# LOYOLA COLLEGE (AUTONOMOUS), CHENNAI – 600 034

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

SECONDSEMESTER – APRIL 2018

**17/16PMT2ES02- NUMBER THEORY AND CRYPTOGRAPHY**

Date: 25-04-2018 Dept. No. Max. : 100 Marks
Time: 01:00-04:00

**Answer all questions:**

1. a) Express as a linear combination for the numbers 841 and 160.

OR

b) Explain the Euclidean algorithm with an example. (5)

c) i) Find the upper bound for the number of bit operations required to compute $n!$.
ii) State and prove Chinese reminder theorem. (7+8)

OR

d) i) Find the smallest non negative integer of the congruencies $x \equiv 2 \bmod 3, x \equiv 3 \bmod 5, x \equiv 4 \bmod 11, x \equiv 5 \bmod 16$.
ii) State and prove Fermat's theorem. (9+6)

2. a) Prove that there exists a sequence of primes p such that the probability that a random $g \in F_p^*$ is a generator approaches zero.

OR

b) Prove that $(a+b)^p = a^p + b^p$, in any field of characteristic *p*. (5)

c) i) Prove that if $F_q$, where $q = p^f$ be a finite field and let $F(X)$ be a irreducible polynomial of degree $f$ over $F_p$. Then two elements of $F_q$ can be multiplied or divided in $O(\log^3 q)$ bit operations. If k is a positive integer, then an element of $F_q$ can be raised to the k-th power in $O(\log k \log^3 q)$ bit operations.
ii) Determine whether 7411 is a residue modulo to the prime 9283. (9+6)

OR

d) i) Prove that $G^2 = (-1)^{\frac{(q-1)}{2}} q$.
ii) State and prove the law of quadratic reciprocity. (6+9)

3. a) Define Affine transformation with an example.

OR

b) Find the inverse of $A = \begin{pmatrix} 1 & 6 \\ 5 & 2 \end{pmatrix} \in M_2(Z/26Z)$. (5)

(P.T.O)

c) i) Intercept the message 'FQOCUDEM" assuming that the most frequently occurring letter in the cipher text is the encryption of E and the most frequently occurring character in the cipher text is U.

ii) Working in the 26- letter alphabet and using the matrix $\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$ to encipher the plain text " NOANSWER". (9+6)

OR

d) With the 26 alphabets and blank space as the $27^{th}$ alphabet and with the digraph having numerical equivalence to $27x + y$ and the most frequently occurring digraphs are in order ZA , IA and IW corresponding to the most frequent language " E " ( E and space), "S " ( S and space) and " T( space and T) use affine transformation of modulo 729 , find the deciphering key and read the message "NDXBHO". (15)

4 a) Define Pseudo prime with an example.

OR

b) What is Kanpsack problem? (5)

c) i) Find the factors of 91 for $f(x) = x^2 + 1$ and $x_0 = 1$.

ii) Find the factor for 200819. (9+6)

OR

d) i) Define B number of a factor base and illustrate it for n=4633 to find its factors.

ii) If *n* is a strong pseudo prime to the base *b* then prove that it is an Euler pseudo prime to the base *b*. (9+6)

5. a) Define and discuss the nature of elliptic curve over the field *K*.

OR

b) On the elliptic curve $y^2 = x^3 - 36x$, let $P = (-3,9)$ and $Q = (-2,8)$. Find $P + Q$ and $2P$. (5)

c) Discuss the nature of the elliptic curve over the rationals.

OR

d) i) State and prove Hasse's theorem.

ii) Find the type of $y^2 = x^3 - x$ over $F_{71}$. (6+9)

**********