Subject Code: KCS074

PAPER ID-410294

Roll No: | | | | | | | | | | | | | |

B.TECH
(SEM VII) THEORY EXAMINATION 2021-22
CRYPTOGRAPY & NETWORK SECURITY

Time: 3 Hours ***Total Marks: 100***

Note: 1. Attempt all Sections. If require any missing data; then choose suitably.

SECTION A

1. Attempt *all* questions in brief. **2 x 10 = 20**

a. What are the requirements of Encrypted Tunnels?
b. Why compression is done before encryption in PGP?
c. Find the value of $\phi(12)$.
d. Compute 3^{61} mod 7.
e. Find gcd (1970, 1066)
f. Explain Transport Layer Security?
g. Explain IPSec ESP Format.
h. What are the requirements of a good hash function?
i. Differentiate between Substitution & Transposition Cipher?
j.What do you mean by cryptanalysis?

SECTION B

2. Attempt any *three* of the following: **10 x 3 = 30**

a. In a public key system using RSA, you intercept the cipher text C=8 sent to a user whose public key is e=13, n=33. What is the plain text M?
b. Differentiate between monoalphabetic ciphers and polyalphabetic ciphers and give one example for each.
c. Explain Chinese Remainder Theorem (CRT) and find X for the given set of congruent equations using Chinese Remainder theorem

X=1 mod 5
X=2 mod 7
X=3 mod 9
X=4 mod 11

d. Give the encryption/decryption procedures using Elliptic Curve Cryptography.
e. Define Euler's Totient Function. Prove that, $\phi(pq) = (p-1)(q-1)$, where p and q are prime numbers.

SECTION C

3. Attempt any *one* part of the following: **10 x 1 = 10**

a. What is the most security-critical component of DES round function? Give a brief description of this function.
b. Write the pseudo code for Miller Rabin primality testing. Test whether 61 is prime or not using the same Miller Rabin test

4. Attempt any *one* part of the following: 10 x 1 = 10

a. Illustrate the working of SHA-1 algorithm with diagram

b.Discuss the Message Authentication Codes. Also give the use of Authentication requirements in MAC.

5. Attempt any *one* part of the following: 10 x 1 = 10

a. Explain the sequence of steps used in Secure Socket Layer handshake Protocol for establishing a new session. Draw a diagram which shows the action of Handshake Protocol.

b. Discuss the stream cipher RC4 in detail.

6. Attempt any *one* part of the following: 10 x 1 = 10

a. Explain the sequence of steps involved in the message generation and reception in Pretty Good Privacy (PGP) with block diagrams.

b**.** Discuss the design of S-Box of AES. How it differs from the S-Boxes of DES.

7. Attempt any *one* part of the following: 10 x 1 = 10

a. Write the Digital Signature Algorithm (DSA) of Digital Signature Standard. What is the implication if same K (secret per message) is used to sign two different message using DSA?

b**.** Define a Group and Ring. Prove that the order of any subgroup of finite group divides the order of the group