

B.E./B.TECH. DEGREE EXAMINATION, DECEMBER 2020

Seventh Semester

CS16701- CRYPTOGRAPHY & NETWORK SECURITY

(Regulation 2016)

Time: Three hours

Maximum:80Marks

Answer **ALL** questions

PART A - (8 X 2 = 16 marks)

1. Compute the value of $2^{10} \bmod 11$
 - a) 1
 - b) 10
 - c) 12
 - d) 5
2. In RSA algorithm the value of $p=7$, $q= 11$ and public key $e= 13$. Find the value of the private key d .
 - a) 32
 - b) 37
 - c) 4
 - d) 14
3. In SHA-512 the length of the original message is 2590 bits. What is the number of padding bits?
 - a) 345
 - b) 354
 - c) 365
 - d) 356
4. The Digital envelope in SET (Secure Electronic Transaction) is encrypted using which algorithm?
 - a) RSA
 - b) DES
 - c) AES
 - d) RC5
5. Compute Euler Totient function of 12.
6. Draw key Expansion process of S-DES algorithm.
7. What do you mean by one-way property in Hash function.
8. Distinguish between Virus and Worm.

PART B - (4 X16 = 64 marks)

9. (a) (i) Apply Extended Euclid algorithm to find the inverse of 15 in mod 26. (8)
- (ii) Find the Primality test for the number 1729 using Miller-Rabin Method (8)

(OR)

- (b) (i) Encrypt and Decrypt the plaintext “daddy” using Playfair cipher for the key value “monarchy”. (8)
- (ii) Encrypt and Decrypt the plaintext “cryptography” using column transposition method for the key value ‘3124’ (8)
10. (a) Explain AES algorithm with neat diagram. Justify why AES is considered to be the Efficient symmetric key algorithm? (16)

(OR)

- (b) Explain how the Elliptical curves are useful for cryptography? Discuss about point addition and Point doubling operations in ECC. (16)
11. (a) Discuss in detail how the message is compressed using MD5 algorithm with a neat diagram (16)

(OR)

- (b) Compare and contrast ElGamal Digital Signature with RSA digital signature scheme with an example. (16)
12. (a) Define Firewall. Explain its design goals, types and characteristics of Firewalls. (16)

(OR)

- (b) Discuss the process of SET(Secure Electronic Transaction) with a neat diagram. (16)