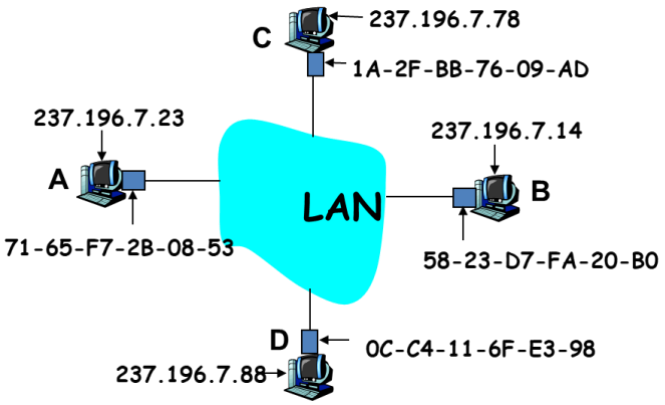
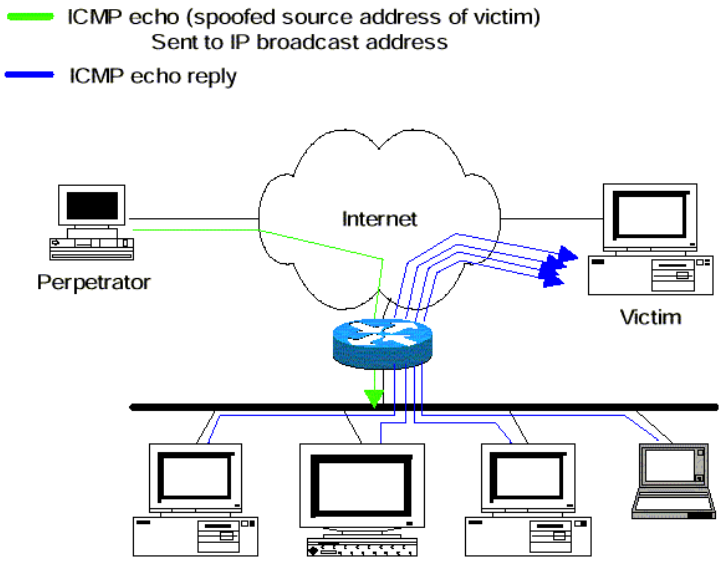
National Forensics Sciences University

Subject Name- Network Security & Forensic

Q. N.	Question	Marks
Q.1 (A)		05
(B)		05
Q.2 (A)	Explain the rotor machine in detail.	05
(B)		05
Q 3 (A)	What is digital signature? What is the use of message digest in Digital Signature?	05
		05
Q 4 (A)	What are the IEEE 802.11 standards for WLAN architectures?	05
(B)	Write short notes on wireless PAN?	05
Q 5		10
Q 6	Using RSA algorithm, Find n, d, and c, if p=11, q=3, e=3. Encrypt "NFSU" Message.	07
	What is TCP Session Hijacking? How is it done?	05
	Differentiate the Host and Network-Based Intrusion Detection Systems	05
	Explain RC-4 encryption technique.	05
	Consider the following Network:	08

	 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	
	Explain following examples/terms: (i) VPN vs VLAN (ii) Local DNS vs TLD (iii) IDS vs IPS	06
	Differentiate the Non repudiation, Eavesdropping, and Masquerading.	06
		08
		08
	What is the significance of **iptable** in the Linux hardening? Also provide the example.	05
		05
	What is the **zero point** of an elliptic curve?	05
	What is the significance of flow control? Why is it important for the security point of view?	05
		07
	Consider the following network scenario:  i. Identify and explain the attack on the above scenario. ii. Also mention the countermeasures to protect this kind of attacks.	08

	Encrypt the following message using **Playfair cipher.** Message: **quillaja** Keyword: **jonquil**	05
	Use **Vigenere Cipher** with key **HEALTH** to encrypt the message **"Life is full of surprises".**	05
	With the help of example, define virtual private network (VPN)? How does it provide the end-to-end security?	05
	What is meant by piggybacking? What are its advantages and disadvantages?	05
	What is the standard procedure used for network forensics?	05
	What is Live Acquisition? How is it performed?	05
	Explain the brute force attack. How to prevent it?	05
	What is port scanning?	05
	What is MITM attack?	05
	Explain TCP Three-way handshake.	05
	What are the disadvantages of penetration testing?	05
	Explain the concept of cross-site scripting.	05
	What are the risks associated with public Wi-Fi?	05
	What are differences between symmetric encryption and asymmetric encryption?	05
	Explain a buffer overflow attack.	05
	Name some tools used for packet sniffing.	05
	What do you understand by Risk, Vulnerability & Threat in a network?	05
	Explain SQL Injection and how to prevent it?	05
	One of the staff members in XYZ subscribes to many free magazines. Now, to activate her subscriptions one of the magazines asked for her month of birth, second asked for her year of birth, the other one asked for her maiden name. What do you infer from this situation? Justify.	05
	What is Cross-Site Scripting and how it can be prevented?	05
	What *tcpdump* and *pcap*? Explain.	05
	Explain various ways in which data integrity can be verified?	05
		05
	What is Directory Listing? What is its impact? How to prevent it?	05
	Will cyber warfare replace traditional warfare?	05
	What are the defining characteristics of information warfare?	05