|cipher text| =14

14/4 =3 -> each row has at least 3 letters

14 mod 4 =2 -> 1st and 2nd rows have 3+1=4 letters

d f s f

h o i s

g o s

i d h

* dhgifoodsishfs

3 5 1 4 6 2

Tcipher =18 k h d g p k

18 /6 =3 s g h i l f

3 is # of rows h d d s a h

Output of S2 is 5 6 7 8 bits

把5 6 7 8 带入P table

找到5 6 7 8 对应的位置 数一下它们所在位置的index 是多少

5->13 : 13th bit of output of P table is the 5th bit input

6->28

7->2

8->18

13在E table 里对应第三行和第四行 ， 则得到S3 S4

同理得到 28-> s7 s8, 2 -> S1, 18->s5

(Pi , Ci)

Pi-1 = (Li-1, Ri-1)

Li-1 = 000000…00

Ri-1 = 00100…000

E(Ri-1) = 000100…000

Output of P:

Ri = 001100…00

Ri XOR Li-1 = 001100..00

Input of P: 20 & 21 are 1

First 4 bits of input are 0000 -> which means output of S1 is 0

Row 0, column 14 = 011100

Row 1, column 0 = 000001

Row 2, column 15 = 111110

Row 3, column 13 = 111011

4 possible key ; input to S1 XOR first 6 bits of output of E table

1. **011000**
2. **000101**
3. **111010**
4. **111111**

Outputs of P : 9 & 17 bits are 1, others are 0;

Input to P: 1100….00

Then first 4 bits of input to P are : 1100

So output of S1 is 1100

Then we have :

010110

010101

110010

100011

Then we have

**011110**

**011101**

**111010**

**101011**

**在加粗内容中，只有111010相同，则 111010是最后的结果**

fermat: if P is a prime and a is a positive int not divisible by P, then a­p-1 mod P =1

##fermat: 310 mod 11 =1 P =11 P-1=10 a =3

3302 mod 11 = [ (310) 30 \* 32 ] mod 11 = [ 310 mod 11 \*…\* 310  mod 11 \* 32 mod 11] mod 11

= 1\* 9 mod 11 = 9