Indian Institute of Technology Patna Date: 26 April 2025 MIDSEM: CS 457: Big Data Security

DURATION: 3 HOURS. 3-6PM Full Marks 100

Instruction: All questions are compulsory. No Free hand diagrams allowed. If free hand diagrams are seen, you will be penalized 50% of marks. No doubts would be entertained. Write suitable assumptions, if necessary. Students are allowed to use scientific calculators. Each question from Q1 should start on a fresh page. So if the Q1 takes 1/2 page to finish, begin Q2 from the next page. **If two questions are written on the same page, both will be marked 0.**

	Master Answers					
Q1	1A=	1B=				
Q2	ENCYPTED MSG =					
Q3	ENCYPTED MSG =					
Q4	S=		M=			
Q5	H=	E=	L=	O=		
Q6	6.1=	6.2=	6.3=	6.4=	6.5=	
Q7	7.1 SQL Injection happens?		7.2 SQL Injection happens if parameterized are used?			
Q8	8A (Packet Allowed?)		8B Justification in main answer please			
Q9	9A		9B Justification in main answer please			
Q10	10A login attempt be allowed or denied?		10B Justification in main answer please			
Q11	IDR =					
Q12	PRECISION		RECALL			
Q13	Backup Tools		Two Anti Virus		Two VPN tools	
Q14	Type 1 IDS Name		Type 2 IDS Name			

Figure 1: Make this master sheet on the first page of your answer sheet using scale pencil. You need to write the final answers for numericals in this table. However, the complete working of the numericals needs to be shown later also. If this table is **absent**, 50 percent marks will be deducted.

Q(1) Consider a plaintext message: "BIGDATA". The key for the Caesar cipher is 5. Ques A). Encrypt the message using the Caesar cipher. Ques B). Decrypt the ciphertext back to the original plaintext. Show detailed steps. **[Marks 5]**

Q(2) Given the following 8-bit binary values: Plaintext: 11011010 Key1: 10101010 Key2: 01100110 Key3: 11110000. Perform the following steps to demonstrate 3DES encryption (using XOR for simplicity in all steps): Step 1) Encrypt the plaintext using Key1. Step 2) Decrypt the result in Step 1 using Key2. Step 3) Encrypt the result in Step 2 again using Key3. What is the final encrypted result post Step 3? **[Marks 5]**

Q(3) Given a plaintext "BIGDATA" and a key "HOSTEL", encrypt the message using the Vigenère cipher. Assume 0 indexing. (a=0, b=1,...,z=25) **[Marks 5]**

Q(4) Given the RSA public key $(e, n) = (7, 33)$, the private key $(d, n) = (3, 33)$, and the message $M = 13$. 1) Create Digital Signature S for the the message M. 2) Verify the Digital Signature S using public key. **[Marks 5]**

Q(5) Using the RSA public key cryptosystem, with a = 1, b = 2 ... y = 25, z = 26. Using p = 3, q = 11, and d = 9, find e and encrypt "hello". Assume suitable assumption. Answer should be in numerical values. Provide the numerical encrypted values for H,E,L,O No doubts to be cleared. **[Marks 5]**

Q(6) True/False Questions with justification **[Marks 5]**

1. AES is a symmetric key encryption algorithm.
2. DES is more secure than AES.
3. Asymmetric encryption uses the same key for encryption and decryption.
4. RSA is an example of an asymmetric encryption algorithm.
5. Symmetric key encryption is generally faster than asymmetric encryption.

Q(7) A database uses the following access control for a table `Users`: Admin role: Full access. Guest role: Read-only access. An attacker attempts to execute the following SQL injection on a website's login form: `' OR 1=1; --` . The website uses parameterized queries to access the database.

1. What does the SQL injection attempt aim to do? Does it succeed if we don't use parameterized queries? Justify.
2. If the website uses parameterized queries, can the SQL injection succeed? Justify. **[Marks 5]**

Q(8) Consider the following stateful inspection scenario: 1) A stateful firewall tracks connections and their states. 2) A client sends a request to a web server on port 443 (HTTP). 3) The server sends a response back to the client on port 443. After the initial request, a second packet arrives from the client to port 443, which was not explicitly permitted by any firewall rule. Part A). Will the second packet be allowed or denied by the firewall? Part B). Explain why. **[Marks 5]**

Q(9) Consider a firewall that uses a packet filtering mechanism. The firewall has the following rule set: * Allow all incoming traffic from IP address 192.168.1.10 on port 80 (HTTP). * Deny all traffic from IP address 192.168.1.15. * Allow all outgoing traffic on port 443 (HTTPS). * Deny all traffic from IP address 192.168.1.20 to any destination.

You receive the following packet: * Source IP: 192.168.1.10 * Destination IP: 192.168.1.25 * Source Port: 80 * Destination Port: 443

Will the packet be allowed or denied by the firewall? Justify your answer. **[Marks 5]**

Q(10) Consider a system with the following Access Control List (ACL) for a database: 1) Allow access to **alice** from IP addr **10.1.1.10** to database **SalesDB** with read-only privileges. 2) Allow access to **bob** from IP address **10.1.1.20** to databa **SalesDB** with read-write privileges. 3) Deny access to **charlie** from any IP to **SalesDB**. 4) Allow access to **david** from IP address **10.1.1.30** to database **HRDB** with read-only privileges. You are given a login attempt with the following details:

User: alice **IP:** 10.1.1.10 **Database:** SalesDB

Part A) Will the login attempt be allowed or denied? Part B) Explain the reasoning behind the decision. **[Marks 5]**

Q(11) A company has deployed an IDS to monitor traffic for unauthorized access attempts. The IDS detected a total of 1400 intrusion attempts, out of which 200 were legitimate. The system also reported 100 missed intrusions. Calculate the Intrusion Detection Rate (IDR). Show detailed steps. **[Marks 5]**

Q(12) An Intrusion Detection System (IDS) monitors network traffic for potential security breaches. The system has been tested over 1000 events, and the following results were obtained: **True Positives (TP):** 120. **False Positives (FP):** 30. **True Negatives (TN):** 800. **False Negatives (FN):** 50. Compute Precision and Recall. Show detailed steps. **[Marks 5]**

Q(13) Provide software names for the following categories: 1) Two Backup & Recovery Tools, 2) Two popular anti-virus, 3) Two VPN tools. Describe each tool in 2-3 lines. **[Marks 5]**

Q(14) Briefly describe two types of IDS. **[Marks 5]**

Q(15) List any 5 cyber hygiene practices with their justification (2-3 lines per justification). **[Marks 5]**

Q(16) List any 5 Best Practices while using Social Media with their justification (2-3 lines per justification). **[Marks 5]**

Q(17) Draw the VPN architecture for Remote Access Virtual Private Network. No free hand diagram allowed. No explanation needed. **[Marks 5]**

Q(18) Describe Authentication issues wrt to Network Security. Describe using the diagram each of the protocol ap1.0, ap2.0, ap3.0, ap4.0, ap5.0 and the flaws associated with it and how the subsequent protocol approach improves over it. Assume Alice and Bob are the good parties communicating and Mallory is the malicious guy in between. (No free hand diagram allowed). **[Marks 20]**