Lab

4

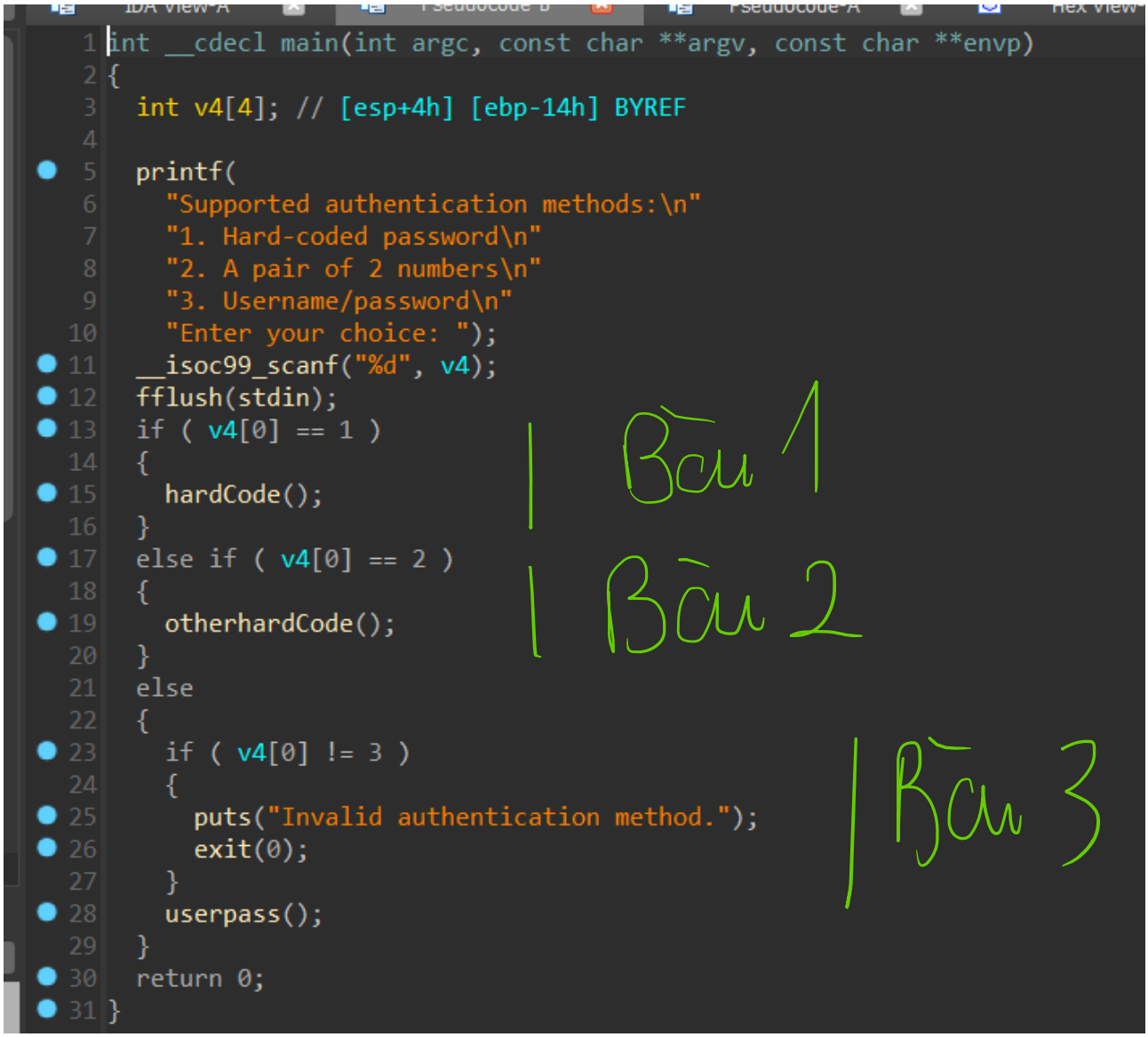
BÁO CÁO BÀI THỰC HÀNH SỐ 4

Kỹ thuật dịch ngược

Môn học: Lập trình hệ thống

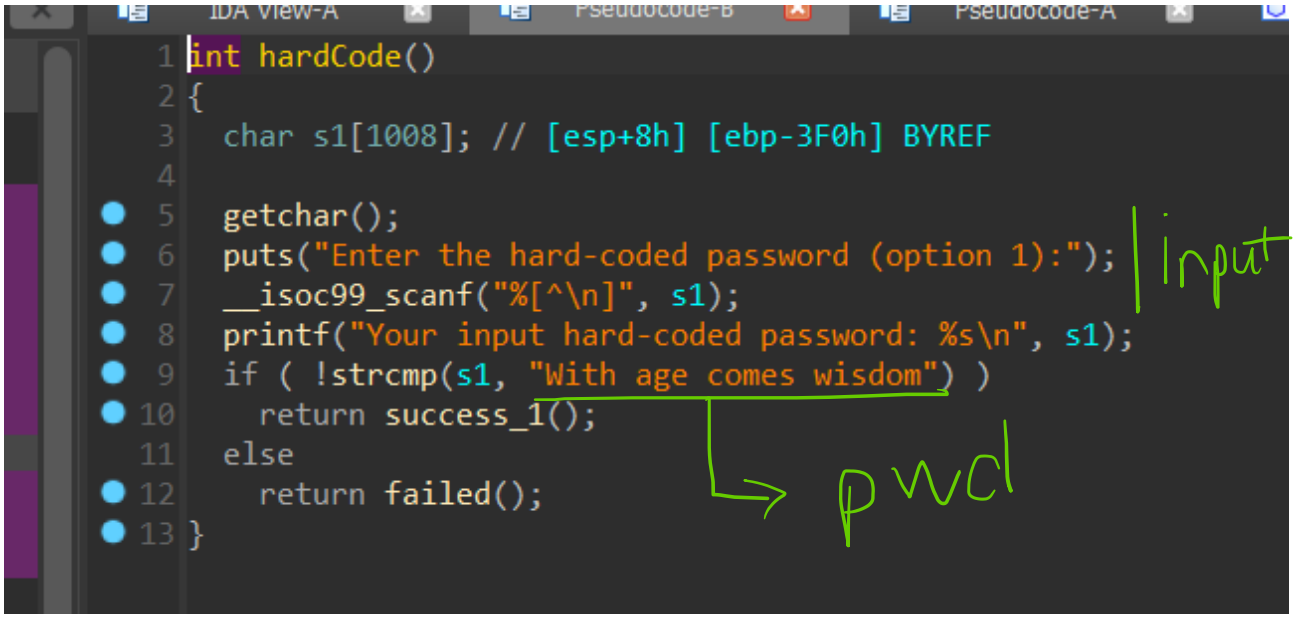
Giảng viên hướng dẫn	ThS. Đỗ Thị Hương Lan
Sinh viên thực hiện	Nguyễn Tuấn Phát (22521076) Đặng Chí Thịnh (22521399) Trần Hoàng Tuấn Kiệt (22520724)
Mức độ hoàn thành	Hoàn thành (3/3)

- Khi đưa file “basic-reverse” vào ida và decompile hàm main dưới dạng “pseudo code” ta được:



- Bấm vào từng hàm ta sẽ coi được các hàm được thực thi thế nào:

