Roll No												

PRESIDENCY UNIVERSITY
BENGALURU

SCHOOL OF ENGINEERING

TEST 1

Winter Semester: 2021 - 22

Course Code: CSE 215

Course Name: Cryptography and Network Security

Program & Sem: B.Tech & 6th Sem

Date: 25 April 2022

Time: 1.30 – 2.30 PM

Max Marks: 30

Weightage: 15 %

Instructions:

(i) Read the all questions carefully and answer accordingly.
(ii) Assume the necessary data if required
(iii) Scientific Non Programmable calculators are allowed

Part A

Answer all the Questions. Each question carries TWO marks. (6Qx2M= 12M)

1. Define Encryption and Decryption [2M] (CO1) [Knowledge]

2. Mention the two scenarios in which you need an extra filler character in Playfair Cipher.

[2M] (CO1) [Knowledge]

3. Encrypt the message “MICROSOFT” using Caesar Cipher [2M] (CO1) [Knowledge]

4. List any four security mechanisms defined by OSI security architecture

[2M] (CO1) [Knowledge]

5. Write a short note on Authentication with example [2M] (CO1) [Knowledge]

6. Define Block Cipher and Stream Cipher [2M] (CO1) [Knowledge]

Part B

Answer all the Questions. Each question carries FIVE marks. (2Qx5M=10M)

1. Alice and Bob are exchanging the secret information by using the key which is already shared between them. Alice has sent a message **“FRIENDSHIP”** which is encrypted using Playfair technique using the key **“PHOTO”**. What is the Cipher Text received by Bob?

[5M] (CO3) [Knowledge]

2. Block Cipher is one technique in which we calculate the cipher by taking the corresponding binary sequence of the Plain Text, divide into equal length blocks and process it. Feistel structure is one of the methods of deriving Block Cipher. Consider the given inputs below

Input plain text is **1100101101**

Encryption key is **10001**.

Mathematical function is XoR

Number of rounds = 5

Using the concept of Feistel Structure, calculate the Cipher Text by taking the above inputs.

[5M] (CO3) [Comprehension]

Part C

Answer all the Questions. Each question carries EIGHT marks. (1Qx8M=8M)

1. Hill Cipher is one substitution technique works on the principle of matrix multiplication. Given the Plain Text as "ATTACK" and the key matrix given as $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$.

Perform Encryption by taking the above inputs. You can take two characters of Plain Text at a time or any other possible matrix for Plain text so that Matrix Multiplication rule is satisfied.

[8M] (CO3) [Comprehension]

Roll No												

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

PRESIDENCY UNIVERSITY
BENGALURU

SCHOOL OF ENGINEERING

TEST 2

Winter Semester: 2021 - 22

Course Code: CSE 215

Course Name: Cryptography and Network Security

Program & Sem: B.Tech & 6th Semester

Date: 31 May 2022

Time: 01.30PM – 02.30 PM

Max Marks: 30

Weightage: 15%

Instructions:

(i) Read the all questions carefully and answer accordingly.

(ii) Scientific, Non programmable calculators are allowed

(iii) Assume any data if necessary

Part A [Memory Recall Questions]

Answer all the Questions. Each question carries TWO marks. (5Qx 2M= 10M)

1. Differentiate between Symmetric and Asymmetric Key Cryptography. Give an example for each. (CO2) [Knowledge]

2. Mention the input block size of DES and AES Cryptographic Algorithms. (CO2) [Knowledge]

3. Which key is used for Encryption and Decryption in Asymmetric Key Cryptography?

(CO2) [Knowledge]

4. Why do you require Fermat's little theorem? Explain with appropriate equation.

(CO3) [Knowledge]

5. What do you mean by relatively prime? Give an example (CO3) [Knowledge]

Part B [Thought Provoking Questions]

Answer both the Questions. Each question carries SIX marks. (2Qx6M=12M)

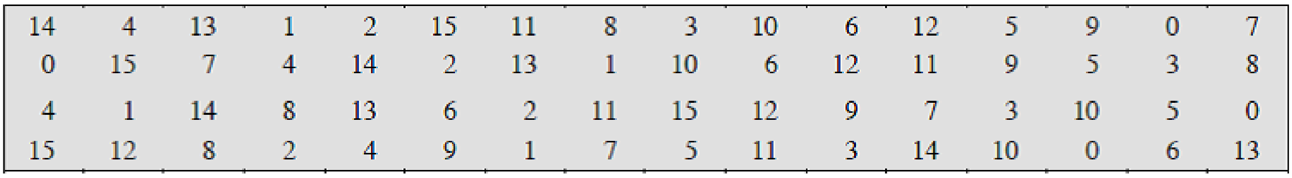
6. Sub_Bytes and Shift_Rows operations are two different operations of AES Algorithm.

(a). How do you map an 8 bit value of a given state into another 8 bit value using Sub_Bytes operation? Explain in detail

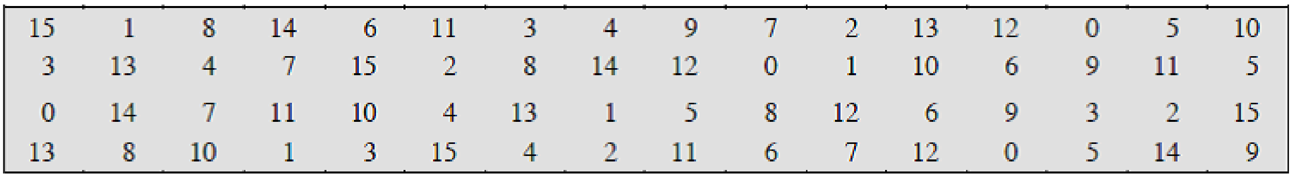
(b). Explain the process to shuffle the cell values of a state using Shift_Rows operation in detail.

