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]

CS850 Database Security

Quiz-1

Q1. Given this HTML and PHD code,

HTML:

```
<form action="sql.php" method="POST"/>
  <p>Username: <input type="text" name="login" /><br />
     Password: <input type="text" value="password" /></p>
</form>
```

PHP:

```
<?php $query = "SELECT * FROM users WHERE username = '{$_POST['login']} AND
    password= '{$_POST['password']}"; $result = mysql_query($query); echo "$_POST['login'] attempted"}>
```

Assume that logins are allowed if $result above is simply checked as being non-empty.

1. Given this PHP code, give a username and password that will allow you to login without knowing the password.
2. Give a username and password that allows you to login without knowing a valid username.
3. Give a username and password that allows a cross-site scripting attack.

Q2. Consider the following login page:

```
set ok = execute( "SELECT * FROM Users
     WHERE user=' "  &  form("user")  & " '
     AND   pwd=' " & form("pwd") & " '" ) ;

if not ok.EOF
     login success
else  fail;
```

Is this exploitable? If so, give possible SQL injection attacks with this code.

Q3. Consider the following code for a stored procedure (which is accessible to 'public' by default) which executes a search query for a web application. In case no search query is provided, the query results the details of all the products in the database. If a query is provided, it returns all products which have the search term in the product name.

```
CREATE PROCEDURE SP_EmployeeSearch @empname varchar(100) = NULL AS
DECLARE @sql nvarchar(4000)
SELECT @sql = ' SELECT EmpID, EmpName, Position, Salary ' +
' FROM Employee Where '
IF @EmpID IS NOT NULL
SELECT @sql = @sql + ' EmpName LIKE '" + @empname + ""
EXEC (@sql)
```

Is the stored procedure vulnerable to SQL injection? Why or why not?

Q4. Given any XACML policy and one example access request for your XML DB. Considering this policy and access request, determine the access response.

CS 850 DATABASE SECURITY
II SEM M.TECH (CSE-IS)
MIDSEM EXAM- 18 Feb 2025

te: Answer ALL Questions **Max.Marks: 50 Marks**

Q1. The CSE department has decided to develop a new electronic grading system. Here are the key features the department wants the system to handle (do not assume any permissions or restrictions other than those explicitly mentioned): (15)

- Each course has some course instructors (CIs) and teaching assistants (TAs) assigned to it.
- TAs and CIs for a given course can both read and write that course's grades; in addition, a course's CI(s) can submit final grades.
- All faculty members can read the grades for every course.
- Graduate students and faculty are disjoint groups.
- No graduate student can be a TA for more than two courses.
- No graduate student can be a Course instructor for any course.
- Faculty members can be teaching assistants or Course instructors for any course, and there are no limits on how they are assigned to courses. (Yes, they may even serve as both the TA and the CI for the same course; I mention this only to make your task easier.)
- Because of the potential for confusion with final grades—especially if instructors have the same students in multiple courses—the electronic grading system must not permit anyone to perform in more than one Course-instructor role at any given time (e.g., login session).

As part of the system's initial test run, the department wants to configure the system to handle just three of the department's courses: CSE 123, CSE 456, and CSE 789. Thus, the department has identified the following roles and permissions for this system:

R = {Fac Grad, 123TA, 123CI , 456TA, 456CI , 789TA, 789CI }
P = {read 123, write123, submit 123, read 456, write456, submit 456, read 789, write789, submit 789}

For example, read 123, write123, and submit 123 are the permissions to (respectively) read, write, and submit the grades for CS 123.

Provide the following RBAC components to accurately meet and fulfill all of the department's desired features/criteria:

i. A role-hierarchy relation and a permission- assignment relation
ii. A static separation-of-duty relation to capture necessary static constraints
iii. A dynamic separation-of-duty relation to capture necessary dynamic constraints

Q2. Suppose you are the database administrator setting up security mechanisms for the Video Stores database (15)

FILM (FNUM, TITLE, OPENED, LENGTH, BUDGET, DIRECTOR, SNUM, RATING, WRITER)
ACTOR (ANUM, FNAME, LNAME, BDATE, GENDER)
ROLES (FNUM, ANUM, PART, SALARY)
STUDIO (SNUM, NAME, ADDRESS, WEBSITE)
ITEM (INUM, FNUM, PRICE, RELEASE, FORMAT, BONUS, INVENTORY)
SHOPPER (SHNUM, FNAME, LNAME, SHIPADDR, CRCARD)
CART (SHNUM, INUM, QUANTITY)

Suppose that the database has the following users:

i. SPIELBERG works in the purchasing department.
ii. SHYAMALN is in the shipping department.
iii. MARSHALL is the manager of the customer service department.

