Midterm Exam

October 25, 1995

Name: _____

1. Draw a hierarchical tree diagram which links the terms:

   block cipher, cryptanalysis, cryptography, cryptology, private-key, protocols, public-key, stream cipher.

2. We want to apply the affine cipher to a 26 letter alphabet. The mapping from letters to integers is according to the attached table ($A \leftrightarrow 0, \ldots, Z \leftrightarrow 25$). We choose the value $b = 2$.

   (a) Which of the integers $9, 10, 11, 12, 13$ can be used as a value for a?

   (b) Use the *largest* possible value from above for a and encrypt the message

   `BLACK ELK`

   If you were not able to do part (a), use $a = 21$.

   (c) The decryption process can be expressed as

   $$d_k(y) = x = c\,y + d \bmod 26$$

   What are the values for c and d here?

3. We consider an LFSR-based stream cipher. The linear feedback shift register is characterized by the polynomial $1 + x^3 + x^4$ and the initial vector $(z_0 = 1, 0, 0, 0)$.

   (a) What are the feedback coefficients c_0, c_1, c_2, c_3?

   (b) Draw the block diagram of the LFSR.

   (c) Is this a maximum-length LFSR?

   (d) Encode the following binary message:
   `1001 1100 1100`

   (e) What is the maximum message length that should be encoded with this stream cipher?

4. Which were the two initial criticisms brought up against DES soon after it was proposed? How valid are these criticisms retrospectively, considering today's ability to break DES?

5. Attached is a description of the DES algorithm. What are the values of (L_1, R_1) if the 64 input bits and the 56 key bits are in hexadecimal notation:

$$\begin{aligned} x &= FF\,FF\,FF\,FF\,FF\,FF\,FF\,FF \\ k &= 00\,00\,00\,00\,00\,00\,00 \end{aligned}$$

   (The answer can be in binary or hexadecimal form.)

6. We use the DES algorithm in the cipher feedback mode (CFB). Each cleartext is 4 bit wide.

   (a) Draw a block diagram of the CFB operation mode, showing the encryption and decryption side. Show the width (in bits) of every connection line/bus.

   (b) Assume ciphertext c_i is corrupted by a single bit error on the transmission line. Which blocks x_j are affected on Bob's side? *How* is each of these blocks affected?

7. Compute

$$100^{160} \bmod 163$$

   using the square-and-multiply algorithm. Note that $160 = 128 + 32 = 2^7 + 2^5$.

8. (**Optional problem, 5 extra points**) A linear shift feedback register (LFSR) of degree m is described by:

$$z_{i+m} = \sum_{j=0}^{m-1} c_j\, z_{i+j} \bmod 2 \quad i = 0, 1, 2, \ldots$$

   where z_k are the outputs and the c_j are the m binary feedback coefficients.

   Breaking and LFSR means to determine the m unknown coefficients c_j, $j = 0, 1, \ldots, m-1$, by observing the output bits z_k. We assume we know m. *Derive* the matrix equation for breaking the LFSR of degree m with $2m$ known outputs z_k.