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

**Date: 10/10/2011**

**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 A, followed by applying B. (Thus, C(x) = B(A(x)), where x is a 16 bit input.) Determine C given the matrices A and B below:

 A = $\left[\begin{matrix}\begin{matrix}3&7\\11&14\end{matrix}&\begin{matrix}12&9\\6&1\end{matrix}\\\begin{matrix}15&16\\2&4\end{matrix}&\begin{matrix}10&13\\5&8\end{matrix}\end{matrix}\right]$ B = $\left[\begin{matrix}\begin{matrix}16&13\\7&4\end{matrix}&\begin{matrix}10&5\\1&12\end{matrix}\\\begin{matrix}2&11\\15&8\end{matrix}&\begin{matrix}14&9\\6&3\end{matrix}\end{matrix}\right]$

2) (4 pts) If the input in DES to S-box 7 is 101101, 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 A3F752C9, what are the first 8 bits of output right after this value is processed by the Expansion Permutation E?

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

4) (10 pts) Explain why the numbers 8, 16, 24, 32, 40, 48, 56 and 64 do NOT appear in the DES matrix PC-1, but why some of those numbers DO appear in the DES matrix PC-2.

5) (12 pts) Determine all of the integers in between 1 and 21, inclusive, that have a multiplicative inverse mod 21.

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

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

7) (20 pts) Let the input to the MixCols (during AES encryption) be $\left[\begin{matrix}\begin{matrix}A0&74\\2B&8D\end{matrix}&\begin{matrix}65&96\\2E&E3\end{matrix}\\\begin{matrix}99&1F\\C5&E5\end{matrix}&\begin{matrix}C8&37\\F7&BB\end{matrix}\end{matrix}\right]$.

What’s the output in row 3 col 2? (The matrix by which to “multiply” is $\left[\begin{matrix}\begin{matrix}02&03\\01&02\end{matrix}&\begin{matrix}01&01\\03&01\end{matrix}\\\begin{matrix}01&01\\03&01\end{matrix}&\begin{matrix}02&03\\01&02\end{matrix}\end{matrix}\right]$.)

8) (10 pts) The smallest version of AES uses a 128 bit key. How many keys would have to be searched per second in order for a brute force attack to break AES in a year? 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] = 8EFA5329 and w[23] = 7EE826D3, what is w[27]?

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

10) (2 pts) Steve Jobs, the founder of Apple Inc. recently passed away. After what fruit did he name his company? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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