Название:	Моя первая игра
Категория:	Реверс-инжиниринг
Уровень:	Средний
Очки:	650
Описание:	Я всегда знал, что смогу создать лучшую игру на всём белом свете. И ты её не пройдёшь!
Теги:	C, Godot
Автор:	ROP

Прохождение:

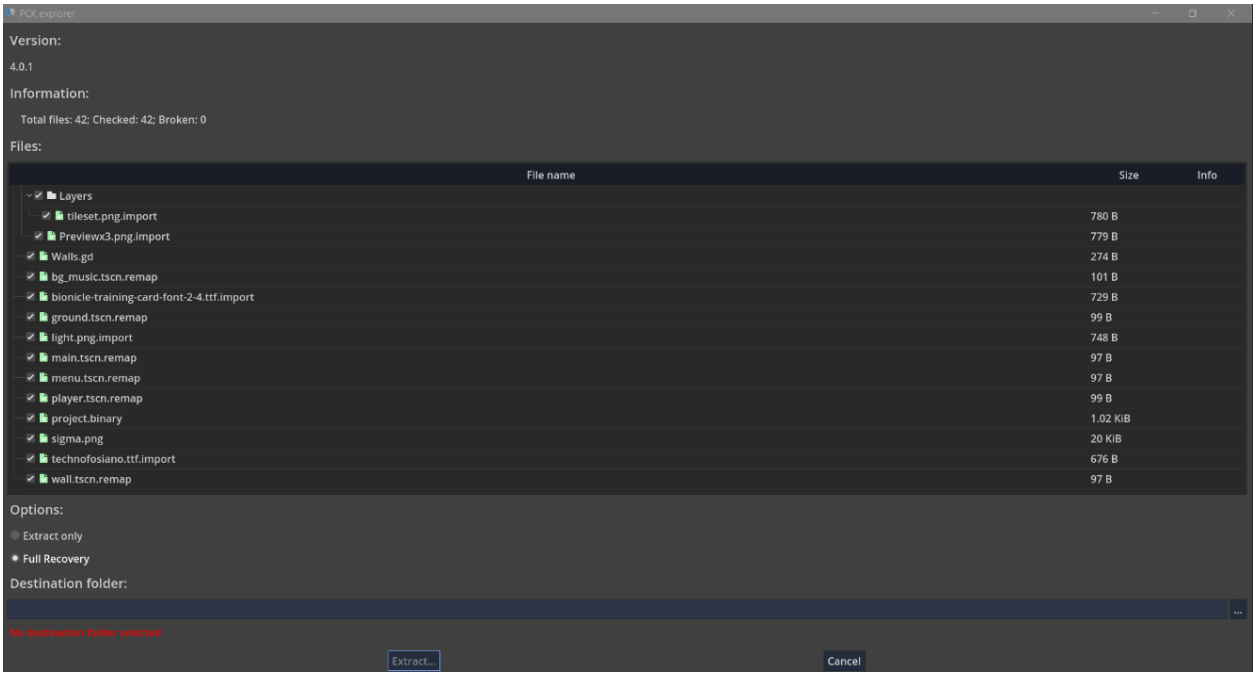
Попробуем запустить файл.

Запускаем файл.

Видим клон игры Flappy Birds. Её цель - "набить" 0xCDB очков в счёте (score). Если даже мы это сделаем, то нам просто дадут подсказку, что дальше нам нужно декомпилировать игру.

Она написана на движке Godot, поэтому юзаем https://github.com/bruvzg/gdsdecomp

Декомпилируем.



Нам нужно определиться, что делать дальше. Ищем информацию в godot-скриптах.

Ground.gd: `# The size of the required file is about 20 KB` Player.gd: `# Use this key: "SupEr_S2crET_C0deBY_X0r_Key" <https://cyberchef.org/#recipe=XOR(%7B'option':'UTF8','string':''%7D,'Standard',true)>`

Ищем файл размером в 20 Кбайт.

