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

SUBJECT CODE : 11MT/PE/NC14

M. Sc. DEGREE EXAMINATION, NOVEMBER 2011
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 160 and 199 in the base 7.
2. If $\gcd(a, m) = 1$, prove that $ax \equiv 1(mod\ m)$ has a solution.
3. Prove that Legendre symbol $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
4. Find the inverse of $\begin{pmatrix} 1 & 4 \\ 5 & 7 \end{pmatrix}$ mod 9.
5. What is a trap-door function?

SECTION – B

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

6. Estimate the time required to convert a k-bit integer n to its representation to the base b.
7. If $gcd(a, m) = 1$, prove that $a^{\varphi(m)} \equiv 1(mod\ m)$.
8. Factor $3^{12} - 1 = 531440$.
9. If $\alpha \in F_q$, prove that conjugates of $\propto$ over F_p are the elements $\sigma^j(\alpha) = \alpha^{p^j}$.
10. Prove that $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1\ if\ p \equiv \pm 1(mod\ 8) \\ -1\ if\ p \equiv \pm 3(mod\ 8) \end{cases}$
11. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(Z/NZ)$, and set $D = (ad - bc)$. Prove that the following are equivalent.
    (a) $gcd(D, N) = 1$
    (b) A has an inverse matrix
    (c) A gives a $1 - to - 1$ correspondence of $(Z/NZ)^2$ with itself.
    (d) If x and y are not both 0 in (Z/NZ), then $A\begin{pmatrix} x \\ y \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$.
12. Describe a Public Key Cryptosystem. What are its advantages over Classical Cryptosystems?

SECTION – C

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

13. a) Describe the Euclidean algorithm . If $a > b$, prove that Time (finding $gcd(a, b)$ by the Euclidean Algorithm) = $0(log^3 a)$.
    b) Find *g.c.d.* $(x^4 - 4x^3 + 6x^2 - 4x + 1, x^3 - x^2 + x - 1$. Also find polynomials $u(x)$ and $v(x)$ such that $gcd = u(x)f(x) + v(x)g(x)$. (12+8)

14. a) Stare and prove the Chinese Remainder theorem. Deduce that the Euler Phi function is multiplicative.
    b) Compute $2^{10,00,000}\ mod\ 77$. (12+8)

15. a) Prove that every finite field has a generator. If g is a generator of ${F_q}^*$, prove that g^j is also a generator iff $gcd(j, q - 1) = 1$. Prove that there are $\varphi(q - 1)$ different generators of ${F_q}^*$.
    b) Determine whether 7411 is a residue module the prime 9283. (12+8)

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, blank = 26. You have found that the most frequently occurring ciphertext digraphs are "PK" and "RZ". You guess that they correspond to the most frequently occurring plaintext digraphs in the 27-letter alphabet, namely, "E" (E followed by blank" and "S" (S followed by blank). find the deciphering matrix, and read the message.

17. a) Describe the RSA Cryptosystem with an example.
    b) Explain how signature is sent in RSA. (12+8)