STELLA MARIS COLLEGE (AUTONOMOUS) CHENNAI 600 086
(For candidates admitted during the academic year 2019 – 20 & thereafter)

SUBJECT CODE : 19MT/PE/NC15

M. Sc. DEGREE EXAMINATION, NOVEMBER 2022
BRANCH I - MATHEMATICS
FIRST SEMESTER

COURSE : ELECTIVE
PAPER : NUMBER THEORY AND CRYPTOGRAPHY
TIME : 3 HOURS **MAX. MARKS : 100**

SECTION – A

ANSWER ALL THE QUESTIONS: **(5 × 2 = 10)**

1. Find the g.c.d (1547,560).
2. Define generator of a Finite Field F_q.
3. Define digraph transformation.
4. Define trapdoor function.
5. Define a pseudoprime.

SECTION – B

ANSWER ANY FIVE QUESTIONS: **(5 × 6 = 30)**

6. State and prove Fermat's Little theorem.
7. Use repeated squaring method to find 38^{75} mod (103).
8. Show that for any $q = p^f$ the polynomial $X^q - X$ factors in Fp [x] into the product of all monic irreducible polynomials of degrees d dividing f.
9. In the 27 letter alphabet (with blank = 26, key a = 13, b = 9) encipher the message "HELP ME".
10. Solve $2x + 3y \equiv 1 \bmod 26$

    $7x + 8y \equiv 2 \bmod 26$.
11. How do you send a signature in RSA.
12. Check whether 91 is a pseudoprime to the base 3.

..2

SECTION – C

ANSWER ANY THREE QUESTIONS: (3 × 20 = 60)

13. a. Estimate the time required to convert a k- bit integer 'n' to its representation in base 'b' where b might be very large.

    b. Find the highest power of p which exactly divides n!.

14. State and prove Quadratic law of Reciprocity using Legendre symbol.

15. a. 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".

    b. Working in a 26 – letter alphabet, use the matrix of A = $\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$ to decipher "FWMDIQ".

16. a. Describe the basic properties of public key cryptosystem.

    b. Write a short note on i) Hash function

    ii) Key exchange.

17. a. Show that every Carmichael number must be a product of 3 distinct primes.

    b. Factor 4087 where $f(x) = x^2 + x + 1$, $x_0 = 2$ using rho – method.