Reg No.:_____ Name:_____

0520MCA263122102

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Third Semester MCA (2 Year) Degree Examination December 2021

Course Code: 20MCA263

Course Name: CYBER SECURITY & CRYPTOGRAPHY

Max. Marks: 60 Duration: 3 Hours

PART A

Answer all questions, each carries 3 marks. Marks

1	Explicate the need of encryption in the cryptographic applications.	(3)
2	Write a note on Symmetric cipher model.	(3)
3	What is avalanche effect?	(3)
4	Represent how public key cryptosystem achieve Authentication and Secrecy using a neat diagram?	(3)
5	What are the requirements for a cryptographic hash functions?	(3)
6	Define Blind Signature.	(3)
7	Compare IPv4 and IPv6.	(3)
8	Summarize the services provided by SSL.	(3)
9	Which are the different forms of XSS and how to prevent it?	(3)
10	What is injection attack?	(3)

PART B

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

Module I

11	Elucidate OSI Security Architecture.	(6)
	OR	
12	Illustrate, Substitution encryption techniques and its features.	(6)

Module II

13	Describe DES encryption algorithm with a neat figure.	(6)
	OR	
14	Explain the steps in Diffie-Hellman Key Exchange algorithm	(6)

Module III

15 Write short note on

(a) HMAC (3)

(b) CMAC (3)

OR

16 Discuss on

(a) Variations and applications for digital signature (3)

(b) Digital Signature attacks. (3)

Module IV

17 Describe S/MIME. (6)

OR

18 Explain IP Security architecture. (6)

Module V

19 Write a note on any four application Security Risks. (6)

OR

20 Explain the attacks scenarios of any four web application security vulnerabilities. (6)

****