LOYOLA COLLEGE (AUTONOMOUS), CHENNAI – 600 034

M.Sc. DEGREE EXAMINATION – **MATHEMATICS**

SECOND SEMESTER – APRIL 2017

16PMT2ES02- NUMBER THEORY AND CRYPTOGRAPHY

Date: 28-04-2017 Dept. No. Max. : 100 Marks
01:00-04:00

Answer ALL the questions:

1. (a) Find the base -2 representation of the decimal numbers -17 and 61. (5)

(OR)

(b) Express the g.c.d of 666, 1414 as a linear combination of these integers. (5)

(c) (i) State and prove Lame's theorem.
(ii) Find the value of the Euler phi-function of the integers 720, 1001 and 20!. (9+6)

(OR)

(d) Find all the solutions to the system of linear congruences $x \equiv 1(mod\,2)$, $x \equiv 2(mod\,3)$, $x \equiv 3(mod\,5)$, $x \equiv 4(mod\,7)$ and $x \equiv 5(mod\,11)$. (15)

2. (a) Let $f(X) = X^4 + X^3 + X^2 + 1$, $g(X) = X^3 + 1$ in $F_2[X]$. Find g.c.d. $(f.g)$ using the Euclidean algorithm for polynomials and express the g.c.d. in the form $u(X)f(X) + v(X)g(X)$. (5)

(OR)

(b) Define Legendre symbol and prove that $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2}(mod\,p)$. (5)

(c) (i) If g is a generator of F_q^* then prove that g^j is also a generator if and only if g.c.d. $(j, q-1) = 1$. In particular, prove that there are a total of $\varphi(q-1)$ different generators of F_q^*.
(ii) Prove that for any $q = p^f$ the polynomial $X^q - X$ factors in $F_p[X]$ into the product of all monic irreducible polynomials of degree d dividing f. (8+7)

(OR)

(d) (i) For any two positive odd integers m and n, prove that $\left(\frac{m}{n}\right) = (-1)^{(m-1)(n-1)/4}\left(\frac{n}{m}\right)$.
(ii) Using the algorithm find the square root of $a = 186$ modulo $p = 401$. (8+7)

3. (a) Using the Ceasar cipher, encipher the message ATTACK AT DAWN. (5)

(OR)

(b) Encipher the message PAYMENOW using the affine transformation $C \equiv 7P + 12(mod\,26)$. (5)

(c) A person is using 2x2 enciphering matrix with a 26 letter alphabet. He receives the message "WKNCCHSSJH" and he knows that the first word is "GIVE". Find the Deciphering matrix A^{-1} and read the message. (15)

(OR)

(d) Suppose Bob wants to send an enciphered message to Alice by means of the RSA cipher system. Let the message be "YES". Let Alice's public key be $(e_A, n_A) = (39423, 46927)$.
(i) Encipher the message that is to be sent from Bob to Alice.
(ii) Let Alice's prime number be $p = 167$ and $q = 281$. Determine Alice's secret key d_A and decipher the ciphertext obtained from Bob. (15)

4. (a) Find all the bases for which 15 is a pseudoprime. (5)

(OR)

(b) Write a short note on Hash functions. (5)

(c) Discuss about any two primality tests. (15)

(OR)

(d) Let n be a composite integer.
(i) If n is divisible by a prefect square > 1, then prove that n is not a Carmicheal number.
(ii) If n is square free, then n is a Carmicheal number if and only if $p-1|n-1$ for every prime p dividing n. (15)

5. (a) Find $2^{1234} mod\ 789$. (5)

(OR)

(b) Write a note on Fermat factorization method. (5)

(c) Let E be the elliptic curvey$^2 = x^3 - 36x$ defined over Z_5. Then
(i) List the points on E.
(ii) Compute $P+Q$ if $P=(-3, 9)$ and $Q=(-2, 8)$.
(iii) Compute $2P$ if $P=(-2, 8)$ (15)

(OR)

(d) Write about elliptic curve discrete log problem. (15)

$$$$$$$$