QPC: RM19MSC141 AR 19 Reg. No.

GIET UNIVERSITY, GUNUPUR – 765022

M. Sc (Fourth Semester) Examinations, May – 2020

MTPC 403 – NUMBER THEORETIC CRYPTOGRAPHY – II (MATHEMATICS)

Time: 2 hrs Maximum: 50 Marks

The figures in the right hand margin indicate marks.)

PART – A **(2 x 10 = 20 Marks)**

Q.1. Answer all the questions

a. Define the discrete logarithm.
b. Define super increasing knapsack problem.
c. When do you say that a graph is colourable?
d. Write a short note on primality test.
e. Define a strong pseudoprime.
f. Define a factor base and give an example.
g. Find the continued fraction representation of $\sqrt{3}$.
h. Give the running time of the quadrative sieve factoring method.
i. Factor 200819.
j. Write a short note on quadratic sieve method.

PART – B **(6 x 5 = 30 Marks)**

Answer ***ANY FIVE*** questions Marks

2. Find the discrete log of 28 to the base 2 in $\mathbb{F}_{37}^*$ using the Silver-Pohlig-Hellman algorithm. (Given that 2 is a generator of $\mathbb{F}_{37}^*$) (6)

3. Explain the construction of Merkle-Hellman knapsack cryptosystem with an example. (6)

4. Explain the zero knowledge proof for "having found a discrete logarithm". (6)

5. Let *n* be an odd composite number. Prove that (6)

   (i) If *n* is divisible by a perfect square > 1, then n is not a Carmichael number.

   (ii) If n is square free, prove that n is a Carmichael number if and only if $(p-1)|(n-1)$ for every prime dividing n.

6. Explain Pollard's rho method and hence factorize 91 by choosing $f(x) = x^2 + 1$ and $x_0 = 1$. (6)

7. Let S be a set of r elements. Given a map f from S to S and an element $x_0 \in S$, let $x_{j+1} = f(x_j)$ for $j = 0, 1, 2, \ldots$. Let λ be a positive real number and let $l = 1 + \lfloor\sqrt{2\lambda r}\rfloor$. Show that the proportion of pairs (f, x_0) for which $x_0, x_1, \ldots, x_l$ are distinct, where f runs over all maps from S to S and x_0 runs over all elements of S, is less than $e^{-\lambda}$. (6)

8. Factor 1042387 by using the quadratic sieve method. (6)

9. Explain the continued fraction factoring algorithm and use it to factor 17873. (6)

--- End of Paper ---