JYOTHI ENGG COLLEGE LIBRARY
THRISSUR EDUCATIONAL TRUST
CHERUTHURUTHY

D 30939 (Pages : 2) Name.....

Reg. No.....

SEVENTH SEMESTER B.TECH. (ENGINEERING) DEGREE EXAMINATION, DECEMBER 2003

CS2K. 703. NUMBER THEORY AND CRYPTOGRAPHY

Time : Three Hours Maximum : 100 Mar

Part A

Answer **all** *questions.*

1. Let a and b be integers, not both zero. Then show that a and b are relatively prime if and or if there exist integers x and y such that $ax + by = 1$.
2. If p is prime and p divides $a_1, a_2, a_3, \ldots a_n$, then show that p divides a_k for some where $1 \leq k < n$.
3. Show that for $ax + by = c$, if x_0, y_0 is a particular solution then all solutions are of the fo $x = x_0 + (b/d)\,t$ and $y = y_0 - (a/d)\,t$ for varying integer t and $d = gcd\,(a, b)$.
4. Show that Wilson's theorem is true for $p = 13$.
5. Classify the security services and explain them briefly.
6. Tabulate the different types of attacks on encrypteal messages.
7. Summarise the important aspects of conventional and public-key encryption.
8. What is kerberos ? What are the requirements for kerberos ?

(8 × 5 = 40 ma

Part B

9. (a) (i) Show that if n is positive integer and $gcd\,(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$ and h deduce Fermat's theorem $a^{p-1} \equiv 1 \pmod{p}$ for a prime p and p does not divide

(10 m

(ii) Show that for any positive integer $n \geq 1$, $n = \sum_{d/n} \phi(d)$, the sum being extended all positive divisors of n.

(5 m

Or

(b) (i) Show that $gcd\,(a, b)$. $lcm\,(a, b) = ab$ and hence show that $lcm\,(a, b) = ab$ if anc if $gcd\,(a, b) = 1$.

(6 + 1 = 7 m

(ii) Show that if $2^k - 1$ is prime ($k > 1$) then $n = 2^{k-1}(2^k - 1)$ is perfect and every perfect number is of this form.

(8 m

10. (a) (i) Solve $172x + 20y = 1000$.

(8 m

(ii) State and prove Wilson's theorem.

(7 m

Or

Tur

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]