

A decorative graphic on the left side of the slide consists of two overlapping parallelograms. The front one is blue and the back one is a light green. They are positioned diagonally, with the blue one partially covering the green one.

# Introduction au Reverse Engineering

# Définition







## Cuisinier

Faire une recette

Cuire le gâteau

Manger le gâteau

## Programmeur

Faire un code

Compiler le programme

Utiliser le programme



## Cuisinier

Faire une recette

Cuire le gâteau

À Partir du gâteau



## Programmeur

Faire un code

Compiler le programme

Utiliser le programme





# Compilation

Traduction du code que l'on écrit en un langage que le processeur comprendra

C'est parti pour un exemple !



# Langage C

```
1  #include "stdio.h"
2
3  int main()
4  {
5      puts("Hello world!\n");
6  }
```



## Langage C

```
1  #include "stdio.h"
2
3  int main()
4  {
5      puts("Hello world!\n");
6  }
```

## Langage Assembleur

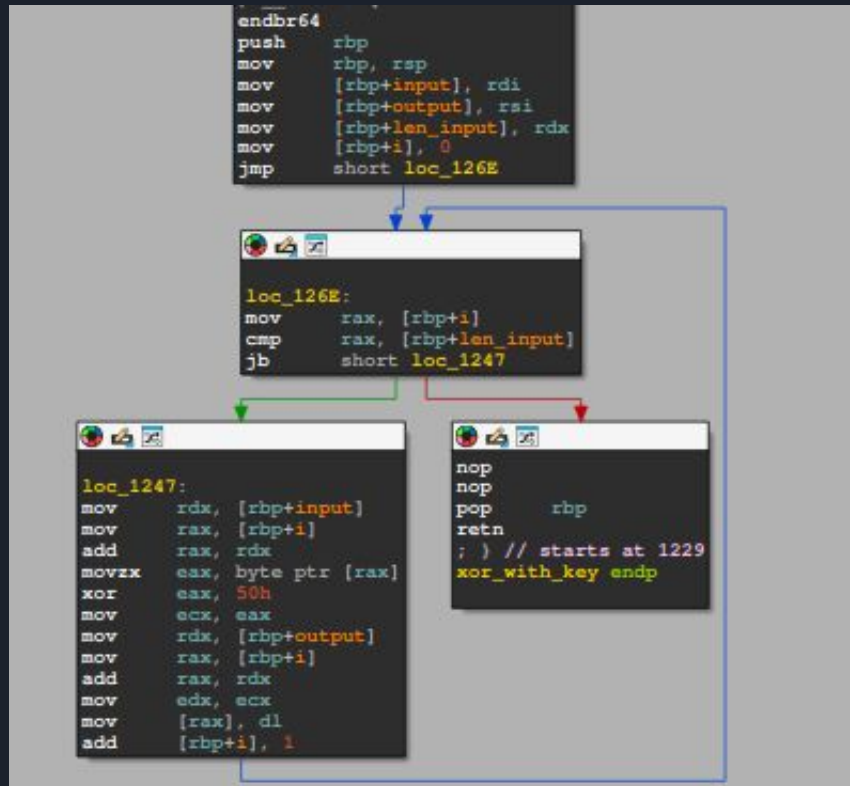
```
1  .LC0:
2      .string "Hello world!\n"
3  main:
4      push    rbp
5      mov     rbp, rsp
6      mov     edi, OFFSET FLAT:.LC0
7      call    puts
8      mov     eax, 0
9      pop     rbp
10     ret
```





Maintenant allons analyser le virus

# Fonction XOR Assembleur





Recherche d'autre élément