STELLA MARIS COLLEGE (AUTONOMOUS) CHENNAI 600 086
(For candidates admitted from the academic year 2009-10 & thereafter)

SUBJECT CODE: MT/PE/NC23

M. Sc. DEGREE EXAMINATION, APRIL 2011
BRANCH I – MATHEMATICS
SECOND SEMESTER

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

SECTION – A

ANSWER ANY FIVE QUESTIONS: **(5 X 8 = 40)**

1. Write $e = 2.7182818$.
   a) in binary, 8 places to the right of the point
   b) to the base 26, 3 places beyond the point (4+4)

2. a) State and prove Fermat's Little Theorem.
   b) Find the last base-7 digit in $2^{10,00,000}$. (5+3)

3. Let F_q be a finite field with $q = p^f$ elements. Let σ be a map that sends every element to its p^{th} power. (ie) $\sigma(a) = a^p$. Prove that σ is an automorphism of the field F_q. Also prove that the elements of F_q which are kept fixed by σ are the elements of F_p. Prove that σ^f is the identity map.

4. (a) For any two positive odd integers m and n, prove that Jacobi symbol
   $$\left(\frac{m}{n}\right) = (-1)^{\frac{(m-1)(n-1)}{4}} \left(\frac{n}{m}\right)$$
   (b) Find Jacobi symbol $\left(\frac{637}{99}\right)$ (5+3)

5. Solve the following system of congruences:
   $17x + 11y \equiv 7 \ (mod\ 29)$
   $13x + 10y \equiv 8 \ (mod\ 29)$

6. Using frequency analysis, cryptanalyse and decipher the following message, which you know was enciphered using a shift transformation of single-letter plain text message units in the 26-letter alphabet:
   PXPXKXENVDRMHXLVTIX

7. Describe the RSA cryptosystem.

..2

SECTION – B

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

8. a) Describe the Euclidean algorithm. Prove that it gives the greatest common divisor in a finite number of steps and also find the time estimate.
   b) Prove that the highest power of a prime p which exactly divides $n!$ is $\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots$ (12+8)

9. a) State and prove the Chinese Remainder theorem.
   b) Find the smallest positive integer which leaves a remainder of 1 when divided by 11, a remainder of 2 which divided by 12, and a remainder of 3 when divided by 13. (10+10)

10. a) State and prove the existence and uniqueness of finite fields with prime power number of elements.
    b) Prove that $\left(\frac{2}{p}\right) = (-1)^{\frac{(p^2-1)}{8}} = \begin{cases} 1 \; of \; p \equiv \pm 1 \; (mod \; 8) \\ -1 \; of \; p \equiv \pm 3 \; (mod \; 8) \end{cases}$ (10+10)

11. You intercept the message, "!WGVIEX!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 the last five letters of plaintext are the senders signature "MARIA".
    a) Find the deciphering matrix and read the message.
    b) Find the enciphering matrix and impersonating Maria's friend Jo, send the following reply in code:
    "DAMN FOG! JO".

12. a) Describe any two classical cryptosystems with examples.
    b) What is a public-key cryptosystem?
    Explain how authentication is done in public-key cryptosystem. (10+10)

****