Total number of printed pages–4

53 (CS 717) CNWS

CENTRAL LIBRARY
NATIONAL INSTITUTE OF TECHNOLOGY KOKRAJHAR

2021

(Held in 2022)

CRYPTOGRAPHY AND NETWORK SECURITY

Paper : CS 717

Full Marks : 100

Time : Three hours

The figures in the margin indicate full marks for the questions.

Answer ***any five*** *questions.*

1. Explain the following : 5×4=20

   (a) Threats and Attacks

   (b) Vulnerabilities

   (c) Confidentiality, Integrity and Availability

   (d) Confusion and Diffusion.

Contd.

CENTRAL LIBRARY
VTRAL INSTITUTE OF TECH

2. *(a)* Explain the extended Euclid algorithm for finding the inverse of a number.

(b) Using extended Euclid algorithm find—

(i) $(102)^{-1}$ *mod* 411

(ii) $(77)^{-1}$ *mod* 411

(c) Compute GCD (662, 646).

5+10+5=20

3. *(a)* Explain Chinese Remainder Theorem.

(b) An integer $n, 0 \le n < 210$ satisfies the following congruences

$n \bmod 5 = 4$

$n \bmod 6 = 3$

$n \bmod 7 = 2$

Using CRT, find n. Show the calculations.

(c) Find GCD $\left(x^3 + x^2 + 1, x^4 + x + 1\right)$.

8+8+4=20

4. *(a)* Explain the term Discrete Logarithm.

(b) Using discrete logarithm, explain the Diffie-Hellman key exchange protocol.

(c) In a particular scenario two entities A and B wants to agree upon a common secret. Given $p = 131$ and $g = 2$. Consider A's random number be 17 and B's random number be 24. Find their common secret.

5+5+10=20

5. (a) Explain El-Gamal algorithm for encryption, decryption and digital signature.

(b) Explain how public keys and private keys impact on the security of a particular entity.

15+5=20

6. (a) What is an Elliptic Curve?

(b) Check whether the following ECs intersect with itself.

(i) EC (–5, 8)

(ii) EC (–5, 3)

(iii) EC (–3, 2)

(c) Explain the point addition and point doubling of ECs over real number.

4+6+10=20

CENTRAL LIBRARY
CENTRAL INSTITUTE OF TECHNOLOGY KOKRAJHAR

7. Consider the group of points on the EC characterised by

<13, 2, 4, (2, 4), 17, 1>

Two persons A and B want to communicate securely using EC-based encryption algorithm. Suppose A's private key is $a = 9$.

(i) Find A's public key

(ii) If message $(m) = 8$, what is the encrypted message? Consider B's random number is $(r) = 5$

(iii) Explain EC-based digital signature algorithm. 5+5+10=20

CENTRAL LIBRARY
INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR