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

Date: 10/7/2024

Name : _____

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;
}
```

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) $S_2(100111)$ = _____

(b) $S_3(011111)$ = _____

(c) $S_5(010110)$ = _____

(d) $S_7(100100)$ = _____

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.

k = _____

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**? _____
(Show work below.)

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

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

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

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?

Polynomial: _____

Where it shows up in the AES reference sheets/tables: _____

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

_____