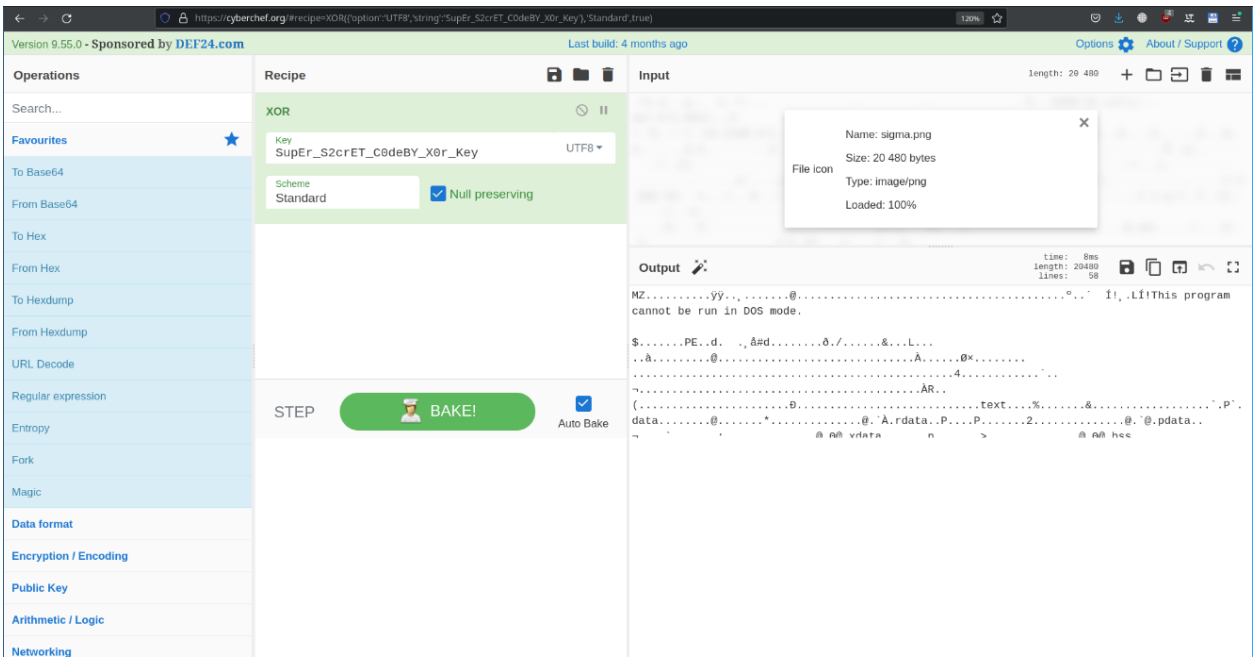
```
drwxrwxr-x 2 mogen mogen 4,0K мар 29 23:01  .assets
-rwxrwxr-x 1 mogen mogen  220 мар 29 23:01  bg_music.tscn
-rwxrwxr-x 1 mogen mogen  729 мар 29 23:01  bionicle-training-card-font-2-4.ttf.import
-rwxrwxr-x 1 mogen mogen 4,2K мар 29 23:01  BirdSpriteBig.png
-rwxrwxr-x 1 mogen mogen  772 мар 29 23:01  BirdSpriteBig.png.import
-rwxrwxr-x 1 mogen mogen  18K мар 29 23:01  CODEBY_Монтажная-область-1.ico
-rwxrwxr-x 1 mogen mogen 4,7K мар 29 23:01 'CODEBY_Монтажная область 1.svg'
-rwxrwxr-x 1 mogen mogen  957 мар 29 23:01 'CODEBY_Монтажная область 1.svg.import'
-rwxrwxr-x 1 mogen mogen 3,2K мар 29 23:01  Decors.png
-rwxrwxr-x 1 mogen mogen  750 мар 29 23:01  Decors.png.import
drwxrwxr-x 2 mogen mogen 4,0K мар 29 23:01  flameshor
-rwxrwxr-x 1 mogen mogen 3,3K мар 29 23:01  gdre_export.log
drwxrwxr-x 4 mogen mogen 4,0K мар 29 23:01  .godot
-rwxrwxr-x 1 mogen mogen  321 мар 29 23:01  Ground.gd
-rwxrwxr-x 1 mogen mogen  11K мар 29 23:01  ground.tscn
-rwxrwxr-x 1 mogen mogen 239K мар 29 23:01  light.png
-rwxrwxr-x 1 mogen mogen  748 мар 29 23:01  light.png.import
-rwxrwxr-x 1 mogen mogen 7,1K мар 29 23:01  main.tscn
-rwxrwxr-x 1 mogen mogen  380 мар 29 23:01  Menu.gd
-rwxrwxr-x 1 mogen mogen 4,9K мар 29 23:01  menu.tscn
drwxrwxr-x 2 mogen mogen 4,0K мар 29 23:01  Music
-rwxrwxr-x 1 mogen mogen 1,9K мар 29 23:01  Player.gd
-rwxrwxr-x 1 mogen mogen 3,4K мар 29 23:01  player.tscn
-rwxrwxr-x 1 mogen mogen 666K мар 29 23:01  Preview_blur.jpg
-rwxrwxr-x 1 mogen mogen  769 мар 29 23:01  Preview_blur.jpg.import
-rwxrwxr-x 1 mogen mogen 1,1K мар 29 23:01  project.godot
-rwxrwxr-x 1 mogen mogen  20K мар 29 23:01  sigma.png
drwxrwxr-x 3 mogen mogen 4,0K мар 29 23:01 'Tall Forest Files'
-rwxrwxr-x 1 mogen mogen  676 мар 29 23:01  technofosiano.ttf.import
-rwxrwxr-x 1 mogen mogen  274 мар 29 23:01  Walls.gd
-rwxrwxr-x 1 mogen mogen 2,6K мар 29 23:01  wall.tscn
/tmp/12 ❯                                                                23:31:57
```

