D 51310 (Pages : 2) Name.....

Reg. No.....

SEVENTH SEMESTER B.TECH. (ENGINEERING) DEGREE EXAMINATION DECEMBER 2008

CS 2K 703.—NUMBER THEORY AND CRYPTOGRAPHY

Time : Three Hours Maximum : 100 Marks

Part A

I. (a) Prove that $a \equiv b \bmod n$ implies $b \equiv a \bmod n$.

(b) Determine the gcd (4655, 12075)

(c) Solve: $2x + 6y \equiv 1 (\text{mod } 7)$

$4x + 3y \equiv 2 (\text{mod } 7)$

(d) Prove that the linear conguence $ax \equiv b (\text{mod } m)$ has exactly one solution if $(a,m) = 1$.

(e) Distinguish between linear and differential cryptanalysis.

(f) Write a note on Avalanche effect.

(g) What are the three broad categories of applications of public key cryptosystems ?

(h) What is a message authentication code ?

$(8 \times 5 = 40$ marks)

Part B

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

Or

(b) (i) Prove that if $2^n - 1$ is prime, then n is prime.

(ii) Prove that if a divides b then a divides any multiple of b.

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

Or

(b) Solve : $x \equiv 1 (\text{mod } 3)$

$x \equiv 2 (\text{mod } 4)$

$x \equiv 3 (\text{mod } 5)$

IV. (a) Explain the triple DES encryption in detail.

Or

(b) (i) What is the difference between statistical randomness and unpredictability ?

(ii) What is traffic padding and what is its purpose ?

Turn over

V. (a) What do you mean by message authentication code. Distinguish between a message authentication code and a one-way hash function.

Or

(b) What do you mean by MD 5 what basic arithmetical and logical functions are used in MD 5.

(4 × 15 = 60 marks)