# Password Maker Overview

Password Maker is software that creates complex passwords from easy to remember.

As the basic method,

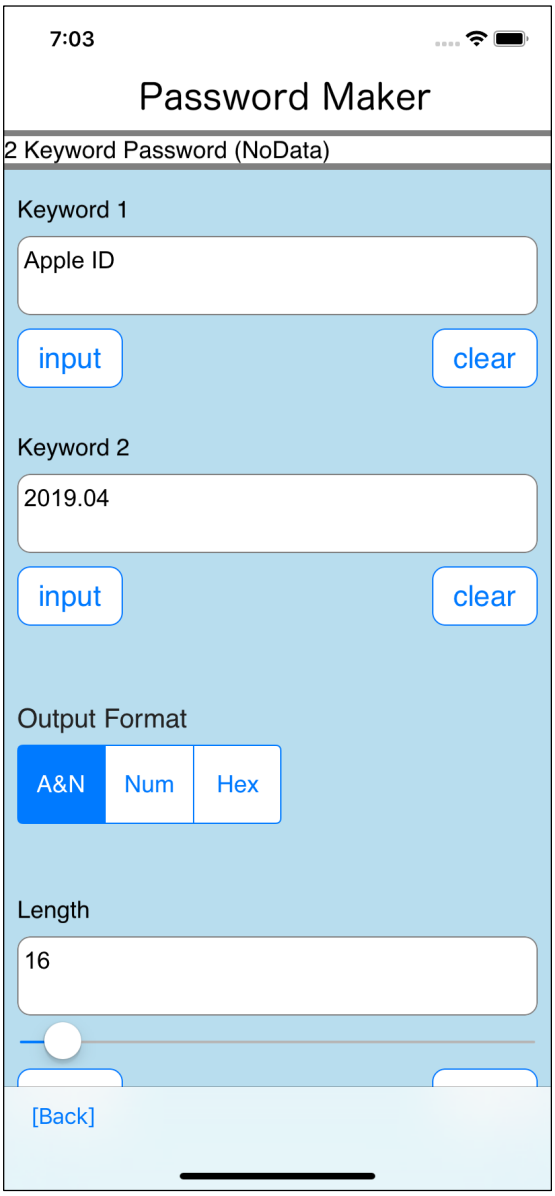
- Two keywords
- One keyword and one file
- Two files

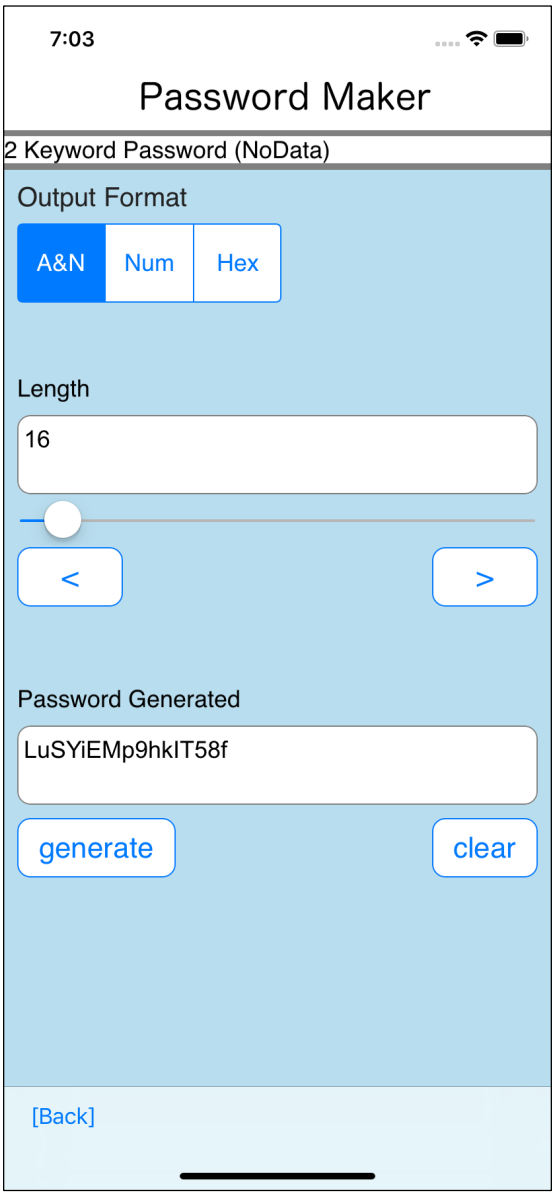
it generates a complex password from them.

