Dept. of Computer Science and Engg.
Indian institute of Technology, Kharagpur
Subject: Cryptography and Network Security, Subject Code: CS60041
Full Marks: 60 Duration: 2 hrs. Date: 30.09.11 (AN)

Instruction: Answer all the questions

1 (a) Suppose that y and y' are two ciphertext elements (i.e. binary n tuples) in the Onetime Pad that were obtained by encrypting plaintext elements x and x', respectively, using the same key, K. Prove that $x + x' \equiv y + y' \pmod 2$.

(b) Find the remainder when 72^{1001} is divided by 31.

(c) For symmetric block cipher explain "Output Feedback Mode (OFB)" of operation with figure. What is the advantage of OFB? (5+5+5 =15)

2 (a) Show that $P(a) \equiv P(b) (\mathrm{mod}\ n)$ if $a \equiv b \pmod n$ where, $P(x) = \sum_{k=0}^{m} c_k x^k$ be a polynomial function of x with integral coefficients c_k and a,b are integers.

(b) Let $N = a_m 10^m + a_{m-1} 10^{m-1} + a_{m-2} 10^{m-2} + \ldots\ldots + a_1 10 + a_0$ be the decimal expansion of the positive integer N, $0 \le a_k < 10$, and let $S = a_0 + a_1 + a_2 + \ldots\ldots + a_m$ and $T = a_0 - a_1 + a_2 - \ldots\ldots + (-1)^m a_m$. Then apply the result (a) to prove the following

(i) $9 \mid N$ if and only if $9 \mid S$

(ii) $11 \mid N$ if and only if $11 \mid T$

(c) Show that the integer N = 1571724 is divisible by 9 and 11. (4+8+3 = 12)

3 (a) Compute the product of the bytes 10010001 and 00100010 where one of the primitive polynomial in $GF(2^8)$ is $p(x) = 1 + x + x^3 + x^4 + x^{8.}$

(b) Write the algorithmic steps of forward transformation function of AES128 substitute bytes stage.

(c) Assume one simple block cipher whose encryption function consists of only AES Substitution. What will be the ciphertext byte for the plaintext byte "83" (hex)?

(5+5+5=12)

4 (a) Suppose that K = (5,21) is a key in Affine Cipher over Z_{29}.

(i) Express the decryption function as $d_k(y) = a'y + b'$, where $a', b' \in Z_{29}$.

(ii) Prove that $d_k(e_k(x)) = x$ for all $x \in Z_{29}$.

(b) Two-Key 3DES encrypts a 64-bit message M in the following manner.

$C = DES_{k1}(DES^{-1}_{k2}(DES_{k1}(M)))$ -- (*); here, k1 and k2 are strings of 56-bits each.

(i) What is the average complexity of a naive exhaustive search?

(ii) Given a box that encrypts a message M according to (*), one may use the box to encrypt plaintext of his choice. Denoting the all-zero message as 0, first a table containing the standard DES decryption of messages 0 under 256 keys can be made. Then one can use the chosen plaintext attack to build a second table containing the 256 ciphertexts resulting from box encryption of the first table. Given these two tables, one can find both k1 and k2 used by the encryption box. Write an explicit algorithm on how one may proceed to know k1, k2. The whole attack should take no more than 260 DES encryptions (or decryptions) and no more than 261 bytes of memory.

(6+9=15)