mechanisms for providing security to the information/data is very important for the students of MCA. The subject covers various important topics concern to information security like symmetric and asymmetric cryptography, hashing, message and user authentication, digital signatures, key distribution and overview of the malware technologies. The subject also covers the applications of all of these in real life applications.

Course Outcome:

After Completion of the Course, Student will able to:

No	Course Outcomes	RBT Level
01	Explain concepts of cryptography.	UN
02	Implement symmetric key cryptography algorithms.	AP
03	Implement asymmetric key cryptography algorithms.	AP
04	Apply concepts of hashing, digital signature and MAC.	AP
05	Analyze security vulnerabilities and breaches of network and use appropriate approach and tools to mitigate it.	AN

**Revised Bloom's Taxonomy (RBT)*

Teaching and Examination Scheme:

Teaching Scheme (in Hours)			Total Credits L+T+ (PR/2)	Assessment Pattern and Marks				Total Marks
				Theory		Tutorial / Practical		
L	T	PR	C	ESE (E)	PA / CA (M)	PA/CA (I)	ESE (V)	
3	0	2	4	70	30	20	30	150

Course Content:

Unit No.	Content	No. of Hours	% of Weightage
1	Introduction – Security attacks, services & security mechanisms, CIA (Confidentiality, Integrity, Availability), AAA (Authentication, Authorization, Accounting), Symmetric Cipher Model, Cryptography, Cryptanalysis and Attacks; Substitution and Transposition techniques	6	15
2	Stream ciphers and block ciphers, Block Cipher structure, Data Encryption standard (DES) with example, AES with structure, its transformation functions, key expansion, example	6	15
	Multiple encryption and triple DES, Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode	5	10
3	Public Key Cryptosystems with Applications, Requirements and Cryptanalysis, RSA algorithm, its computational aspects and security, Diffie-Hillman Key Exchange algorithm, Man-in-Middle attack	6	15
4	Cryptographic Hash Functions, their applications, Simple hash functions, its requirements and security, Secure Hash Algorithm (SHA)	5	10
	Message Authentication Codes , Digital Signature, its properties, NIST digital Signature algorithm	6	15
5	Concepts of DNS,DHCP, Public & Private IP address, NAT, CIDR, DMZ, Firewall, IDS, IPS, WHOIS, NSLOOKUP, TRACERT, ICMP Ping	4	5
	port scanning using Nmap, Traffic Capturing & Packet Analysis using wireshark	2	5
	Security at Application layer-HTTPS, Security at transport layer-TLS,SSL	3	5
	Security at internet layer-IPSec Security at Network interface layer-Network access control(MAC filtering)	2	5
	Total	**45**	**100**

Suggested Specification Table with Marks (Theory):

Distribution of Theory Marks (in %)					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
10	50	30	10	0	0

Where R: Remember; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create (as per Revised Bloom's Taxonomy)

References/Suggested Learning Resources:

(a) Books:

1. Cryptography And Network Security, Principles And Practice , William Stallings, Pearson
2. Information Security Principles and Practice By Mark Stamp, Willy India Edition
3. Cryptography & Network Security, Forouzan, Mukhopadhyay, McGrawHill
4. Cryptography and Network Security Atul Kahate, TMH
5. Cryptography and Security, C K Shyamala, N Harini, T R Padmanabhan, Wiley-India
6. Information Systems Security, Godbole, Wiley-India
7. Information Security Principles and Practice, Deven Shah, Wiley-India
8. Security in Computing by Pfleeger and Pfleeger, PHI
9. Build Your Own Security Lab : A Field Guide for network testing, Michael Gregg, Wiley India

(b) Open source software and website:

1. https://www.wireshark.org/
2. https://nmap.org/
3. https://www.whois.com/
4. https://www.vlab.co.in/

Suggested Practical List, if any:

1.	Implement Caesar cipher.
2.	Implement Brute Force attack on Caesar cipher.
3.	Implement Mono-alphabetic cipher.
4.	Implement Play-fair cipher.
5.	Implement Hill cipher.
6.	Perform DES encryption technique with cryptool.
7.	Write a program to implement RSA algorithm.
8.	Write a program to implement Diffi-Hellmen Key exchange Method.
9.	Perform digital signature algorithm with cryptool.
10.	Perform various types of port scanning using Nmap/Zenmap.
11.	Study and demonstrate use of ping, tracert, nslookup, whois
12.	Demonstrate use of Wireshark to capture and analyze the network traffic.

Suggested Activities for Students, if any:

- Study of security architecture of your institute's network.
- Study recent case studies related to this course.
- Visit national as well as state level cyber crime portal.
- Study and discuss different types of cyber attacks.

- Study of tools to launch different cyber attacks and preventive ways for the same.

CO- PO Mapping:

Semester-3	**Information and Network Security**							
	POs							
Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	3	3	3	3	-	-	1	-
CO2	3	3	2	3	-	-	-	-
CO3	3	3	3	3	-	-	-	-
CO4	3	3	1	2	-	-	-	-
CO5	3	3	2	3	-	-	-	3

*Legend: '**3**' for high, '**2**' for medium, '**1**' for low and '**-**' for no correlation of each CO with PO.*

Note: The CO-PO mapping is indicative; the institute/faculty member can change as required.

* * * * * * *