**CIS 3362 Test #2: Modern Symmetric Encryption Schemes (DES, AES)**

**Date: 10/10/2012**

**Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1) (16 pts) Consider a cipher that uses a 16 bit key and 16 bit blocks. Let A and B both be permutations matrices used in the cipher, assuming that A and B are expressed in a similar manner to how IP is expressed in DES. Let C be a matrix that represents the equivalent permutation to applying B, followed by applying A. (Thus, C(x) = A(B(x)), where x is a 16 bit input.) Determine C given the matrices A and B below:

A = B =

2) (4 pts) If the input in DES to S-box 6 is 111010, what is the output?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3) (8 pts) The first part of the function F in a round of DES expands the 32-bit input (from the right half of the previous round) to 48 bits. If this input, in HEX to the function F is AE38E774, what are the first 8 bits of output right after this value is processed by the Expansion Permutation E?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4) (10 pts) It is possible to come up with permutation matrices for each of the keys for the 16 rounds of DES. In class, we viewed this permutation matrix for the first round key. The first six values in this matrix were 10, 51, 34, 60, 49 and 17. What are the next six values? In order to earn more than 2 points on this question, you have to justify your answer using PC-1 and PC-2.

5) (12 pts) Determine all of the integers in between 1 and 42, inclusive, that have a multiplicative inverse mod 42.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

6) (10 pts) Determine the product of the two polynomials x4 + x2 + 1 and x5 + x3 + x + 1 with coefficients in Z2 mod x8 + x4 + x3 + x + 1.

7) (20 pts) Let the input to the MixCols (during AES encryption) be .

What’s the output in row 4 col 2? (The matrix by which to “multiply” is .)

8) (10 pts) The largest version of AES uses a 256 bit key. How many keys would have to be searched per second in order for a brute force attack to break this version of AES in ten years? Express your answer in scientific notation. Please show your work. Write down answers from your calculator.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

9) (8 pts) In the key expansion algorithm of AES, if w[26] = AE8F236B and w[23] = 6AB57C93, what is w[27]?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

10) (2 pts) Facebook recently announced that it has 1 billion active users. What’s the most number of friends (roughly) one could theoretically have on Facebook, now? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Scratch Page – Please clearly label any work on this page you would like graded.**