

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

Date: 10/4/2013

Name: _____

1) (20 pts) Consider a simple cryptosystem with a 16 bit block and 16 bit key as follows:

Step 1: Compute $C_0 = A(P)$, where A is the permutation matrix shown below.

Step 2: Compute $C_1 = C_0 \oplus K$, where K is the input key.

Step 3: Compute $C_2 = S(C_1)$. S splits its input into four blocks of four bits. For each block of four bits, it substitutes for it values shown in B . For example, if the four bits of input were 0101, which corresponds to 5, we would look in spot #5 in B , in row 1, column 2, which is 12 and substitute 1100. As another example if the input were 1110, the output would be 0101.

Step 4: Let $C_2 = LR$, where L is the left byte and R is the right byte. Compute the ciphertext $C = RL$.

$$A = \begin{bmatrix} 3 & 7 & 12 & 9 \\ 11 & 14 & 6 & 1 \\ 15 & 16 & 10 & 13 \\ 2 & 4 & 5 & 8 \end{bmatrix} \quad B = \begin{bmatrix} 6 & 1 & 11 & 4 \\ 13 & 12 & 15 & 8 \\ 0 & 3 & 10 & 9 \\ 7 & 2 & 5 & 14 \end{bmatrix}$$

Compute the encryption of the plaintext A349 with the key 5DF7.

2) (4 pts) If the input in DES to S-box 5 is 001111, 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 7DA839B2, what are the last 8 bits of output right after this value is processed by the Expansion Permutation E?

4) (10 pts) Without examining all entries in the 16 round key schedule of DES, determine whether or not each number (which represents a bit location in the original key in each of the 16 boxes labeled "Round 1" through "Round 16") appears the exact same number of times collectively in the 16 boxes. (As an example, 10 appears in round except rounds 4, 12 and 14, so it appears 13 times.) Give proof of your answer.

5) (15 pts) One mathematical idea that has come up multiple times in this course is matrix multiplication. To multiply two square matrices of size $n \times n$, our answer will also be a matrix of size $n \times n$. To compute the answer in row i , column j , we take each item in row i of the first matrix, multiply it by the corresponding item in column j of the second matrix and add these n products to get the desired result. Complete the C function below to multiply the two input matrices `mat1` and `mat2` of size 10×10 and store the result in `mat3`. You may assume that `mat1` and `mat2` store the desired values before the function is called. Do not worry about integer overflow.

```
void matMult(int mat1[][10], int mat2[10], int mat3[][10]) {
```

```
}
```

6) (8 pts) In the key expansion algorithm of AES, if $w[30] = 79AEC508$ and $w[27] = FD1B6423$, what is $w[31]$?

7) (20 pts) Let the input to the MixCols (during AES encryption) be $\begin{bmatrix} A0 & 74 & 65 & B7 \\ 2B & 8D & 2E & C6 \\ 99 & 1F & C8 & EB \\ C5 & E5 & F7 & 23 \end{bmatrix}$.

What's the output in row 2 col 4? (The matrix by which to "multiply" is $\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$.)

8) (12 pts) Consider an AES plaintext of $\begin{bmatrix} 01 & 89 & FE & 76 \\ 23 & AB & DC & 54 \\ 45 & CD & BA & 32 \\ 67 & EF & 98 & 10 \end{bmatrix}$ with a key of 128 1s. Show the state matrix after the shift rows step in Round 1.

9) (3 pts) What is the three dimensional shape of the Rubix Cube, a puzzle that became popular in the 1980s?

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