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
Amongst Top 300 Colleges in the Country, Ranked 151st in NIRF India Ranking 2019 in Engineering College category
ISO 9001:2015, 14001: 2015, 50001: 2018 Certified • Programmes Accredited by National Board of Accreditation (NBA), New Delhi
• Institute Accredited by National Assessment and Accreditation Council (NAAC), Bangalore

IN-SEMESTER EXAMINATION-I

TE (Semester-V)

SUBJECT – Cryptography and Network Security

Branch: IT
Div.: IT
Duration: 60 Minutes

Date: 29/08/2024
Timing: 12:00 PM to 1:00 PM
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.	State the Kerckhoff's Principle?	2	1	U
	b.	Encrypt the following message using a mono-alphabetic substitution cipher with key = 4 "This is a book on Security".	2	1	A
	c.	Define mono-alphabetic cipher? Why is mono-alphabetic cipher difficult to crack?	2	1	U
	d.	Identify the Broad steps in DES.	2	2	U
	e.	Draw Block diagram of RC5.	2	2	A
	f.	Enlist Authentication Functions.	2	3	R
	g.	List out the Hashing algorithms.	2	3	R
Q.2	a.	Explain Cipher Feedback (CFB) mode of block cipher operation with suitable diagram.	5	2	U
		OR			
	b.	Explain encryption steps in RC5 algorithm.	5	2	R
Q.3	a.	Differentiate between MD5, SHA-1, SHA-2, SHA-3.	5	3	U
		OR			
	b.	Compare HMAC and CMAC.	5	3	AN

Estd. 2001

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
Amongst Top 200 Colleges in the Country, Ranked 151st in NIRF India Ranking 2019 in Engineering College category
• ISO 9001:2015, 14001:2015, 50001:2018 Certified • Programmes Accredited by National Board of Accreditation (NBA), New Delhi
• Institute Accredited by National Assessment and Accreditation Council (NAAC), Bangalore

IN-SEMESTER EXAMINATION-II

T.E. (Semester-V)

SUBJECT – CRYPTOGRAPHY AND NETWORK SECURITY

Branch: IT
Div.: ALL
Duration: 60 Minutes

Date: 19/10/2024
Timing: 12:00 PM to 01:00 PM
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.	Define buffer overflow vulnerability.	2	4	R
	b.	State difference between viruses and worms.	2	4	R
	c.	Define Honey pot.	2	5	U
	d.	List and explain types of Intruders.	2	5	R
	e.	Discuss Message Integrity and Confidentiality Services of SSL protocol.	2	6	AN
	f.	Compare and analyze transport mode and tunnel mode of IPsec.	2	6	AN
	g.	State the main purpose of the PGP protocol in secure communication.	2	6	U
Q.2	a.	Explain the concept of "something you know, something you have, and something you are" in the context of authentication factors.	5	4	A
		OR			
	b.	Explain the role of a buffer overflow in executing arbitrary code. Provide an example scenario.	5	4	U
Q.3	a.	Define Intrusion Detection Systems (IDS) and explain two general types of IDS.	5	5	U
		OR			
	b.	Explain the concept of a DNS spoofing attack. How can it be used to redirect users to malicious websites?	5	5	U

Lingdo 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
Amongst Top 200 Colleges in the Country, Ranked 193rd in NIRF India Ranking 2019 in Engineering College category
• ISO 9001:2015 Certified • Programmes Accredited by National Board of Accreditation (NBA), New Delhi
• Institute Accredited by National Assessment and Accreditation Council (NAAC), Bangalore
Estd. in 2001
Website : www.tcetmumbai.in

END SEMESTER EXAMINATION, DEC 2024

03 DEC 2024

T.E. SEMESTER V (CBCGS-HME 2023)

Branch:	**IT**	**Q.P. Code:**	**ED245ITR6S5-1**
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) (Fundamental, Core Types)**				**(10 Marks)**
Q. No.		**Marks**	**CO**	**RBT Level**	**PI**
1	Encrypt the message "She is listening" using the 5-character keyword "MAGIC" using Vigenere cipher	2	1	A	1.7.1
2	List the modes of operation of Block Cipher.	2	2	R	1.7.1
3	Enlist the possible attacks on Hash Function and MAC.	2	3	R	1.7.1
4	State one difference between viruses and worms.	2	4	R	2.6.4
5	Differentiate between IDS and IPS.	2	5	R	2.6.4
6	Discus the need of security services at transport layer of Internet protocol.	2	6	R	1.7.1
Section-II	**Descriptive Answer Questions (Answer any 04 out of 06) (Descriptive, Comprehension Types)**				**(20 Marks)**
1	Explain Affine cipher with example.	5	1	U	1.7.1
2	Compare DES and Triple DES.	5	2	AN	2.6.4
3	Explain why Authentication Required in cryptography.	5	3	U	1.7.1
4	Explain trapdoors with examples	5	4	U	2.5.2
5	Discuss the use of honeypots as a security mechanism and their advantages in detecting malicious activities	5	5	U	2.5.3
6	Discuss how Secure / Multipurpose Internet Mail Extension (S/MIME) can provide security services for e-mail	5	6	AN	2.5.3
Section-III	**Long Answer Question (Answer any 03 out of 05) (Application, Analytical, Evaluation, Design Type)**				**(30 Marks)**
1	Perform encryption and decryption using RSA algorithm with p=7,q=11,e=17 and M=8.	10	2	A	2.5.1
2	Which hashing algorithm, MD5 or SHA-3, is more effective for securing data? Why?	10	3	A	2.5.3
3	Analyze the risks associated with using weak passwords and password reuse across multiple online accounts. Propose strategies for users to manage their passwords securely.	10	4	AN	2.5.1

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	U	2.5.1
5	Discus four protocols defined by Secure Socket Layer (SSL) with neat diagram.	10	6	AN	2.5.2