DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

NITK-SURATHKAL

II Sem M.Tech (CSE-IS) Sub: Network Security Surprise Test :01

Date: 30-1-2025 Max Marks: 25

Note : Answer all the questions. Missing data may be suitably assumed.

1. What is Perfect Secrecy? Describe a system that achieves it. – 05 Marks
2. Explain briefly the concepts: one-way function, one-way hash function, trapdoor one-way function. --05 Marks
3. Describe the three main concerns with the use of passwords for authentication. Explain what is meant by a social engineering attack on a password. – 05 Marks
4. Explain how access control lists are used to represent access control matrices. Describe the environments in which they are widely used and their advantages and disadvantages. --05 Marks
5. An ideal password authentication scheme has to withstand a number of attacks. Describe five of these attacks. --05 Marks

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

NITK-SURATHKAL

II SEM M.Tech (CSE-IS)

Sub: Network Security Max Marks : 25 Course Code : CS851 Quiz No:2 Duration : 1.0 hrs

Note: Answer all the questions. Missing data may be suitably assumed.

1. Alice and Bob participate in a public-key infrastructure that enables them to exchange legally binding digital signatures.
   (i) Name two reasons why, for some purposes, Alice might prefer to use a message authentication code, instead of a digital signature, to protect the integrity and authenticity of her messages to Bob. [4 marks]
   (ii) Outline a protocol for protecting the integrity and authenticity of Alice's messages to Bob that combines the benefits of a public-key infrastructure with those of using a message authentication code. [4 marks]
2. Explain briefly mechanisms that software on a desktop computer can use to securely generate secret keys for use in cryptographic protocols. [5 marks]
3. Explain SSH keystroke timing attack. How does SSH defend against keystroke timing attacks? [5 marks]
4. What is a web application side channel attack? How do you defend against the same? [7 marks]

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

NITK-SURATHKAL

II SEM M.Tech (CSE-IS) Mid-Semester Examinations

Sub: Network Security — Max Marks : 50

Course Code : CS851 — Duration : 1.5 hrs

Note: Answer all the questions. Missing data may be suitably assumed.

1. a) Block ciphers usually process 64 or 128-bit blocks at a time. To illustrate how their modes of operation work, we can use instead a pseudo-random permutation that operates on the 26 letters of the English alphabet:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
M	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ek(m)	D	G	W	X	T	E	R	L	Y	Z	O	J	N	S	I	Q	P	C	U	H	B	V	F	A	M	K

As the XOR operation is not defined on the set {A, . . . , Z}, we replace it here during encryption with modulo-26 addition (e.g., C ⊕ D = F and Y ⊕ C = A).

(i) Decrypt the following ciphertexts, which were encrypted using

(A) Electronic codebook mode: UOMHDJT [2 marks]

(B) Cipher feedback mode: RVPHTUH [4 marks]

(C) Output feedback mode: LNMSUUY [4 marks]

(ii) Determine the CBC-MAC for the message TRIPOS. [4 marks]

b) Consider another small pseudo-random permutation, this time defined over the set of decimal digits {0, 1, 2, . . . , 9}, using modulo-10 addition instead of XOR (e.g., 7 ⊕ 3 = 0).

(i) You have intercepted the message 100 with appended CBC-MAC block 4.

The message represents an amount of money to be paid to you and can be of variable length. Use this information to generate a message that represents a much larger number, and provide a valid CBC-MAC digit, without knowing the pseudo-random permutation or key that the recipient will use to verify it. [4 marks]

(ii) What mistake did the designer of the communication system attacked in part (b)(i) make (leaving aside the tiny block size), and how can this be fixed? [2 marks]

2. Show how the DES block cipher can be used to build a 64-bit hash function. Is the result collision resistant? [5 Marks]

3. An automatic teller machine (ATM) communicates with a central bank computer for PIN verification. A 32-bit CRC code is added to each packet to detect transmission errors and then the link is encrypted using a block cipher in counter mode. Describe an attack that is possible in this setup. [5 marks]

4. Consider the problem of mitigation of DDoS attack on a web server. We discussed a solution to this problem using DLP in the class. Propose a solution using Integer Factorization problem.

    a) How do you generate the challenge for the attacker? [5 Marks]
    b) How do you generate different challenges for the different attackers? [5 Marks]
    c) How do you verify the response given by the attacker? [5 Marks]
    d) Explain the total solution along with its merits and demerits [5 marks]

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

NITK-SURATHKAL

II SEM M.Tech (CSE-IS) End-Semester Examinations

Sub: Network Security Time:2:00-5:00PM Max Marks : 100

Course Code : CS851 Date: 28-04-2025 Duration : 3 hrs Roll No:_____

Note: Answer all the questions. Missing data may be suitably assumed.

