

Roll No



**PRESIDENCY UNIVERSITY  
BENGALURU**

**SCHOOL OF ENGINEERING  
END TERM EXAMINATION - JUN 2023**

**Semester :** Semester VI - 2020

**Course Code :** CSE3078

**Course Name :** Sem VI - CSE3078 - Cryptography and Network Security

**Program :** B.Tech - All Programs

**Date :** 12-JUN-2023

**Time :** 9.30AM - 12.30PM

**Max Marks :** 100

**Weightage :** 50%

**Instructions:**

- (i) Read all questions carefully and answer accordingly.
- (ii) Question paper consists of 3 parts.
- (iii) Scientific and non-programmable calculator are permitted.
- (iv) Do not write any information on the question paper other than Roll Number.

**PART A**

**ANSWER ALL THE QUESTIONS**

**(10 X 2 = 20M)**

1. What is a man in the middle attack?  
(CO3) [Knowledge]
2. Define public key cryptography.  
(CO4) [Knowledge]
3. What are the two general approaches to attack a cipher?  
(CO1) [Knowledge]
4. Define field in number theory.  
(CO2) [Knowledge]
5. Find GCD(125, 20).  
(CO2) [Knowledge]
6. Mention the technical deficiencies of Kerberos 4 & 5.  
(CO4) [Knowledge]
7. Define one time pad.  
(CO2) [Knowledge]
8. What is a message authentication code?  
(CO3) [Knowledge]
9. How many keys are required for any two entities to communicate over a secure communication channel?  
(CO1) [Knowledge]

10. Differentiate between Monoalphabetic and Polyalphabetic cipher.

(CO1) [Knowledge]

### PART B

#### ANSWER ALL THE QUESTIONS

(5 X 10 = 50M)

11. Encrypt the message "COE" using Hill cipher with the following key matrix.

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

(CO1) [Comprehension]

12. Illustrate the structure of AES with suitable diagram. How the process of subbytes and shiftrows with respect to AES.

(CO2) [Comprehension]

13. List the design objectives of HMAC and explain the algorithm in detail.

(CO3) [Comprehension]

14. Explain Kerberos authentication mechanism in detail with suitable diagram.

(CO4) [Comprehension]

15. Describe in detail about the architecture of SSL with a neat diagram.

(CO4,CO3) [Comprehension]

### PART C

#### ANSWER ALL THE QUESTIONS

(2 X 15 = 30M)

16. User Alice and Bob use the Diffie-Hellman key exchange technique with a common prime  $q = 11$  and a primitive root  $\alpha = 2$ .

a. Show that 2 is a primitive root of 11.

b. If user A has public key  $Y_A = 9$ , what is A's private key  $X_A$ ?

c. If user B has public key  $Y_B = 3$ , what is B's Private key  $X_B$ ?

d. What is the shared secret key?

(CO3) [Application]

17. With a neat diagram, explain the steps involved in SHA algorithm for encrypting a message with maximum length of less than  $2^{128}$  bits and produce as output a 512 – bit message digest.

(CO2,CO3) [Application]