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

SUBJECT CODE : 15MT/PE/NC14

M. Sc. DEGREE EXAMINATION, NOVEMBER 2015
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. Using Euclidean Algorithm , find g.c.d. (1547, 560).
2. If a ≡ b mod m and $c \equiv d \, mod \, m$ then prove that $a \pm c \equiv b \pm d \, mod \, m$.
3. Define the Legendre symbol.
4. Find the inverse of $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \in M_2(Z/\, 26\, Z)$.
5. Define a Carmichael number.

SECTION – B

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

6. Estimate the time required to convert a k-bit integer to its representation in the base 10.

7. If b is prime to m, and a and c are positive integers and if $b^a \equiv 1 \, mod \, m$ and $b^c \equiv 1 \, mod \, m$ and if $d = g.c.d\,.(a, c)$, prove that $b^d \equiv 1 \, mod \, m$.

8. Show that the order of any $a \in F_q^{\,*}$ divides $q - 1$.

9. Imagine our adversary is using a 2×2 enciphering matrix with a 29 – letter alphabet where A – Z have the numerical equivalents , blank = 26, ? = 27, ! = 28. Also a digraph DP and LW corresponds to the plaintext digraphs AR and LA respectively. Form a matrix from AR and LA and decipher the message “ GFPYJP X?UYXSTLADPLW ”.

10. Using frequency analysis , decipher the message “FQOCUDEM” and U in the cipher text is the encryption of E.

11. Show that a Carmichael number must be the product of at least three distinct primes.

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

SECTION – C

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

13. (a) Divide $(\text{HAPPY})_{26}$ by $(\text{SAD})_{26}$.
    (b) Find an upper bound for the number of bit operations required to compute $n!$.
    (c) Prove that the Euclidean algorithm always gives the greatest common divisor in a finite number of steps . Also verify Time (finding g.c.d.(a,b)) = O ($\log^3$ (a)).

(4+6+10)

14. (a) State and prove Chinese remainder theorem and hence show that the Euler phi function is multiplicative.
    (b) State and prove Fermat's Little theorem. (14+6)

15. (a) Show that every finite field has a generator. If g is a generator of $F_q^{\,*}$, then g^j is also a generator if and only if g.c.d.$(j, q - 1) = 1$. In particular prove that there are a total of $\varphi(q-1)$ different generators of $F_q^{\,*}$.
    (b) Prove $(a+b)^p = a^p + b^p$ in any field of characteristic p. (14+6)

16. (a) Solve the following systems of simultaneous congruences.

$$2x + 3y \equiv 1 \, mod \, 26$$
$$7x + 8y \equiv 2 \, mod \, 26$$

    (b) Explain in detail about affine cryptosystem for enciphering and deciphering with suitable examples. (10+10)

17. (a) Discuss (i) Classical Cryptography versus Public key (ii) Authentication in Public key Cryptography.
    (b) Explain how signature can be sent in RSA. (12+8)

⅄⅄⅄⅄⅄⅄⅄⅄⅄⅄