Provide the SQL commands to grant appropriate access privileges and grant propagation privileges. Explain your choices based on how each user will be expected to use the database. If you make any assumptions about these types of users, be sure to explain them.

Q3. a) Describe a scenario in which mandatory access controls prevent a breach of security that cannot be prevented through discretionary controls. (5)

b) In a medical information system that controls access to patient records and prescriptions, doctors may read and write patient records and prescriptions, nurses may read and write prescriptions only but should learn nothing about the contents of patient records. (10)

i. How can you capture this policy in a lattice model that prevents information flow from patient records to prescriptions?
ii. In your opinion, which security model is most appropriate for this policy? (Why?) Sketch a security model capturing the requirement.
iii. A doctor should not be allowed to make a prescription for herself. How can you augment your model above to prevent this kind of prescription abuse?

c) Assume that a database table named Students (SID, SNAME, DEPTID, LOANAMOUNT). Possible queries are COUNT, SUM and MEAN. The database does not reveal results when a small or large number of people are covered by the query. In our database it has been decided that 4-7 people must be covered by the query. We want to find a sequence of queries that tells us the size of Erika's loan. The obvious query SELECT SUM(Loan) FROM Students WHERE name = 'Erika' will not work because the result, 1, is not in the range 4-7. The query will be ignored. Find a general tracker and a sequence of queries that will give you the information. You are allowed to do 4 queries. (5)

---Good luck---

Department of Computer Science & Engineering
N.I.T.K.-Surathkal
II Sem M.Tech (CSE-IS) - ENDSEM EXAM APRIL 2025
CS 850 DATABASE SECURITY

Time: 3 Hrs **Max Marks: 100**

Note : Answer ALL

Q1. Assume that you are the DBA for the ABC Toy Company and create a relation called Employees with fields *ename*, *dept*, and *salary*. For authorization reasons, you also define views EmployeeNames (with *ename* as the only attribute) and DeptInfo with fields *dept* and *avgsalary*. The latter lists the average salary for each department. [25]

a. Show the view definition statements for EmployeeNames and DeptInfo.
b. What privileges should be granted to a user who needs to know only average department salaries for the Toy and CS departments?
c. You want to authorize your secretary to fire people (you will probably tell him whom to fire, but you want to be able to delegate this task), to check on who is an employee, and to check on average department salaries. What privileges should you grant?
d. Continuing with the preceding scenario, you do not want your secretary to be able to look at the salaries of individuals. Does your answer to the previous question ensure this? Be specific: Can your secretary possibly find out salaries of *some* individuals (depending on the actual set of tuples), or can your secretary always find out the salary of any individual he wants to?
e. You want to give your secretary the authority to allow other people to read the EmployeeNames view. Show the appropriate command.
f. Your secretary defines two new views using the EmployeeNames view. The first is called AtoRNames and simply selects names that begin with a letter in the range A to R. The second is called HowManyNames and counts the number of names. You are so pleased with this achievement that you decide to give your secretary the right to insert tuples into the EmployeeNames view. Show the appropriate command and describe what privileges your secretary has after this command is executed.
g. Your secretary allows Todd to read the EmployeeNames relation and later quits. You then revoke the secretary's privileges. What happens to Todd's privileges?
h. Give an example of a view update on the preceding schema that cannot be implemented through updates to Employees.
i. You decide to go on an extended vacation, and to make sure that emergencies can be handled, you want to authorize your boss Joe to read and modify the Employees relation and the EmployeeNames relation (and Joe must be able to delegate authority, of course, since he is too far up the management hierarchy to actually do any work). Show the appropriate SQL statements. Can Joe read the DeptInfo view?
j. After returning from your (wonderful) vacation, you see a note from Joe, indicating that he authorized his secretary Mike to read the Employees relation. You want to revoke Mike's SELECT privilege on Employees, but you do not want to revoke the rights you gave to Joe, even temporarily. Can you do this in SQL?

