D 26537

Name.....

Reg. No.....

SEVENTH SEMESTER B.TECH. (ENGINEERING) DEGREE EXAMINATION, DECEMBER 2006

CS 2K 703—NUMBER THEORY AND CRYPTOGRAPHY

Time : Three Hours Maximum : 100 Marks

Answer **all** *questions.*

1. (a) What are relatively Prime Numbers ? Give example.
   (b) What is congruence ? Give any *two* properties of congruence.
   (c) Solve $172x + 20y = 1000$.
   (d) What is meant by quadratic residue ?
   (e) Differentiate symmetric and asymmetric algorithms of cryptography.
   (f) What is secure hash algorithm ? Explain.
   (g) Discuss different design goals of firewalls.
   (h) Discuss about digital signature.

(8 × 5 = 40 marks)

2. (a) State and explain the fundamental theorem of arithmetic.

Or

   (b) State and prove Fermat's theorem.

(15 marks)

3. (a) (i) State and explain Chinese Remainder theorem.
   (ii) If a and b are relatively prime and bc is a multiple of a, show that c is a multiple of a.

Or

   (b) (i) State and prove Wilson's theorem. Give example.
   (ii) Prove that 5 is the quadratic residue of 209.

(15 marks)

4. (a) Compare DES and IDEA.

Or

   (b) Write notes on blowfish.

(15 marks)

5. (a) Explain merits and features of MO5 algorithm with example.

Or

   (b) Briefly explain RSA algorithm.

   In a public key system using RSA the cipher text C = 10 sent to a user whose public key is $e = 5$, $n = 35$. What is the plain text M ?

(15 marks)

[4 × 15 = 60 marks]