In addition, it supports the method of using "key file" together with these.

Keywords and files are, in a sense, something that is easy to guess.

The generation method using the "key file" together is to shake off the analogy.



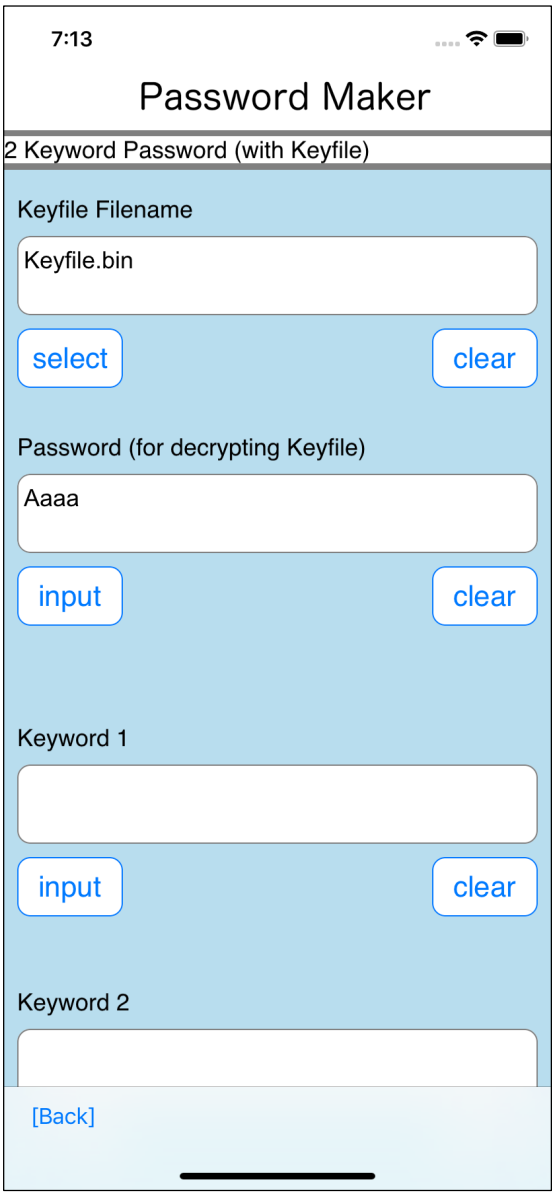

