QP Code: RD19MSC053 | Reg. No | | | | | | | | | | | AR 19

GIET UNIVERSITY, GUNUPUR – 765022

M. Sc (Third Semester) Examinations, December' 2020

MTPC302 / CC 302 – NUMBER THEORETIC CRYPTOGRAPHY-I

(Mathematics)

Time: 2 hrs | Maximum: 50 Marks

(The figures in the right hand margin indicate marks.)

Q.1. Answer **ALL** the questions (2 x 10 = 20)

a. Multiply $(212)_3$ by $(122)_3$.

b. Find φ(120).

c. If $\left(\frac{a}{p}\right)$ denotes the Legendre's symbol, show that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

d. Define Legendre's symbol.

e. Encrypt the message YES by Caesar's cryptosystem.

f. What is cryptanalysis?

g. What do you mean by probabilistic encryption?

h. Who are the inventors of RSA cryptosystem?

i. Show that the order of any $a \in \mathbb{F}_q^*$ divides $q - 1$.

j. What do you mean by authentication?

PART – B (6 x 5 = 30 Marks)

Answer ***ANY FIVE*** questions — Marks

2. Find an upper bound for the number of bit operations required to compute the binomial coefficient $\binom{m}{n}$. (6)

3. State and prove Fermat's little theorem. (6)

4. With usual notations, Show that $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & if\ p \equiv \pm 1\ (mod\ 8) \\ -1 & if\ p \equiv \pm 3\ (mod\ 8) \end{cases}$ (6)

5. If $\mathbb{F}_q$ is a field of $q = p^f$ elements, then every element satisfies the equation $X^q - X = 0$ and $\mathbb{F}_q$ is precisely the set of roots of that equation. Conversely, for every prime power $q = p^f$ the splitting field over $\mathbb{F}_p$ of the polynomial $X^q - X$ is a field of q elements. (6)

6. Solve the following system of simultaneous congruence. (6)

   $2x + 3y \equiv 1 \mod 26$ $\quad\quad$ $7x + 8y \equiv 2 \mod 26$

7. Suppose that we know that our adversary is using 2 x 2 enciphering matrix with 29-letter alphabet, where A – Z have the usual numerical equivalents, blank = 26, ? = 27, ! = 28. We receive the message "GFPYJP X?UYXSTLADPLW" and we suppose that we know that the last five letters of plaintext are our adversary's signature "KARLA". Find the deciphering matrix and the message. (6)

8. Describe the basis properties of public key cryptosystems. (6)

9. Describe RSA cryptosystem and illustrate with an example. (6)

---End of Paper---