Indian Institute of Technology, Kharagpur

Date..... FN/AN Time: 3 Hrs Full Marks: 50 No. of Students: 50
END (Autumn) Semester 2010-11, Deptt: MA/SI Sub. No. MA 60031/MA 51115
Subject Name: Cryptography and security issues/Cryptography and network security

Instruction: Answer **all** questions.

Question 1 [2 × 10 marks]

What is the difference between

a) Shift cipher and substitution cipher;

b) Symmetric key encryption and public key encryption;

c) Pseudorandom number generator and stream cipher;

d) Message authentication code and hash function;

e) SHA-1 and MD5;

f) Birthday attack and Boomerang attack;

g) CBC mode of operation and hash function;

h) Side channel attack and slide attack;

i) Exhaustive search and Time Memory-Trade-Off attack;

j) Linear cryptanalysis and Impossible cryptanalysis.

Question 2 [3+3 marks]

a) Briefly outline the **triple DES** scheme and give two reasons as to why it was not chosen as the next cryptographic standard.

b) Describe a general stream cipher system.

Question 3 [4+2+6 marks]

a) When is a hash function said to be (*i*) weakly collision-free, (*ii*) strongly collision-free, and (*iii*) one-way?

b) Suppose $h : X \to Y$ is a hash function and let $h^{-1}(y) = \{x : h(x) = y\}$ for any $y \in Y$. Let ϵ denote the probability that $h(x_1) = h(x_2)$, where x_1, x_2 are random (not necessarily distinct) elements of X. Prove that $\epsilon = \frac{1}{|Y|}$ iff $|h^{-1}(y)| = \frac{|X|}{|Y|}$ for every $y \in Y$.

——P.T.O——

c) Describe the main elements of the **SHA-1** secure hash algorithm. Include all relevant block diagrams.

Question 4 [2+2+2 marks]

a) Describe the main ingredients of the Knapsack scheme developed by Markle mentioning whether each value is private, public, chosen or calculated.

b) Define Digital Signature.

c) Describe ElGamal Signature Scheme.

Question 5 [2+2+2 marks]

a) Find the quadratic residues and quadratic non-residues modulo 13.

b) Use the **Extended Euclidean Algorithm** to compute 17^{-1} mod 101.

c) Apply the **Chinese Remainder Theorem** to solve the following system of congruences:

$$x \equiv 12 \pmod{25}$$
$$x \equiv 9 \pmod{26}$$
$$x \equiv 23 \pmod{27}$$

——The End——