C　　　　　**Reg. No. :** □□□□□□□□□□

Question Paper Code: 56801

B.E./B.Tech. DEGREE EXAMINATION, NOV 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 extended Euclidean algorithm is of interest to cryptographers because　　CO1- R

(a) It allows us to quickly factorize large composites.

(b) It provides a mechanism to calculate a multiplicative inverse.

(c) It allows us to quickly check primality of large primes.

(d) None of A,B,C.

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. SSL provides only ___________.　　CO4-R

(a) authentication　　(b) confidentiality　　(c) integrity　　(d) durability

5. …………… programs can be used to accomplish functions indirectly that an unauthorized user could not accomplish directly.　　CO5- R

(a) Zombie　　(b) Worm　　(c) Trojan Horses　　(d) Logic Bomb

PART – B (5 x 3= 15Marks)

6. Find gcd (1970, 1066) using Euclid’s algorithm? CO1- R

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

8. Compare DES and AES. CO3- R

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

10. Which types of Intrusion Detection Systems is suitable to your networking Environment and explains why? CO5- R

PART – C (5 x 16= 80Marks)

11. (a) (i) Make use of One time pad cipher encryption and decryption for the plain text 00101001 and key 10101100 and explain where it is used. CO1- U (8)

(ii) Apply the various transposition techniques in detail for the plaintext: meet at the school house CO1- App (8)

Or

(b) 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- U (16)

12. (a) Draw the general structure of DES and describe how encryption and decryption are carried out and identify the strength of DES algorithm. 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) Perform decryption and encryption using RSA algorithm with p=3, q=11, e=7 and M=5 and identify the possible threats for RSA algorithm with its counter measures 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) Explain various firewall design principles and how they prevent intrusions. CO5- U (16)

Or

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