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

Question Paper Code: 96202

B.E./B.Tech. DEGREE EXAMINATION, NOV 2023

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. Caesar Cipher is an example of CO1- U

   (a) Poly-alphabetic Cipher (b) Mono-alphabetic Cipher

   (c) Multi-alphabetic Cipher (d) Bi-alphabetic Cipher

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. Basically, in SHA-512, the message is divided into blocks of size ___ bits for the hash computation. CO3- U

   (a) 1024 (b) 512 (c) 256 (d) 1248

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)	Illustrate the Classical Encryption Technique with an example	CO1-U	(16)
		Or		
	(b)	Discuss the differences between steganography and cryptography with example in details	CO1-U	(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. (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.	CO4-Ana	(16)
14.	(a)	Develop the process of deriving eighty 64-bit words from 1024 bits for processing Of a single blocks and also discuss single round function in SHA-512 algorithm. Show the values of W16, W17, W18 and W19	CO2- App	(16)
		Or		
	(b)	Design the steps involved in Signature generation and Verification functions of DSS.	CO1- U	(16)
15.	(a)	Explain the architecture of IPsec in detail in detail with a neat block diagram	CO1-U	(16)
		Or		
	(b)	Describe PGP cryptographic functions in detail with suitable block diagrams.	CO1-U	(16)