STELLA MARIS COLLEGE (AUTONOMOUS) CHENNAI 600 086
(For candidates admitted during the academic year 2023 – 24)

M. Sc. DEGREE EXAMINATION, NOVEMBER 2023
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.	Define Big O – notation.	1	1
2.	Define a generator of a finite field.	1	1
3.	What is a Shift transformation?	1	1
4.	Define Hash function.	1	1
5.	What is a Carmichael number?	1	1

Q. No.	SECTION B $(10 \times 1 = 10)$ Answer ALL questions	CO	KL
6.	The number of base - b digits in an integer n is $a)$ $[log_b\ n] + 1$ b) $(\ log_b\ n)$ c) $(\ log_b\ n) + 1$ d) $[log_e\ n] + 1$.	2	2
7.	If a is divisible by p and if $n \equiv m$ (mod $p - 1$), then $a)$ $a^m \equiv a^n$ (mod p) b) $a^m \not\equiv a^n$ (mod p) c) $a^m \equiv a^n$ (mod $p - 1$) d) $a^{p-1} \equiv 1$ (mod p).	2	2
8.	The order of any $a \in F_q^*$ divides a) q b) p^f c) $q - 1$ d) q^f	2	2
9.	If a is an integer and $p = 2$, then a) $\left(\frac{a}{p}\right) = 1$ b) $\left(\frac{a}{p}\right) = -1$ c) $\left(\frac{a}{p}\right) = 0$ d) $\left(\frac{a}{p}\right)$ is not defined.	2	2
10.	The transformation of the type $C \equiv aP + b$ (mod N) is called a) Shift transformation b) Affine transformation c) Deciphering transformation d) linear transformation	2	2
11.	$M_2(R)$ is a a) Commutative ring b) Matrix ring over R c) Field d) none of the above.	2	2
12.	In the function $f : P \rightarrow C$ a) f is onto b) f is invertible c) f is not invertible d) f is a hash function.	2	2
13.	Public key cryptosystem is also called as a) symmetrical cryptosystem b) prime c) pseudoprime d) none of the above	2	2
14.	A primality test is a criterion for a number n a) not to be a prime b) is a prime c) is a pseudoprime d) Mersenne prime.	2	2
15.	If n is an Euler pseudoprime to the base b, then it is a) a pseudoprime b) not a pseudoprime c) a composite d) none of the above	2	2

Q. No.	**SECTION C** $(\mathbf{2 \times 15 = 30})$ **Answer ANY TWO questions**	CO	KL
16.	Find an upper bound for the number of bit operations to compute $n!$.	3	3
17.	Show that $\left(\frac{a}{p}\right) = a^{(p-1)/2}$ mod p.	3	3
18.	In a long string of ciphertext which was encrypted by means of an affine map on single letter message units in the 26 letter alphabet, you observe that the most frequently occurring letters are "Y" and "V", in that order. Assuming that those ciphertext message units are the encryption of "E" and"t" , respectively, read the message "QAOOYQQEVHEQV".	3	3
19.	Check whether 91 is a pseudoprime to the base 2.	3	3

Q. No.	**SECTION D** $(\mathbf{2 \times 15 = 30})$ **Answer ANY TWO questions**	CO	KL
20.	Find the smallest nonnegative solution of each of the following system of congruences: $x \equiv 2 \bmod 3$ $x \equiv 3 \bmod 5$ $x \equiv 4 \bmod 11$ $x \equiv 5 \bmod 16$	4	4
21.	If $g.c.d(a,m) = 1$ and $n \equiv n' \bmod \varphi\ (m)$,then show that $a^n \equiv a^{n'}$ (mod m).	4	4
22.	Determine whether 7411 is a residue modulo the prime 9283.	4	4
23.	Write short note on key exchange.	4	4

Q. No.	**SECTION E** $(\mathbf{2 \times 10 = 20})$ **Answer ANY TWO questions**	CO	KL
24.	Find 160^{-1} (mod 841).	5	5
25.	In the 27 letter alphabet (with blank = 26), use the affine enciphering transformation with key $a = 13, b = 9$ to encipher the message "HELP ME".	5	5
26.	The Legendre symbol satisfies the following properties: a) $\left(\frac{a}{p}\right)$ depends only on the residue of a modulo p. b) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. c) for b prime to p, $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$. d) $\left(\frac{1}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.	5	5
27.	Give an example to show that if n is a pseudoprime then it is not an euler pseudoprime.	5	5

⅄⅄⅄⅄⅄⅄⅄⅄⅄