Seat No.: _____ Enrollment No.: _____

NATIONAL FORENSIC SCIENCES UNIVERSITY

PRACTICAL EXAMINATION MAY 2025

Date: 05/05/2025

Subject Code: CTMSCS SII L1/ CTMSDFIS SII L1 **Total Marks: 50**

Subject Name: Network Security Lab/ NSF LAB **Time: 30 Minutes**

Instructions:

1. **Attempt all questions.**
2. **Figures to the right indicate full marks.**
3. **Assume Suitable data.**

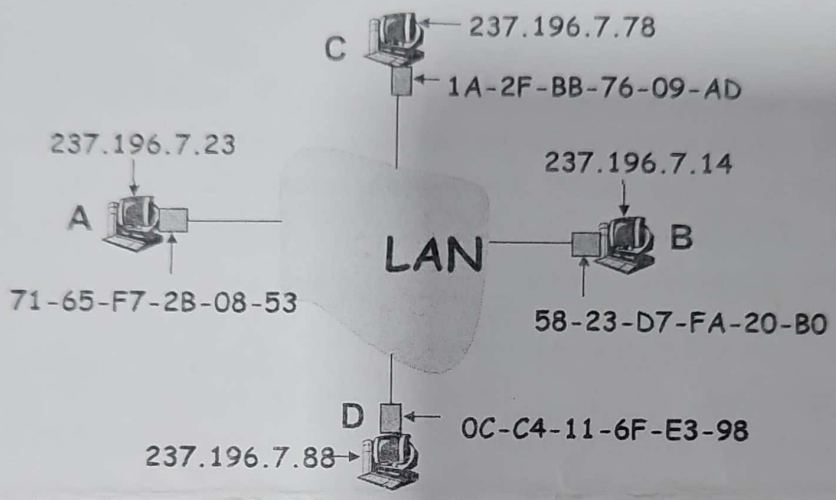
SET-1: Roll Number ending with 4, 8, 12, 16, 20, 24 28
SET-2: Roll Number ending with 3, 7, 11, 15, 19, 23 27
SET-3: Roll Number ending with 2, 6, 10, 14, 18, 22 26
SET-4: Roll Number ending with 1, 5, 9, 13, 17, 21 25

SET		Questions	Marks
SET-1	Q.1	Write a Python program that implements the ***RSA encryption algorithm***. Demonstrate its usage by encrypting, decrypting and digital signature a given message.	25
	Q.2	Imagine a scenario where a distributed denial of service (DDoS) attack is targeting your organization's web servers. Outline the steps you would take to mitigate the impact and prevent future occurrences.	
SET-2	Q.1	Configure Quality of Service parameters in ***Cisco Packet Tracer*** to prioritize specific types of network traffic of NFSU website. Test and verify the effectiveness of QoS settings in managing network bandwidth.	
	Q.2	In the event of a security incident, such as a data breach or malware infection, describe the steps you would take to contain the incident, investigate the root cause, and communicate effectively with stakeholders.	
SET-3	Q.1	Requirement (an open-source rainbow table-based password cracking tool) Hash values of passwords to crackOptional: Any additional rainbow tables or wordlists Task: • Compare the cracked passwords with the original list. • Note how many passwords were successfully cracked.	
	Q.2	An employee's laptop has been lost or stolen. Describe the steps you would take to ensure that sensitive data on the device remains secure and cannot be accessed by unauthorized individuals.	
SET-4	Q.1	Task: Perform a vulnerability assessment on a NFSU website to identify open ports, running services, and potential weaknesses. Compile a report with identified vulnerabilities and remediation suggestions. Tools: Nmap, Nessus, OpenVAS, Metasploit, etc. Objectives: Discover network vulnerabilities, evaluate risk levels, and propose security improvements to harden the network.	
	Q.2	Imagine an employee falls victim to a phishing attack and unknowingly installs malware on their workstation. Detail the measures you would take to detect and remove the malware, as well as prevent similar incidents in the future.	

END OF PAPER

National Forensics Sciences University, Goa Campus
M.Sc. CS and MSc DFIS - Semester -II
Mid- Semester Examination

Subject Code: CTMSCS SII P1/ CTMSDFIS SII P3 **Date: 18/03/2025**
Subject Name: Network Security and Forensics
Time: 90 Minutes **Total Marks: 50**
Instructions –
1) Answer all questions.
2) Assume suitable data.
3) Scientific Calculator is allowed.
4) Parts of the question should attend the same place.

Q.1	Attempt all.	**20 marks**
(a)	 Consider the above network topology, **User A** wants to communicate with **User B**. Explain the explain ARP protocol with respect to this scenario. Further consider **User C** as the attacker and explain the ARP spoofing in the same topology. Also highlight the all-possible attack vectors and attack surfaces.	5 Marks
(b)	A company wants to set up a web server accessible from the internet. Explain the role of the DNS server in this scenario.	5 Marks
(c)	Encrypt the following message using **Playfair cipher**. Message: **jacuzzi operation** Key: **extrajudicially**	5 Marks
(d)	(i) Calculate the power modulo, $191^{930} \bmod 103$. (ii) What is the purpose of TTL field in IP packet? How is TTL useful for forensic purpose?	5 Marks
Q.2	Attempt three.	**15 Marks**
(a)	Write note on DOS and distributed denial-of-service (DDoS) attacks.	5 marks
(b)	What would you do if ***nmap*** port scans are blocked by network security administrator? How would you gather host information in such case?	5 marks
(c)	Explain the differences between error control and flow control.	5 marks
(d)	Explain the WLAN architecture?	5 marks

