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

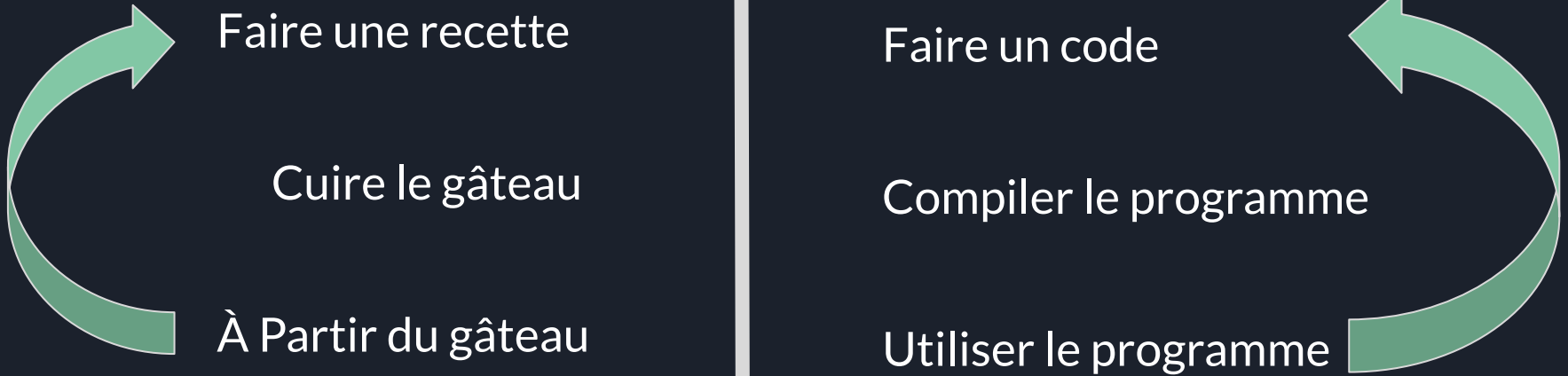
À Partir du gâteau

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

```c
#include "stdio.h"

int main()
{
        puts("Hello world!\n");
}
```

Langage C

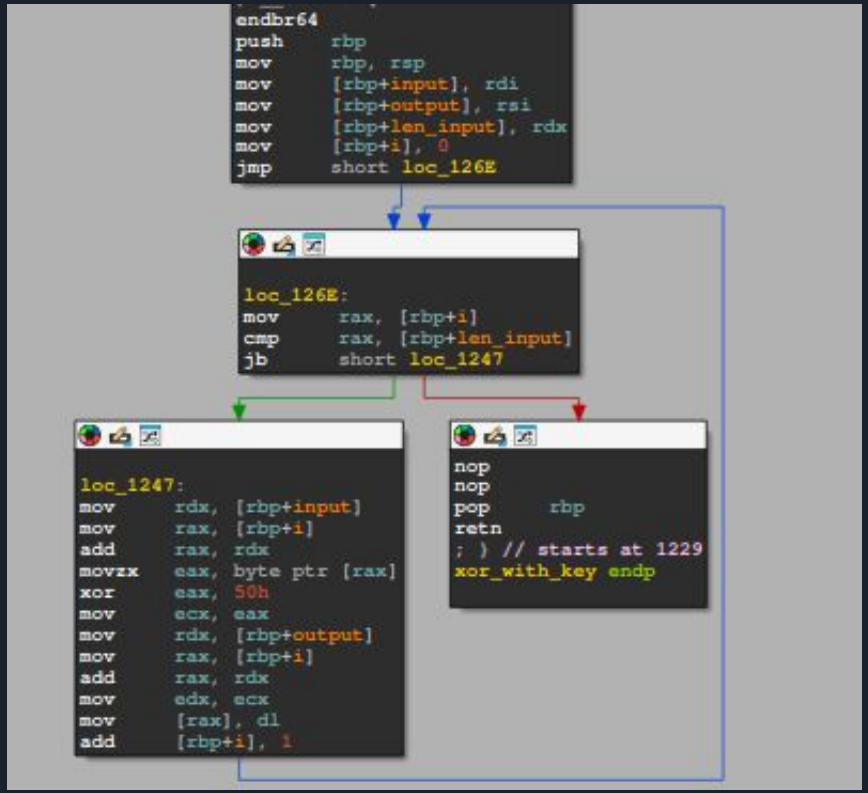
```c
#include "stdio.h"

int main()
{
        puts("Hello world!\n");
}
```

Langage Assembleur

```
.LC0:
        .string "Hello world!\n"
main:
        push    rbp
        mov     rbp, rsp
        mov     edi, OFFSET FLAT:.LC0
        call    puts
        mov     eax, 0
        pop     rbp
        ret
```

Maintenant allons analyser le virus

Fonction XOR Assembleur



Recherche d’autre élément