k. Later you realize that Joe has been quite busy. He has defined a view called All- Names using the view EmployeeNames, defined another relation called StaffNames that he has access to (but you cannot access), and given his secretary Mike the right to read from the AllNames view. Mike has passed this right on to his friend Susan. You decide that, even at the cost of annoying Joe by revoking some of his privileges, you simply have to take away Mike and Susan's rights to see your data. What REVOKE statement would you execute? What rights does Joe have on Employees after this statement is executed? What views are dropped as a consequence?

Q2. Assume that a database table named Students (SID, SNAME, DEPTID, LOANAMOUNT). Possible queries are COUNT, SUM and MEAN. The database does not reveal results when a small or large number of people are covered by the query. In our database it has been decided that 4-7 people must be covered by the query. We want to find a sequence of queries that tells us the size of Erika's loan. The obvious query SELECT SUM(Loan) FROM Students WHERE name = 'Erika' will not work because the result, 1, is not in the range 4-7. The query will be ignored. Find a general tracker and a sequence of queries that will give you the information. You are allowed to do 4 queries. [05]

Q3. Consider the following PHP script for a login page: [20]

```
$username = $_GET[user];
$password = $_GET[pwd];
$sql = "SELECT *
        FROM usertable
        WHERE username = '$username'
        AND password = '$password' ";
$result = $db->query($sql);
if ($result->num_rows > 0) { /* Success */ }
else { /* Failure */ }
```

i. Because addslashes did not eliminate the problem of SQL injection, we decide to employ some form of input filtering. A recommends the use of JavaScript to validate the input before passing it over to the server. Is this enough to ensure that SQL injection will not happen? Why?

ii. As an extension to input filtering, we decide to strip the -- characters in the input so that attackers cannot inject a comment and thereby execute an injection. Can an attacker bypass this restriction? How?

iii. Stored Procedures have a reputation for being able to defend against SQl injection attacks. With this in mind, we decide to employ the following stored procedure:

```
CREATE PROCEDURE VerifyUser
        @username varchar(50),
        @password varchar(50)
AS
BEGIN
        SELECT * FROM UserTable
        WHERE UserName = @username
        AND Password = @password;
END
GO
```

The stored procedure is called from the PHP file using the following code:

```
$sql = "CALL VerifyUser ("+ $_GET[user] + "," + $_GET[pwd]+")";
```

Is the web application susceptible to an SQL injection? Why or why not?

Q4. Assume that multiple groups simultaneously query the same XML to specify access policies at various levels of granularity. Suggest ways to efficiently enforce those access policies? Compare the XACML and XACL models of XML security. [15]

Q5. a) How does Scale-Out occur in MongoDB? b) Explain Aggregation in MongoDB and its usefulness? c) Why is the covered query important in MongoDB? [10]

Q6. a) Explain the difference Signature-based vs. Anomaly-Based intrusion detection systems? [5] b) Suggest atleast two ways to improve the efficiency of Anomaly-Based IDS? [10] c) Is there anything interesting about the false positives? [5] d) Highlight the various issues in testing the intrusion detection systems? [5]

---Good Luck---

Department of Computer Science and Engineering
National Institute of Technology Karnataka, Surathkal

242ISO15

Mid-Semester Examination (February 2025)

Course Name: Quantum Cryptography
Semester: II
Duration: 1 Hour 30 Minutes

Course Code: CS826
Course: M.Tech. (CSE-IS)
Marks: 40

Note: Answer all the questions.

Q1. (a) Consider the complex number z=1+2i. **[08]**

- **(i)** Find the real component *z* of $\Re(z)$.
- **(ii)** Find the imaginary component z of $\Im(z)$.
- **(iii)** Write z in the polar form $re^{i\theta}$.
- **(iv)** Find the conjugate z*.

(b) A qubit is in the state **[04]**

$$\frac{1+i\sqrt{3}}{3}|0\rangle+\frac{2-i}{3}|1\rangle.$$

If you measure the qubit, what is the probability of getting
(a) $|0\rangle$?
(b) $|1\rangle$?

