C **Reg. No. :**

Question Paper Code: 56801

B.E./B.Tech. DEGREE EXAMINATION, MAY 2018

Sixth Semester

Information Technology

15UIT601- CRYPTOGRAPHY AND NETWORK SECURITY

(Regulation 2015)

Duration: Three hours Maximum: 100 Marks

PART A - (5 x 1 = 5 Marks)

Answer All Questions

1. The multiplicative inverse of 13 in Z_{15} is _______________ CO1- R

   (a) Five (b) Seven (c) Nine (d) Eight

2. Which of the following modes of operations does not make use of an initialization vector? CO2- R

   (a) cipher block chaining (b) Output feedback

   (c) Cipher feedback (d) Electronic code book

3. A is using the ElGamal encryption system to transmit a message to B, with p =11, primitive root in G is 2, and private key of A is 3. Calculate e_2 and public key of A CO3- R

   (a) 7 (b) 8 (c) 3 (d) 6

4. The _______________ Protocol uses the Fortezza Algorithm CO4-R

   (a) TLS (b) SET (c) ESP (d) SSL

5. A virus is a computer _________________ CO5- R

(a) File (b) Network (c) Program (d) Database

PART – B (5 x 3= 15Marks)

6. Give the key “MONARCHY”, apply the Playfair cipher to the plaintext “FACTIONALISM”. Encrypt the plaintext. CO1- R

7. Write a short note on meet-in-the-middle attack. CO2- R

8. In the Diffie – Hellman key exchange algorithm, let the prime number be 353 and one of its primitive root be 3. Let the user A and B secret keys XA = 97 and XB = 233. What is a common secret key? CO3- R

9. Discuss the authentication procedure of X.509 CO4- R

10. What do you mean by the term intruders? CO5- R

PART – C (5 x 16= 80Marks)

11. (a) Explain various security mechanisms. CO1- U (16)

Or

(b) (i) Write a Short Note on Transposition Techniques. CO1- U (8)

(ii) Explain Euclidean algorithm for finding the greatest common divisor. CO1- U (8)

12. (a) Explain Advance Encryption Standard. CO2- U (16)

Or

(b) What do you mean by modes of operation in block ciphers? Explain block cipher modes of operation. CO2-U (16)

13. (a) Encrypt the plaintext 20 using RSA public key encryption algorithm. Use prime number 11 and 3 to compute the public key and private key. Also, decrypt the cipher text using the private key. CO3- Ana (16)

Or

(b) Explain MD5 algorithm with the help of a block diagram. CO3- Ana (16)

14. (a) Explain the X.509 authentication service and its certificates. CO4- U (16)

Or

(b) What is SSL? Discuss about its architecture. CO4- U (16)

15. (a) What is a virus? Explain different types of viruses CO5- U (16)

Or

(b) What do you mean by the term intruders? Explain intruder techniques in brief. CO5- U (16)