In this way,

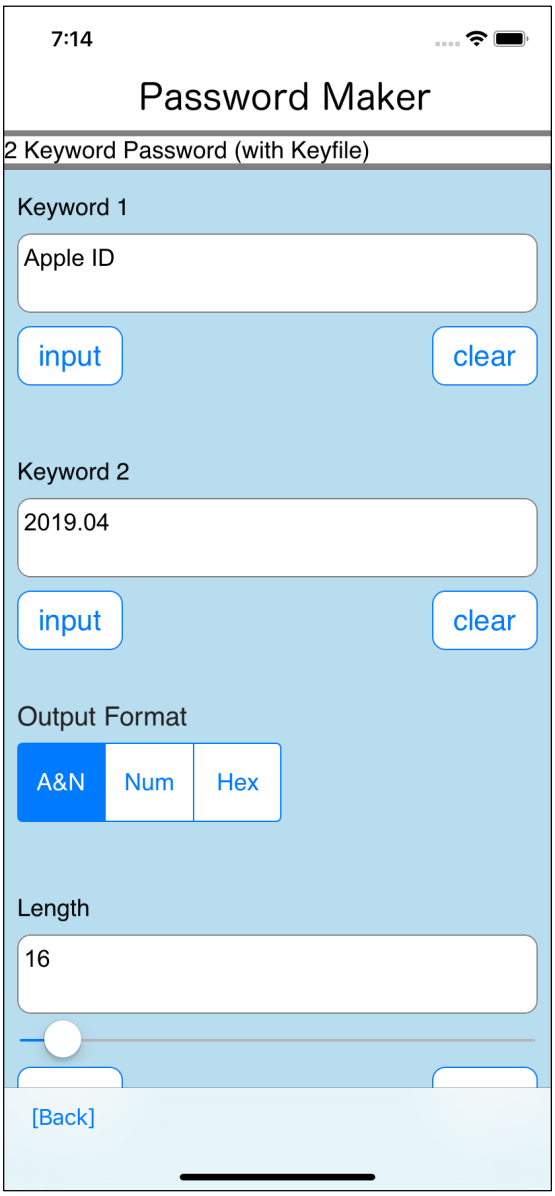
| | |
|---|---|
| Keyword 1 | Apple ID |
| Keyword 2 | 2019.04 |
| Length | 16 |

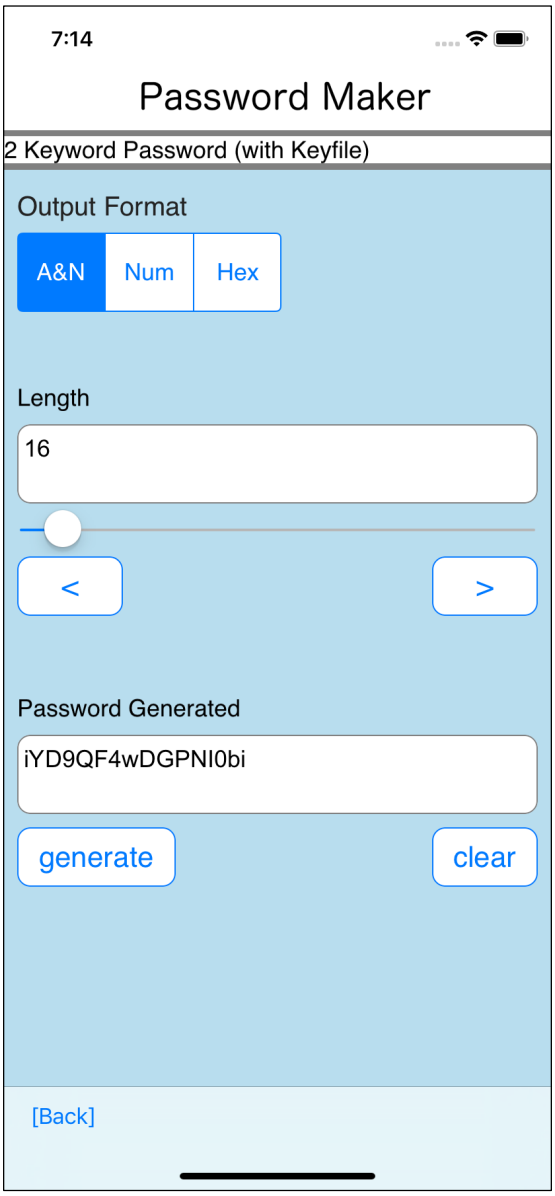
from these, the password

LuSYiEMp9hkIT58f

is generated.