Кажется, это он. Смотрим в HexDump.

```
00000000  1e 2f e0 00 71 00 00 00  67 00 00 00 a0 bc 00 00  |./..q...g.......|
00000010  dd 00 00 00 00 00 00 00  0b 00 00 00 00 00 00 00  |................|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000030  00 00 00 00 00 00 00 00  00 00 00 00 d3 00 00 00  |................|
00000040  4b 4b e5 4d 00 d0 6c 8f  78 e7 59 7c bf 7e 1f 0d  |KK.M..l.x.Y|.~..|
00000050  10 20 55 70 37 1d 38 21  53 0e 52 26 35 31 2d 5f  |. Up7.8!S.R&51-_|
00000060  10 45 20 3c 7f 2a 45 1c  7f 22 0b 59 17 3a 23 65  |.E <.*E..".Y.:#e|
00000070  1f 30 37 57 4d 7f 48 5e  7b 00 00 00 00 00 00 00  |.07WM.H^{.......|
00000080  08 75 00 00 2f e3 70 00  cd 95 66 16 00 00 00 00  |.u../.p...f.....|
00000090  00 00 00 00 b3 00 4b 67  49 5b 5d 46 00 54 00 00  |......KgI[]F.T..|
000000a0  00 35 00 00 00 4f 00 00  b3 26 00 00 00 44 00 00  |.5...O...&...D..|
000000b0  00 00 25 00 00 00 00 00  00 4f 00 00 00 51 00 00  |..%......O...Q..|
000000c0  41 00 00 00 00 00 00 00  51 00 41 00 00 00 00 00  |A.......Q.A.....|
000000d0  00 98 00 00 00 4f 00 00  8b a2 00 00 71 00 00 00  |.....O......q...|
000000e0  00 00 65 00 00 00 00 00  00 52 00 00 00 00 00 00  |..e......R......|
000000f0  00 00 69 00 00 00 00 00  00 43 00 00 00 00 00 00  |..i......C......|
00000100  00 00 00 00 52 00 00 00  00 00 00 00 00 00 00 00  |....R...........|
00000110  00 d5 00 00 67 3a 00 00  00 00 00 00 00 00 00 00  |....g:..........|
00000120  00 3f 00 00 de 5d 00 00  00 00 00 00 00 00 00 00  |.?...]..........|
00000130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000150  9f 11 00 00 4d 00 00 00  00 00 00 00 00 00 00 00  |....M...........|
00000160  00 00 00 00 00 00 00 00  7e d7 00 00 93 31 00 00  |........~....1..|
00000170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000180  00 00 00 00 00 00 00 00  1e 10 65 3a 2d 00 00 00  |..........e:-...|
00000190  6a 7a 00 00 00 43 00 00  00 54 00 00 00 67 00 00  |jz...C...T...g..|
000001a0  00 00 00 00 00 00 00 00  00 00 00 00 3f 00 35 19  |............?.5.|
000001b0  7d 11 11 31 13 00 00 00  00 7a 00 00 00 03 00 00  |}..1.....z......|
```

