

```

1 C:\Users\haibo\dev\Study\AlgoImage\venv\Scripts\python.exe
  C:/Users/haibo/dev/Study/Cryptho/tp1.py
2 WOED [1, 1, 0, 1, 1, 0, 1, 0]
3 <module> ['KEY', [0, 1, 1, 0, 1, 0, 1, 1, 0, 0]]
4 <module> ['WORD', [1, 1, 0, 1, 1, 0, 1, 0]]
5 encrypt ['IP', [1, 0, 0, 1, 1, 0, 1, 1]]
6 generate_key ['P10', [1, 1, 1, 1, 0, 0, 0, 0, 1, 0]]
7 generate_key ['2*LS-1', [1, 1, 1, 0, 1, 0, 0, 1, 0, 0]]
8 generate_key ['P8', [0, 1, 0, 0, 1, 1, 0, 0]]
9 encrypt ['KEY1', [0, 1, 1, 0, 1, 0, 1, 1, 0, 0]]
10 generate_key ['P10', [1, 1, 1, 1, 0, 0, 0, 0, 1, 0]]
11 generate_key ['2*LS-1', [1, 1, 1, 0, 1, 0, 0, 1, 0, 0]]
12 generate_key ['2*LS-1', [1, 0, 1, 1, 1, 1, 0, 0, 0, 0]]
13 generate_key ['P8', [1, 1, 0, 1, 0, 1, 0, 0]]
14 encrypt ['KEY2', [1, 1, 0, 1, 0, 1, 0, 0]]
15 FK ['SubKEY', [0, 1, 0, 0, 1, 1, 0, 0]]
16 FK ['E/P', [[1, 1, 0, 1], [0, 1, 1, 1]]]
17 FK ['XOR(KEY1 and E/EP)', [[1, 0, 0, 1], [1, 0, 1, 1]]]
18 FK ['sboxResult', [1, 1, 0, 1]]
19 FK ['LeftBloc', [1, 0, 0, 1]]
20 FK ['P4', [1, 1, 0, 1]]
21 FK ['XOR P4', [0, 1, 0, 0]]
22 encrypt ['FK1', [0, 1, 0, 0, 1, 0, 1, 1]]
23 encrypt ['SW', [1, 0, 1, 1, 0, 1, 0, 0]]
24 FK ['SubKEY', [1, 1, 0, 1, 0, 1, 0, 0]]
25 FK ['E/P', [[0, 0, 1, 0], [1, 0, 0, 0]]]
26 FK ['XOR(KEY1 and E/EP)', [[1, 1, 1, 1], [1, 1, 0, 0]]]
27 FK ['sboxResult', [1, 0, 0, 1]]
28 FK ['LeftBloc', [1, 0, 1, 1]]
29 FK ['P4', [0, 1, 0, 1]]
30 FK ['XOR P4', [1, 1, 1, 0]]
31 encrypt ['FK2', [1, 1, 1, 0, 0, 1, 0, 0]]
32 CRYPTED [0, 1, 1, 0, 0, 1, 0, 1]
33 DECRYPTAGE -----
34 generate_key ['P10', [1, 1, 1, 1, 0, 0, 0, 0, 1, 0]]
35 generate_key ['2*LS-1', [1, 1, 1, 0, 1, 0, 0, 1, 0, 0]]
36 generate_key ['P8', [0, 1, 0, 0, 1, 1, 0, 0]]
37 decrypt ['KE2', [0, 1, 0, 0, 1, 1, 0, 0]]
38 generate_key ['P10', [1, 1, 1, 1, 0, 0, 0, 0, 1, 0]]
39 generate_key ['2*LS-1', [1, 1, 1, 0, 1, 0, 0, 1, 0, 0]]
40 generate_key ['2*LS-1', [1, 0, 1, 1, 1, 1, 0, 0, 0, 0]]
41 generate_key ['P8', [1, 1, 0, 1, 0, 1, 0, 0]]
42 decrypt ['KEY2', [1, 1, 0, 1, 0, 1, 0, 0]]
43 decrypt ['IP', [1, 1, 1, 0, 0, 1, 0, 0]]
44 FK ['SubKEY', [1, 1, 0, 1, 0, 1, 0, 0]]

```

```
45 FK ['E/P', [[0, 0, 1, 0], [1, 0, 0, 0]]]
46 FK ['XOR(KEY1 and E/EP)', [[1, 1, 1, 1], [1, 1, 0, 0]]]
47 FK ['sboxResult', [1, 0, 0, 1]]
48 FK ['LeftBloc', [1, 1, 1, 0]]
49 FK ['P4', [0, 1, 0, 1]]
50 FK ['XOR P4', [1, 0, 1, 1]]
51 decrypt ['FK1', [1, 0, 1, 1, 0, 1, 0, 0]]
52 decrypt ['SW', [0, 1, 0, 0, 1, 0, 1, 1]]
53 FK ['SubKEY', [0, 1, 0, 0, 1, 1, 0, 0]]
54 FK ['E/P', [[1, 1, 0, 1], [0, 1, 1, 1]]]
55 FK ['XOR(KEY1 and E/EP)', [[1, 0, 0, 1], [1, 0, 1, 1]]]
56 FK ['sboxResult', [1, 1, 0, 1]]
57 FK ['LeftBloc', [0, 1, 0, 0]]
58 FK ['P4', [1, 1, 0, 1]]
59 FK ['XOR P4', [1, 0, 0, 1]]
60 decrypt ['FK1', [1, 0, 0, 1, 1, 0, 1, 1]]
61 DECRYPTED [1, 1, 0, 1, 1, 0, 1, 0]
62
63 Process finished with exit code 0
64
```