Q2. (a) A qubit is in the state

$$A\left(2e^{i\pi/6}|0\rangle-3|1\rangle\right).$$

(i) Normalized the state (i.e., find A.). **[04]**

(ii) If you measure the qubit, what is the probability that you get $|0\rangle$? **[04]**

Q3. Consider a map *U* that transforms the Z-basis states as follows.

$$U|0\rangle=\frac{\sqrt{3}}{2}|0\rangle+\frac{\sqrt{3}+i}{4}|1\rangle.$$
$$U|1\rangle=\frac{\sqrt{3}+i}{4}|0\rangle-\frac{\sqrt{3}+3i}{4}|1\rangle.$$

Say $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$ is a normalized quantum state, i.e., $|\alpha|^2+|\beta|^2=1$.

(i) Calculate $U|\psi\rangle$. **[05]**

(ii) From your answer to (i), is *U* a valid gate? Explain your reasoning. **[05]**

Q4. **(a)** The Hadamard gate turns $|0\rangle$ into $|+\rangle$, and $|1\rangle$ into $|-\rangle$.

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle,$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle.$$

From the definition of Hadamard gate, prove that H|+> = |0>, H|-> = |1> and H|i> = |-i>. **[02+02+02]**

(b) Consider each logical classic gate with inputs A and B, outputs C and D, and the truth table below. Is each gate a valid quantum gate? Why? **[02+02]**

(a)

A	B
0	0
1	1

(b)

A	B
0	1
1	1

C D

H|i> = |-i>

Department of Computer Science and Engineering
National Institute of Technology Karnataka, Surathkal

End-Semester Examination (May 2025)

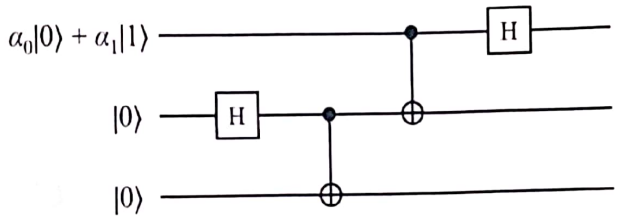
Course Name: Quantum Cryptography
Course Code: CS826
Semester: II
Course: M.Tech. (CSE-IS)
Duration: 03 Hours
Marks: 80

Note: Answer all the questions.

Q1. (a) Explain Shor's Algorithm and describe through a suitable example how it can pose a threat to RSA. **[6]**

(b) A SWAP gate takes two inputs x_1 and x_2 and outputs x_2 and x_1; i.e., it swaps the values of two registers. Show how to build a SWAP gate using only CNOT gates. **[6]**

Q2. Consider the following quantum circuit:



An equivalent description of the circuit (calling the registers x_1, x_2, x_3) is:

1. Initialize x_1 to $\alpha_0 |0\rangle + \alpha_1 |1\rangle$
2. Initialize x_2 to $|0\rangle$
3. Initialize x_3 to $|0\rangle$
4. Hadamard(x_2)
5. CNOT(x_2, x_3)
6. CNOT(x_1, x_2)
7. Hadamard(x_1)

a) Determine with proof the state of the three qubits at the end of the circuit's operation. **[05]**

b) If we then measure the three qubits, give the outcomes and their probabilities that arise. **[05]**

Q3. Calculate the following inner products. **[03+03+03]**

a) $\langle 10|11\rangle$.

b) $\langle +-|01\rangle$.

c) $\langle 1+0|1-0\rangle$.

Q4. (a) If you measure the left qubit, what outcomes can you get, what are the corresponding probabilities of those outcomes, and what does the state collapse to for each outcome? Is this state a product state, partially entangled state, or maximally entangled state? [03+03+03]

$$\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle).$$

(b) Alice and Bob share an EPR-pair,

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Suppose they each measure their qubit with an X-observable (which corresponds to a particular projective measurement with possible outcomes +1, −1). Find the following. [10]

(a) P_{00}.

(b) P_{01}.

(c) P_{10}.

