Roll No												

PRESIDENCY UNIVERSITY
BENGALURU

SCHOOL OF ENGINEERING

MAKE UP EXAMINATION – JAN 2023

Course Code: CSE215
Course Name: Cryptography and Network Security
Program : B.Tech - CSE

Date: 25-JAN-2023
Time: 09:30AM to 12:30PM
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. (10Qx 2M= 20M)

1.

a). Differentiate between Symmetric and Asymmetric Key Cryptography with an example each. (CO1) [Knowledge]

b). Define active and passive attack. (CO2) [Knowledge]

c). Which are the operations of AES that doesn't makes use of Galois Field. (CO1) [Knowledge]

d). Describe Euler Totient Function with an example. (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). How many rounds are there in DES and AES symmetric key Cryptographic Algorithm? (CO1) [Knowledge]

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

Part B [Thought Provoking Questions]

Answer all the Questions. Each question carries EIGHT marks. (5Qx10M=50M)

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. (CO1) [Comprehension]

3. Alice and Bob are supposed to perform authentication using concept of Diffie-Hellman key exchange algorithm. Both agree upon prime number '5'.
   (a). Calculate the primitive root of 5
   (b). Calculate the shared key at both Alice and Bob side. (CO3) [Comprehension]

4. Using playfair Cipher, Calculate the Ciphertext for the given inputs below
   Plaintext: UNIVERSITY Key: EXAMINATION (CO3) [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. (2Qx15M=30M)

7. Perform Hill Cipher Encryption for the following inputs
   Plaintext : MICROSOFT
   Key
   $$\begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix}$$
   (CO3) [Comprehension]

8. Two users 'A' and 'B' are willing to establish secure connection using RSA Algorithm. Following inputs are given
   Two primes: 7 and 11
   Plaintext: 12
   pCalculate the Encryption and Decryption keys. Perform Encryption and Decryption for given plaintext.
   (CO3) [Comprehension]