Reg. No □□□□□□□□□□ AY - 23

GANDHI INSTITUTE OF ENGINEERING AND TECHNOLOGY UNIVERSITY, ODISHA, GUNUPUR

(GIET UNIVERSITY)

M. Sc. (Fourth Semester) Regular Examinations, April 2025

22MTPC404 – 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. Multiply $(212)_3$ by $(122)_3$	CO1	K2
b. Find the $g.d.c(1547,560)$	CO1	K1
c. Using any Shift transformation encrypted the message “GIETU”.	CO2	K2
d. Determine A^{-1} if $A = \begin{pmatrix} 15 & 17 \\ 4 & 9 \end{pmatrix}$ $mod\ 26$ using enciphering matrices.	CO2	K2
e. Find the solution of the Knapsack problem $\{v_i\} = \{2,3,7,20,35,69\}, V = 45$.	CO3	K2
f. Check whether the number 2465 is Carmichael numbers or not	CO3	K2
g. Find the Continued fraction of $\frac{55}{89}$.	CO4	K2
h. Let $n = 4633$. Find the smallest factor base B such that the square of $68,69\ and\ 96$ are B-numbers	CO4	K2
i. Using Gauss Lemma find $\left(\frac{3}{13}\right)$	CO2	K2
j. Find the Quadratic Residue and Non- Quadratic Residue of F_{13}^{*}?	CO2	K2

PART – B **(10 x 5 = 50 Marks)**

Answer ***ANY FIVE*** questions	Marks	CO #	Blooms Level
2. Solve $\begin{matrix} x \equiv 2\ mod\ 3 \\ x \equiv 3\ mod\ 5 \\ x \equiv 4\ mod\ 11 \\ x \equiv 5\ mod\ 16 \end{matrix}$. Find the non-negative solution	10	CO1	2
3.a. State and prove Fermat’s Little Theorem.	5	CO1	2
b. Find a 3-digit number which leaves a reminder of 4 when divided by 7, 9, or 11.	5	CO1	2
4. Find the $g.c.d$ of $f(x) = x^4 + x^3 + x^2 + 1$ and $g(x) = x^3 + 1$ in $F_{2(x)}$, using Euclidean Algorithm.	10	CO2	2
5. State and prove Law of Quadratic Reciprocity for Legendre Symbol.	10	CO2	2
6. Decrypt the message “NMYSOZGK” using Affine transformation with $a = 7, N = 26, b = 12$.	10	CO3	2
7. Suppose that plain text message units are single letter 26-letter alphabet with A to Z corresponding to 0 to 25. The public key is the sequence $w_i = \{57,14,3,24,8\}$ and the 2nd key $b = 23, m = 61$. Use above public key to encrypt “TENFOUR”.	10	CO4	2
8. Using Continued fraction factoring algorithm to factor 9073	10	CO4	2

End of Paper