STELLA MARIS COLLEGE (AUTONOMOUS) CHENNAI 600 086
(For candidates admitted during the academic year 2004 – 05 & thereafter)

SUBJECT CODE : MT/PE/NC34

M. Sc. DEGREE EXAMINATION, NOVEMBER 2007
BRANCH I - MATHEMATICS
THIRD SEMESTER

COURSE	**:**	**ELECTIVES**
PAPER	**:**	**NUMBER THEORY AND CRYPTOGRAPHY**
TIME	**:**	**3 HOURS** **MAX. MARKS : 100**

SECTION – A **(5 X 8 = 40)**

ANSWER ANY FIVE QUESTIONS

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

2. a) Show that if p is prime and a is any integer not divisible by p and if $n \equiv m \bmod (p-1)$, then $a^n \equiv a^m (\bmod\ p)$.
   b) Find the last base 7 digit in $2^{1000000}$.

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

4. Show that if 'f' is prime, then the number of monic irreducible polynomial of degree f over F_p is $\dfrac{p^f - p}{f}$.

5. Solve the system of simultaneous congruences
$$2x + 3y \equiv 1 \bmod 26$$
$$7x + 8y \equiv 2 \bmod 26$$

6. You intercept the message '!IWGVIEX!ZRADRYD', which was sent using a linear enciphering transformation of digraph vectors in a 29 letter alphabet, in which A – Z have numerical equivalents 0 – 25, blank = 26, ? = 27, ! = 28. You know that last five letters of plain text are the sender's signature 'MARIA'. Find the deciphering matrix and read the message.

7. Explain briefly the method of sending a signature in RSA.

SECTION – B **(3 X 20 = 60)**

ANSWER ANY THREE QUESTIONS

8. a) Show that the time estimate to find the g.c.d (a,b) by Euclidean algorithm o($\log^3$a).
   b) Show that the highest power of a prime p which exactly divides n! is equal to $\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\ldots+\left[\frac{n}{p^{k-1}}\right]$ where $\left[\frac{n}{p^k}\right]=0$.

(12+8)

9. a) State and prove Chinese Remainder theorem.
   b) If g.c.d $(a,m)=1$, then show that $a^{\phi(m)} \equiv 1(\bmod m)$. (10+10)

10. a) State and prove the quadratic reciprocity law for the Jacobi Symbol.
    b) Show that, if α is any element of F_q, then the conjugates of α over F_p (the elements of F_q which satisfy the same monic irreducible polynomial with co-efficients in F_p) are the elements $\sigma^j(\alpha)=\alpha^{p^j}$. (10+10)

11. In order to increase the difficulty of breaking your cryptosystem you decide to encipher a digraph-vector in the 26-letter alphabet by first applying the matrix $\begin{pmatrix} 3 & 11 \\ 4 & 15 \end{pmatrix}$, working modulo 26, and then applying the matrix $\begin{pmatrix} 10 & 15 \\ 5 & 9 \end{pmatrix}$, working modulo 29. thus, your plain text are 26 – letter alphabet, your cipher texts will be in the 29-leeter alphabet, A – Z$\rightarrow$ 0 – 25, blank = 26, ? = 27, ! = 28.
    a) Encipher the message 'SEND'.
    b) Describe how to decipher a cipher text by applying 2 matrices in succession and decipher 'ZMOY'. (HINT:- C = A_2A_1P)

(20)

12. a) Describe the Diffie – Hellman Key exchange system with an example.
    b) Describe the El-Gamal cryptesystem.

(12+8)

⅄⅄⅄⅄⅄⅄⅄⅄⅄⅄⅄