# GIET UNIVERSITY, GUNUPUR – 765022

RN19MSC006

Roll No: | | | | | | |

Total Number of Pages : 2 AR-18 M.Sc

M.Sc 3rd SEMESTER REGULAR EXAMINATIONS, NOV/DEC 2019-20

Subject code: CC302

Subject: NUMBER THEORITIC CRYPTOGRAPHY – I

Time: 3 Hours Max Marks: 80

The figures in the right hand margin indicate marks.

## SECTION A

**Q.1** Answer **any four** of the following: **[4 X4 =16]**

| | | |
|---|---|---|
| a | Find the $g.c.d(1547, 560)$ by using Euclidean algorithm. How many divisors do 945 have? List them all. | 4 marks |
| b | For any integer b and any positive integer n show that $b^n - 1$ is divisible by b – 1 . | 4 marks |
| c | Find $\left(\frac{91}{167}\right)$ using quadratic reciprocity. | 4 marks |
| d | Find the inverse of $A = \begin{pmatrix} 1 & 3 \\ 4 & 3 \end{pmatrix} \bmod 29$ | 4 marks |
| e | Explain the role of Euler phi function in RSA algorithm. | 4 marks |
| f | How can you find the deciphering key in RSA algorithm. | 4 marks |

OR

**2**. Answer all questions from the following **[2 x 8 =16]**

| | | |
|---|---|---|
| a | For the following pair of integers, find the greatest common divisor and express them as linear combination of two numbers 807, 481. | 2 marks |
| b | Multiply YES by NO modulo 26. | 2 marks |
| c | Prove that $\left(\frac{-2}{P}\right) = 1$ if $P \equiv 3 \bmod 8$ | 2 marks |
| d | Define Gauss sum with an example | 2 marks |
| e | Use Shift transformation with key a = 13 to encipher the message HELPME | 2 marks |
| f | Explain affine transformation with an example. | 2 marks |
| g | Define Authentication in public key cryptography. | 2 marks |
| h | Write the RSA algorithm. | 2 marks |

## SECTION-B

**3**. Answer all Questions: **[16 x4 =64]**

3a 8+8 marks

i) Show that $\sum_{d/n} \varphi(d) = n$

ii) Find the smallest non negative solution of the following system of congruences $x \equiv 2 \bmod 3$, $x \equiv 3 \bmod 5$, $x \equiv 4 \bmod 11$, $x \equiv 5 \bmod 16$

OR

b i) Find the smallest non negative solution of the following system of congruence $x \equiv 12 \bmod 31$, $x \equiv 87 \bmod 127$, $x \equiv 91 \bmod 255$ — 8+8 marks

ii) Find the smallest positive integer which leaves a remainder of 1 when divide by 11,a remainder of 2 when divided by 12,and a remainder of 3 when divided by 13.

4a If $F_q$ is a field of $q = p^f$ elements, then every element satisfies the equation $X^q - X = 0$ and $F_q$ is precisely the set of roots of the equation. Conversely for every prime power $q = p^f$ the splitting field over $F_p$ of the polynomial $X^q - X$ is a field of q elements. — 8+8 marks

OR

b i) Show that $(a+b)^p = a^p + b^p$ in any field of characteristic p. — 8+8 marks

ii) $Show\,that \left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$

5a — 8+8 marks

i) Solve the following system of simultaneous conruences $x + 3y \equiv 1 \bmod 26$, $7x + 9y \equiv 2 \bmod 26$

ii) Working in the 26-letter alphabet ,use the matrix $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$ to encipher the message NOANSWER

OR

b Suppose that we know that our adversary using 2X2 enciphering matrix with a 29-letter alphabet, where A-Z have the usual numerical equivalents, blank = 26, ? = 27 and! = 28. We receive the message " GFPYJP X?UYXSTLADPLW" and we suppose that we know that the last five letters of plain text are our adversary's signature "KARLA" .then decipher the message " GFPYJP X?UYXSTLADPLW". — 8+8 marks

6a i) Explain key exchange in public key cryptography. — 8+8 marks

ii) Explain Probabilistic encryption.

OR

b i) Explain RSA algorithm — 8+8 marks

ii) How do we send a signature in RSA