STELLA MARIS COLLEGE (AUTONOMOUS) CHENNAI 600 086
(For candidates admitted during the academic year 2015 – 16& thereafter)

SUBJECT CODE : 15MT/PE/NC14

M. Sc. DEGREE EXAMINATION, NOVEMBER 2016
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 x 2 = 10)**

1. Multiply $(212)_3$ by $(122)_3$.
2. Find the number of divisors of 945.
3. Define the Legendre symbol $\left(\frac{a}{p}\right)$.
4. Working with the 26 letter alphabet, using the matrix $\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$encipher the message unit "NO".
5. Explain the term Hash function.

SECTION – B

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

6. Find an upper bound for the number of bit operations required to compute $n!$.
7. Prove that $\sum_{d/n} \varphi(d) = n$.
8. State and prove Fermat's little theorem.
9. Let Fqbe the finite field of$q = p^f$elements and let $\sigma: Fq \to Fq$ be defined by$\sigma(a) = a^p$. Prove thatσ is an automorphism of the field Fq.
10. 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".
11. Find the inverse of $\begin{pmatrix} 1 & 3 \\ 4 & 3 \end{pmatrix}$mod 29.
12. Explain public key cryptosystem and mention its advantages over the classical cryptosystem.

..2

SECTION – C

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

13. (a) Show that the Euclidean algorithm always gives the g.c.d in a finite number of steps. Also show that if $a > b$, time (finding g.c.d (a, b) by Euclidean algorithm) is $O(log^3(a))$.

(b) Estimate the time required to convert k-bit integer to its base 10. Deduce the case when the representation is in the base b where b is very large. (10+10)

14. (a) State and Chinese remainder theorem.

(b) Factor $2^{11} - 1$. (14+6)

15. (a) State and prove the Law of Quadratic reciprocity.

(b) Determine whether 7411 is a quadratic residue modulo the prime 9283. (14+6)

16. You intercept the message “ZRIXXYVBMNPO”, which you know resulted from a linear enciphering transformation of digraph vectors, in a 27-letter alphabet in which A–Z have numerical equivalents 0–25 and blank =26. You have found that the most frequently occurring cipher text digraphs are “PK” and “RZ”. You guess that they correspond to the most frequently occurring plain text digraphs in the 27-letter alphabet, namely, “E” (E followed by blank) and “S .” Find the deciphering matrix, and read the message. (20)

17. (a) Explain briefly the method of sending a signature in RSA.

(b) Factor 4087, using$f(x) = x^2 + x + 1$ and $x_0 = 2$. (10+10)