Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

FIFTH SEMESTER REGULAR AND THIRD SEMESTER SECOND YEAR DIRECT MCA DEGREE EXAMINATION(S) MAY 2019

Course Code: RLMCA305

Course Name: CRYPTOGRAPHY AND CYBER SECURITY

Max. Marks: 60 Duration: 3 Hours

PART A

Answer all questions, each carries3 marks. Marks

1	Explain Distributed Denial of Service (DDoS) attack on network security.	(3)
2	Discuss on Euler Totient function.	(3)
3	Draw the block diagram of Cipher block chaining mode(CBC) in Block ciphers. Give one of its advantage compared to Electronic code book(ECB).	(3)
4	Explain birth day attack.	(3)
5	Explain Scrooge Coin.	(3)
6	Describe the main applications of Public key cryptography.	(3)
7	Briefly explain the Authentication header format in IP security.	(3)
8	Briefly describe the different PGP services.	(3)

PART B

Answer six questions, one full question from each module and carries 6 marks.

Module I

9	With the help of a neat diagram, explain network security model.	(6)

OR

10	Construct a Playfair matrix with the key *largest* , Using this playfair matrix encrypt the message “Happiness is a Journey not a destination”	(6)

Module II

11	Discuss on Miller Rabin Algorithm for primality testing.	(6)

OR

12	Determine the GCD of the polynomials $x^6+x^5+x^4+x^3+x^2+x+1$ and x^4+x^2+x+1 over GF(2).	(6)

Module III

13	Explain an Diffie-hellman key exchange algorithm	(6)

OR

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

Module IV

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

OR

16	With the help of a block diagram explain the RSA algorithm for digital signature.	(6)

Module V

17	Explain how bitcoin Achieves Decentralization.	(6)

OR

18	Explain the different methods used for bitcoin storage.	(6)

Module VI

19	With the help of neat diagram explain SSL protocol stack.	(6)

OR

20	Draw the top-level format of an ESP packet and explain the different fields	(6)

****