D 1682 (Pages : 2)

Name.....

Reg. No.....

SEVENTH SEMESTER B.TECH. (ENGINEERING) DEGREE EXAMINATION, NOVEMBER 2004

CS 2K 703. NUMBER THEORY AND CRYPTOGRAPHY

(New Scheme)

Time : Three Hours Maximum : 100 Marks

Part A

Answer **all** *questions.*

1. Define perfect number and show that any even perfect number n ends in the digit 6 or 8 that is $n \equiv 6 \pmod{10}$ or $n \equiv 8 \pmod{10}$.
2. Show that if $K > 0$, then gcd $(Ka, Kb) = K\,gcd\,(a, b)$.
3. Solve $17x \equiv 9 \pmod{276}$.
4. Use Chinese Remainder theorem solve $x \equiv 2 \pmod 3$; $x \equiv 3 \pmod 5$ and $x \equiv 2 \pmod 7$.
5. What are the characteristics of IDEA related to its cryptographic strength ?
6. What are the uses of random numbers and the criteria used to validate random numbers ?
7. What are the conditions to be fulfilled by public-key cryptography ?
8. List the major design goals of MD5.

(8 × 5 = 40 marks)

Part B

9. (a) State and prove Fundamental theorem of arithmetic. (15 marks)

Or

(b) (i) State and prove Fermat's Little theorem and hence show that $a^{21} = a \pmod{15}$ for all a. Also show that $a^p \equiv a \pmod p$, when p is prime for any integer a.

(8 + 2 + 2 = 12 marks)

(ii) If p and q are distinct primes such that $a^p \equiv a \pmod q$ and $a^q \equiv a \pmod p$, then show that $a^{pq} \equiv a \pmod{pq}$.

(3 marks)

10. (a) Let p be an odd prime and $gcd\,(a, p) = 1$. Then a is a quadratic residue of p if and only if $a^{(p-1)/2} \equiv 1 \pmod p$. Also deduce that a is a quadratic residue or nonresidue of p according as $a^{(p-1)/2} \equiv 1 \pmod p$ or $a^{(p-1)/2} \equiv -1 \pmod p$.

(13 + 2 = 15 marks)

Or

(b) Let a be an odd integer. Then show that

(i) $x^2 \equiv a \pmod 2$ always has a solution. (1 mark)

(ii) $x^2 \equiv a \pmod 4$ has a solution if and if only $a \equiv 1 \pmod 4$. (2 marks)

(iii) $x^2 \equiv a \pmod{2^n}$, for $n \geq 3$, has a solution if and only if $a \equiv 1 \pmod 8$. (12 marks)

Turn over

11. (a) Discuss in detail the simplified DES scheme illustratives the key generation and Encryption schemes.

Or

(b) Discuss in detail the working of DES decryption algorithm and explain the avalanche effect in DES.

(15 marks)

12. (a) List and explain any *two* types of functions that may be used to produce an authenticator.

Or

(b) Write the Secure Hash Algorithm explaining its working.

(15 marks)

[4 × 15 = 60 marks]