

Author: ByridianBlack

Challenge Won: April 18<sup>th</sup>, 2022

Author of Challenge: Danofred

Source of Challenge: Crackmes.one

Level of Difficulty: Easy

Challenge Link: <https://crackmes.one/crackme/624700c033c5d42a191a5a7e>

This challenge was simple, but I put a constraint on myself that I would not patch the binary in any way to make it more difficult for me to solve and force me to analyze the code to determine how to solve it. Let us get into it!

The challenge takes in a person's name which can be anywhere between 4 and 9 characters long and then asks for a serial number which is then copied into a 30-character buffer.

---

```
v5 = 0;
((void (__fastcall *)(__int64, __int64))print_header)(a1, a2);
printf("Enter your name : ");
scanf_s("%s", v10);
if ( (int)strlen((__int64)v10) <= 4 || (int)strlen((__int64)v10) > 10 )
    exit_with_error("min 4 characters and max 10 characters\n");
printf("Enter your serial key here : ");
scanf_s("%s", Buf1);
```

The program then calls a function called gen, short for generator. Reverse engineering the code showed that it was generating the same 5-character string every time during its execution, being "hijkl". This string is then added to the end of a Destination buffer, but this destination buffer contains the first 5 elements of your name.

```

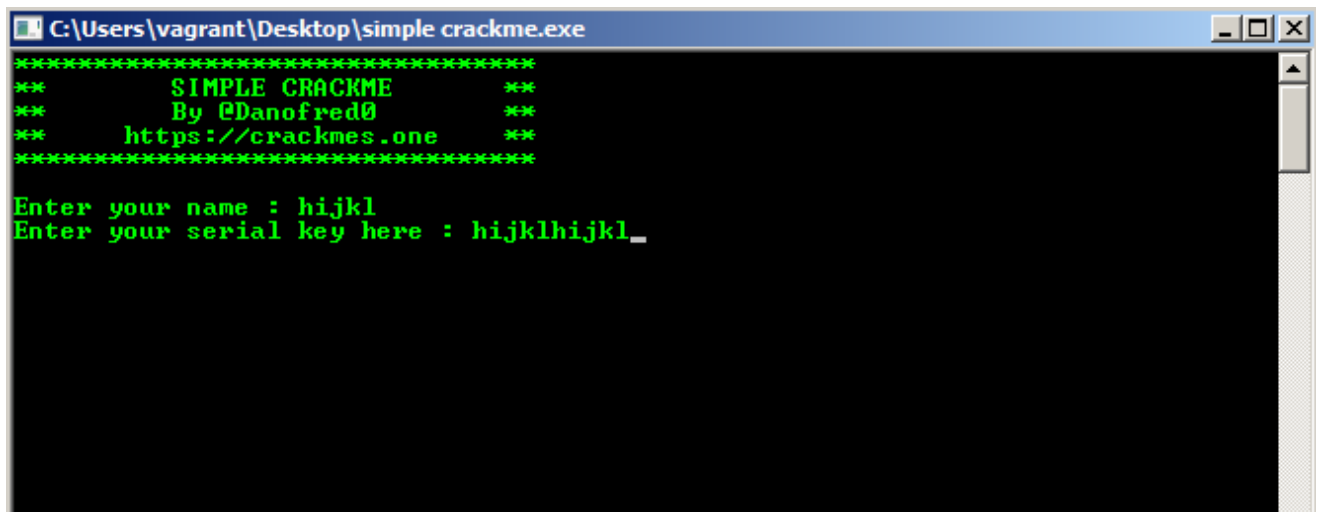
__int64 __fastcall gen(__int64 a1, unsigned __int64 a2)
{
    __int64 result; // rax
    _BYTE v3[25]; // [rsp+20h] [rbp-20h] BYREF
    char v4; // [rsp+3Bh] [rbp-5h]
    unsigned int i; // [rsp+3Ch] [rbp-4h]

    qmemcpy(v3, "abcdefghijklmopqrstuvwxyz", sizeof(v3));
    for ( i = 0; ; ++i )
    {
        result = i;
        if ( a2 <= i )
            break;
        v4 = (char)(v3[i] ^ key) % (int)strlen((__int64)v3);
        *(_BYTE *)(i + a1) = v3[v4];
    }
    return result;
}

```

This is then compared with the serial number provided. What is being compared is (<name><hijkl>) and (<serial number>). Since I know that the first part of the name should be hijkl, I want to input hijkl as the name so that what will be compared will be “hijklhijkl.” Then the serial number should be inputted as “hijklhijkl.”

Correct: When correct the program just executes



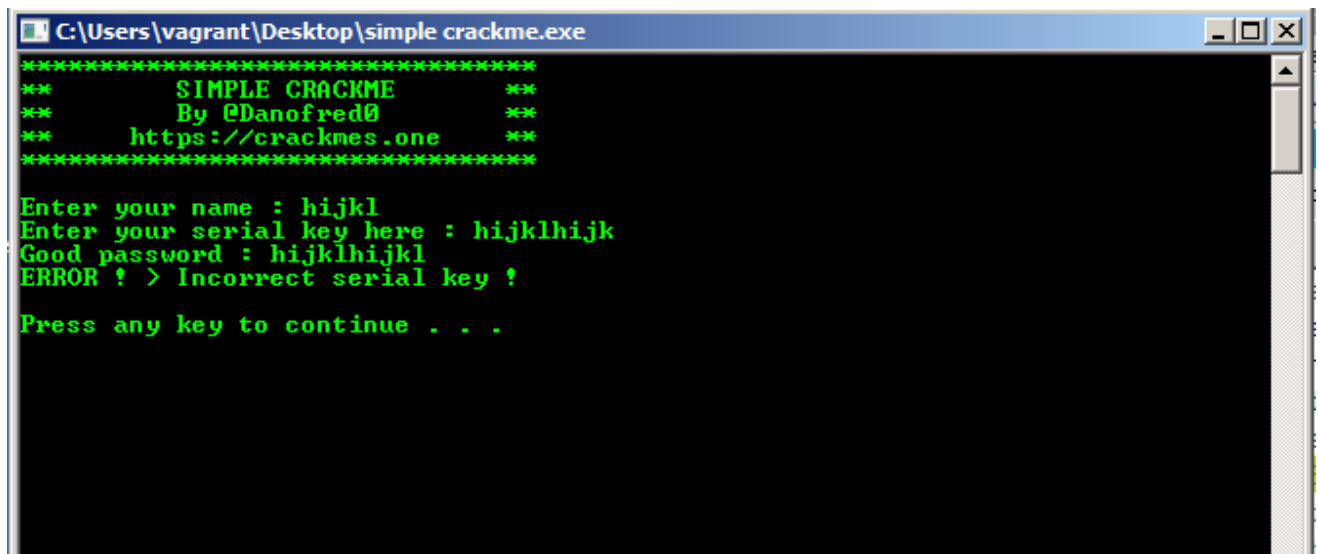
```

C:\Users\vagrant\Desktop\simple crackme.exe
*****
**      SIMPLE CRACKME      **
**      By @Danofred0      **
**      https://crackmes.one  **
*****

Enter your name : hijkl
Enter your serial key here : hijklhijkl_

```

Incorrect:



```
C:\Users\vagrant\Desktop\simple crackme.exe
*****
**      SIMPLE CRACKME      **
**      By @Danofred0      **
**      https://crackmes.one  **
*****

Enter your name : hijkl
Enter your serial key here : hijklhijk
Good password : hijklhijkl
ERROR ! > Incorrect serial key !
Press any key to continue . . .
```

Tools Used:

1. IDA Pro
2. X64dbg