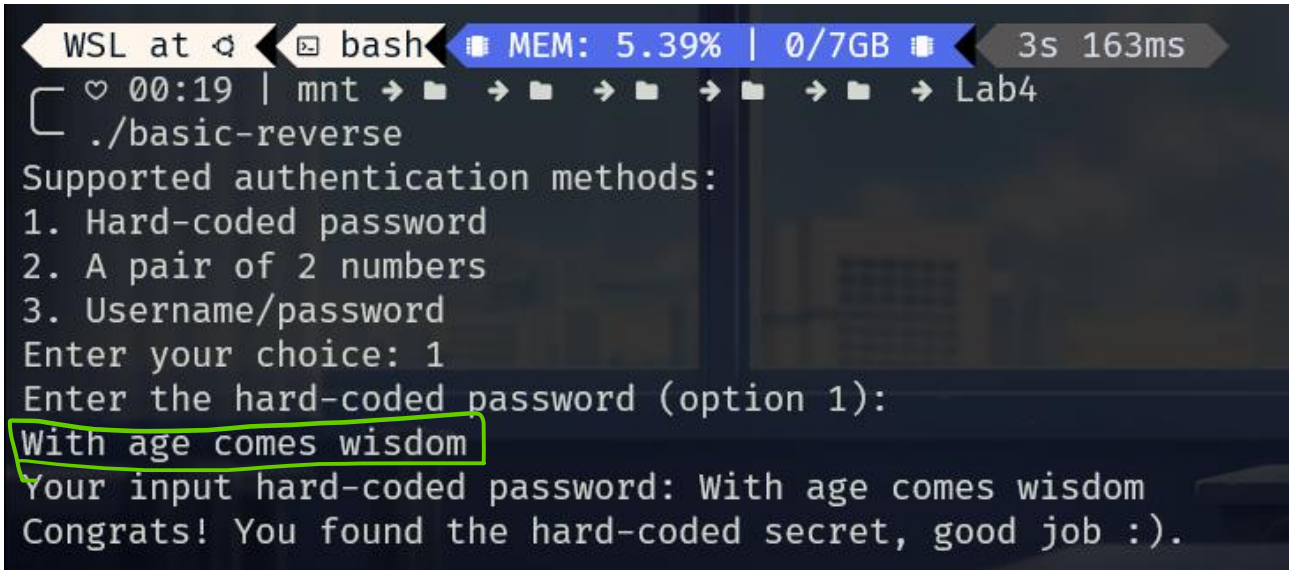
- Bài 1:



- function sẽ kiểm tra input nhập vào so với string “With age comes wisdom” bằng strcmp, khi 2 string bằng nhau trả về 0, ngược lại != 0.

=> password: “With age comes wisdom”

- Minh chứng:



- Bài 2:

```
1  int otherhardCode()
2  {
3    int v0; // edx
4    int v2; // [esp+4h] [ebp-14h] BYREF
5    int v3[4]; // [esp+8h] [ebp-10h] BYREF
6
7    getchar();
8    puts("Enter your 2 numbers (separated by space) (option 2):");
9    __isoc99_scanf("%d %d", v3, &v2);
10   printf("Your input: %d %d\n", v3[0], v2);
11   v3[1] = 9;
12   if ( v3[0] == 9 && (v0 = funny_func(9, funny_seq[9]), v0 == v2) )
13     return success_2();
14   else
15     return failed();
16 }
```

input

- Hàm của bài 2 sẽ nhập vào 2 số, và so sánh 2 số đó với các số khác trong hàm, nếu bằng thì trả về success.
- Phân tích dòng code kiểm tra điều kiện if ta biết được:
+ Số đầu tiên nhập vào phải = 9 :

```
v3[0] == 9
```

+ Số thứ 2 bằng 1 số nào đó = funny_func(9, funny_seq[9])

```
(v0 = funny_func(9, funny_seq[9]), v0 == v2)
```

- Phân tích hàm "funny_func()": hàm này sẽ lấy 2 giá trị a1, a2. Ở đây a1 == 9, a2 == funny_seq[9], và trả về kết quả của phép toàn: a1 * (a1 + a2) + a2, qua đó ta tính được số thứ 2 cần nhập vào.

```
1  int __cdecl funny_func(int a1, int a2)
2  {
3    return a1 * (a1 + a2) + a2;
4  }
```

