

JK Lakshmipat University Jaipur

INSTITUTE OF ENGINEERING AND TECHNOLOGY

End Term Examination, December 2024

B. Tech. and BCA Vth Semester

Roll No.....

CS1233: Introduction to Cyber Security

Time: 2.5 hours

Max. Marks: 30

Instructions to students:

1. Scientific calculator (Non-programmable) is allowed.
2. Assume suitable data wherever required and mention it clearly.
3. Writing appropriate units, nomenclature, and drawing neat sketches/schematics/ flow chart wherever, required are an integral part of the answer.

Q.1B	Decode the following messages. (2 Marks) i). Caesar cipher using frequency analysis ESPNTASPCSLDMPPYMCZVPV ii). Use the Vigenere cipher Maplet to decipher the message (2 Marks) DUSLZ AHXSP VAWRM QGXSBILOH YYCVB BTRLZ I That was enciphered using the keyword "Knowledge".	04 Marks CO3
Q.1B	Define social engineering in the context of cybersecurity. Provide an example.	02 Marks CO1

Q.2A	Sumit has public RSA key ($N = 77$, $e = 13$), Sheetal wants to send the message $M = 7$ to Sumit. She encrypts the message using Sumit's public key. What is the value of the cipher text that Sheetal sends to Sumit? Also find out Sumit's private key? Show the complete process.	03 Marks CO4, CO3
Q.2B	The input into S-box 5 in DES is i). 101011 ii). 010011 What is the output, expressed in Binary and decimal (a single value in between 0 and 15, inclusive)? Note: - (S box 5 table given on second page)	03 Marks CO4, CO2
Q.2C	You are given - Prime number $p=31$ Generator $g=7$ Alice's private key is $a=3$ Bob's private key is $b=12$ You need to calculate Diffie Hellman Key Exchange for the followings - • Calculate Alice's public key A. • Calculate Bob's public key B. • Derive the shared secret S.	03 Marks CO5

Q.3A	The following was encrypted with a Playfair Cipher with keyword "RANSOMWARE". Decrypt the Cipher Text to original message. ICEKN SGCNY NQGEK DFTTF RSORG FATVW AORSG DNMFW PVQAG EMOXQ ZTRSN SHRBM RMWNE ZMBNY RHWXT IBNNS FDQOC REGVB NOPCG U	04 Marks CO2
Q.3B	You are tasked with testing the security of a web application for a company. Outline the steps you would take during the penetration testing process, specifying the tools you would use and justifying their selection for each step. List at least three tools commonly used at each stage.	03 Marks CO4
OR		
Q.3C	Explain the difference between symmetric and asymmetric encryption and give examples of when each type should be used in a corporate environment.	03 Marks CO3

Q.4A	A company experiences a ransomware attack, encrypting critical business files. Discuss the possible responses and the long-term measures to prevent such attacks in the future.	03 Marks CO3
Q.4B	"A multinational corporation recently faced a multi-faceted cyberattack involving a virus and a worm that exploited vulnerabilities in the network. The attack bypassed the company's firewall and generated multiple alerts in the IDS, but these alerts were not addressed in time. (A) Analyze how a virus and a worm could have been used together to maximize the impact of the attack. (B) Explain the possible firewall weaknesses that allowed the attack to succeed and suggest configurations to mitigate similar issues in the future. (C) Discuss the role of the IDS in this scenario, its limitations, and how it could be improved to detect and respond to threats effectively. (D) Recommend a layered cybersecurity approach, combining firewalls, IDS, antivirus solutions, and organizational best practices to prevent such attacks." (E) Highlight the importance of employee training, regular security audits, and patch management in ensuring long-term security for organizations.	05 Marks CO4, CO5, CO7

S[5]																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

***** All The Best *****