

Reg No.: _____

Name: _____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY
THIRD SEMESTER MCA DEGREE EXAMINATION, DECEMBER 2017

Course Code: RLMCA305

Course Name: CRYPTOGRAPHY AND CYBER SECURITY

Max. Marks: 60

Duration: 3 Hours

PART A

Answer all questions, each carries 3 marks.

		Marks
1	Explain about steganography.	(3)
2	Distinguish between groups and rings.	(3)
3	Explain the concept of public key cryptography.	(3)
4	What is Cipher Feed Back mode (CFB)?	(3)
5	Write short notes on birthday attacks.	(3)
6	Define the term Goofy coin.	(3)
7	Explain about S/MIME.	(3)
8	Define the term pretty good privacy.	(3)

PART B

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

Module I

9	Explain network security model with the help of a neat diagram.	(6)
---	---	-----

OR

10	Explain about play fair cipher and Hill cipher.	(6)
----	---	-----

Module II

11	Explain Chinese remainder theorem with example.	(6)
----	---	-----

OR

12	State and prove Fermat's theorem.	(6)
----	-----------------------------------	-----

Module III

13	Explain Diffie Hellman key exchange algorithm.	(6)
----	--	-----

OR

14	Explain RSA algorithm with example.	(6)
----	-------------------------------------	-----

Module IV

15	Explain about Message Authentication Code algorithm.	(6)
----	--	-----

OR

16	Explain about digital signature scheme.	(6)
----	---	-----

Module V

17	What is bitcoin script? Explain applications of Bitcoin scripts.	(6)
----	--	-----

OR

18	What are bitcoin exchanges? Explain about online wallets?	(6)
----	---	-----

Module VI

19	Explain about IP security.	(6)
----	----------------------------	-----

OR

20	Discuss web security in detail.	(6)
----	---------------------------------	-----
