P-Box

Key → Value	Key → Value
0 → 4	6 → 3
1 → 6	7 → 2
2 → 1	8 → 10
3 → 11	9 → 7
4 → 8	10 → 0
5 → 5	11 → 9

S-Box

Key → Value	Key → Value
0 → 4	4 → 7
1 → 2	5 → 0
2 → 6	6 → 5
3 → 1	7 → 3

Input

Plaintext : Ci20

Key 1 : 3L

Key 2 : KrT

Step 1: Conversion To Binary

①

Char	ASCII	Binary
C	67	01000011
i	105	01101001
2	97	01100001
0	48	00110000

②

Char	ASCII	Binary
3	51	00110011
L	76	01001100

③

Char	ASCII	Binary
K	75	01001011
r	114	01110010
T	84	01010100

Step 2: Padding with Zeroes by Setting a Multiple of 12

Plaintext : 01000011011010010110000100110000 (32 bit)

Key 1 : 0011001101001100 (16 bit)

Key 2 : 010010111011100100101 0100 (24 bit)

The multiple of 12 next to the maximum lenght : 36

Plaintext : 0000 01000011011010010110000100110000

Key 1 : 000000000000000000000000 0011001101001100

Key 2 : 000000000000 010010111011100100101 0100

Step 3: Xor between Plaintext and Key 1

```
000001000011011010010110000100110000
000000000000000000000000001100110100 1100
------------------------------------
000001000011011010010101001001111 1100
```

Step 4: Division into 12 bit Blocks

block 3 : 000001000011

block 2 : 011010010101

block 1 : 001001111100

Step 5: P-Box Application

block 3 : 100001000100

block 2 : 011100011100

block 1 : 011101010010

Step 6: S-Box Application

For each 12-bit block, divide into groups of 3 and apply the S-Box

block 3 : 111010010111

block 2 : 001100011111

block 1 : 001000110110

Step 7 : Xor between Key 1 and Key 2

```
000000000000000000001100111010011100
000000000000001001011011100100101000
------------------------------------
000000000000001001011010000010001000
```

Step 8 : Xor between the previous Xor and S-Box

```
000000000000001001011010000010001000
111010100111001100011111001000110110
------------------------------------
111010100111011101010110011001011110
```

Step 9 : Division into 12 bit Blocks

block 3 : 111010010111

block 2 : 011110101011

block 1 : 001100101110

Step 10: P-Box Application

block 3 : 110110111100

block 2 : 110100101111

block 1 : 110100010011

Step 11: S-Box Application

For each 12-bit block, divide into groups of 3 and apply the S-Box

block 3 : 101101011111

block 2 : 101111000011

block 1 : 101111110001

Step 12: Padding with Zeroes by Setting a Multiple of 12

Ciphertext : 101101011111101111000011101111110001 (32 bit)

multiple of 12 next to the maximum lenght : 36

Ciphertext : 000010110101111101111000011101111110001

Step 13: Final Conversion into Text

Binary	ASCII	Char
00001011	11	VT
01011111	95	_
10111100	188	¼
00111011	59	;
11110001	241	ñ