DEPARTMENT OF MATHEMATICS, IIT - KHARAGPUR
End Semester Examination, Autumn 2012
Subject No.: MA61027/MA51115, Subject Name: Cryptography
Number of Students: 70, Instructor: Dr. Sourav Mukhopadhyay
Full Marks: 50 Time: 3 Hours

Instruction: ANSWER ALL THE QUESTIONS.

---

1. a) Decrypt the ciphertext 111111111111 using CBC mode. Use the permutation cipher with block length 3 and key $k = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

   The initialization vector is 000.

   b) Draw a detailed diagram of a one round DES **decryption** function (including the operations on the round key).

   c) Describe Mixcolumn operation used in the AES-Rijndael encryption function. [4+3+3=10]

2. a) What is stream cipher? describe an l-bit LFSR based stream cipher.

   b) An S-box $S : \{0,1\}^m \to \{0,1\}^n$ is said to be balanced if $|S^{-1}(y)| = 2^{m-n}$ for all $y \in \{0,1\}^n$. Consider the following DES S-box $S_5 : \{0,1\}^6 \to \{0,1\}^4$:

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

Table 1: DES S-box S_5

   (i) Determine the set ${S_5}^{-1}(1001)$.

   (ii) Prove/Dis-prove that S_5 is balanced. [5+5]

3. a) What is message authentication code (MAC)? Explain how CBC mode of operation can be used to compute MAC.

——P.T.O.——

b) Consider the encrypted CBC MAC built from AES. Suppose we compute the tag for a long message m comprising of n AES blocks. Let m^* be the n-block message obtained from m by flipping the last bit of m (i.e. if the last bit of m is 0 then the last bit of m^* is 1, if the last bit of m is 1 then the last bit of m^* is 0,). How many calls to AES would it take to compute the tag for m^* from the tag for m and the MAC key? (in this question please ignore message padding and simply assume that the message length is always a multiple of the AES block size).

c) Draw a detailed diagram of Secure Hash Code. [3+3+4]

4. a) Suppose Bob has an RSA Cryptosystem with modulus N and encryption exponent e_1 and Charlie has an RSA Cryptosystem with (the same) modulus N and encryption exponent e_2. Suppose also that $gcd(e_1, e_2) = 1$. Now consider the situation that aries if Alice encrypts the same plaintext m to send to both Bob and Charlie. Thus, she computes $c_1 = m^{e_1} \mod N$ and $c_2 = m^{e_2} \mod N$ and then she sends c_1 to Bob and c_2 to Charlie. Suppose Oscar intercepts c_1 and c_2, and performs the the computations indicated in the following algorithm:

Algorithm: RSA Common Modulus Decryption (N, e_1, e_2, c_1, c_2)

$b_1 = e_1^{-1} \mod e_2$

$b_2 = \frac{(b_1 e_1 - 1)}{e_2} \mod e_1$

$x = {c_1}^{b_1} ({c_2}^{b_2})^{-1} \mod N$

return (x)

Prove that the value x computed in the above algorithm is in fact Alice's plaintext m. Thus, Oscar can decrypt the message Alice sent, even though the cryptosystem may be "secure".

b) Describe RSA signature scheme. [6+4]

5. a) Describe ElGamal cryptosystem on Elliptic curve points over Z_p

b) Let E be the modular elliptic curve defined by $y^2 = x^3 + 3x + 3(\mod 5)$.

(i) Find all points of E (including the point at infinity)

(ii) Suppose Alice wants to send the plaintext $x = (4, 2)$ to Bob. Let $\alpha = (3, 2)$ (the primitive element) and Bob's private key be 3, so Bob's public key is $\beta = 3\alpha$. Find the ciphertext while Alice chooses the random value $k = 2$. [4+6]

——-The End———