National Forensics Sciences University, Goa Campus
Mid- semester Examination
M.Sc. Cyber Security- Semester -II

Branch – Cyber Security	**Sem – II**	**Date- 26/03/2024**
Subject Name- Network Security & Forensic		Subject Code- CTMSCS SII P1
Time- 1.5 Hours		Max. Marks- 50

Instructions - 1) Answer all questions. 2) Assume suitable data.

Q.1	Attempt all.	**20 Marks**
	a. If a brute-force attack is attempted on a symmetric encryption algorithm with a key size of 56 bits, and the attacker can try 1 million keys per second, how long will it take on average to break the encryption?	5 Marks
	b. Use *Vigenere Cipher* with key ***Forensic*** to encrypt the message *"Context is everything".*	5 Marks
	c. Encrypt the following message using *Playfair* cipher. Message: ***The jail is a key component of the judicial system's enforcement arm.*** Keyword: ***judiciary***	5 marks
	d. Explain the difference between a router and a switch in terms of their functionalities.	5 Marks
Q.2	Attempt all questions **(Q 2(a)- 2 (c)):**	**15 Marks**
	a. Your company recently experienced a security breach. As part of the response team, explain how IDS, IPS, and Firewalls function to detect and prevent unauthorized access and malicious activities within the network perimeter. Provide examples of how these devices could have mitigated the recent security breach.	5 Marks
	b. What is the significance of flow control? Why is it important for the security point of view?	5 Marks
	c. A competitor company has recently suffered a data breach, leading to the exposure of sensitive information. Analyze common cryptographic attacks such as brute-force attacks and cryptographic vulnerabilities. Propose defensive strategies and best practices to mitigate these attacks,	5 Marks

	including the use of strong encryption algorithms, proper key management, and regular security audits. Evaluate the effectiveness of these defenses in preventing similar attacks in your organization.	
Q. 3	Attempt any **two:**	**8 Marks**
	a. Describe a scenario where a chosen plaintext attack can be conducted on a symmetric encryption system. Discuss possible countermeasures to mitigate this attack.	4 Marks
	b. What is the **zero point** of an elliptic curve?	4 Marks
	c. What is the significance of **iptable** in the Linux hardening? Also provide the example.	4 Marks
Q.4	Attempt **any one**	**7 Marks**
	a. 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.	7 Marks
	OR	
	a. *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.* $x_a = 3$ $x_b = 7$	7 Marks

10 17

—14—