STELLA MARIS COLLEGE (AUTONOMOUS) CHENNAI – 86
(For candidates admitted from the academic year 2023 – 2024 and thereafter)

M.Sc. DEGREE EXAMINATION, NOVEMBER 2024
BRANCH I - MATHEMATICS
FIRST SEMESTER

COURSE	**:**	**ELECTIVE**	
PAPER	**:**	**NUMBER THEORY AND CRYPTOGRAPHY**	
SUBJECT CODE	**:**	**23MT/PE/NC15**	
TIME	**:**	**3 HOURS**	**MAX. MARKS: 100**

Q. No.	SECTION A $(5 \times 2 = 10)$ Answer ALL questions	CO	KL
1.	What is the decimal equivalence of $(N\ O\ W)_{26}$?	1	1
2.	Define the Legendre symbol.	1	1
3.	Define cryptosystem.	1	1
4.	What is Hash function?	1	1
5.	Define a strong pseudoprime.	1	1

Q. No.	SECTION B $(10 \times 1 = 10)$ Answer ALL questions	CO	KL
6.	The decimal equivalent of $(1\ 0\ 1\ 1)_2$is __________. a) 11 b) 12 c) 21 d) 22	2	2
7.	The g.c.d. of (360, 294) is _____. a) 14 b) 4 c) 16 d) 6	2	2
8.	The order of a non-zero element is the least positive power that gives ____. a) 1 b) 10 c) 0 d) same element	2	2
9.	A generator g of a finite field F_q is an element of order _____. a) $q\ - 1$ b) $q + 1$ c) $q^2 - 1$ d) $q^2 + 1$	2	2
10.	A message unit cannot be a ___________. a) single letter b) digraph c) trigraph d) block of 23 letters	2	2
11.	The map is the map $C = aP + b\ mod\ N$ where a and b are enciphering keys is ______________. a) linear b) affine c) shift d) all of the above	2	2
12.	A function in cryptosystem whose inverse is hard to compute is called as a _____________ function. a) encipher b) decipher c) trapdoor d) shift	2	2
13.	The last names of the inventors of RSA are _____. a) Reagen, Shamir & Adleman b) Reagen, Shanine & Aden c) Rivest, Shamir & Adleman d) Rivest, Shamir & Aden	2	2
14.	The smallest pseudoprime to the base 2 is _____. a) 301 b) 311 c) 353 d) 341	2	2
15.	The factor of 91 using $f(x) = x^2 + 1$ & $x_0 = 1$ is ____________. a) 5 b) 3 c) 7 d) 21	2	2

..2

Q. No.	**SECTION C** $(\mathbf{2 \times 15 = 30})$ **Answer ANY TWO questions**	**CO**	**KL**
16.	State and prove Fermat’s Little theorem and hence prove if a is not divisible by p and if $n \equiv m\ mod(p-1)$, then $a^n \equiv a^m mod\ p$.	3	3
17.	a) Construct a field with 9 elements. b) Prove that $\left(\frac{a}{p}\right) \equiv a^{\left(\frac{p-1}{2}\right)} mod\ p$. (8+7)	3	3
18.	Find the solution for the following system of simultaneous congruences: $2x + 3y \equiv 1(\text{mod } 26)$ $7x + 8y \equiv 2(\text{mod } 26)$	3	3
19.	Explain about (i) Classical cryptosystem versus private key cryptosystem (ii) Authentication. (8+7)	3	3

Q. No.	**SECTION D** $(\mathbf{2 \times 15 = 30})$ **Answer ANY TWO questions**	**CO**	**KL**
20.	Find the smallest nonnegative solution of the following system of congruences: $x \equiv 2\ mod\ 3;\ x \equiv 3\ mod\ 5;\ x \equiv 4\ mod\ 11;\ x \equiv 5\ mod\ 16.$	4	4
21.	a) With usual notations prove that $G^2 = (-1)^{\frac{q-1}{2}} q$. b) Determine whether 7411 is a residue modulo the prime 9283. (10+5)	4	4
22.	Intercept the coded message “DXM SCE DCCUVGX”, which was enciphered using an affine map on digraphs in a 30 – letter alphabet, in which A – Z have numerical equivalents 0 – 25, blank = 26, ? = 27, ! = 28, ’ = 29. A frequency analysis shows that the most common digraphs in earlier cipher texts are “M ”, “U ” and “IH”, in that order. Suppose that in the English language the most frequently occurring digraphs are “E ”, “S ” and “ T”, in that order. a) Find the deciphering key and read the message b) Find the enciphering key and encrypt the message “A DEMO”	4	4
23.	If *n* is an strong pseudoprime to the base *b*, then prove that it is an Euler pseudoprime to the base *b*. Is the converse true? Justify.	4	4

Q. No.	**SECTION E** $(\mathbf{2 \times 10 = 20})$ **Answer ANY TWO questions**	**CO**	**KL**
24.	Find an upper bound for the number of bit operations required to compute n!	5	5
25.	State and prove the law of quadratic reciprocity.	5	5
26.	Decipher the message “FQOCUDEM” which is enciphered using shift transformation on single letters of 26 alphabets. Given that the letter “U” in the coded message is “E”.	5	5
27.	Prove that if *n* is an odd composite integer and if *n* is divisible by a perfect square greater than 1, then *n* is not a Carmichael number.	5	5