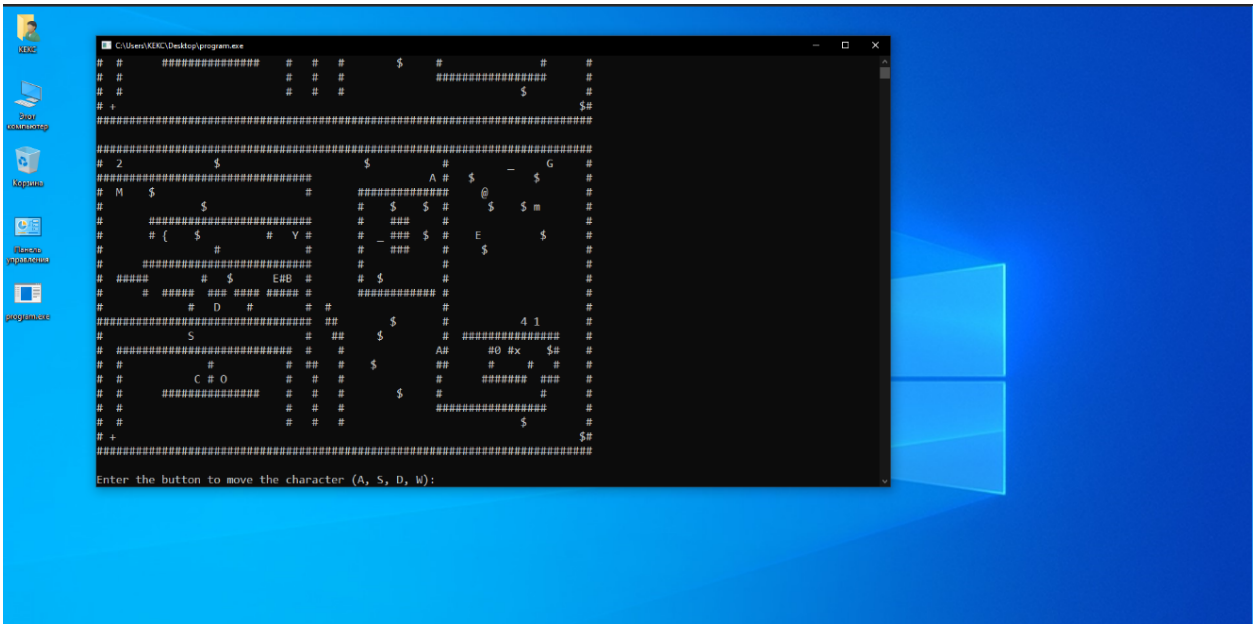
Видимо, он зашифрован.

Идём на https://cyberchef.org/#recipe=XOR({'option':'UTF8','string':''},'Standard',true) из подсказки выше. Передаём наш файл и ключ.



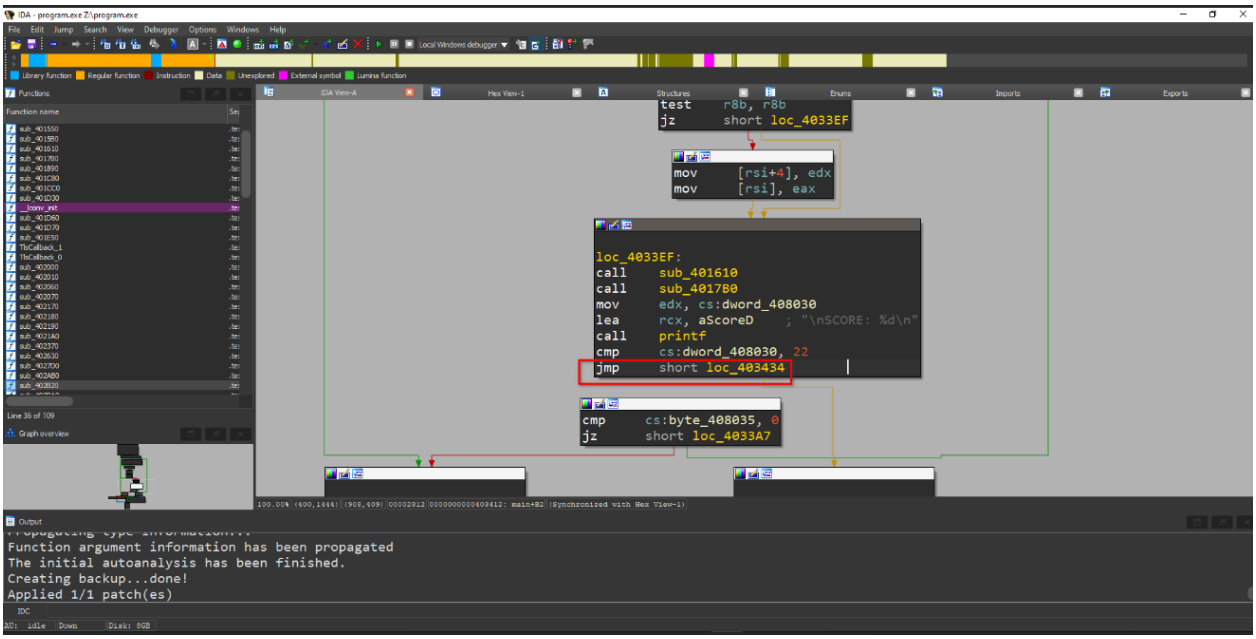
Бинго!

