Average 3

1 — What is the algorithm used to check the validity of a password?

The algorithm is in 2 parts:

- Part 1: Lot of instructions (30k) to calculate some constants.
- Part 2: Use these constants to calculate each of the 12 letters of the passwords.

2 — This program relies on a specific trick. How does it work?

Most of the code is useless. Only the last instruction is useful. At the end, the algorithm doesn't provide directly the letters of the password, but the index on a character array.

3 — Can you recover the secret password? You must send 1 the valid password by email to pascal+sre25@mod-p.ch before Apr. 28th, 2025, 12h00 CET to validate this lab and get 10 points.

JFuzhFSI4YShfqE7

4 — Difficulties encountered during the lab

I didn't encounter particular difficulties. I quickly identified the main function for the algorithm with Ghidra. I copy past this main function in my IDE (Zed) and change the end of the function with the code bellow to as directly the right password:

```c
pw[0] = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ+-"[uVar6 >> 0x1a];
pw[1] = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ+-"[uVar6 >> 0x14 & 0x3f];
pw[2] = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ+-"[uVar6 >> 0xe & 0x3f];
pw[3] = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ+-"[uVar6 >> 8 & 0x3f];
pw[4] = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ+-"[uVar6 >> 2 & 0x3f];
pw[5] = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ+-"[(uVar6 & 3) << 4 | uVar4 >> 0x1c];
pw[6] = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ+-"[uVar4 >> 0x16 & 0x3f];
pw[7] = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ+-"[uVar4 >> 0x10 & 0x3f];
pw[8] = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ+-"[uVar4 >> 10 & 0x3f];
pw[9] = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ+-"[uVar4 >> 4 & 0x3f];
pw[10]= "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ+-"[uVar5 >> 0x1e | (uVar4 & 0xf) << 2];
pw[11]= "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ+-"[uVar5 >> 0x18 & 0x3f];
pw[12]= "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ+-"[uVar5 >> 0x12 & 0x3f];
pw[13]= "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ+-"[uVar5 >> 0xc & 0x3f];
pw[14]= "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ+-"[uVar5 >> 6 & 0x3f];
pw[15]= "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ+-"[uVar5 & 0x3f];
```

With that I only print the passowrd at then end

```c
printf("%s\n", password);
```

I test it, and it's work!