# 4CR - Reversing 200

El reto nos proporciona con un archivo encriptado, y un programa con el cual se encripto. El objetivo del reto es poder desencriptar el archivo, el cual suponemos que es la flag.

Podemos descompilar el programa utilizando Ghidra.

Dentro del programa, podemos ver fácilmente la clave con la cual podemos desencriptar el archivo

```
undefined4 __cdecl _KSA(int param_1)

{
  size_t sVar1;
  int local_18;
  int local_14;
  int local_10;

  sVar1 = _strlen("hackdef_command&control_key");
  local_10 = 0;
  local_14 = 0;
  while (local_14 < _range) {
    *(undefined *)(param_1 + local_14) = (char)local_14;
    local_14 = local_14 + 1;
  }
  local_18 = 0;
  while (local_18 < _range) {
    local_10 = (int)((int)"hackdef_command&control_key"[local_18 %
                     (uint)*(byte *)(param_1 + local_18) + local_10)
    _swap((undefined *)(param_1 + local_18),(undefined *)(local_10
    local_18 = local_18 + 1;
  }
  return 0;
}
```

**Con eso, y nuestra clave,2E62DD6F7BE9BDB80322DBEF52ECA8360E4E9CDABDA85D0936683EB7CE41CE91E6CCDFA433C3BB3F, podemos simplemente introducir esos valores a un programa que lo desencripte, y podemos obtener la flag, la cual es:**

**hackdef{RC4_is_c0mm0nly_used_by_m4lwar3}**