CS558 Assignment 2

① Yuejing Zhu yzhu103@binghamton.edu
② Sijie Meng smeng4@binghamton.edu

1. "dfsfhoisgosidh" depth = 4
① # message letters = 14 |row| = 4
② # row = 14/4 = 3
③ # letter each row: 14%3 = 2 (1st and 2nd have 4 letter)
④ Write down:

d f s f
h o i s
g o s
i d h

⑤ Result: dhgifoodsishfs

2. Message: "dhdplakshgiskfnhgd" key: 351462
① |cipher| = 18 |key| = 6 → |row| = 3
②

3	5	1	4	6	2
k	h	d	g	p	k
s	g	h	i	l	f
h	d	d	s	a	n

③ Result: khdgpksghilfhddsan

3. $3^{302} \bmod 11 \Rightarrow$

$3^{302} \equiv 3^{30\times10+2} \pmod{11}$
$\equiv (3^{10})^{30} \cdot 3^2 \pmod{11}$
$\equiv 1^{30} \cdot 3^2 \pmod{11}$
$\equiv 9 \pmod{11}$
$\equiv 9 \pmod{11}$

So. $3^{302} \bmod 11 = 9$

4 Pair 1

① L_{i-1}: 0000000000000000 0000000000000000 R_{i-1}: 0010000000000000 0000000000000000

L_i: 0010000000000000 0000000000000000 R_i: 0011000000000000 0000000000000000

② Since L_{i-1} ⊕ Output of P Table = R_i

Output of P Table is: 0011 0000 0000 0000 0000 0000 0000 0000

③ Using P Table to get Output of S-box:

Output of S-box Table is: 0000 0000 0000 0000 0001 1000 0000 0000

④ Using S_1 to get first 6 bit of input of S-box:

$S_1 = 0000 \Longrightarrow$ Input of S_1: 011100 / 000001 / 111110 / 111011

⑤ Using R_{i-1} and E Table to get output of E Table:

The first 6 bit of output of E table is 000100

Pair 2:

① L_{i-1}: 0110000010000000 1000000000000000 R_{i-1}: 0100000000000000 0000000000000000

L_i: 0100000000000000 0000000000000000 R_i: 0110000000000000 0000000000000000

② As Pair1 ②step, Output of P Table is: 0000000010000000 1000000000000000

③ As Pair1 ③step, Output of S-box Table is: 1100 0000 0000 0000 0000 0000 0000 0000

④ As Pair1 ④step, $S_1 = 1100$

So input of S_1 has 4 passibilities: 010110 / 010101 / 110010 / 100011

⑤ As Pair1 ⑤ step. The first 6 bit of output of E-table is: 001000

In Pair ①: 000100 (XOR) $K_{i(6bit)}$ = 011100/000001/111110/111011

K_i = 011000/000101/111010/111111

In Pair ②: 001000 (XOR) $k_{i(6bit)}$ = 010110/010101/110010/100011

K_i = 011110/011101/111010/101011

So, the first 6 bits of key K_i is 111010

3. ① if S-box 2 change to different value, which means in P Table. 5 (row 1, column 4), 6 (row 3, column 3), 7 (row 0, column 1). 8 (row 2, column 1), these four position's value will be changed.

② Then in the XOR process, these four values are changed too

③ In next round, this 32 bits result will be used as a new R_{i-1}, at the same time, it's the E Table's input. So P(7) (the number at value 7's position in P Table) is put in E(2) (the number at value 2's position in E Table). So we can get:

P(7) => E(2); P(5) => E(13); P(8) => E(18); P(6) => E(29)

④ Since E(2), E(13), E(18), E(29) are located in different Six rows. And the each row's Six number correspond to a S-box. (Eg: the first 6 bit in row 1 will be the input of S-box 1)

So, the change 4 numbers will located in different six rows, which means they will affect Six different S-boxes on next round.