D 11248

Name.....

Reg. No.....

SEVENTH SEMESTER B.TECH. (ENGINEERING) DEGREE EXAMINATION, DECEMBER 2005

CS 2K 703. NUMBER THEORY AND CRYPTOGRAPHY

Time : Three Hours Maximum : 100 Marks

Answer **all** *questions.*

Part A

1. Define Euler's function. If $n = ab$, where $(a, b) = 1$, prove that $\phi(n) = \phi(a) \cdot \phi(b)$.
2. Find the gcd of 595 and 252 and express it as a linear combination of two integers.
3. Solve $9x \equiv 6 \pmod{24}$.
4. Solve by Chinese Remainder Theorem $4x \equiv 6 \pmod{10}$ and $9x \equiv 15 \pmod{21}$.
5. Write a note on DES.
6. What do you mean by Pseudorandom Number generation ?
7. Explain the digital signature algorithm.
8. What are the conditions to be fulfilled by public-key cryptography ?

(8 × 5 = 40 marks)

Part B

9. State and prove Fundamental Theorem of arithmetic. (15 marks)
10. (a) State and prove Wilson's Theorem. (7 marks)

    (b) If $f(x) = x^2 + x + 7$, show that :

    (i) solutions of $f(x) \equiv 0 \pmod{7}$ is $x \equiv 0, 6 \pmod{7}$.

    (ii) solutions of $f(x) \equiv 0 \pmod{7^2}$ is $x \equiv -7, 6 \pmod{7^2}$.

    (8 marks)

11. (a) What do you mean by IDEA ? Describe in detail the IDEA Encryption Scheme only. (10 marks)

    (b) Explain the avalanche effect in DES. (5 marks)

12. (a) Write an essay on Kerberos. (7 marks)

    (b) Perform encryption and decryption using RSA algorithm given the following :—

    $p = 3, q = 11, d = 7$ message M = 5 (plain text).

    (8 marks)

[4 × 15 = 60 marks]