(CO3) [Comprehension]

7. Substitution Box plays an important role in DES Algorithm to convert 48 bits sequence to 32 bits sequence. There are 8 such S-Boxes exists in DES Algorithm which are well defined by IBM. Two different S-Boxes are given below.



S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13



S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

Two 6 bits binary sequence are given as 101011 and 010011. Find corresponding 4 bits values after mapping first set of six bits to S1 and second set of six bits to S2 box?

(CO3)[Comprehension]

Part C [Problem Solving Questions]

Answer the Question. The question carries EIGHT marks. **(1Qx8M=8M)**

8. Alice and Bob want to share the secure information using RSA Algorithm. They agreed upon two prime numbers 7 and 17. The plain text to be send by Alice is 8.

Calculate the Encryption and Decryption keys used by Alice and Bob.

What is the Cipher Text received by Bob?

Perform Decryption to verify the Plain Text sent by Alice.

(CO3)[Comprehension]

Roll No												

PRESIDENCY UNIVERSITY
BENGALURU

SCHOOL OF ENGINEERING

END TERM EXAMINATION

Winter Semester: 2021 - 22

Course Code: CSE 215

Course Name: Cryptography and Network Security

Program & Sem:B.Tech & VI Sem

Date: 28th June 2022

Time: 09:30 AM to 12:30 PM

Max Marks: 100

Weightage: 50%

Instructions:

(i) Read the all questions carefully and answer accordingly.

(ii) Assume any data if necessary

(iii) Scientific non-programmable calculators are allowed

Part A [Memory Recall Questions]

Answer all the Questions. Each question carries TWO marks. (12Qx 2M= 24M)

1.

a). Define Block Cipher and Stream Cipher. Give an example for each. (CO1) [Knowledge]

b). Differentiate between active and passive attacks. (CO2) [Knowledge]

c). Mention the operations of AES that makes use of Galois Field. (CO1) [Knowledge]

d). Explain Euler Totient Function. What is the Euler Totient function for a given prime number? (CO3) [Knowledge]

e). List the mathematical operations required to find the Encryption and Decryption key in RSA. (CO3) [Knowledge]

f). What is the rule for choosing private key of an user in Diffie-Hellman key exchange Algorithm? (CO3) [Knowledge]

g). Which key is used for deriving and verifying Digital Signature? (CO3) [Knowledge]

h). Mention the Block Size and number of rounds in SHA-512 Algorithm. (CO3) [Knowledge]

i). Discuss the scenario in which inverse modulo operation is not possible for given two numbers. (CO3) [Knowledge]

j). How many rounds are there in DES and AES symmetric key Cryptographic Algorithm? (CO1) [Knowledge]

k). What are the Network Security tools used for Authentication and Remote login? (CO4) [Knowledge]

l) Write the equation for Hill Cipher encryption and decryption. Also mention the matrix multiplication rule. (CO4) [Knowledge]

Part B [Thought Provoking Questions]

Answer all the Questions. Each question carries EIGHT marks. (5Qx8M=40M)

2. OSI Security architecture provides a well-defined services, mechanisms and attacks which are to be incorporated in any security algorithm. List all the security services offered by this OSI security architecture. Describe all the security services in detail with sub component under each service. (CO1) [Comprehension]

3. Alice and Bob are supposed to perform authentication using concept of Prime number and primitive roots. Both agree upon prime number ‘7’. For this given prime, you can choose ‘4’ as primitive root of given prime number.

(a). How does both Alice and Bob are going to select private key

(b). Calculate the corresponding Public Keys

(c). Calculate the shared key at both Alice and Bob side. (CO3) [Comprehension]

4. In each round of DES algorithm, 56 bits key is converted into 48 bits. What are the operations involved in this process? Explain with the appropriate diagram. Also highlight how many bits shifting needs to be done in each round. (CO1) [Comprehension]

5. Hash functions play an important role in storing any of your digital assets in a secure way. What do you mean by Hash? Answer the following questions with respect to hash.

(a). Explain the properties of Hash functions

(b). what is the role of 8 different buffer registers used in SHA 512. Discuss the same.

(CO3) [Comprehension]

6. What do you mean by IPSecurity? Explain the following with respect to IPSec

(a). Applications (b). Benefits (c). Services (CO4) [Comprehension]

Part C [Problem Solving Questions]

Answer all the Questions. Each question carries TWELVE marks. (3Qx12M=36M)

7. Perform Hill Cipher Encryption for the following inputs

Plain text : MICROSOFT

Key :

$$\begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix}$$

Note: Divide the plain text into 3 characters each and perform matrix multiplication 3 times.

(CO3) [Comprehension]

8. Two users ‘A’ and ‘B’ are willing to establish secure connection using RSA Algorithm. Following inputs are given

Two primes: 11 and 29

Select ‘e’ more than 20

Plaintext: 18 and 25

What are the Encryption and Decryption keys? Also Perform Encryption and Decryption separately for given two plaintext. (CO3) [Comprehension]

9.

(a). Consider the scenario where a user may gain access to particular workstation and pretend to be another user operating from that workstation. This is one scenario comes under authentication. Apply the knowledge of Kerberos to give solution to the given scenario. Use appropriate Kerberos dialogue to solve the same.

(b). Secure Shell (SSH) is a protocol for secure network communications designed to be relatively simple and inexpensive to implement. It is the widely used method for remote login. Using the concept of SSH protocol stack to achieve the authentication. Write appropriate protocol stack diagram; highlight the importance of each layer in handling authentication. (CO4)[Application]