Roll No											

PRESIDENCY UNIVERSITY
BENGALURU

SCHOOL OF ENGINEERING
END TERM EXAMINATION - JAN 2023

Semester : Semester V - 2020
Course Code : CSE3078
Course Name : Sem V - CSE3078 - Cryptography and Network Security
Program : B.Tech. CCS

Date : 11-JAN-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.

PART A

ANSWER ALL THE TEN QUESTIONS **10 X 2 = 20M**

1. What are the Classical Encryption Techniques? (CO1) [Knowledge]

2. List out the problems of one time pad. (CO1) [Knowledge]

3. When is a Group said to be Abelian? (CO2) [Knowledge]

4. Write down the purpose of S-Boxes in DES. (CO2) [Knowledge]

5. What is the difference between a block cipher and a stream cipher? (CO1) [Knowledge]

6. What are the properties of Hash function? (CO3) [Knowledge]

7. Write an importance of Public-Key Cryptography? (CO3) [Knowledge]

8. What is meant by Authentication? (CO3) [Knowledge]

9. Define PGP. What is use of PGP? (CO4) [Knowledge]

10. What are the top web security threats? (CO4) [Knowledge]

PART B

ANSWER ALL THE FIVE QUESTIONS **5 X 10 = 50M**

11. (i) Give the types of Attacks. Differentiate passive and active attacks.
(ii) How Stegnography can be differ from Cryptography and Write shoort notes on few of the Stegnographic Techniques.

(CO1) [Comprehension]

12. Justify the necesity of Triple DES rathar than DES Symmetric Encryption;- Apply the DES functionality with 64 bit key Block for an information communication.Dscuss the chances of cryptanalysis and its limitations?.

(CO1) [Comprehension]

13. How AES General Structure is highly Secured Symmetric Encryption? Discuss with General Structure and its Functionality in detail.

(CO2) [Comprehension]

14. How security can be achieved on the basis of Authentication through (a) Message Authentication and MAC. Consider any application and Justify it.

(CO3) [Comprehension]

15. What are the Web Security Threats and Countermeasures ? Discuss them in detail.

(CO4) [Comprehension]

PART C

ANSWER ALL THE TWO QUESTIONS **2 X 15 = 30M**

16. How you relate the Rijindeal & AES ? Also Explain how the key is expanded in AES and describe therole of Expanded key in AES.

(CO2) [Application]

17. Give some of the possibilities to attack RSA Algorithms and How can they would be countered? Take an Example : p=7,q=23 and Plain Text is 88. Generate public keys and private keys and proceed encryption and decryption for finding cipher text and plain text using RSA algorithm

(CO3) [Application]

*****