Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

FIFTH SEMESTER MCA DEGREE EXAMINATION, DECEMBER 2018

Course Code: RLMCA 305

Course Name: CRYPTOGRAPHY AND CYBER SECURITY

Max. Marks: 60 Duration: 3 Hours

PART A

Answer all questions, each carries 3 marks. Marks

1	List out the security services provided in cryptography.	(3)
2	Determine the multiplicative inverse of X^2+1 in $GF(2^4)$ with $m(x)=X^4+X+1$.	(3)
3	Compare and contrast DES and AES.	(3)
4	Discuss any three modes of operation in block ciphers.	(3)
5	List out criteria of a cryptographic hash function.	(3)
6	Define a simple crypto currency with examples.	(3)
7	Describe security association of IPSEC.	(3)
8	Write short note on S/MIME services.	(3)

PART B

Each question carries 6 marks.

9	Explain in detail about the Substitution ciphers with suitable examples.	(6)
	OR	
10	Illustrate and explain symmetric cipher model with various attacks.	(6)
11	Write short notes on the following. i) Group ii) Ring iii) Field	(6)
	OR	
12	Explain extended Euclidean algorithm and apply extended Euclidean algorithm to calculate gcd(161,28).	(6)
13	List out and explain the components of block ciphers in symmetric key encryption.	(6)
	OR	

14	Discuss the four types of transformations used by AES.	(6)
15	Explain various digital signature schemes with suitable diagram.	(6)
	OR	
16	Describe the various components used for message integrity in cryptography.	(6)
17	Define a bitcoin. Explain how bitcoin achieves decentralization.	(6)
	OR	
18	Explain the process of splitting and sharing keys in bitcoin network.	(6)
19	Name the seven types of packets used in PGP and explain their purpose.	(6)
	OR	
20	Explain in detail about the SSL architecture and SSL message format with suitable diagram.	(6)

****