

```

void encrypt(char *plain, char *cipher){
    if(!(*plain)){
        *cipher = 0;
        return;
    }

    char pad = get_pad();
    *cipher = *plain + pad;
    encrypt(plain+1, cipher+1);
}

void test(){
    char *msg = "Ark";
    char cipher[] = "-----";
    cipher[4] = '0';

    encrypt(msg, cipher);

    printf(cipher);
}

```

ebp(test)
ret(test)
* 1

le
give
haga
printf

Como sigue
la pila
luego de 41

5 20
6
mn 24
3

32 →

29 →

18 →

11 →

5 →

3 →

ebp(test)
ret(test)
* msg + 3
* 4
2
ebp(test)
ret(test)
* msg + 2
* 3
1
ebp(test)
ret(test)
* msg + 1
* 2
0
ebp(test)
ret(test)
* msg
* 1
* msg
ebp(main)
ret(main)

← 31 ← 34

← 30 ← 35

← 29

← 28

← 26

← 24 ← 36

← 23 ← 37

← 22

← 21

← 19

← 17

← 16

← 15

← 14

← 12

← 10

← 9

← 8

← 7

← 6

← 5

← 4

← 3

← 2

← 1

← 0

← 38

← 39

← 40

← 41

← 42

← 43

← 44

← 45

← 46

← 47

← 48

← 49

← 50

← 51

← 52

← 53

← 54

call GetPad
ret
Push eax

← 4 bytes →

<p> call test push ebp (main) mov ebp, esp sub esp, 12 mov [esp+4], *msg $\left\{ \begin{array}{l} \text{mov [esp+7], "-----"} \\ \text{mov [esp+11], "0"} \end{array} \right.$ $\text{push } *1$ push *msg call encrypt push ebp (test) mov ebp, esp pad $\text{mov } 1, (\underbrace{'A' + 0}_{'A'})$ $\text{push } *2$ push *msg+1 call encrypt push ebp mov ebp, esp pad $\text{mov } 2, (\underbrace{'r' + 1}_s)$ $\text{push } *3$ push *msg+2 call encrypt push ebp mov ebp, esp pad $\text{mov } 3, (\underbrace{'k' + 2}_m)$ $\text{push } *4$ </p>	<p> push *msg+3 call encrypt push ebp mov ebp, esp $\text{mov } 4, 0$ leave ret leave ret leave ret leave ret leave ret $\text{push } *1$ call printf ret leave ret </p>
---	---