Yagna Singh Charitable Trust's (Regd.)
THAKUR COLLEGE OF
ENGINEERING & TECHNOLOGY
Autonomous College Affiliated to University of Mumbai
Approved by All India Council for Technical Education(AICTE) and Government of Maharashtra(GoM)
Conferred Autonomous Status by University Grants Commission (UGC) for 10 years w.e.f. A.Y. 2019-20
Among Top 250 Colleges in the Country where NIRF India Ranking 2020 in Engineering College category
• ISO 9001:2015, 14001:2015, 45001:2018 Certified • Programmes Accredited by National Board of Accreditation (NBA), New Delhi
• Institute Accredited by National Assessment and Accreditation Council (NAAC), Bengaluru
tcet
Estd. 2001

10 SEP 2025

IN-SEMESTER EXAMINATION-I
TE (Semester-V)
SUBJECT – Cryptography and Network Security

Branch: IT
Div.: ALL
Duration: 60 Minutes
Instructions –

Date: 04/09/2025
Timing: 4:00 PM to 5:00 PM
Maximum Marks: 20

1. All questions are compulsory.
2. Assume suitable data wherever necessary and state the assumptions made.
3. Diagrams / sketches should be given wherever necessary.
4. Use of logarithmic table, drawing instruments and non-programmable calculators is permitted.
5. Figures to the right indicate full marks.

Q.1		Answer any 5 of the following questions	Marks	Course Outcomes	Learning Levels
	a.	Enlist the possible attacks on Hash Function and MAC.	2	3	R
	b.	Enlist Authentication Functions.	2	3	R
	c.	Differentiate Confusion and Diffusion.	2	2	AN
	d.	Define the Block Cipher Design principles.	2	2	U
	e.	Define is a 'denial of service' attack?	2	1	U
	f.	Encrypt the following message using a mono-alphabetic substitution cipher with key = 4 "This is a book on Security".	2	1	A
	g.	Encrypt the message "She is listening" using the 5-character keyword "MAGIC" using Vigenere cipher	2	1	A
Q.2	a.	Explain Electronic Code Block (ECB) mode of block cipher operation with suitable diagram.	5	2	U
		OR			
	b.	Compare DES and Triple DES.	5	2	AN
Q.3	a.	Explain why Authentication Required in cryptography.	5	3	U
		OR			
	b.	Explain characteristics of Hash Function.	5	3	U

IN-SEMESTER EXAMINATION-II

T.E. (Semester-V)

SUBJECT – Cryptography and Network Security

Branch: IT
Div.: ALL
Duration: 60 Minutes

Date: 17/10/2025
Timing: 3:30-4:30PM
Maximum Marks: 20

Instructions –

1. All questions are compulsory.
2. Assume suitable data wherever necessary and state the assumptions made.
3. Diagrams / sketches should be given wherever necessary.
4. Use of logarithmic table, drawing instruments and non-programmable calculators is permitted.
5. Figures to the right indicate full marks.

Q.1		Answer any 5 of the following questions	Marks	Course Outcomes	Learning Levels
	a.	Describe and differentiate Authentication and Authorization.	2	4	U
	b.	State one advantage of multi-factor authentication over single-factor authentication.	2	4	R
ESE	c.	Differentiate between IDS and IPS.	2	5	R
ISE-II	d.	List and explain types of Intruders.	2	5	R
	e.	State the main purpose of the PGP protocol in secure communication.	2	6	U
	f.	State Fragmentation and Compression services of SSL.	2	6	U
	g.	Compare and analyse transport mode and tunnel mode of IPsec.	2	6	AN
Q.2	a.	Explain the difference between a virus and a Trojan horse. Provide an example of each.	5	4	U
		OR			
	b.	Explain Software Flaws and explain any one in detail.	5	4	R
Q.3	a.	Define Spoofing? Explain any two types with examples	5	5	U
		OR			
	b.	Explain distributed denial of service (DDOS) with proper figure.	5	5	U

END SEMESTER EXAMINATION, NOV 2025
T.E. SEMESTER V (CBCGS-HME 2023)

04 DEC 2025

Branch:	**Information Technology**	**Q.P. Code:**	**E566RN255-2**
Subject:	**Cryptography and Network Security**	**Duration:**	**2 Hours**
Subject Code:	**PCC-IT 504**	**Max. Marks:**	**60**

Instructions: 1. **All sections are compulsory**
2. **Figures to the right indicate full marks.**
3. **Assume suitable data if necessary and state the assumptions clearly.**

Section-I **Short Answer Questions (Answer any 05 questions out of 06)** **(10 Marks)**
(Fundamental, Core Types)

Q. No.		Marks	CO	RBT Level	PI
1	Encrypt the following message using a mono-alphabetic substitution cipher with key = 4 "This is a book on Security".	2	1	A	1.7.1
2	State the modes of operation of Block Cipher.	2	2	R	1.7.1
3	List out the Hashing algorithms.	2	3	R	1.7.1
4	Explain incomplete mediation in software security.	2	4	U	2.5.2
5	State the primary purpose of a firewall in network security?	2	5	R	1.7.1
6	Compare transport mode and tunnel mode of IPsec.	2	6	U	2.6.4

Section-II **Descriptive Answer Questions (Answer any 04 out of 06)** **(20 Marks)**
(Descriptive, Comprehension Types)

1	Distinguish between passive and active security attacks. Name some passive attacks. Name some active attacks.	5	1	AN	2.6.4
2	Explain Cipher Feedback (CFB) mode of block cipher operation with suitable diagram.	5	2	U	1.7.1
3	Discuss working of Digital Signature.	5	3	AN	1.7.1
4	Explain the difference between a virus and a Trojan horse. Provide an example of each.	5	4	U	2.6.4
5	Describe a SYN flood attack and a UDP flood attack, including their impact on network services.	5	5	AN	2.6.4
6	Discuss and analyze the security mechanisms SSL/TLS uses to protect against common attacks, such as man-in-the-middle (MITM) attacks and eavesdropping.	5	6	AN	2.5.2

Section-III **Long Answer Question (Answer any 03 out of 05)** **(30 Marks)**
(Application, Analytical, Evaluation, Design Type)

1	In an information exchange scenario, A and B are exchanging data and decide to use the Diffie Hellman key exchange where prime no. q is 7, alpha is 5. Each chooses its own private key to exchange are 3 & 4 respectively. Determine What is the common secret key? What are their public key to exchange?	10	2	A	2.5.1
2	A school wants to protect student report cards stored on a computer. The IT teacher decides to encrypt all report card files using AES-128 before saving them. Explain why using AES-128 is a good choice for protecting the report card files. Justify your answer by describing how AES keeps the data safe from unauthorized people, and what could happen if the encryption key is shared or leaked.	10	3	AN	1.7.1

3	Explain the concept of "something you know, something you have, and something you are" in the context of authentication factors.	10	4	AN	2.6.4
4	Create a scenario involving ARP spoofing and explain how it could be used by an attacker to intercept network traffic. Describe countermeasures to prevent or detect such an attack.	10	5	E	2.5.1
5	Describe Authentication Header (AH) Protocol od IPsec in detail with neat diagram. Mention its applications.	10	6	AN	2.5.2