MCA DEGREE II SEMESTER EXAMINATION, APRIL 2008

CAS 2202 NUMBER THEORY AND CRYPTOGRAPHY

Time: 3 Hours Maximum marks : 50

PART A

(Answer ***ALL*** questions)

(All questions carry ***EQUAL*** marks)

(15 x 2 = 30)

I. a. State the Euclidean algorithm and its extension.
b. Show that the number of primes is infinite.
c. Find the number of divisors of 9504.

II. a. Find the least positive incongruent solutions of $36x \equiv 27(\text{mod}\,45)$.
b. If p is prime, then show that $2(p-3)!+1$ is a multiple of p.
c. Evaluate the Legendre symbol (221/399).

III. a. What do you mean by cryptanalysis? Why is cryptanalysis important?
b. Differentiate between confusion and diffusion as applied to cryptosystems.
c. Discuss the 4 important aspects of information security.

IV. a. Compare the security aspects of RSA and ECC cryptosystems.
b. Write the Diffie-Hellman protocol for key exchange.
c. What are the schemes for commercial key distribution in symmetric and public key cryptography?

V. a. Write the desirable properties of hash functions.
b. Compare the features of MD5 and SHA-1.
c. What are the features of Kerberos?

PART B

(All questions carry ***EQUAL*** marks)

(5 x 4 = 20)

VI. A. Using the fundamental principles, show that if $a \equiv b(\text{mod}\,m)$ and $c \equiv d(\text{mod}\,n)$, then (i) $ax + cy \equiv bx + dy(\text{mod}\,m)$ (ii) $ac \equiv bd(\text{mod}\,m)$ and (iii) $a^n \equiv b^n(\text{mod}\,m)$, where $a, b, c, d, m, n \in Z^+$.

OR

B. State and prove the Euler's theorem. Deduce the Fermat's little theorem from Euler's theorem.

VII. A. Solve $x \equiv 1(\text{mod}\,3)$, $x \equiv 2(\text{mod}\,4)$, $x \equiv 3(\text{mod}\,7)$ and $x \equiv 4(\text{mod}\,11)$.

OR

B. Show that if $\gcd(a, m) = g$ and g / b, then the congruence $ax \equiv b(\text{mod}\,m)$ has exactly g incongruent solutions, where $a, b, g, m \in Z^+$.

(Turn over)

VIII. A. Discuss the different modes of block cipher operation. Which mode is the best? Justify your answer.

OR

B. Analyse the strength of DES using parameters such as SAC, BIC, confusion, diffusion, etc. Discuss the after effects of DES challenges.

IX. A. Prove the RSA algorithm.

OR

B. How are key exchange and encryption/decryption done in elliptic curve cryptography?

X. A. Write the digital signature algorithm describing the key generation, signature generation and verification.

OR

B. Write the SHA-1 algorithm.

***