Total No. of Printed Pages : 4 Roll No.....

MIT (CS)-204/PGDCS-08

COMPUTATIONAL NUMBER THEORY AND CRYPTOGRAPHY

P.G. Diploma in Cyber Security (PGDCS-17)

2nd Semester, Examination-2020

Time Allowed : 2 Hours Maximum Marks : 80

Note : This paper is of Eighty (80) marks divided into Two (02) sections A and B. Attempt the question contained in these sections according to the detailed instructions given therein.

Section-A

(Long Answer type Questions)

Note : Section-'A' contains Five (05) long answer type questions of Twenty (20) marks each. Learners are required to answer any two (02) questions only. (2×20=40)

1. What are the principle elements of a public-key cryptosystem? Explain in detail the three broad categories of application of public-key cryptosystems.

2. A common formulation of the Chinese remainder theorem (CRT) is as follows : Let m_1,..... m_k be integers that are pair wise relatively prime for $1 \leq i, j \leq k$, and $i \neq j$. Define M to be the product of all the m_1's. Let a_1, ... a_k, be integers. Then the set of congruences :

$$x \equiv a_1 (\text{mod } m_1)$$
$$x \equiv a_2 (\text{mod } m_2)$$
$$\vdots$$
$$x \equiv a_k (\text{mod } m_k)$$

Has a unique solution modulo M. Show that the theorem stated in this form in true.

3. Explain Diffie – Hellman key exchange with algorithm.

4. Write about the following :

(a) Elementary Number theory

(b) Digital Signature and Digital Certificate

(c) Time and Space Complexity

(d) Stream Cipher

5. Answer the following :

(a) What is a hash in cryptography? 3

(b) How digital Signatures differs from authentication protocols. 5

(c) State and prove Chinese Remainder Theorem. 7

Section-B

(Short answer type questions)

Note: Section-B Contains Eight (08) short answer type questions of Ten (10) marks each. Learners are required to answer any four (04) questions only. (4×10=40)

1. What GCD Recursion Theorem.
2. What do you understand by Sub Groups? Explain the properties of Sub Groups.
3. What is Chinese Remainder Theorem? Determine the numbers that leave remainders 2, 3 and 2 when divided by 3, 5 and 7 respectively.
4. Write short notes on the following :
   (a) Massey Omura Cryptosystem
   (b) Elgamal Cryptosystem
5. Explain RSA and attacks on RSA public key Cryptosystem.
6. Explain SHA hash functions.
7. Prove that if AKS algorithm returns Prime then n is prime.
8. Define Zero Knowledge proof for Elliptic Curve Discrete Logarithm Problem (ECDLP).

****