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

SUBJECT CODE : 15MT/PE/NC14

M. Sc. DEGREE EXAMINATION, NOVEMBER 2018
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. Convert 10^6 to the base 26.
2. Find $\varphi(105)$.
3. If p is prime, when do you say that the field F has characteristic p?
4. Find the inverse of the matrix $\begin{pmatrix} 15 & 17 \\ 4 & 9 \end{pmatrix} mod 26$.
5. Show that 561 is a Carmichael number.

SECTION – B

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

6. (i) Multiply $(212)_3$ by $(122)_3$ (ii) Divide $(40122)_7$ by $(126)_7$.
7. Find *d* = g.c.d.(1547, 560) also express *d* as a linear combination of 1547 and 560.
8. State and prove Wilson's theorem.
9. If F_q is a field of $q = p^f$ elements, then prove that every element satisfies the equation $X^q - X = 0$ and F_q is precisely the set of roots of that equation. Also prove that for every prime power $= p^f$, the splitting field over F_q of the polynomial $X^q - X$ is a field of q elements.
10. Prove that $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} mod p$.
11. You intercept the Crypto text "OFJDFOHFXOL" which was enciphered using an affine transformation of single-letter plaintext units in the 27 letter alphabet (with blank = 26). You know that the first word is "I" ("I" followed by blank). Find the original plaintext.
12. Let n be an odd composite integer. If n is divisible by a perfect square > 1, then prove that n is not a Carmichael number.

SECTION – C

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

13. (a) Find an upper bound for the number of bit operations required to compute $n!$.
    (b) Show that the power of a prime p which exactly divides n! is equal to $\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots \left[\frac{n}{p^k}\right]$, where $p^k \leq n \leq p^{k+1}$.
    (c) Show that the Euclidean algorithm always gives the greatest common divisor in a finite number of steps. Also Show that if $a > b$, Time (finding g.c.d.(a, b) by Euclidean algorithm) $= O(log^3(a))$. (5+5+10)

14. (a) State and prove Chinese remainder theorem.
    (b) Prove that for any integer b and any positive integer n, $b^n - 1$ is divisible by $b - 1$ with quotient $b^{n-1} + b^{n-2} + \cdots + b^2 + b + 1$.
    (c) Compute 2^{100000} mod 77. (10+5+5)

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 if and only if $g.c.d.(j, q - 1) = 1$. Show also that, there are a total of $\varphi(q - 1)$ different generators of F_q^* .
    (b) State and prove the law of Quadratic Reciprocity (10+10)

16. (a) In the 27-letter alphabet (with blank = 26), use the affine enciphering transformation with key a =13, b = 9 to encipher the message ''HELP ME''.
    (b) Suppose we know that our adversary is using an enciphering matrix A in the 26 letter alphabet. We intercept the cipher text "WKNCCHSSJH", and we know that the first word is "GIVE". Find the deciphering matrix A^{-1} and read the message. (6 + 14)

17. (a) If $n \equiv 3 \; mod \; 4$, then prove that n is a strong pseudoprime to the base b if and only if it is an Euler pseudoprime to the base b.
    (b) Prove that a carmichael number must be the product of at least three distinct primes.
    (c) Explain the following terms:
    Authentication, Hash function, Key Exchange, Probabilistic Encryption. (5+5+10)