Fall 2024 CIS 3362 Homework #4: DES, AES Solutions

1) Consider creating a DES-like block cipher with a block size of 16. Assume that the cipher has a fixed matrix IP, just like DES, that operates exactly as DES's IP matrix. Given the IP matrix shown below, calculate the corresponding matrix, IP^{-1}.

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

$IP^{-1} =$

15	7	4	16
12	8	1	13
5	3	10	6
2	11	14	9

Helpful phrase to remember '7 goes in 1, so 1 goes in 7'

2) The input to the expansion matrix E in DES, expressed in hexadecimal is B4F392C6. What is the output? Please express your answer in **hexadecimal** and put a little space between each group of **2** hex characters. Use words to explain how you arrived at the answer so that the grader can verify that the answer is correct **for the right reason.**

Convert B4F392C6 to binary:
1011 0100 1111 0011 1001 0010 1100 0110

Grab the bits listed below:

(c) Expansion Permutation (E)

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Place the bits in the order in which the E expansion matrix places them, here we group 6 bits at a time as the rows are in the table:
010110 101001 011110 100111 110010 100101 011000 001101, now separate into groups of 4:
0101 1010 1001 0111 1010 0111 1100 1010 0101 0110 0000 1101
Place into groups of 2 hex characters:
5A 97 A7 CA 56 0D

3) Consider a portion of a single DES round where the input (expressed in HEX) to S boxes S_1, S_2, S_3, S_4 S_5, S_6, S_7, and S_8 is `2413ACBD5F6E`. What are the 32 bits of output from the S-boxes? Express your result in **binary (so 32 separate bits)**. (Note: Partial credit on this question will be limited for obvious reasons, so double check your answers.)

Convert 2413ACBD5F6E to binary:
0010 0100 0001 0011 1010 1100 1011 1101 0101 1111 0110 1110

Grouped into 6 bits:
001001 000001 001110 101100 101111 010101 111101 101110

Place our groups into the S-boxes:
S_1(001001) = 14
S_2(000001) = 3
S_3(001110) = 5
S_4(101100) = 7
S_5(101111) = 13
S_6(010101) =13
S_7(111101) = 3
S_8(101110) = 2

*Remember the outer two bits represent the row and in the inner four bits represent the column (all 0 based)

1110 0011 0101 0111 1101 1101 0011 0010

Refer to SBoxTester.java or DES Tables

4) Consider calculating the round 16 key in DES. Given that the input key, with odd parity bits, when described in HEX is **`"C761 4592 BCC2 5D38"`**, **determine the first 10 bits of the round 1 key. Credit will only be given if appropriate work is shown since it's easy to randomly put bits down and get around half of them. I'll decide what appropriate work is!!!**
C761 4592 BCC2 5D38 in binary:

1100011**1** 0110000**1** 0100010**1** 1001001**0** 1011110**0** 1100001**0** 0101110**1** 0011100**0**

*Highlighted bits are the parity bits (it's helpful to mark these when calculating these by hand)

Looking at PC-1, apply the 1 left shift to it:

49 41 33 25 17 9 1

58 50 42 34 26 18 10

2 59 51 43 35 27 19

11 3 60 52 44 36 57

---

55 47 39 31 23 15 7

62 54 46 38 30 22 14

6 61 53 45 37 29 21

13 5 28 20 12 4 63

Next, grab the first 10 values of PC-2: 14, 17, 11, 24, 1, 5, 3, 28, 15, 6

*Each of the highlighted numbers in PC-1 represent the indices highlighted here

Use those values as an index into PC-1, grab those values: 10, 51, 34, 60, 49, 17, 33, 57, 2, 9

Grab those values from the original key:

11000111 01100001 01000101 10010010 10111100 11000010 01011101 00111000

^ ^ ^

| | |

bit 1 bit 32 bit 64

So, the first ten bits turn out to be: 1001001010

Refer to DES Tables for PC-1 and PC-2

5) In the past I offered a DES challenge where I gave students some bits of the 56-bit key and they had to brute force the rest. Consider that most of the students in the course take one of two approaches to break the key, exemplified by Student X and Student Y below:

(a) Student X has decided to use the professor's slow Java implementation (so no time to code the DES portion of the code) and add the brute force mechanics (this takes 1 hour), and then check each key at a rate of 200,000 keys per second.

(b) Student Y has decided to rewrite the professor's code in C++ and write the corresponding brute force mechanics (takes 2 days/48 hours, including adding the brute force mechanics), and then check each key at a rate of 2,000,000 keys per second.

The professor would like for both Student X and Student Y's approaches to take the same total time (or as close as possible). How many bits of the key should the professor reveal?

The first thing that we will do is set up expressions to solve for the total time it will take for each student to find the key for a DES key where 'b' bits are already known.

x) $\frac{2^{56-b}}{7.2*10^8 \frac{keys}{hr}} + 1hr$

y) $\frac{2^{56-b}}{7.2*10^9 \frac{keys}{hr}} + 48hr$

*Note that 2^{56-b} represents the **rest of the key space** a student would have to search to find the key. Also note the conversion of all time to hours.

