Fall 2020 CIS 3362 Quiz #3 Part A: DES Solutions

Date: 10/12/2020

1) (9 pts) Let S_k represent applying the k^{th} S-box in DES. The input for S_k is 6 bits. Show the output, **in binary**, for the three following S-box look ups:

a) $S_3(010111)$ b) $S_6(101110)$ c) $S_7(001000)$

Solution

Input	Box	Row(bin)	Row(dec)	Col(bin)	Col(dec)	Output(dec)	Output(bin)
010111	3	01	1	1011	11	14	**1110**
101110	6	10	2	0111	7	3	**0011**
001000	7	00	0	0100	4	15	**1111**

Grading: For each part, 1 pt for the correct row, 1 pt for the correct column, 1 pt for the correct binary output. If output is in decimal or HEX don't award the last point.

For each answer, please clearly indicate which row and which column you have found the appropriate entry, and then also convert it to binary.

2) (8 pts) Let the plaintext for a DES block (in hex) be 7e 9f 3c 62 1a 80 5b 4d. Give the first eight bits of the transformed input after applying the IP matrix. In order to get credit, show your work clearly (indicate WHICH bits you are grabbing.) No credit will be given for the correct answers since randomly guessing will get half the credit. Rather, all the credit will be given for showing the process to use.

Solution
The first eight entries of IP are:

58 50 42 34 26 18 10 2

Thus, we must grab the 58^{th} bit, then the 50^{th} bit and so forth.

Bits 57-60: 0100 (4)
Bits 49-52: 0101 (5)
Bits 41-44: 1000 (8)
Bits 33-36: 0001 (1)
Bits 25-28: 0110 (6)
Bits 17-20: 0011 (3)
Bits 9-12: 1001 (9)
Bits 1-4: 0111 (7)

The bits to select are the second bit in each of the 4 bit strings listed above, and each are highlighted in yellow.

It follows that the first 8 bits of output after applying IP are **11001001.**

Grading: 4 pts for stating the bit numbers (58, 50,…,2), 2 pts for finding where those bits are in the plaintext, 2 pts for grabbing the bits in the correct location. (If the system is correct and there are one or two simple errors, just take one point off.)

3) (8 pts) Consider doing a brute force search on a DES key when the even key bits, k_2, k_4, k_6, …, k_{64} are known and you can test 2^{20} keys per second. (Note: the bit representation is the one given in the official documentation where the key is given with parity bits.) How long will it take to finish the search in hours, minutes and seconds?

Solution

Of the 32 bits known, 8 are parity bits, so actually only 24 bits are known. But, consider any block of 8 bits. Three of the real bits are known and one parity bit is known (one with the bit number divisible by 8). So, there are 4 other bits unknown. With the parity bit though, out of the 16 possibilities of the other four bits, only 8 are possible. For example, if we had

X0X1X1X1

Where the X's represent the unknown bits, the 3 known 1s indicate that out of the four X's there must be an even number of 1s and this can only be done in 8 ways (0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111). Thus, for each of 8 rows, there are only 8 possible settings of the unknown bits that are viable. Thus, there are $8^8 = (2^3)^8 = 2^{24}$ possible keys to try.

Since we can try 2^{20} keys per second, we would need $2^{24}/2^{20} = 2^4 = 16$ seconds total to try all of the possible keys. To answer in hours, minutes and seconds, it would be 0 hours, 0 minutes and 16 seconds.

Grading: 3 pts for figuring out that there are 32 unknown bits (this can also be done directly since all odd bits are unknown and none of these are parity bits), 2 pts to figure out that we only need to try 8^8 of these options due to parity information, 2 pts for dividing this by 2^{20} to obtain 2^{12}, 1 pt to convert this to hours, minutes and seconds.

Fall 2020 CIS 3362 Quiz #3 Part B: AES Solution

Date: 10/12/2020

1) (14 pts) If the state matrix is the following right before the Mix Columns step of AES, what is the entry in row 4, column 2, right after the Mix Columns step? ***(Note: Please be very, very, very careful that you work out the correct entry. If you find the entry of row 2, column 4, you will earn a maximum of 3 points out of 14.)***

$$\begin{pmatrix} 7B & A4 & CD & 12 \\ 2C & 3D & 96 & 4F \\ 97 & 16 & A0 & 62 \\ B2 & D7 & 7E & D3 \end{pmatrix}$$

Note that the fixed matrix multiplier for the Mix Columns step in AES is $\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$.

Solution

The appropriate entry is equal to 03 x A4 + 01 x 3D + 01 x 16 + 02 x D7.

Let's work out the first and last product individually:

03 x A4 = 02 x A4 + 01 x A4

02 x A4 = 02 x (1010 0100) = 1 0100 1000 = 0100 1000
+ 1 1011

0101 0011 (53)

Using the Hex XOR chart, we find that 53 + A4 = F7.

02 x D7 = 02 x (1101 0111) = 1 1010 1110 = 1010 1110
+ 1 1011

1011 0101 (B5)

Thus, our final answer will be F7 + 3D + 16 + B5. Separating out the hex chars, we must calculate

F + 3 + 1 + B = C + A = 6
7 + D + 6 + 5 = A + 3 = 9

Thus, the final output is **69 = 0110 1001.** (Note: Either form is acceptable since the question didn't specify.)

Grading: 6 pts 03 product, 4 pts 02 product, 4 pts final XOR. If wrong entry calculated give max 3 pts out of 14. Take off 1 pt per error otherwise.

2) (10 pts) Consider the process of AES Key Expansion. Imagine that we have:

w[36] = B1 89 C4 07 (in hex)
w[39] = 9C 2F 63 DE (in hex)

Calculate w[40], 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
2F 63 DE 9C	**15 FB 1D DE**	**36 00 00 00**	**23 FB 1D DE**	**92 72 D9 D9**

Grading: 1 pt RotWord, 4 pts SubWord (1 pt per byte), 1 pt Rcon, 1 pt XOR, 3 pts final answer

3) (1 pt) On what day of the week does the sketch comedy show Saturday Night Live air?

Saturday (Grading: Give to All)