Midterm Exam

November 1, 1999

Name: _____

1. Why was the number of round for DES fixed at 16?

2. Although Gilbert Vernam did not invent the one time pad, his invention was a major stepping stone towards modern cryptography. What was the **main** advantage of his invention compared to earlier encryption systems?

3. Given is the following string of ciphertext which was encrypted with an affine cipher

   `JNNDLBVNEXGBO`

   You know that the first plaintext letter is a `C` and that the last one is an `R`.

   Find the coefficients c and d, with $0 \leq c, d \leq 25$, such that

   $$x = c\,y + d \bmod 26$$

   and decrypt the message, using the attached mapping from letters to elements in Z_{26}.

4. Given is a stream cipher which uses a single LFSR as key stream generator. The LFSR has a degree of 256.

   (a) How many plaintext/ciphertext bit pairs are needed to launch a successful attack?

   (b) Describe all steps of the attack in detail. Provide the formulae that must be used as appropriate. However, you do not have to provide formulae for solving matrix equations.

   (c) What is the key in this system? Why doesn't it make sense to use the initial contents of the LFSR as the key or as part of the key?

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 (after PC-1) are:

   $$\begin{aligned} X &= FF\,FF\,FF\,FF\,FF\,FF\,FF\,FF \\ K &= 00\,00\,00\,00\,00\,00\,00 \end{aligned}$$

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

6. Given are the two primes $p = 101$ and $q = 103$ as set up parameters for an RSA cryptosystem. We would like to use one of the integers 3, 17, or 31 as the public key.

   (a) Which of the values can be used as public key?

   (b) Compute the corresponding private key for all of the valid public key(s).

7. One major drawback of public-key algorithms is that they are relatively slow. In this problem we study one of the standard acceleration techniques that is available for the RSA encryption which uses "short exponents". Short exponents are public keys which are only a few bits long.

   (a) Assume that in an implementation of the RSA cryptosystem one modular squaring takes 75% of the time of a modular multiplication. How much quicker is one encryption on average if instead of a 2048 bit public key the short exponent $b = 2^{16} + 1$ is being used? Assume that the square-and-multiply algorithm is being used in both cases.

   (b) Why would a choice of $b = 2^{16} - 1$ not be as advantageous as $b = 2^{16} + 1$?

8. As described in problem 7, a standard acceleration techniques for RSA encryption is to use "short exponents", that is integers which are only a few bits long, as public keys. In particular, $b = 3$, 17, and $2^{16} + 1$ are widely used.

   (a) Why can't we use these three short exponents as values for the exponent a in applications where we want to accelerate decryption?

   (b) Can you suggest a minimum bit lengths for the exponent a? Provide a rationale for your answer.