Now that we have set up expressions to represent the time it will take each student to solve for the key, all we need to do is solve for 'b' since that is the only unknown.

$$\frac{2^{56-b}}{7.2*10^8} + 1 = \frac{2^{56-b}}{7.2*10^9} + 48$$

Now, pull out your algebra skills…

$$\frac{2^{56-b}}{7.2 * 10^8} + 1 = \frac{2^{56-b}}{7.2 * 10^9} + 48$$

$$\frac{2^{56-b}}{\frac{36}{5} * 10^8} + 1 = \frac{2^{56-b}}{\frac{36}{5} * 10^9} + 48$$

$$\frac{5 * 2^{56-b}}{36 * 10^8} + 1 = \frac{5 * 2^{56-b}}{36 * 10^9} + 48$$

$$50 * 2^{56-b} + 36 * 10^9 = 5 * 2^{56-b} + 1728 * 10^9$$

$$45 * 2^{56-b} = 1692 * 10^9$$

$$2^{56-b} = \frac{1692 * 10^9}{45}$$

$$56 - b = \log_2 \frac{1692 * 10^9}{45}$$

$b = -\log_2 \left(\frac{1692*10^9}{45}\right) + 56 \approx 20.870$

$b \approx 21\ bits$

Therefore, we find that the professor should reveal roughly 21 bits for students X and Y to take (roughly) the same amount of time.

6) 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:

01	23	45	67
8F	9E	AD	BC
40	51	62	73
FC	EB	DA	98

7C	26	6E	85
73	0B	95	65
09	D1	AA	8F
B0	E9	57	46

Refer to AES S-Boxes

7) Let the state matrix to AES right before the ShiftRows step be your answer from problem 7. Show the state of the matrix right AFTER the ShiftRows step. (This will be graded solely based on what your answer to problem 7 was. You can get this one correct even if you got problem 7 incorrect.)

7C	26	6E	85
0B	95	65	73
AA	8F	09	D1
46	B0	E9	57

Refer to AES ShiftRows

8) Consider the process of AES Key Expansion. Imagine that we have:

w[32] = A3 B4 C7 D9 (in hex)
w[35] = 05 18 2E 6F (in hex)

Calculate w[36], 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
18 2E 6F 05	AD 31 A8 6B	1B 00 00 00	B6 31 A8 6B	15 85 6F B2

RotWord is just a cyclic left shift of 1 byte (which is 2 hex characters).

SubWord is just a SubBytes step using the AES S-box to replace the bytes.

Rcon[i/4] is also given. Since our i=36 and 36/4 = 9, we grab '1B' from the Rcon table provided in AESReferenceSheet.

Note that temp is just w[35] = 05 18 2E 6F

For XOR all you must do is reference any Hex xor table for the first byte (1B ^ B6), the rest of the bytes stay the same.

Lastly, we take w[32] ^ XOR

A3 B4 C7 D9
B6 31 A8 6B ^
---
15 85 6F B2

Again, any Hex xor chart will help you do this faster than calculating the xor by hand.

9) 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 9D. Display your final result with two hexadecimal characters.

First, let's convert everything to binary:
0111 x 1001 1101 =

001 x 1001 1101
010 x 1 0011 1010
  1 1011 ^

~~1~~ 1011 1100 (BC) --> this is 03 x 9D.

100 x 10 0111 0100
11 0110 ^

~~10~~ 0100 0010 (42)

BC $\oplus$ 42 = FE

Therefore, the final answer is FE

10) Let the input to the MixCols (during AES encryption) be $\begin{bmatrix} BC & 34 & 29 & 06 \\ A6 & 19 & 79 & 97 \\ 63 & F5 & 4C & C2 \\ BB & D2 & FD & A3 \end{bmatrix}$.

What's the output in row 3 col 2? (The matrix by which to "multiply" is $\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$.)

$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} * \begin{bmatrix} BC & 34 & 29 & 06 \\ A6 & 19 & 79 & 97 \\ 63 & F5 & 4C & C2 \\ BB & D2 & FD & A3 \end{bmatrix}$ = $01 * 34 + 01 * 19 + 02 * F5 + 03 * D2$

Multiplying by 01 is simple (yay, two done!)

$01 * 34 = 34$

$01 * 19 = 19$

$02 * F5 = 11110101 \ll 1 = 111101010$

000011011 ^ (doing XOR)

111110001 (F1)

$03 * D2 = 03 * 11010010 = 11010010$ (D2)

110100100 ⊕ (02*D2)

101110110

000011011 ⊕

01101101 (6D)

Final Answer = (34 ⊕ 19) ⊕ (11 ⊕ 6D) = B1

Refer to AESMixCols.java (ensure you enter your matrix **column wise** instead of row wise)