Indian Institute of Technology, Kharagpur

Date..... FN/AN Time: 2 Hrs Full Marks: 30 No. of Students: 50
Mid (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 [3+3 marks]

a) Use the Playfair cipher to encrypt the followong plaintext with the keyword provided:-

Plaintext	you will see me tonight at the town hall
keyword	cryptography

b) Use exhaustive key search to decrypt the following ciphertext, which was encrypted using a *Shift Cipher*:-

BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD

Question 2 [2+2+2 marks]

a) Draw a detailed diagram of a single DES round (including the operations on the round key).

b) Draw a diagram of a AES CBC (Cipher Block Chaining) mode of operations.

c) How are block ciphers different than stream cipher?

Question 3 [3+3 marks]

a) What is an l-bit LFSR? Describe an 5-bit LFSR based stream cipher.

b) Making use of the extended Euclid's algorithm, perform RSA-encryption of the plaintext message M with the following parameter values:-

Primes	$p = 2, q = 2;$
Plaintext	$M = 2;$
Value of the public key	$a = 7$

to produce ciphertext C. Using C perform the decryption to verify your answer.

——P.T.O——

Question 4 [1+3+2 marks]

a) Describe the discrete logarithm problem in Z_p where p is prime.

b) Describe the ElGamal cryptosystem in Z_p.

c) You are given the following parameters for the Diffie-Hellman key exchange algorithm:-

Prime	$p = 11$
Primitive element	$\alpha = 6$
User A selects private key	$X_A = 5$
User B selects private key	$X_B = 3$

Show that $\alpha = 6$ is indeed a primitive element of Z_p^*. What is the value of the shared secret key K?

Question 5 [3+3 marks]

a) Describe how an elliptic curve over $Z_p (p > 3)$ can be made into an abelian group by defining suitable operation on its points.

b) Describe RSA signature scheme.

——-The End———