CIS 3362 Quiz #3: Bitwise Operators, DES, AES Solutions

Date: 10/7/2024

1) (5 pts) Explain in words what the function f (shown below) computes, in terms of the input string str. (Assume all necessary libraries are included.) **No credit will be given to a literal translation of each line of code.**

```
int f(char* str) {

    int len = strlen(str);

    int res = 0;
    for (int i=0; i<len; i+=4) {

        for (int j=0; j<4; j++)
            if (i+j<len)
                res = res ^ (str[i+j]<<(24-8*j));
    }

    return res;
}
```

It breaks the input string into blocks of 4 characters each, which can be interpreted as a 32 bit number. Each of these blocks of 4 characters are XORED together. If the last block has fewer than 4 characters, the empty characters in the block are treated as 0. The value for each character is simply its Ascii value.

Grading: 2 pts for mentioning blocks of size 4 characters.
2 pts for explaining that each block gets XORED
1 pt for addressing the last block.

2) (8 pts) Provide the output for the designated inputs for each of the four S-boxes described below. Please give your answers as **4 binary bits.** (Each answer is worth 2 pts, no partial credit, so carefully make sure you are using the correct S-box and look up the correct row and column. 1 pt for correct answers in decimal or HEX.)

(a) S_2(100111) = **0001** (row 3, col 3 S2)

(b) S_3(011111) = **0001** (ro1 1 col 15 S3)

(c) S_5(010110) = **1111** (row 0, col 11 S5)

(d) S_7(100100) = **1011** (row 2 col 2 S7)

Grading: 2 pts for correct binary answer for each part, 1 pt for correct decimal or hex answer to each part, 0 pts otherwise

3) (6 pts) Let P = [3 2 12 8 1 7 11 6 4 10 5 9] be a permutation matrix similar to the permutation matrix P in DES, which could be applied to an input of 12 bits. Consider applying P

to some input, X, over and over again. (In particular, define $P^k(X) = P(P^{k-1}(X)$, for all integers k > 1.) What is the smallest positive integer value of k for which it is guaranteed that $P^k(X) = X$ for all possible inputs X? Please show your work. Credit is for work and explanation.

Here is where each item goes (old pos new pos):

3 --> 1	1 --> 5	4 --> 9
2 --> 2	7 --> 6	10 --> 10
12 --> 3	11 --> 7	5 --> 11
8 --> 4	6 --> 8	9 --> 12

Let's Follow where the item that starts in spot one goes in multiple applications of P:
1 --> 5 --> 11 --> 7 --> 6 --> 8 --> 4 --> 9 --> 12 --> 3 --> 1 (returns back to position 1) This is a cycle length of 10.

Only items not mentioned here are 2 and 10. These are both in cycles of length 1. (They always stay in the same position no matter how many times P is applied.)

It follows that every bit in X returns to the exact same position every 10 applications of P.

k = **10**

Grading: 4 pts for mapping out cyclic movement (forward or backwards), 2 pts to use that information and come to the conclusion that the answer is 10.

4) (6 pts) In the DES Key Schedule algorithm, consider a situation where

C_{10} = 1010 1111 0011 0101 0110 1011 0001

(a) (2 pts) What is C_{11}, represented using **7 Hex characters**? **BCD5AC6**
(Show work below.)

Since LS[10] = 2, we'll do a cyclic left shift of 2 bits on what is above:
C_{11} = 10 1111 0011 0101 0110 1011 0001 10, regroup:
1011 1100 1101 0101 1010 1100 0110

(b) (4 pts) What are the first 8 bits of the **Round 10 Key, in binary**? **10111111**
(Show work below.)

Use the original C_{10}, since we're building the Round 10 key. We want the 14, 17, 11, 24, 1, 5, 3 and 28th bits respectively. These are highlighted below:

C_{10} = 1010 1111 0011 0101 0110 1011 0001
Grading: 4 pts if all correct, 3 pts if 7 bits right, 2 pts if 6 bits right, 1 pt if 5 bits right, or 0

5) (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

26	A1	74	CD

0B	57	98	F3
59	6A	7B	8C
D1	E2	4F	30

F7	**32**	**92**	**BD**
2B	**5B**	**46**	**0D**
CB	**02**	**21**	**64**
3E	**98**	**84**	**04**

Grading: 1/2 each round down to an integer (15 right = 7. 13 right = 6 etc.)

6) (10 pts) Let the state matrix to AES right before the MixCols step be the matrix shown below. What is the value of the entry in row 4, column 1, right AFTER the MixCols step? Express your answer as **2 HEX characters.** (Note: Max credit for correctly computing the wrong entry is 3 points out of 10. So be careful!!!)

CB	88	AD	63
A6	23	72	E7
B7	FF	EB	86
D2	BC	D7	2F

We need to calculate the 03xCB + 01xA6 + 01xB7 + 02xD2

```
  CB    =  1100 1011            D2 =    1101 0010
2 x CB = 11001 0110          2 x D2 = 11010 0100

3 x CB =  1100 1011          2 x D2 =  1010 0100
          1001 0110                       1 1011
             1 1011                    ----------
          ---------                     1011 1111 (BF)
          0100 0110 (46)
```

Final answer is (46 ⊕ A6) ⊕ (B7 ⊕ BF), using XOR chart we get

E0 ⊕ 08 =

E8

Grading: 4 pts for 3 x CB, 3 pts for 2 x D2, 3 pts for final XOR, automatic 0 out of 10 if wrong entry is calculated or if sum of products is wrong beyond a typo.

7) (6 pts) We spent some class time investigating multiplication in the AES field. What is the value of x^9 mod ($x^8 + x^4 + x^3 + x + 1$)? Instead of expressing your answer in HEX, **please express your answer as a polynomial of degree 7 or less.** (Note: $x^8 + x^4 + x^3 + x + 1$ is the irreducible polynomial used for AES calculations.) This exact calculation shows up somewhere in the set of AES reference tables. Where is it?

Note in the AES field $x^8 \equiv x^4 + x^3 + x + 1 \pmod{x^8 + x^4 + x^3 + x + 1}$.

It follows that $x^9 = x(x^8) \equiv x(x^4 + x^3 + x + 1)$
$\equiv x^5 + x^4 + x^2 + x \pmod{x^8 + x^4 + x^3 + x + 1}$.

The final answer is $x^5 + x^4 + x^2 + x$. This shows up in the AES table Rcon[10]. In particular, Rcon[i] equals x^{i-1} mod $x^8 + x^4 + x^3 + x + 1$. Thus, Rcon[10] is x^9 mod $x^8 + x^4 + x^3 + x + 1$, which, when rewritten in HEX, we have $x^5 + x^4 + x^2 + x = 0011\ 0110 = 36$.

Polynomial: **$x^5 + x^4 + x^2 + x$ (4 pts - 2 pts showing what x^8 is, 2 pts multiplying this by x correctly)**

Where it shows up in the AES reference sheets/tables: **Rcon[10] (1 pt for Rcon, 1 pt for index 10 or round 10)**

8) (1 pt) What type of food is the local area restaurant Island Wing Company known for?

Wings (Give to all)