- Phân tích funny_seq[9]: ta biết được funny_seq là mảng gồm có độ dài 10, mỗi phần tử có kiểu Int, nhìn vào data dưới đây ta biết được funny_seq[9] = 8

```
.rodata:08048B60 ; int funny_seq[10]
.rodata:08048B60 funny_seq       dd 0Ah                  ; DATA XREF: otherhardCode+5D↑r
.rodata:08048B64                 db   3
.rodata:08048B65                 db   0
.rodata:08048B66                 db   0
.rodata:08048B67                 db   0
.rodata:08048B68                 db   6
.rodata:08048B69                 db   0
.rodata:08048B6A                 db   0
.rodata:08048B6B                 db   0
.rodata:08048B6C                 db   9
.rodata:08048B6D                 db   0
.rodata:08048B6E                 db   0
.rodata:08048B6F                 db   0
.rodata:08048B70                 db   1
.rodata:08048B71                 db   0
.rodata:08048B72                 db   0
.rodata:08048B73                 db   0
.rodata:08048B74                 db   4
.rodata:08048B75                 db   0
.rodata:08048B76                 db   0
.rodata:08048B77                 db   0
.rodata:08048B78                 db   7
.rodata:08048B79                 db   0
.rodata:08048B7A                 db   0
.rodata:08048B7B                 db   0
.rodata:08048B7C                 db   2
.rodata:08048B7D                 db   0
.rodata:08048B7E                 db   0
.rodata:08048B7F                 db   0
.rodata:08048B80                 db   5
.rodata:08048B81                 db   0
.rodata:08048B82                 db   0
.rodata:08048B83                 db   0
.rodata:08048B84                 db   8
.rodata:08048B85                 db   0
.rodata:08048B86                 db   0
.rodata:08048B87                 db   0
.rodata:08048B88 aYouScratchMyBa db 'You scratch my back and I',27h,'ll scratch yours',0
```


- Quay lại hàm funny_func, ta thay a1 = 9 và a2 = 8 vào,hàm sẽ trả về giá trị **161**
<u>=> 2 số cần nhập vào là 9 và 161</u>

<u>- Minh chứng:</u>

```
WSL at  bash  MEM: 5.63% | 0/7GB  1s 507ms
 ♡ 00:28 | mnt → ■ → ■ → ■ → ■ → ■ → Lab4
 ./basic-reverse
Supported authentication methods:
1. Hard-coded password
2. A pair of 2 numbers
3. Username/password
Enter your choice: 2
Enter your 2 numbers (separated by space) (option 2):
9 161
Your input: 9 161
Congrats! You found a secret pair of numbers :).
```

- Bài 3:

```
1  int userpass()
2  {
3    size_t username_length; // ebx
4    long double res; // fst7
5    size_t username_length_2; // eax
6    size_t username_length_3; // edx
7    char newStr[9]; // [esp+1Ah] [ebp-2Eh]
8    char password[10]; // [esp+23h] [ebp-25h] BYREF
9    char username[10]; // [esp+2Dh] [ebp-1Bh] BYREF
10   char someRandomString[5]; // [esp+37h] [ebp-11h] BYREF
11   int i; // [esp+3Ch] [ebp-Ch]
12
13   qmemcpy(someRandomString, "cRVlg", sizeof(someRandomString));
14   getchar();
15   puts("Enter your username:");
16   __isoc99_scanf("%[^\n]", username);
17   getchar();
18   puts("Enter your password:");
19   __isoc99_scanf("%[^\n]", password);
20   printf("Your input username: %s and password: %s\n", username, password);
21   if ( strlen(username) != 9 )
22     return failed();
23   username_length = strlen(username);
24   if ( username_length != strlen(password) )
25     return failed();
26   for ( i = 0; i <= 8; ++i )
27   {
28     if ( i > 1 )
29     {
30       if ( i > 3 )
31         newStr[i] = someRandomString[8 - i];
32       else
33         newStr[i] = username[i + 2];
34     }
35     else
36     {
37       newStr[i] = username[i + 5];
38     }
39   }
40   for ( i = 0; ; ++i )
41   {
42     username_length_2 = strlen(username);
43     if ( username_length_2 <= i )
44       break;
45     res = ceil(((username[i] + newStr[i]) / 2));
46     if ( password[i] != res )
47       break;
48   }
49   username_length_3 = strlen(username);
50   if ( username_length_3 == i )
51     return success_3();
52   else
53     return failed();
54 }
```

declare variables

input username

input pwd

checking input's len

1st for loop

2nd for loop

checking pwd

- **Phân tích qua hàm của bài 3**, ta thấy có vài biến quan trọng: someRandomString, newStr và res.

+ someRandomString: có giá trị là "cRVlg" sau khi được gán giá trị ở dòng 12, dùng trong vòng for đầu để gen ra một string mới dùng cho vòng for thứ hai.