1. Consider the example of Web application side channel attacks discussed in the class. Kindly provide the details of actual information leaks in web applications. Also give details of mitigation of such side channel threats. – 10 Marks

2. Consider the situation of performing the forensic analysis of a HDD. You as a legal officer is required to perform the forensic analysis of the HDD used by a business establishment. Kindly outline the Standard Operating Procedure to be followed for the same. -- 10 Marks

3. How can AIML be used to improve the network security? What are the potential drawbacks or challenges of using AIML in network security? --10 Marks

4. How encryption is handled in Tor? What is an Onion address and how are they generated? -- 10 Marks

5. An RSA encryption routine calculates the value m^e mod n using a square-and multiply algorithm. During the execution of that algorithm, you can briefly hear a buzzing sound (through radio-frequency interference) on an AM radio receiver located near the computer. You record that sound, and discover that it is actually the following sequence of two different sounds A and B: BABAABABAAB. What is the value of e? --- 10 Marks

6. Consider a small pseudo-random permutation, defined over the set of decimal digits $\{0, 1, 2, \ldots, 9\}$, using modulo-10 addition instead of XOR (e.g., $7 \oplus 3 = 0$).
(i) You have intercepted the message 100 with appended CBC-MAC block 4. The message represents an amount of money to be paid to you and can be of variable length. Use this information to generate a message that represents a much larger number, and provide a valid CBC-MAC digit, without knowing the pseudo-random permutation or key that the recipient will use to verify it. --- 15 Marks

7. Briefly explain
(a) the function of a salt value in a password database [3 marks]
(b) two examples of covert channels in a file system protocol that is restricted to read-only operations under a mandatory access-control policy [2 marks]
(c) three types of common software vulnerabilities, with examples [9 marks]

(d) two problems solved by Cipher Block Chaining [2 marks]

(e) under which conditions will user U be able to remove a directory D in Berkeley Unix [4 marks]

8. (a) You have received a shipment of hardware random-number generators, each of which can output one 128-bit random number every 10 milliseconds. You suspect that one of these modules has been tampered with and that it actually produces only 30-bit random numbers internally, which it then converts via a pseudo-random function into the 128-bit values that it outputs

   (i) How does this form of tampering reduce the security of a system that uses a generated 128-bit random number as the secret key of a block cipher used to generate message authentication codes? [3 marks]

   (ii) Suggest a test that has a more than 0.5 success probability of identifying within half an hour that a module has been tampered with in this way. [6 marks]

   (b) Explain briefly

   (i) the encryption and decryption steps of Cipher Feedback Mode; [3 marks]

   (ii) why some operating systems ask the user to press a special key combination (e.g., Alt-Ctrl-Del) before each password login; [3 marks]

Mid-Semester Examination February 2024

Course Code: CS851 **Course Name:** Network Security

Duration: 90 Minutes **Max. Marks:** 40

Note: Answer all questions.

Q1. There are three typical ways to use Nonces as challenges. Suppose N_a is a nonce generated by A. A and B share key K, and f() is a function (such as an increment). The three usages of Nonce are shown below. [2+2+2]

(i) A → B: N_a
B → A: $E_K(N_a)$

(ii) A → B: $E_K(N_a)$
B → A: N_a

(iii) A → B: $E_K(N_a)$
B → A: $E_K(f(N_a))$

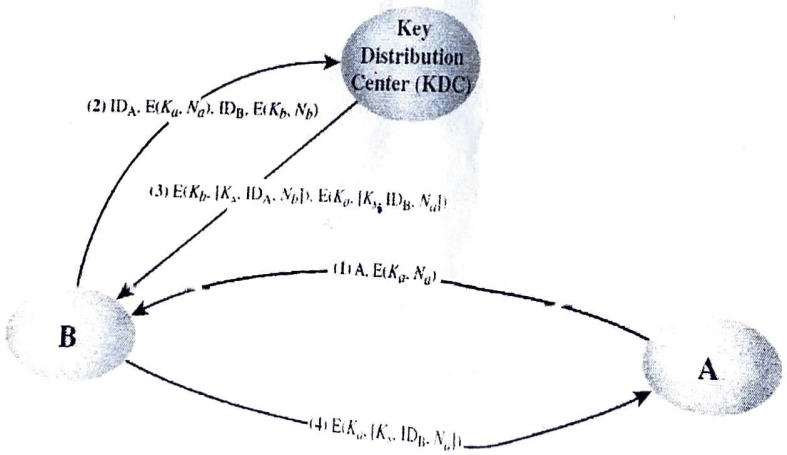
Describe situations for which each usage is appropriate.

Q2. (i) Design a lightweight protocol to enable secure online payment using the web client and server environment over the Internet. The proposed protocol must meet the following. [1.5×6]

- Provide Server Authentication
- Ensure Confidentiality and Integrity of payment-related data
- Provide Plain text access of payment-related data to the payment-approving bank only.
- Send payment approval intimation to the merchant and Gateway.
- Enforce the "Need-to-Know" security principle.
- Should use X.509 certificates

(ii) Compare the above-proposed protocol with SET (Secure Electronic Transaction) to show lightness. [5]

Q3. The following figure shows that one local area network vendor provides a key distribution facility.



(i) Explain the key distribution scheme. [5]

(ii) Highlights the advantages and disadvantages of the key distribution scheme. [2.5+2.5]

Q4. (i) What is Secure Socket Layer (SSL) Protocol, and explain how it can protect web traffic from confidentiality and integrity breaches. [5]

(ii) What is end-to-end encryption, and explain how it can be used to secure app-based chat. [5]
