QP Code: R253G064 | Reg. No | | | | | | | | | | | AY 24

Gandhi Institute of Engineering and Technology University, Odisha, Gunupur
(GIET UNIVERSITY)

M.Sc. (Third Semester – Regular) Examinations, December – 2025

24MPCMA23003 – Number Theoretic Cryptography

(Mathematics)

Time: 3 hrs | Maximum: 60 Marks

Answer ALL questions
(The figures in the right-hand margin indicate marks)

PART – A **(2 x 5 = 10 Marks)**

Q.1. Answer ***ALL*** questions	CO #	Blooms Level
a. Find the inverse of 3 modulo 7.	CO1	K1
b. Find A^{-1}, if $A = \begin{bmatrix} 3 & 5 \\ 2 & 4 \end{bmatrix} mod 26$	CO1	K2
c. Define discrete logarithm.	CO3	K1
d. Check the number 1729 is Carmichael or not?	CO5	K1
e. Find the Continued fraction of $\frac{45}{89}$	CO6	K2

PART – B **(10 x 5 = 50 Marks)**

Answer ***ALL*** the questions	Marks	CO #	Blooms Level
2. a. The hexadecimal system means base b = 16 with letters A-F representing the tenth to fifteenth digits respectively, divide $(131B6C3)_{16}$ by $(1A2F)_{16}$.	7	CO1	K1
b. Find the 3-digit number which leaves a remainder of 4 when divided by 7, 9, or 11	3	CO1	K1
(OR)			
c. How many divisors 840 has? List them	5	CO2	K2
d. Make a table showing all quadratic and non-quadratic residues modulo p for p = 3, 5, 7, 13, 17, 19	5	C02	K2
3.a. Suppose the plain text 'HELP' is encrypted to 'DRPA' with an enciphering matrix A, then find A.	5	CO4	K3
b. Select value(s) of x so as to simultaneously satisfy the equations x ≡ 2(mod5), x ≡ 3(mod7) and x ≡ 5(mod11)	5	CO5	K2
(OR)			
c. Given $2^{100000} \equiv x(mod 33)$ then find the value of x	5	CO5	K2
d. Using matrix $A = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} mod\ 26$, decipher the text "WSRZFRDSDP".	5	CO5	K3
4.a. Explain RSA algorithm with an example.	5	CO6	K2
b. Show that 561 is the smallest Carmichael number.	5	CO4	K1
(OR)			

c.	Explain the Knapsack cryptosystem and encrypt the message 'WHY' by using, $\{v_i\} = \{2,3,7,15,31\}, a = 45, m = 61.$	7	CO5	K2
d.	Show that the discrete logarithm of 7 to the base 2 is 6 in F_{19}^*	3	CO4	K2
5.a.	Find all the bases for which 15 is a pseudoprime.	5	CO4	K2
b.	If n is a Euler pseudoprime to the base b then prove that n is pseudoprime to the base b.	5	CO2	K2
	(OR)			
c.	Show that 65 is a strong pseudoprime to the base 8 and to the base 18.	5	CO2	K3
d.	Prove that a Carmichael number is product of at least three prime numbers.	5	CO2	K2
6.a.	Explain the Factor base algorithm to factor a number n and factor n = 1829 using b numbers 42, 43, 61, 74, 85, 86	10	CO6	K2
	(OR)			
b.	Discuss the continued fraction factoring algorithm and factor 9073 using this algorithm.	10	C06	K2

--- End of Paper ---