ZED-frequency

Phân tích file với IDA

```
12  if ( argc <= 1 )
13  {
14    printf("usage: %s <keyfile>\n", *argv);
15    exit(1);
16  }
17  stream = fopen(argv[1], "rt");
18  for ( i = 0; i <= 25; ++i )
19    v8[i] = 0;
20  while ( 1 )
21  {
22    v5 = fgetc(stream);
23    if ( v5 == -1 )
24      break;
25    if ( v5 <= 96 || v5 > 122 )
26    {
27      if ( v5 > 64 && v5 <= 90 )
28        ++v8[v5 - 65];
29    }
30    else
31    {
32      ++v8[v5 - 97];
33    }
34  }
35  printf("the generated key is: ");
36  for ( j = 0; j <= 25; ++j )
37  {
38    printf("%d", (unsigned int)v8[j]);
39    s1[j] = LOBYTE(v8[j]) + 48;
40  }
41  s1[26] = 0;
42  putchar(10);
43  if ( !strcmp(s1, "01234567890123456789012345") )
44    puts("you succeed!!");
45  else
46    puts("you failed!!");
47  return 0;
48}
```

Đầu tiên chương trình mở một file có đường dẫn từ argv[1], sau đó tạo mảng v8 gồm 26 giá trị bằng 0.

Mục tiêu của chúng ta là sau vòng lặp while thì chuỗi s1 = "01234567890123456789012345". Chuỗi s1 được tạo thành từ việc chuyển các giá trị của mảng v8 thành chữ số và nối lại với nhau (s[j] = LOBYTE(v8[j]) + 48

Tiến đến vòng lặp while, vòng này sẽ lặp cho đến hết file, mỗi lần lấy 1 kí tự a, và sẽ tăng giá trị tại v8[thứ tự của a trong ascii] lên 1.

Vậy để tạo mảng phù hợp, ta cần tăng các giá trị trong mảng v[8] chính xác số lần như sau:

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, 1, 2, 3, 4, 5

Để tăng vị trí v8[1] 1 lần, ta cần 1 kí tự ‘b’, v8[2] 2 lần cần 2 kí tự ‘c’. Cứ thế ta tìm được chuỗi cần tìm.

```
>>> weight = [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, 1, 2, 3, 4, 5]
>>> for i in range(len(weight)):
...     print(chr(ord('a') + i) * weight[i], end='')
... else:
...     print()
...
bccdddeeeeffffffgggggghhhhhhhiiiiiiiijjjjjjjjjlmmnnnooooppppppqqqqqqrrrrrrrsssssssstttttttttvwwxxxyyyyzzzzz
```

Chuỗi keyfile là:
bccdddeeeeffffffgggggghhhhhhhiiiiiiiijjjjjjjjjlmmnnnooooppppppqqqqqqrrrrrrrsssssssstttttttttvwwxxxyyyyzzzzz

```
┌──(kali㉿DESKTOP-6TCCJEL)-[/mnt/c/Users/BILL/Desktop/Release_3/ZED-frequency]
└─$ echo "bccdddeeeeffffffgggggghhhhhhhiiiiiiiijjjjjjjjjlmmnnnooooppppppqqqqqqrrrrrrrsssssssstttttttttvwwxxxyyyyzzzzz" > keyfile
┌──(kali㉿DESKTOP-6TCCJEL)-[/mnt/c/Users/BILL/Desktop/Release_3/ZED-frequency]
└─$ cat keyfile
bccdddeeeeffffffgggggghhhhhhhiiiiiiiijjjjjjjjjlmmnnnooooppppppqqqqqqrrrrrrrsssssssstttttttttvwwxxxyyyyzzzzz
┌──(kali㉿DESKTOP-6TCCJEL)-[/mnt/c/Users/BILL/Desktop/Release_3/ZED-frequency]
└─$ ./ZED-Frequency.bin keyfile
the generated key is: 01234567890123456789012345
you succeed!!
```