STELLA MARIS COLLEGE (AUTONOMOUS) CHENNAI-86
(Effective from the academic year 2019-2020)

M.Sc. Degree Examination – NOV 2021

19MT/PE/NC15

Number Theory and Cryptography

Course: Post Graduate Elective Time: 3 Hours
Max. marks: 100

SECTION – A
ANSWER ALL THE QUESTIONS: (2×4 = 8)

1. Estimate the time requires to convert a k-bit integer 'n' to it's representation in the base b, where b might be very large.
2. Define Strong and Euler Pseudoprimes.

SECTION – B
ANSWER ANY TWO QUESTIONS: (2×12 = 24)

3. Divide $(JQVXHJ)_{26}$ *by* $(WE)_{26}$.
4. Define a generator of a finite field. Show that every finite field has a generator. Also show that there exists a total of $\phi(q-1)$ different generators of F_{q^*}, where F_{q^*} is the set of all non-zero elements of F_q.
5. Find the inverse of A = $\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \in M_2\left(\frac{Z}{26Z}\right)$ and verify the same.

SECTION – C
ANSWER ANY TWO QUESTIONS: (2×34 = 68)

6. a) State and prove Fermat's Little Theorem.
   b) Compute $\pi = 3.141592654$ to base 2 and base 26 number.
   c) Find $160^{-1}\ mod\ 841$. (12+12+10)

7. a) State and prove the properties of Legendre's symbol.
   b) Prove that for any positive n, $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.
   c) Prove that a Carmichael number must be the product of atleast three distinct primes. (15+9+10)

8. a) Intercept the message "!IWGVIEX!ZRADRYD" which was sent using a linear enciphering transformation of digraph vectors in a 29 letter alphabet in which A- Z have numerical equivalents 0-25, blank = 26, ? = 27, ! = 28. The last five letters of the plaintext are "MARIA". Find the deciphering matrix and read the message.
   b) What is RSA Algorithm? Explain how it works. (20+14)