C

Reg. No. : | | | | | | | | | | |

Question Paper Code: 56801

B.E./B.Tech. DEGREE EXAMINATION, APRIL 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. Find the GCD of 2740 and 1760 CO1- U

   (a) 2 (b) 20 (c) 5 (d) 0

2. Find the result of 3^{12} mod 11 CO2- U

   (a) 11 (b) 3 (c) 9 (d) 2

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

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

4. Which of the following is the strongest password CO4- R

   (a) Frank (b) 10251960 (c) P0kemON (d) FSa&Yago.

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. Using the extended Euclidean algorithm, find the GCD of the 291 and 42 and the value of s and t. CO1 R

7. Compare DES and AES. Which one is bit-oriented? Which one is byte-oriented? CO2 R

8. Differentiate between SHA-1 and MD5 CO3 R

9. List out the basic requirements for Kerberos. CO4 R

10. What are the importance's of trust in context to system security. CO5 R

PART – C (5 x 16= 80 Marks)

11. (a) (i) What is the modulo operator, and what is its application? CO1- App (8)

(ii) Using play fair cipher algorithm encrypts the message using the key "MONARCHY" andExplains the poly alphabetic key. CO1- App (8)

Or

(b) (i) Define Fermat's theorem and explain its application. CO1- App (8)

Find the result of the following Fermat's theorem:

a. $5^{15}\ mod\ 13$

(ii Define Euler's theorems and explain its application. CO1- App (8)

Find the result of the following Euler's theorem:

$a.\ \ 12^{-1} mod\ 77$

12. (a) Write short notes on: CO2- U (8)

(i) Chinese Remainder theorem

(ii) Modes of operation CO2- U (8)

Or

(b) Explain Data Encryption Standard (DES) in detail. CO2 - U (16)

13. (a) (i) Briefly explain Diffie – Hellman key Exchange algorithm. Users A and B use Diffie – Hellman key exchange technique with a common prime q=353 and a primitive root α = 3. Users A and B have private keys XA = 17, XB = 21 respectively. What is the shared secret key K1 and K2? CO3- Ana (12)

(ii) How man in middle attack can be performed in Diffie Hellman algorithm. CO3- Ana (4)

Or

(b) Describe the MD5 message digest algorithm with necessary block diagrams. CO3- Ana (16)

14.	(a)	(i) Explain the working principle of the Kerberos protocol	CO4- U	(8)
		(ii) How the encryption is key generated from the password in Kerberos?	CO4- U	(8)
		Or		
	(b)	What are key rings in PGP? Explain the services of PGP.	CO4- U	(16)
15.	(a)	(i) What are the types of analysis adopted by IDPS?	CO5- U	(8)
		(ii) Compare the various generation of firewalls.	CO5- U	(8)
		Or		
	(b)	(i) Explain a logic bomb and a time bomb.	CO5- U	(6)
		(ii) Explain the various types of viruses.	CO5- U	(10)