Reg. No................................ Name.................................... P3643

M.SC DEGREE END SEMESTER EXAMINATION OCTOBER 2016

SEMESTER – 3: MATHEMATICS

COURSE: P3MATT14– NUMBER THEORY AND CRYPTOGRAPHY

Common for Regular (2015 Admission) & Supplementary / Improvement (2014 Admission)

Time: Three Hours Max. Marks: 75

Part A

Answer **any Five.** Each question carries 2 marks.

1. Divide $(11001001)_2$ by $(100111)_2$

2. Define time estimate.

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

4. Define the Legendre Symbol.

5. Define a hash function.

6. Define Discrete logarithm.

7. Show that 561 is a Carmichael number.

8. What is a factor base B? What is a B-number?

(2 x 5 = 10)

Part B

Answer **any Five**. Each question carries 5 marks.

9. Find an upper bound for the number of bit operations it takes to compute the binomial coefficient $\binom{n}{m}$.

10. How can you find all divisors of a natural number n?

11. Prove that the order of any $a \in F_q^*$ divides q-1.

12. Let $f(x)=x^4+x^3+x^2+1$ and $g(x)=x^3+1$ be polynomials 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)

13. What is a one-way function? What is G.Purdy's one-way function?

14. Explain ElGamal cryptosystem.

15. What do you mean by primality test? What is the simplest primality test?

16. Let d=gcd(k,m).Then prove that there are exactly d elements in the group $\{g,g^2,\ldots g^m=1\}$ which satisfy $x^k=1$

(5 x 5 = 25)

Part C

Answer **(a) or (b)** from each question. Each question carries 10 marks

17. (a) State and prove the Chinese Remainder Theorem.

(b) Show that the Euclidean algorithm always gives the greatest common divisor in a finite number of steps. Further estimate the time required to find gcd (a, b) for a>b by the Euclidean algorithm.

18. (a) Prove that if F_q is a finite field of $q=p^f$ elements, then every element satisfies the equation $x^q-x=0$ and that F_q is precisely the set of roots of that equation. Conversely prove that for every prime power $q=p^f$,the splitting field over F_p of the polynomial x^q-x is a field of q elements.

(b) State and prove the General Law of Quadratic Reciprocity.

19. (a) Explain the RSA cryptosystem.

(b) Explain the Diffie-Hellman key exchange system

20. (a) When do you say that an odd composite number n is an Euler pseudo prime to the base b? a strong pseudo prime to the base b? Suppose that $n\equiv 3 \mod 4$ and then show that n is a strong pseudo prime to the base b if and only if it is an Euler pseudo prime to the base b.

(b) Factorize 4087 by rho method by taking $f(x) = x^2+x+1$ and $x_0=2$.

(10 x 4 = 40)

*****