C **Reg. No. :** □□□□□□□□□□

Question Paper Code: 96202

B.E./B.Tech. DEGREE EXAMINATION, NOV 2022

Sixth Semester

Computer science and Engineering

19UCS602- CRYPTOGRAPHY AND NETWORK SECURITY

(Regulations 2019)

Duration: Three hours Maximum: 100 Marks

Answer All Questions

PART A - (5x 1 = 5 Marks)

1. A symmetric cipher system has an IC of 0.041. What is the length of the key 'm'? CO1- U

   (a) 1 (b) 3 (c) 2 (d) 5

2. The number of tests required to break the DES algorithm are CO2- U

   (a) 2.8×1014 (b) 4.2×109 (c) 1.84×1019 (d) 7.2×1016

3. What is the output of the N 1024-bit blocks from the Nth stage in this? CO3- U

   (a) 512 bits (b) 1024 bits (c) N x 1024bits (d) N x 512 bits

4. Extensions were added in which version? CO1- U

   (a) 1 (b) 2 (c) 3 (d) 4

5. In _____, there can be multiple paths from fully or partially trusted authorities. CO1- U

   (a) X509 (b) PGP (c) KDC (d) none of the above

PART – B (5 x 3= 15Marks)

6. Define Model of network security CO1- U

7. Assume that a = 255 and n = 11. We can find q = 23 and r = 2 using the division algorithm we have learned in arithmetic. Calculate q and r for a= -255 and n=11 CO2- App

8. Using the properties of discrete logarithms, show how to solve the following congruence: x 2 ≡ 36 (mod 77). CO2- App

9. Design the role of Ticket Granting Server in inters realm operations of Kerberos. CO2- App

10. Does the firewall ensure 100% security to the system? Comment CO4- Ana

PART – C (5 x 16= 80Marks)

11. (a) Compare transposition cipher and substitution cipher. Apply two stage transpositions Cipher on the “treat diagrams as single units” using the keyword “sequence”. CO2-App (16)

Or

(b) Illustrate the rules to perform encryption using play fair cipher and encrypt ‘snow shooos’ using ‘monarchy’ I and J count as one letter and x is the filler letter. CO2-App (16)

12. (a) Describe AES algorithm with all its round functions in detail. CO1-U (16)

Or

(b) Describe DES algorithm with neat diagram and explain the steps. CO1-U (16)

13. (a) Examine Elliptic Curve Cryptography Simulating ElGamal. CO4-Ana (16)

Or

(b) Users A and B use the Diffie-Hellman key exchange technique, a common prime q=11 and a primitive root alpha=7. CO4-Ana (16)

(i) If user A has private key XA=3.What is A’s public key YA?

(ii) If user B has private key XB=6. What is B’s public key YB?

(iii) What is the shared secret key? Also write the algorithm.

14. (a) Describe Challenge-Response protocols in detail. CO1- U (16)

Or

(b) Design the steps involved in Signature generation and Verification functions of DSS. CO1- U (16)

15. (a) Explain the working principle of SET relate EST for Ecommerce applications CO1-U (16)

Or

(b) Describe PGP cryptographic functions in detail with suitable block diagrams. CO1-U (16)