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 2017
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. In the base 26, with digits A-Z representing 0-25 multiply YES by No.
2. Prove that n^5- n is always divisible by 30.
3. Find $\left(\frac{168}{11}\right)$.
4. Find the inverse of the matrix $\begin{pmatrix} 1 & 3 \\ 4 & 3 \end{pmatrix}$ *mod 5* .
5. Define Euler Pseudo-prime.

SECTION – B

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

6. Find an upper bound for the number of bit operations required to compute the binomial coefficient*nCm*.
7. Find the prime factorization of 2^{35}-1.
8. Let $q = p^f$, where p is prime. Show that the splitting field of the polynomial $X^q - X$ is a field with q elements.
9. Solve the following system of simultaneous congruence
   $2x + 3y \equiv 1 mod 26, \quad 7x + 8y \equiv 2 mod 26.$
10. Write a note on RSA cryptosystem.
11. State and prove the Fermat's Little theorem.
12. Prove that $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} mod p.$

SECTION – C

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

13. (a) Find an upper bound for the number of bit operations required to compute n!.
    (b) Divide $(11001001)_2$ by $(100111)_2$, and divide $(\text{HAPPY})_{26}$ by $(\text{SAD})_{26}$
    (c) Prove that the g.c.d of two numbers can be expressed as a linear combination of the numbers with integer coefficients and express 7 as a linear combination of 1547 and 560. (6+6+8)

14. (a) Find the smallest non-negative solution of the following system of congruence.
$x \equiv 2 \bmod 3$; $x \equiv 3 \bmod 5$; $x \equiv 4 \bmod 11$; $x \equiv 5 \bmod 16$.
(b) Prove :$\sum_{d/n} \varphi(d) = n$. (12 + 8)

15. (a) Prove that for any $q = p^f$ the polynomial $X^q - X$ factors in $F_p[x]$ into the product of all monic irreducible polynomials of degrees d dividing f .
(b) Prove with usual notations $G^2 = (-1)^{(q-1)/2}q$.
(c) Determine whether 7411 is a quadratic residue modulo the prime 9283. (10+5+5)

16. (a) In a long string of cipher text which was encrypted by means of an affine map in 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 cipher text message units are the encryption of “E” and “T”, respectively, read the message “QAOOYQQEVHEQV”.
(b) Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(Z/NZ)$ and set $D = ad - bc$.
Then prove that the following are equivalent.
(i) g.c.d (D, N) =1
(ii) A has an inverse matrix
(iii) If x and y are not both 0 in Z/NZ , then $A\begin{pmatrix} x \\ y \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$;
(iv) A gives a 1-1 correspondence of $(Z/NZ)^2$ with itself. (12 + 8)

17. (a) Explain the following terms with example.
Authentication, Hash function, Key Exchange, Probabilistic Encryption.
(b) If n is a strong pseudo prime to the base b, then prove that it is an Euler pseudo prime to the base b. (8+12)