GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Bachelor of Computer Applications

Level: Under Graduate

Course / Subject Code: BC04001031

Course / Subject Name: Cryptography and Network Security

w. e. f. Academic Year:	2025-26
Semester:	4
Category of the Course:	Core Course

Prerequisite:	Fundamental knowledge of Networking, Mathematical Concepts: Random Number, Number Theory, Finite Field.
Rationale:	• The information exchange through the network plays a vital role for end users. The confidentiality of such information is a prime importance. • Various cryptographic techniques are being used to achieve confidentiality. • The subject covers various important topics concern for confidentiality like symmetric and asymmetric cryptography along with the network security concepts like authentication, digital signature and key distribution.

Course Outcome:

After Completion of the Course, Student will able to:

No.	Course Outcomes	RBT Level*
1	Describe the basic concepts of cryptography and network security	RM, UN
2	Compare and contrast various cryptographic algorithms	UN, AN
3	Illustrate the asymmetric key cryptography and Diffie-Hellman Key Exchange Algorithm	AP, AN
4	Analyze the message authentication code and hash functions	AP, AN
5	Discuss Network security at transport layer and application layer	UN, AN

*RM: Remember, UN: Understand, AP: Apply, AN: Analyze, EL: Evaluate, CR: Create

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	Weightage (%)
1	**Introduction:** Cyber Security, Information Security and Network Security, Security Objective, Challenges of Information Security, OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, Cryptography, Network Security, Trust and Trustworthiness, Standards	6	10
2	**Symmetric Ciphers:** Symmetric Cipher Model, Cryptography, Cryptanalysis and Brute-Force Attack, Substitution Techniques: Caesar Cipher, Monoalphabetic Ciphers, Playfair Cipher, Hill Cipher, Polyalphabetic Ciphers, One-Time Pad, Transposition Techniques, Stream Cipher and Block Cipher, Feistel Cipher Structure, Data Encryption Standard (DES) Encryption, Advance Encryption Standard (AES) Encryption, Block Cipher Modes of Operation: ECB, CBC, CFB,OFB, CTR, Principal of Pseudorandom Number Generation, RC4	12	30
3	**Asymmetric Ciphers:** Public Key Cryptosystem, Applications for Public Key Cryptosystems, Requirements for Public key Cryptosystem, RSA Algorithm, Diffie Hellman Key Exchange Algorithm, Man-in-the-Middle Attack	9	20
4	**Cryptographic Data Integrity:** Application of Cryptographic Hash Functions: Message Authentication and Digital Signatures, Secure Hash Algorithm (SHA), Message Authentication Code (MAC), Requirements for Message Authentication Codes, HMAC, Pseudo Random Number Generation (PRNG) Using Hash Functions and MACs, Digital Signature Properties, Digital Signature Requirements	9	20
5	**Network Security:** Web Security Threads, Web Traffic Security Approaches, Transport Layer Security (TLS) Architecture, TLS Record Protocol, Alert Protocol, Handshake Protocol, SSL/TLS Attacks, Hyper Text Transfer Protocol Secure (HTTPS), Secure Shell (SSH)	9	20
	Total Hours:	**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	20	30	30	10	-

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

References/Suggested Learning Resources:

Textbook:

1. Cryptography and Network Security Principles and Practice, By: William Stallings, 8th Edition, Pearson Education India, ISBN: 978-1-292-43748-4

Reference Books:

1. Cryptography and Network Security, By: Behrouz A. Forouzan and Debdeep Mukhopadhyay, 3rd Edition, Mc Graw Hill Publication, ISBN: 978-9339220945
2. Network Security: The Complete Reference, By: Roberta Bragg, Mark Rhodes-Ousley, Keith Strassberg, Mc Graw Hill Publication, ISBN: 978-0070586710
3. Cryptography and Network Security, By: Atul Kahate, 3rd Edition, Mc Graw Hill Publication, ISBN: 978-1-25-902988-2
4. Cryptography and Security, By: C K Shyamala, N Harini, Dr. T R Padmanabhan, Wiley Publication, ISBN: 978-8126580392

List of Useful websites / MOOCs

1. Learners are advised to opt for NPTEL and SWAYAM courses that are relevant to this course

Suggested Course Practical List:

List of Experiments using any programming language (Preferably use Java)

1	Write a program to implement caesar cipher.
2	Write a program to implement brust force on caesar.
3	Write a program to implement mono alphabetic cipher.
4	Write a program to implement playfair cipher.

5	Write a program to implement hill cipher.
6	Write a program to implement poly-alphabetic cipher.
7	Write a program to implement DES encryption.
8	Write a program to implement AES encryption.
9	Write a program to implement RSA algorithm.
10	Write a program to implement diffi-hellmen key exchange.
11	Write a program to implement SHA-1 algorithm.
12	Write a program to implement digital signature.
13	Study and use of wireshark to capture and analyze the network traffic.

CO- PO Mapping:

Semester : 4	**Course Name : Cryptography and Network Security**										
	POs										
Course Outcomes	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**
CO1	2	2	3	2	-	-	2	-	-	-	-
CO2	2	2	2	2	-	-	-	2	-	-	-
CO3	3	3	2	2	-	2	-	-	-	-	-
CO4	3	2	3	2	-	2	-	-	-	-	-
CO5	2	2	3	1	2	2	-	-	-	-	-

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

* * * * * * *