C **Reg. No. :** | | | | | | | | | | |

Question Paper Code: 56801A

B.E./B.Tech. DEGREE EXAMINATION, NOV 2019

Sixth Semester

Information Technology

15UIT601- CRYPTOGRAPHY AND NETWORK SECURITY

(Regulation 2015)

Duration: Three hours Maximum: 100 Marks

Answer ALL Questions

PART A - (5 x 1 = 5 Marks)

1. DES has an initial and final permutation block and _____ rounds. CO1- U

   (a) 14 (b) 15 (c) 16 (d) None of the above

2. RC4 are examples of: CO2- U

   (a) Block ciphers. (b) Hashes. (c) Stream ciphers (d) Public key systems.

3. Which of the following algorithm is also known as NP-complete? CO3- R

   (a) Knapsack (b) RSA (c) DH (d) DES

4. A session symmetric key between two parties is used CO4- R

   (a) only once (b) twice (c) multiple times (d) depends on situation.

5. Which of the following is defined as unwanted and unsolicited bulk e-mail? CO5- R

   (a) Spam. (b) Virus (c) Worm (d) Hackers

PART – B (5 x 3= 15 Marks)

6. Encrypt ‘dlla pqrabkqp’ with Caesar cipher. CO1 R

7. Choose a 4x4 matrix and perform shift rows transformation using AES. CO2 R

8. Specify the applications of the public key cryptosystem? CO3 R

9. Sketch the architecture model of PKI. CO4 R

10. Select an suitable example and how does the firewall protects the security systems CO5 R

PART – C (5 x 16= 80 Marks)

11.	(a)	Apply extended Euclidean algorithm to find multiplicative inverse of 11 in Z_{26}. Use Square and multiply method to calculate 17^{22} mod 21.	CO1- App	(16)
		Or		
	(b)	(i) Define Fermat's theorem and explain its application. Find the result of the following Fermat's theorem: a. $5^{15}\ mod\ 13$	CO1- App	(8)
		(ii) Define Euler's theorems and explain its application. Find the result of the following Euler's theorem: *a.* $12^{-1} mod\ 77$	CO1- App	(8)
12.	(a)	Discuss RC4 algorithm in detail and how it is differ from DES?	CO2- U	(16)
		Or		
	(b)	Explain Data Encryption Standard (DES) in detail.	CO2 - U	(16)
13.	(a)	Explain the principles of public key cryptography	CO3- Ana	(16)
		Or		
	(b)	Describe the MD5 message digest algorithm with necessary block diagrams.	CO3- Ana	(16)
14.	(a)	Analyze the role of TGS in the operations of Kerberos, Explain with an example.	CO4- U	(16)
		Or		
	(b)	What are key rings in PGP? Explain the services of PGP.	CO4- U	(16)
15.	(a)	Analyze the Password selection strategies and Management with suitable example	CO5- U	(16)
		Or		
	(b)	(i) Explain a logic bomb and a time bomb.	CO5- U	(6)
		(ii) Explain the various types of viruses.	CO5- U	(10)