QP Code: RM22MSC129 Reg. No □□□□□□□□□□ AY 22

GIET UNIVERSITY, GUNUPUR – 765022

M. Sc. (Fourth) Regular Examinations, May – 2024

20MTPC404 - 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.	Divide (11001001) by 100111	CO1	K1
b.	Divide JQVXHJ by WE	CO1	K1
c.	Compute $2^{1000000} \bmod 77$	CO1	K1
d.	For P = 11,13,17 find the smallest positive integer which generates $F_p^{\,*}$	CO2	K2
e.	Find the inverse of $A=\begin{pmatrix}15 & 17\\ 4 & 9\end{pmatrix}\in M_2(Z/26Z)$	CO2	K2
f.	Explain the idea of public key cryptography	CO2	K1
g.	Define Authentication in public key cryptography	CO3	K2
h.	What are the devices that Picara has in Zero knowledge proof of three color problem	CO3	K2
i.	Define Strong Pseudo prime	CO4	K3
j.	Show that n=561 is Carmichael number	CO4	K3

PART – B **(10 x 5 = 50 Marks)**

		Marks	CO#	Blooms Level
2.a	State and prove Chinese Remainder Theorem.	5	CO1	K2
b.	If $g.c.d(a,m)=1$ then prove that $a^{\varphi(m)}=1 \bmod m$.	5	CO1	K2
3.	For any positive odd integer n show that $\left(\dfrac{2}{n}\right)\equiv(-1)^{(n^2-1)/8}$	10	CO1	K2
4.	Working in the 26-letter alphabet ,use the matrix $A=\begin{pmatrix}2 & 3\\ 7 & 8\end{pmatrix}$ to encipher the message **NOANSWER.**	10	CO2	K3
5.	Suppose that we our adversary is using an enciphering matrix A in the 26-letter alphabet. We intercept the cipher text “WKNCCHSSJH” and we know that the first word is “GIVE” then decipher the message “WKNCCHSSJH”.	10	CO2	K3
6.	Let n be an odd composite number. If n is divisible by a perfect square, then show that n is not a Carmichael number.	10	CO3	K2
7.	Using factor base algorithm factor 1829 using 42.43,61,74,85 and 86.	10	CO4	K3
8.	Use Fermat factorization factor 200819.	10	CO4	K3

--- End of Paper ---