+ newStr: string nhận được sau khi chạy hết vòng for đầu tiên

+ res: để so sánh với từng kí tự trong password nhập vào

- Dòng 21-25, kiểm tra độ dài của 2 input, ta thấy được username và pwd đều phải có độ dài là 9.

```
21  if ( strlen(username) != 9 )
22    return failed();
23  username_length = strlen(username);
24  if ( username_length != strlen(password) )
25    return failed();
```

- Phân tích vòng for đầu tiên: ta chuyển dòng code sang python để tính newStr:

```
26  for ( i = 0; i <= 8; ++i )
27  {
28    if ( i > 1 )
29    {
30      if ( i > 3 )
31        newStr[i] = someRandomString[8 - i];
32      else
33        newStr[i] = username[i + 2];
34    }
35    else
36    {
37      newStr[i] = username[i + 5];
38    }
39  }
```

```
1   username = input("---> Enter your username: ")
2   # username = "399076724"
3
4   randomStr = "cRVlg" # random string
5   newStr = ''
6
7   for i in range(0, len(username)):
8       if i > 1:
9           if i > 3:
10              newStr += randomStr[8-i]
11          else:
12              newStr += username[i+2]
13      else:
14          newStr += username[i+5]
15
16  print("(+) New generated string: " + newStr)
```

- Chạy file python với username: “399076724” ta sẽ có được **newStr = “6776glVRc”**

```
PS D:\Mon hoc\HK4\LTHT\SystemProgramming\Lab4> python -u "d:\Mon hoc\HK4\LTHT\SystemProgramming\Lab4\pwd_gen.py"
---> Enter your username: 399076724
(+) New generated string: 6776glVRc
```

- Phân tích vòng for thứ 2 và kiểm tra pwd:

```
40  for ( i = 0; ; ++i )
41  {
42    username_length_2 = strlen(username);
43    if ( username_length_2 <= i )
44      break;
45    res = ceil(((username[i] + newStr[i]) / 2));
46    if ( password[i] != res )
47      break;
48  }
49  username_length_3 = strlen(username);
50  if ( username_length_3 == i )
51    return success_3();
52  else
53    return failed();
```

+ Trong vòng for (40-48): i sẽ chạy từ 0 đến 8 (= username_length), qua từng vòng for, hàm sẽ tính ra giá trị “res” = *ceil((username[i] + newStr[i]) / 2)*, ở đây *(username[i] + newStr[i])* sẽ tính tổng 2 kí tự thứ i của 2 string username và newStr sau khi chuyển thành int, nên phép chia / 2 sẽ là phép chia lấy nguyên.

=> nên res có thể rút gọn lại thành: *res = (username[i] + newStr[i]) / 2*, sau đó sẽ kiểm tra res với password[i], nếu khác thì sẽ thoát khỏi vòng lặp for

+ Kiểm tra pwd (49-53): kiểm tra nếu i == 9, nếu đúng trả về success, ngược lại failed. Vậy để i == 9 thì i cần chạy từ 0 đến 9 và break ở dòng 44. Để nó xảy ra được thì với **0 <= i <= 8 thì *password[i] == res_i.*** Vậy để tính được đúng password, ta sẽ thay đổi vài dòng code ở cuối vòng for, thay vì kiểm tra và break thì ta sẽ chuyển res thành char và push vào một string rỗng, lặp lại đến khi i == 9 và break, khi đó string ta nhận được sẽ là password.

