Midterm Exam

October 21, 1997

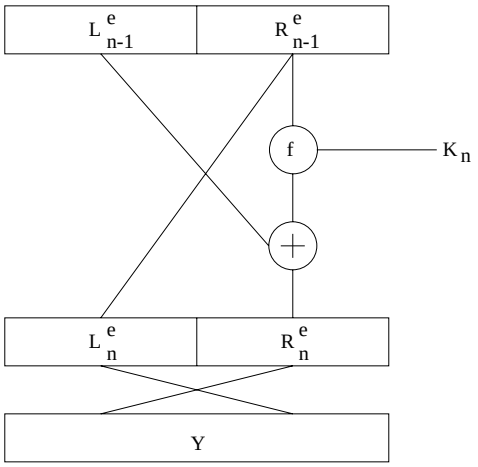
Name: _____

1. Which of the following two polynomials yield a maximum length linear feedback shift register?

   (a) $x^4 + x^2 + 1$

   (b) $x^4 + x^3 + 1$

2. Many block ciphers such as DES are based on Feistel networks. One central reason for building ciphers from Feistel networks is that encryption and decryption are almost identical operations. We will study this characteristic in the following problem.



   (a) Given is the last round of an n-round Feistel network. Draw the first round of the corresponding decryption network. Use superscripts "d" to denote the variables.

   (b) Show that $L_1^d = R_{n-1}^e$ and that $R_1^d = L_{n-1}^e$.

   (c) Express L_n^d and R_n^d through values from the encryption operation.

3. Attached is a description of the DES algorithm. We consider the output of the first DES round (L_1, R_1) for an arbitrary input x and an arbitrary key k.

   (a) We apply now an input x' that differs only by one bit from x. Assume that R'_0 differs also by one bit from R_0. What is the *minimum* number of bits in (L'_1, R'_1) that are different from (L_1, R_1)?

   (b) Let the input x be all zero and the key be all one generating a first-round output (L_1, R_1). We now apply x' which is all zero except in position 7 where it is one. The first-round output becomes now (L'_1, R'_1). Which bit positions in (L'_1, R'_1) are different from (L_1, R_1)? Note that you don't have to provide (L_1, R_1) or (L'_1, R'_1) explicitly but merely the bit positions in which changes occur.

4. Which were the two initial criticisms brought up against DES soon after it was proposed? Comment on these two criticisms in retrospect, considering today's ability to break DES?

5. (a) How many pieces of plaintext and ciphertexts are required for breaking a block cipher in ECB mode with k key bits. Assume that the block length is much longer than the key length.

   (b) Let's assume now that we do not know the vector IV of the block cipher used in CBC mode. Describe how many pieces of (i) plaintext and (ii) ciphertext are required in order to break a CBC cipher by an exhaustive key search. How many search steps are required in a worst-case scenario?

   (c) Is breaking a block cipher in CBC mode by means of an exhaustive key search considerably more difficult than breaking the same block cipher in ECB mode? Why is the CBC mode often preferred over the ECB mode?

6. Given are the following parameters of the RSA cryptosystem: $p = 101, q = 107, b = 4497$. You receive the ciphertext $y = 7411$. Compute the cleartext.

7. Assume an RSA implementation where the modulus n and all other variables have 1024 bits. Assume one modulo multiplication or squaring with 1024 bit integers takes 100 μs. How long does encryption of a message x take on average using the square-and-multiply algorithm?