Q.3	Attempt all.	**15 Marks**
(a)	Use two global prime number ***17*** and ***31***, the value of ***e*** is ***7*** and message ***M= 3***, calculate the public key, private key, and the corresponding cipher text. Also prove that *RSA* decryption is the inverse of *RSA* encryption.	08 Marks
	OR	
	Use two global prime number ***37*** and ***43***, the value of ***e*** is ***71*** and message ***M= 2***, calculate the *public key*, *private key*, and the corresponding cipher text. Also prove that *RSA* decryption is the inverse of *RSA* encryption.	
(b)	*Alice* and *Bob* wish to swap keys by using *Diffie-Hellman* key exchange algorithm and are agreed on prime ***p = 23*** and base or generator is ***g= 5***. Calculate the *secret key* of each user and *shared session key* for both the users. Also explain with the same question that how can *Eve* (untrusted third person) exploit *Man-in-Middle attack*.	07 Marks
	OR	
	Alice and *Bob* wish to swap keys by using *Diffie-Hellman* key exchange algorithm and are agreed on prime ***p = 31*** and base or generator is ***g= 3***. Calculate the secret key of each user and shared session key for both the users. Also explain with the same question that how can *Eve* (untrusted third person) exploit Man-in-Middle attack.	

~~~~END OF PAPER~~~~

Enrolment No._____

NATIONAL FORENSIC SCIENCES UNIVERSITY
GOA CAMPUS
M.Sc. DFIS - Semester -II/ M.Sc. Cyber Security Term Assessment-I

Subject Code: CTMSDFIS SII P1/ CTMTCS SII P1 **Date: 11/02/2025**
Subject Name: Network Security & Forensics/ Network Security
Time: 45 Minutes **Total Marks: 25**

Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**

Q1 To Q10 each for 1 mark (10x1=10)

Fill the appropriate answer:

Q 1 The process of adding headers and trailers to data when it moves down the OSI layers is called_____

Q 2 A router uses a shortest path to determine the path for forwarding packets.

Q 3 A gateway can connect two networks with different architectures, protocols, or data formats

Q 4 The transport layer of the OSI model is responsible for end-to-end communication.

Q 5 In the Playfair cipher, if two letters in a digraph appear in the same row of the matrix, they are replaced by the letters immediately _____ in the same row.

Q 6 The ling analysis attack is a cryptanalysis method that attempts to deduce the encryption key by analyzing multiple ciphertexts encrypted with the same key.

Q 7 The Vigenère cipher is a type of _____ cipher that uses a repeated keyword to encrypt plaintext.

Q 8 A cryptographic system is considered highly secure if the ciphertext provides no additional information about the plaintext beyond what is already known.

Q 9 A product cipher is a combination of _____ and _____ techniques applied repeatedly to enhance security.

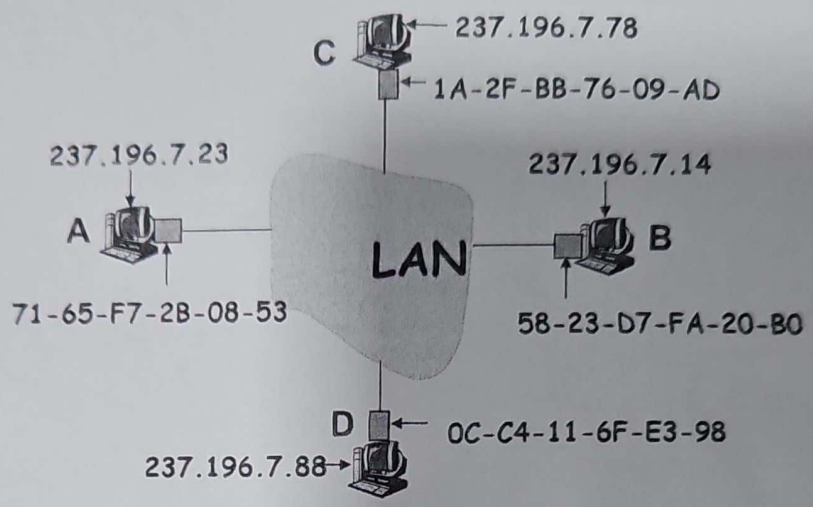
Q 10 _____ is a security measure that involves restricting user access to certain systems, applications, or data based on predefined policies.

Q11 to Q15 Descriptive 3 marks for each question (3x5=15)

Q11 Encrypt the plain text "prejudications" with the key "microprojectors" using Playfair cipher. Also, verify the plain text from the generated cipher text. **03 Marks**

Q12 Describe the role of the network layer in the OSI model. **03 Marks**

Consider the following Network: **(for Q 13-14)**



Q13 Consider the above network topology, **User A** wants to communicate with **User B**. explain ARP protocol with respect to this scenario. Further consider **User C** as the attacker and explain the ARP spoofing. **03 Marks**

Q14 With respect to the same network topology, explain TCP Session Hijacking and its countermeasures for this network attacks mentioned in question 13. **03 Marks**

Q 15 Explain following examples/terms: (Any two) **03 Marks**

(i) VPN vs VLAN

(ii) Local DNS vs TLD

(iii) IDS vs IPS