Midterm Exam

October 18, 2000

Name: _____

Problem	1	2	3	4	5	6	7
Points							

1. What is the block size of AES? Which key lengths are supported by AES?

2. We use the affine cipher for encryption and decryption. However, we would like to be able to distinguish between uppercase and lowercase characters, so that we have a cleartext and ciphertext space of size 52. How large is the key space of the affine cipher in this case?

3. Assume we have a stream cipher whose period is quite short. We happen to know that the period is between 150–200 bits in length. In slight violation of Kerckhoff's Principle, we assume that we do *not* know anything else about the internals of the stream cipher. In particular, we should not assume that it is a simple LFSR. For simplicity, assume that English text in ASCII format is being encrypted.

   Describe in detail how such a cipher can be attacked. Specify exactly what Oscar has to know in terms of cleartext/ciphertext, and how he can decrypt all ciphertexts.

4. A block diagram of the DES key schedule is given in the attachment. The number of bit position shifts per round are given as:

   for LS_i where $i = 1, 2, 9, 16$, the block is shifted once.
   for LS_i where $i \neq 1, 2, 9, 16$, the block is shifted twice.

   Draw a block diagram for the decryption key schedule such that the subkey needed in the first decryption round is generated first, the subkey for the second round next, etc. Exactly specify the numbers of shifts for every round.

5. 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 the first bit (of four) of the ciphertext block c_i is flipped due to an error on the transmission line. Which blocks x_j are affected on Bob's side? *How* is each of these blocks affected?

6. We now look at the following variant of key whitening with DES, which we'll call DESB:

$$DESB_{K_A,K_B}(x) = DES_{K_A}(x \bigoplus K_B)$$

   Even though the method looks similar to key whitening, it hardly adds to the security.

   (a) Show that breaking the scheme is roughly as difficult as a brute force attack against single DES.

   (b) How many encryptions and decryptions are needed in the worst case?

   Assume you have a few pairs of plaintext/ciphertext. (Hint: To get started, it is recommended that you draw a diagram of the scheme. Name the variable between the XOR and the DES input x'.)

7. Assume that modular squaring and modular multiplication both have a quadratic complexity with respect to the bit length. That is, doubling the bit length of the operands yields an operation which takes four times as much time.

   Given is an RSA systems with 1024 bit. An RSA decryption (with an exponent of full length, i.e., 1024 bits) takes time τ. For security reasons we are forced to use RSA with 3072 bits. How long will an RSA decryption with a full length exponent take now?