Скачиваем новый EXE. Запускаем новый EXE.

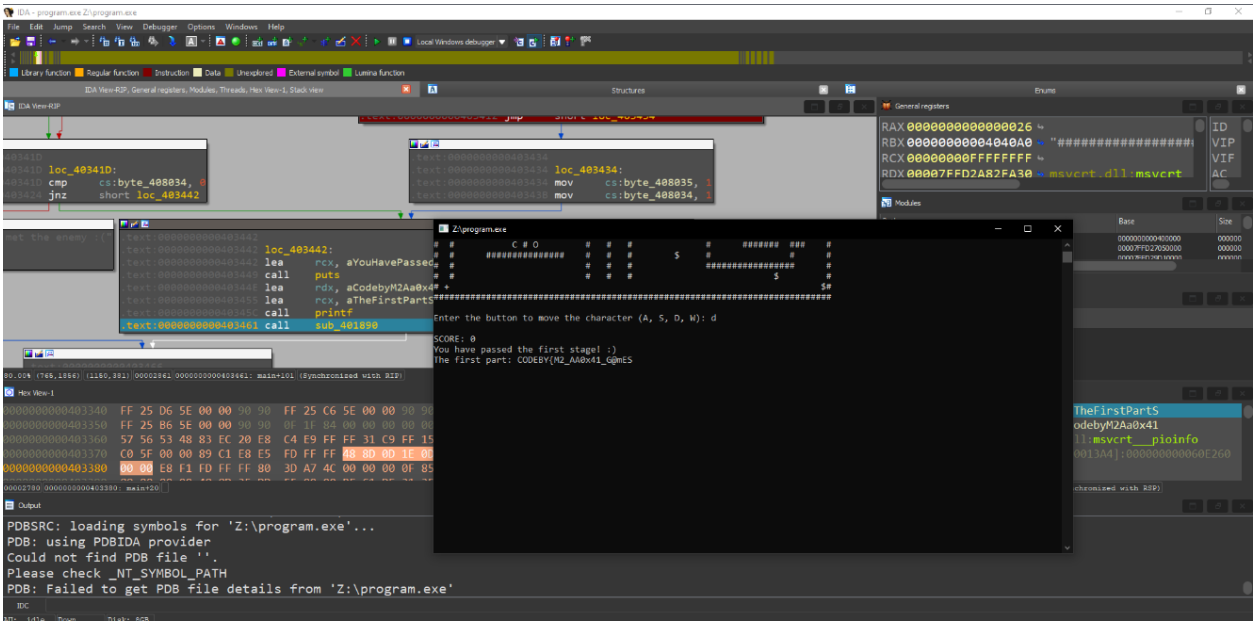


Видим какой-то лабиринт.

Изучив программу в IDA, через патчинг или Cheat Engine меняем score на нужное значение - 22.



Пример патча.



Первая часть флага: `CODEBY{M2_AA0x41_G@mES`

Теперь нам нужно ввести вторую часть. Ревёрсим код функции, которая проверяет введённую вторую часть. После реверса восстанавливаем её и собираем в флаг.