CIS 3362 Test #2: Modern Symmetric Encryption Schemes (DES, AES)
Date: 10/26/2016

Last Name: _____ , First Name: _____

1) (8 pts) Consider a 16 bit block cipher that uses a permutation matrix, P', in the same format as IP in DES, given below. Let the 16 bit plaintext input to the matrix P' be `1001 0111 1011 0011`. What is the output? (Express your answer as 16 bits.)

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

_____

2) (12 pts) You are attempting to brute force a DES key. Luckily, you have obtained the following bit locations of the key (out of the locations k_1, k_2, ... k_{64} given in the official specification):

k_1, k_5, k_8, k_{17}, k_{18}, k_{19}, k_{20}, k_{21}, k_{22}, k_{23}, k_{24}, k_{42}, k_{44}, k_{45}, k_{47}, k_{56}, k_{60}, and k_{64}

How many keys do you have to try to ensure that you find the appropriate key? (Assume that we have a matching plaintext and ciphertext block we can use to verify if a guess to the key is correct or not and the correct bits for the bit locations specified above in the key.) Please leave your answer as a power of 2.

_____

3) (16 pts) Consider a portion of a single DES round where the first 24 bits of input (expressed in HEX) to S boxes S_1, S_2, S_3, S_4 is `3A7ED8`. What are the 16 bits of output from those 4 S-boxes? Express your result in binary. (Note: Partial credit on this question will be limited for obvious reasons, so double check your answers.)

---

4) (10 pts) In the DES key schedule, the algorithm keeps a buffer of bits whose left half is C_i and whose right half is D_i, for values of i from 0 to 16. Let C_5 = `F560B94`, represented in hex. Calculate C_6 and give your result as 7 hex characters.

---

5) (2 pts) Why doesn't the value 24 appear in the DES key schedule matrix PC-1?

6) (2 pts) Why are all of the values from 57 to 64 missing in the DES key schedule matrix PC-2?

7) (2 pts) Why is it possible for the value 24 to appear in the DES key schedule matrix PC-2? (It does appear, in the 4^{th} position.)

8) (8 pts) Let the state matrix to AES right before the SubBytes step be the matrix shown below. Show the state of the matrix right AFTER the SubBytes step:

3D	FF	09	31
85	4B	75	E2
C6	BD	2E	18
5A	6C	A0	E4

9) (8 pts) Let the state matrix to AES right before the ShiftRows step be your answer from problem 8. Show the state of the matrix right AFTER the ShiftRows step:

10) (12 pts) Consider the process of AES Key Expansion. Imagine that we have:

w[16] = 54 9E B6 38 (in hex)
w[19] = 01 F7 AD C2 (in hex)

Calculate w[20], showing each of the following intermediate results: RotWord(temp), SubWord(RotWord(temp)), Rcon[i/4], and the result of the XOR with Rcon[i/4].

RotWord	SubWord	Rcon[i/4]	XOR	FinalResult

11) (18 pts) In class we discussed multiplication in the AES field GF(2^8) with the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$. Based on this discussion, derive the answer for the calculation of 07 x E5 in this field. Express your result as 8 bits.

_____

12) (2 pts) What does a football player playing the position of running back primarily do when holding a football?

_____

Scratch Page - Please clearly mark any work on this page you would like graded.