MCA.D.II/04.13.0169

M.C.A. DEGREE II SEMESTER EXAMINATION APRIL 2013

CAS 2205 NUMBER THEORY AND CRYPTOGRAPHY

(*Supplementary*)

Time : 3 Hours | Maximum Marks : 50

PART A

(Answer *ALL* questions)

(15 x 2 = 30)

I. (a) Find the greatest common divisor of 24871 and 3468.
(b) Prove that these are infinitely many primes in Z.
(c) Show that if P is a prime, then either p/b or p/c.

II. (a) Solve the congruence $5x \equiv 3(\text{mode } 24)$.
(b) Determine the quadratic residues and non residues of prime 17.
(c) Show that the Legendre's symbol (n/p) is a complete multiplicative function of n.

III. (a) Define (i) Cipher (ii) Cryptanalysis
(b) Distinguish between passive and active security threats.
(c) What is steganography?

IV. (a) Write a note on traffic confidentiality.
(b) Give any three applications of public key crypto systems.
(c) Distinguish between a session key and a master key.

V. (a) What are the desirable properties of a hash function?
(b) Define Kerberos.
(c) Write the basic requirements for a digital signature.

PART B

(5 x 4 = 20)

VI. A. State and prove the fundamental theorem of arithmetic.

OR

B. Define Euler function ϕ and if $(a,b)=1$, show that $\phi(a,b)=\phi(a).\phi(b)$.

VII. A. Prove that an integer $P>1$ is prime if and only if $(p-1)!+1 \equiv 0(\text{mod } p)$

OR

B. Find all x which satisfy the system of congruences $x \equiv 1(\text{mod}\,3)$, $x \equiv 2(\text{mod}\,5)$, $x \equiv 3(\text{mod}\,7)$, and $x \equiv 4(\text{mod}\,11)$.

VIII. A. Explain the important ingredients of a symmetric encryption scheme and requirements for secure use of conventional encryption.

OR

B. Describe the DES encryption and decryption.

IX. A. Prove the RSA algorithm.

OR

B. Describe elliptic curve cryptography.

X. A. Explain the requirements for message authentification codes.

OR

B. Write secure hash algorithm.

***