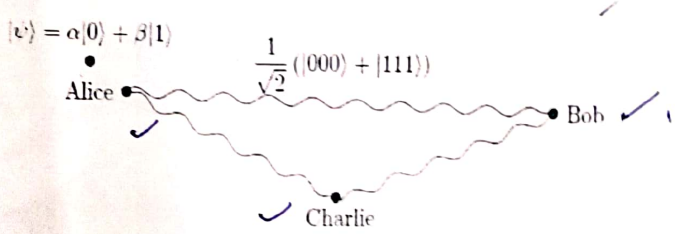
(d) P_{11}.

(e) $E(A',B') = P00 - P01 - P10 + P11$.

Q5. Alice wants to teleport a qubit in an unknown state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to Charlie, and Bob is helping her. They share three entangled qubits in the GHZ state:

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle).$$

The left qubit is Alice's, the middle qubit is Bob's, and the right qubit is Charlie's.



Altogether, the initial state of the system is

$$|\psi\rangle|GHZ\rangle = (\alpha|0\rangle + \beta|1\rangle)\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

$$= \frac{1}{\sqrt{2}}(\alpha|0000\rangle + \alpha|0111\rangle + \beta|1000\rangle + \beta|1111\rangle$$

Q4. (a) If you measure the left qubit, what outcomes can you get, what are the corresponding probabilities of those outcomes, and what does the state collapse to for each outcome? Is this state a product state, partially entangled state, or maximally entangled state? **[03+03+03]**

$$\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle).$$

(b) Alice and Bob share an EPR-pair,

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Suppose they each measure their qubit with an X-observable (which corresponds to a particular projective measurement with possible outcomes +1, −1). Find the following. **[10]**

(a) P_{00}.

(b) P_{01}.

(c) P_{10}.

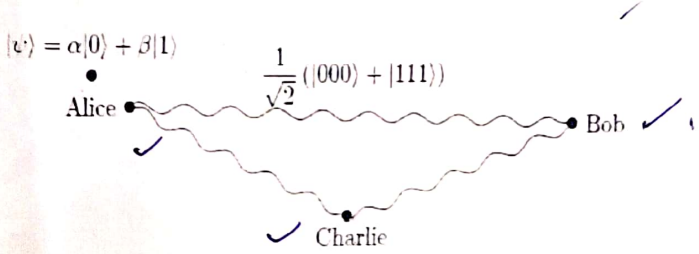
(d) P_{11}.

(e) $E(A',B') = P00 - P01 - P10 + P11$.

Q5. Alice wants to teleport a qubit in an unknown state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to Charlie, and Bob is helping her. They share three entangled qubits in the GHZ state:

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle).$$

The left qubit is Alice's, the middle qubit is Bob's, and the right qubit is Charlie's.



Altogether, the initial state of the system is

$$|\psi\rangle|GHZ\rangle = (\alpha|0\rangle + \beta|1\rangle)\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

$$= \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)$$

So, the left two qubits are Alice's, the second-to-right qubit is Bob's, and the right qubit is Charlie's.

(a) Show that if Alice applies CNOT to her qubits (so the far left qubit is the control and the second-to-left qubit is the target) and then the Hadamard gate to her left qubit, the state of the system becomes **[5]**

$$\frac{1}{2}\big[|00\rangle(\alpha|00\rangle+\beta|11\rangle)+|01\rangle(\beta|00\rangle+\alpha|11\rangle)$$
$$+|10\rangle(\alpha|00\rangle-\beta|11\rangle)+|11\rangle(-\beta|00\rangle+\alpha|11\rangle)\big].$$

(b) Next, Alice measures her two qubits and makes the results known. What values can she get, with what probabilities, and what does the state collapse to in each case? **[5]**

Q6. (a) Explain the Crystal-Kyber public encryption algorithm. **[6]**

(b) Show that the following gates are reversible or irreversible. **[4]**

(i) OR. (ii) XOR. (iii) NAND. (iv) NOR

Q7. (a) Let's assume:

Alice's key:

A = 1 0 1 1 0 1 1 0

Bob's key:

B = 1 0 1 1 1 1 1 0

The above Alice and Bob raw keys contain discrepancies. Demonstrate how the Cascade protocol can be used to detect and correct errors. **[5]**

(b) Explain the BB84 Quantum Key Distribution protocol with the help of a suitable example. **[5]**

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]