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

SUBJECT CODE : 19MT/PE/NC15

M. Sc. DEGREE EXAMINATION, NOVEMBER 2019
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. Multiply $(212)_3$ by $(122)_3$.
2. Define charachteristic of a field.
3. Define Cryptosystem.
4. Explain Key exchange.
5. Define a Carmichael number.

SECTION – B

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

6. Express 7 as a linear combination of 1547 and 560.
7. For any integer b and a positive integer n show that $b^n - 1$ is divisible by $b - 1$ with quotient $b^{n-1} + b^{n-2} + \ldots + b^2 + b + 1$.
8. If f is prime, then show that there are $\frac{p^f - p}{f}$ distinct monic irreducible polynomials of degree f in $F_p[X]$.
9. In the 27 letter alphabet (with key a = 13, b = 9) encipher the message "HELP ME".
10. Working on a 26 letter alphabet encipher the message "NO" using $\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$.
11. Write a short note on Authentication.
12. Check whether 91 is a pseadoprime to the base 3.

..2

SECTION – C

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

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

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 atleast 3 distinct primes.

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

⅄⅄⅄⅄⅄⅄⅄⅄⅄⅄⅄