D 40789

Name.....

Reg. No.....

SEVENTH SEMESTER B.TECH. (ENGINEERING) DEGREE EXAMINATION, DECEMBER 2007

CS 2K 703 – NUMBER THEORY AND CRYPTOGRAPHY

Time : Three Hours | Maximum : 100 Marks

Part A

I. (a) Prove that there are infinitely many primes.

(b) The sum of 2 positive integers is 5264 and their l.c.m. is 200340. Determine the two integers.

(c) State and prove Wilson's theorem.

(d) Solve the congruence $25x \equiv 15 \pmod{120}$.

(e) Distinguish between linear and differential cryptanalysis.

(f) What is the difference between diffusion and confusion ?

(g) Write short note on Kerberos.

(h) Define elliptic curve and the zero point of it.

(8 × 5 = 40 marks)

Part B

II. (a) State and prove fundamental theorem of arithmetic.

Or

(b) If a prime p does not divide a then prove that $a^{p-1} \equiv 1 \pmod{p}$.

III. (a) State and prove Chinese Reminder theorem.

Or

(b) Solve the system of congruences :

$x \equiv 1 \pmod{3}$

$x \equiv 2 \pmod{4}$

$x \equiv 3 \pmod{5}$.

IV. (a) Explain the DES design criteria.

Or

(b) Show that in DES the first 24 bits of each subkey come from same subject of 28 bits of initial key and that second 24 bits of each subkey come from a disjoint subset of 28 bits of initial key.

V. (a) Explain the elliptic curve cryptography.

Or

(b) Briefly explain Diffie-Hellman key exchange.

(4 × 15 = 60 marks)