QP Code: RD21MSC071 | Reg. No | | | | | | | | | | | AR 21

# GIET UNIVERSITY, GUNUPUR – 765022

M. Sc. (Third Semester) Examinations, December – 2022

## 20MTPC302 - Number Theoretic Cryptography

(Mathematics)

Time: 3 hrs | Maximum: 70 Marks

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

**PART – A** **(2 x 10 = 20 Marks)**

**Q.1. Answer ALL Questions**

| | | CO# | Blooms Level |
|---|---|---|---|
| a. | Convert $10^6$ to the base 2,7 and 26 | CO1 | K1 |
| b. | Divide $(40122)_7$ by $(126)_7$ | CO1 | K1 |
| c. | Find $\varphi(n)$ for all n from 90 to 95 | CO1 | |
| d. | Make a table showing all quadratic residues and non-quadratic modulo p for p = 3,5,7,13,17 | CO2 | K2 |
| e. | Evaluate the Legendre symbol $\left(\frac{1801}{8191}\right)$ | CO2 | K2 |
| f. | Find the inverse of the matrix $\begin{pmatrix} 15 & 17 \\ 4 & 9 \end{pmatrix} \bmod 26$ | CO2 | K1 |
| g. | Prove that 2465 is a Carmichael number. | CO3 | K2 |
| h. | Factor 200819 using Fermat factorization. | CO3 | K2 |
| i. | Find all bases for which 15 is a pseudo prime. | CO4 | K3 |
| j. | Find the smallest pseudo prime to the base 5. | CO4 | K3 |

**PART – B** **(10 x 5 = 50 Marks)**

Answer ***ANY FIVE*** questions

| | | Marks | CO# | Blooms Level |
|---|---|---|---|---|
| 2. a. | Let p be a prime number. Then show that any integer a not divisible by p satisfies $a^{p-1} \equiv 1 \bmod p$ | 5 | CO1 | K2 |
| b. | If $a$ is relatively prime to $m$ then prove that $a^{\varphi(m)} \equiv 1 \bmod m$ | 5 | CO1 | K2 |
| 3.a. | Find the smallest positive integer which leaves a remainder of 1 when divided by 11, a remainder of 2 when divided by 12, and a remainder of 3 when divided by 13. | 5 | CO1 | K2 |
| b. | Prove that the Legendre symbol satisfies the following properties. | 5 | CO2 | K2 |

i) $\left(\frac{a}{p}\right)$ depends only on the residue of modulo p

ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

iii) For b prime to 'p', $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$

| | | | | |
|---|---|---|---|---|
| 4. a. | In the 27- letter alphabet (with blank = 26), use the affine transformation with key a = 13, b = 9 to encipher the message "HELP ME". | 5 | CO2 | K3 |
| b. | Working in the 26-letter alphabet, use $\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \bmod 26$. Encipher the plain text "NOANSWER" | 5 | CO2 | K3 |
| 5.a. | Explain RSA algorithm with an example. | 6 | CO3 | K2 |
| b. | Prove that a Carmichael number must be product of at least three distinct primes. | 4 | CO3 | K2 |
| 6. | Factor 29895581 by using Fermat Factorization | 10 | CO4 | K3 |
| 7. | Factor 9509 using continued fraction algorithm | 10 | CO4 | K3 |
| 8. | Factor 1829 by taking $b_i$ = 42,43,61,74,85,86 using factor base algorithm. | 10 | CO4 | K3 |

--- End of Paper ---