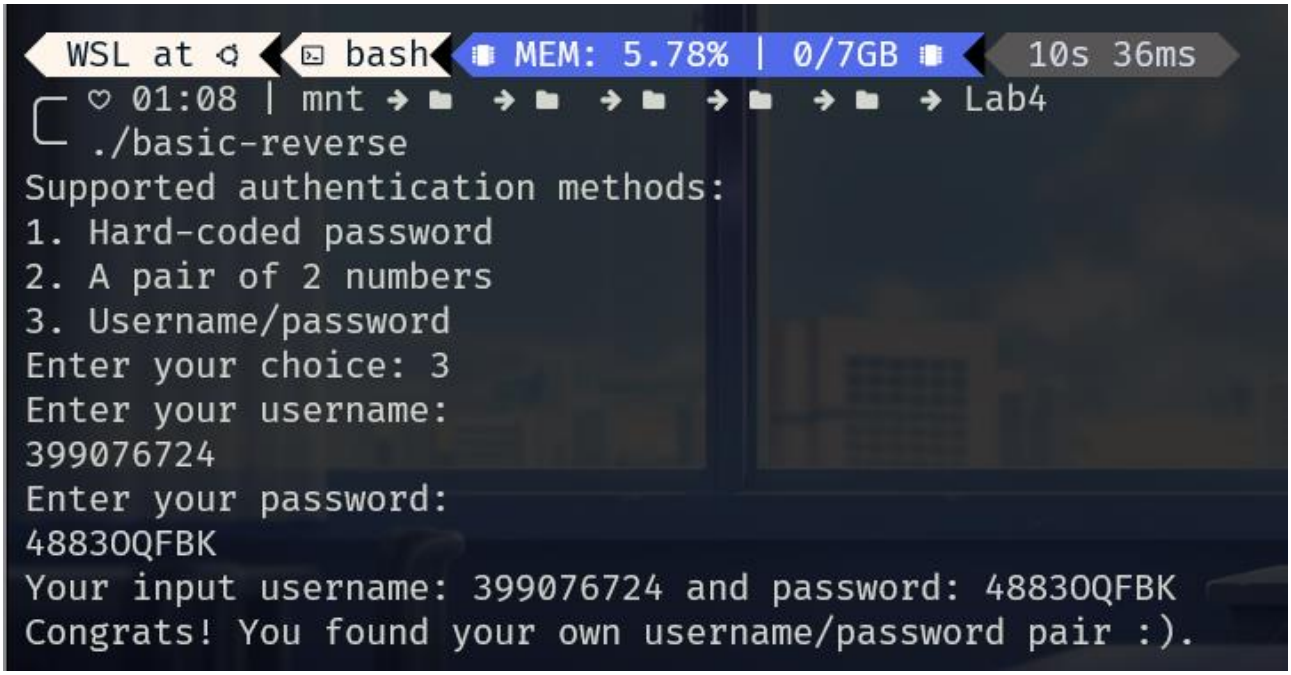
```
20  pwd = ''
21
22  i = 0
23  while True:
24      v3 = len(username)
25      if v3 <= i:
26          break
27      v22 = (ord(username[i]) + ord(newStr[i])) // 2
28      pwd += chr(v22)
29      i += 1
30
31  print("(+) Your generated password: " + pwd)
```

- Chạy file python với username: “399076724” ta được **password = “4883OQFBK”**

```
PS D:\Mon hoc\HK4\LTHT\SystemProgramming\Lab4> python -u "d:\Mon hoc\HK4\LTHT\SystemProgramming\Lab4\pwd_gen.py"
---> Enter your username: 399076724
(+) New generated string: 6776glVRc
(+) Your generated password: 4883OQFBK
```

<u>=> Vậy username và password cần nhập vào: 399076724 và 4883OQFBK</u>

<u>- Minh chứng:</u>



- Full code file python:

```python
username = input("---> Enter your username: ")
# username = "399076724"

randomStr = "cRVlg" # random string
newStr = ''

for i in range(0, len(username)):
    if i > 1:
        if i > 3:
            newStr += randomStr[8-i]
        else:
            newStr += username[i+2]
    else:
        newStr += username[i+5]

print("(+) New generated string: " + newStr)

pwd = ''

i = 0
while True:
    v3 = len(username)
    if v3 <= i:
        break
    v22 = (ord(username[i]) + ord(newStr[i])) // 2
    pwd += chr(v22)
    i += 1

print("(+) Your generated password: " + pwd)
```

```
PS D:\Mon hoc\HK4\LTHT\SystemProgramming\Lab4> python -u "d:\Mon hoc\HK4\LTHT\SystemProgramming\Lab4\pwd_gen.py"
---> Enter your username: 399076724
(+) New generated string: 6776glVRc
(+) Your generated password: 4883OQFBK
```