MANIPAL UNIVERSITY

Reg. No.										

Deemed- to -be -University under Section 3 of the UGC Act, 1956

DEPARTMENT OF SCIENCES, M.Sc (P/C/M/G)
IV SEMESTER END SEMESTER EXAMINATIONS, APRIL 2017

SUBJECT: NUMBER THEORY AND CRYPTOGRAPHY
[710.4]

(REVISED CREDIT SYSTEM)

Time: 3 Hours Date:28/04/2017 MAX. MARKS: 50

Note: (i) Answer any **FIVE FULL** questions. (ii) Each question has 3 sub questions.

1A) Express the prime 12277, which divides $20^6 + 1$, as a sum of two squares.

1B) Factor: $14348906 = 3^{15} - 1$.

1C) Prove that if $g.c.d.(a,\ m) = 1$, then $a^{\varphi(m)} \equiv 1 mod\ m$.

(Marks: 4+3+3)

2A) Prove that there are exactly $\varphi(q-1)$ generators of a finite field F_q.

2B) Define Euler phi-function. If $\varphi(18{,}281) = 18{,}000$ which are the two primes whose product is 18,281.

2C) Define the Jacobi symbol. Determine whether the prime 3083 is a residue modulo the prime 3911. **(Marks: 4+3+3)**

3A) Read the message "OAG?", which was encrypted by a linear enciphering transformation of digraph vectors over 29 letter alphabets with numerical equivalents of A-Z being 0-25, blank=26, ?=27 and !=28. The same encryption process was used to encipher the message "SHOT" as the ciphertext "HANG".

3B) Police could identify the name of a criminal as "RAVI", which was encrypted as "V&LN" using an affine mapping of digraphs $31x + y$ over 31 letter alphabets with 26=&, 27=blank, 28=?, 29=! and 30=@.

Who was the killer from the same group of criminals with encrypted name "NLQJ" escaped last week ?

3C) Define an Euler pseudoprime. Prove that a Carmichael number must be the product of at least three primes. **(Marks: 4+3+3)**

4A) State and prove the law of Quadratic Reciprocity.

4B) Use the continued fraction algorithm to factor 13561.

4C) Use the Rho method with $f(x) = x^2 - 1,\ \ x_0 = 5$ to factor 7031.

(Marks: 4+3+3)

5A) Using Silver-Pohlig-Hellman algorithm, find the discrete log of 37 to the base 2 in F_{73}^*.

5B) Use generalized Fermat factorization to factor 29895581.

5C) You received a trigraph message "AIR", which was an encryption of a digraph plaintext in 26 letter alphabet using RSA cryptosystem. Suppose your public key is $K_E = (n, e) = (713,\ 283)$. Decode the message and read it. **(Marks: 4+3+3)**

6A) Find a square root of 32 modulo 97.

6B) A message is encrypted as a pair (12, "VX") using the ElGamal cryptosystem over single letter message units and sent to an user who selected a secret integer $a = 15$ and the generator g = 2 of the finite field F_{29}. How can the user read the actual message?

6C) Explain how a set of partners exchange the keys for their secured communication using Diffie-Hellman key exchange protocol. Establish this by an example of exchanging secret keys which are elements of the finite field with 11 elements, by three individuals, taking 2 as a generator. **(Marks: 4+3+3)**

****