STELLA MARIS COLLEGE (AUTONOMOUS) CHENNAI 600 086
(For candidates admitted during the academic year 2011 – 12 & thereafter)

SUBJECT CODE : 11MT/PE/NC14

M. Sc. DEGREE EXAMINATION, NOVEMBER 2014
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. Find the g.c.d. (1547, 560)
2. State Fermat's Little theorem.
3. Prove that $\left(\frac{1}{p}\right) = 1$ and $\left(-\frac{1}{p}\right) = (-1)^{p-1/2}$.
4. Using the matrix $\begin{pmatrix}2 & 3\\ 7 & 8\end{pmatrix} \in M_2({}^{Z}/_{26z})$, encipher the message unit 'No'.
5. Define hash function.

SECTION – B

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

6. Find the upper bound for the number of bit operations required to compute n!.
7. If g.c.d $(a.m) = 1$ and if n' is the least nonnegative residue of a modulo $\phi(m)$. then show that $a^n \equiv a^{n'}$ mod m.
8. If $b^a \equiv 1$ mod m and $b^c \equiv 1$ mod m where b is prime to m, a and c are positive integers and if $d =$ g.c.d.(a, c), then show that $b^d \equiv 1$ mod m.
9. If f is a prime number then show that there are $(p^f - p)/f$ distinct monic irreducible polynomials of degree f in $F_p[X]$.
10. Determine whether 7411 is a residue module the prime 9283.
11. In the 27-letter alphabet with (with blank = 26), use the affine enciphering transformation with key $a = 13, b = 9$ to encipher the message 'HELP ME'.
12. How do you send signature in RSA.

SECTION – C

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

13. (i) Prove that the Euclidean algorithm always gives the greatest common divisor in a finite number of steps. In addition, for $a > b$ Time (finding g.c.d.(a, b) using Euclidean algorithm) = $O(log^3(a))$.

 (ii) Find the g.c.d.(2613, 2171) using Euclidean algorithm and express it as an integer linear combination of the two numbers. (12+8)

14. (i) State and prove Chinese remainder theorem.

 (ii) Find the smallest non negative solution of the system of congruence.

 $19x \equiv 103\, mod\, 900$

 $10x \equiv 511\, mod\, 841$ (10+10)

15. (i) Show that the order of any $a \in F_q{}^*$ divides $q - 1$.

 (ii) Obtain the reciprocity law for the Jacobi symbol. (10+10)

16. (i) 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 letter 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".

 (ii) You intercept the message "SONAFQCHMWPTVEVY", which you know resulted from a linear enciphering transformation of digraph-vectors, where the sender used the usual 26 – letter alphabet A-Z with numerical equivalents 0-25, respectively. An earlier statistical analysis of a long string of intercepted ciphertext revealed that the most frequently occurring ciphertext digraphs were "KH" and "XW" in that order. Those digraphs correspond to "TH" and "HE" respectively. Find the deciphering matrix and read the message. (10+10)

17. Write a detailed note on public key cryptography.

⅄⅄⅄⅄⅄⅄⅄⅄⅄⅄