Reg No.:_____ Name:_____

0520MCA263122202

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Third Semester MCA (Two Year) Degree Regular and Supplementary Examination December 2022

Course Code: 20MCA263

Course Name: CYBER SECURITY & CRYPTOGRAPHY

Max. Marks: 60 Duration: 3 Hours

PART A

Answer all questions, each carries3 marks. Marks

1	Explain passive and active attacks.	(3)
2	Write note on substitution cipher technique with an example.	(3)
3	Differentiate block cipher and stream cipher.	(3)
4	Briefly explain Diffie Hellman Key exchange.	(3)
5	Write short note on blind signatures.	(3)
6	Distinguish between message integrity and message authentication	(3)
7	What are the functionalities provided by Secure MIME (S/MIME)?	(3)
8	What are the key features provided by SET?	(3)
9	How can we prevent injection attack?	(3)
10	Illustrate the attack scenarios in cross site scripting.	(3)

PART B

Answer any one question from each module. Each question carries 6 marks.

Module I

11	Explain the security services and mechanisms in cryptography.	(6)

OR

12	Write short note on i) Symmetric cipher model. ii) Stegnography	(6)

Module II

13	With the help of block diagram explain DES.	(6)

OR

14	Explain different block cipher modes of operation.	(6)

Module III

15 With a neat diagram explain HMAC algorithm. (6)

OR

16 Explain Elgamal digital signature scheme in cryptography. (6)

Module IV

17 Explain AH and ESP protocols in IP Sec. (6)

OR

18 Explain the working of SSL protocol in detail. (6)

Module V

19 Write a note on attack scenarios and prevention of following web application security vulnerabilities. (6)

i) Broken access control

ii) Security misconfiguration

OR

20 Write a note on attack scenarios and prevention of following web application security vulnerabilities. (6)

i) Sensitive data exposure

ii) Security misconfiguration

****