STELLA MARIS COLLEGE (AUTONOMOUS) CHENNAI 600 086
(For candidates admitted during the academic year 2008–09)

SUBJECT CODE : MT/PE/NC34

M. Sc. DEGREE EXAMINATION, NOVEMBER 2009
BRANCH I - MATHEMATICS
THIRD SEMESTER

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

SECTION – A **(5 X 8 = 40)**

ANSWER ANY FIVE QUESTIONS

1. a) In the base – 26, with digits A – 2 representing 0 – 25, multiply YES by NO.
   b) Find an upper bound for the number of bit operations required to compute $n!$.

2. Prove that the congruence $ax \equiv 1 (\text{mod } m)$ has a unique solution iff $\gcd(a,m) = 1$.

3. Construct a finite field with nine elements.

4. Prove that $\left(\frac{2}{p}\right) = (-1)^{\left(\frac{p^2-1}{8}\right)} = \begin{cases} 1 & if \quad p \equiv \pm 1 \text{ mod } 8 \\ -1 & if \quad p \equiv \pm 3 \text{ mod } 8 \end{cases}$

5. Working in the 26 letter alphabet, use the matrix $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$ to encipher the plain text "NOANSWER" .

6. What are the disadvantages of classical cryptosystems and how are they overcome in public key cryptosystem.

7. Discuss the El-Gamal cryptosystem.

SECTION – B **(3 X 20 = 60)**

ANSWER ANY THREE QUESTIONS

8. a) Describe the Euclidean algorithm to find $\gcd(a,b)$ where $a > b$. Also prove that Time (finding $\gcd(a,b)$ by the Euclidean Algorithm) = $0(\log^3 a)$.
   b) Find $216^{-1} \text{ mod } (562)$.

(14+6)

9. a) State and prove Generalized Fermat's theorem.
   b) Prove that the subfields of $F_p{}^f$ are the $F_p{}^d$ for d dividing f. Also prove that if an element of $F_p{}^f$ is adjoined to F_p, one obtains one of these fields.

..2

(10+10)

10. a) State and prove the Law of Quadratic Reciprocity.

b) Evaluate the Jacobi Symbol $\left(\frac{99}{637}\right)$.

(14+6)

11. You intercept the ciphertext message "PWULPZTQAWHF" which was encrypted using an affine map or digraphs in the 26-letter alphabet, where the sender used the usual alphabets A-Z with numerical equivalents 0-25 respectively. An analysis of the ciphertext revealed that the most frequently occurring ciphertext digraphs were "IX" and "TQ" respectively. These correspond to the common digraphs in the English language "TH" and "HE" in that order. Find the deciphering key and read the message.

12. a) Explain how authentication is done in public key cryptosystem.

b) Describe the ESA cryptosystem. Illustrate with an example.

(6+14)

▲▲▲▲▲▲▲▲▲▲▲▲