7:13
Password Maker
2 Keyword Password (with Keyfile)
Keyfile Filename
Keyfile.bin
select
clear
Password (for decrypting Keyfile)
Aaaa
input
clear
Keyword 1
input
clear
Keyword 2
[Back]




Also, in this way, when using a "key file",

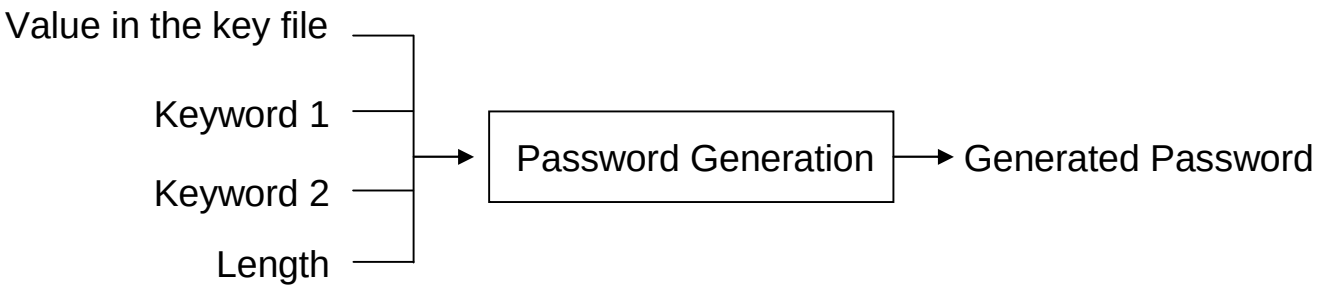
| | |
|---|---|
| Keyfile | Keyfile.bin |
| Keyword 1 | Apple ID |
| Keyword 2 | 2019.04 |
| Length | 16 |

from these, the password

iYD9QF4wDGPNI0bi

is generated.

In password generation with “Key file”,




like this,

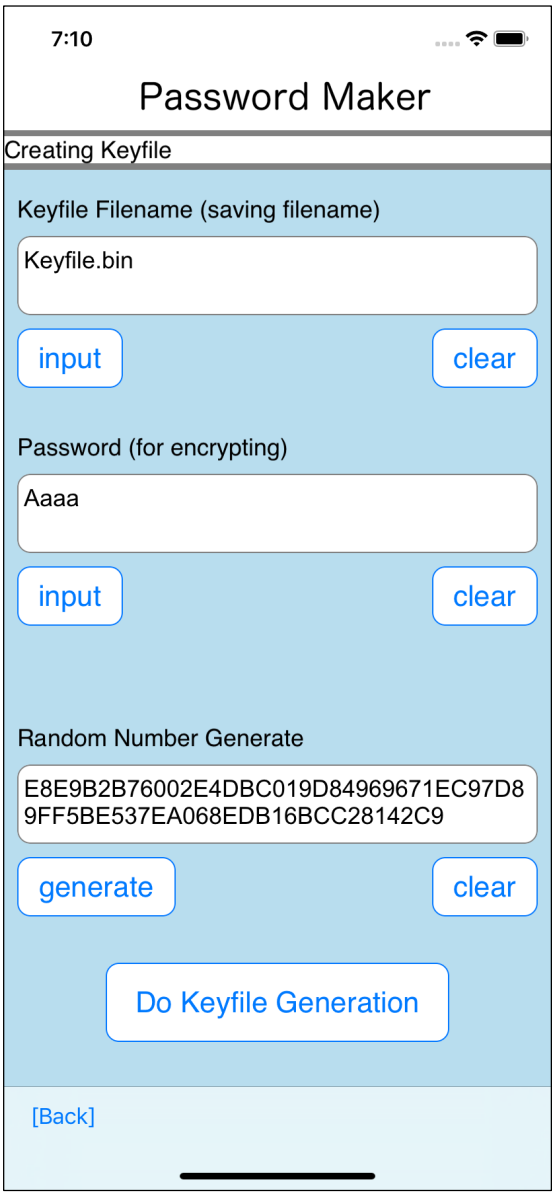
value in the key file

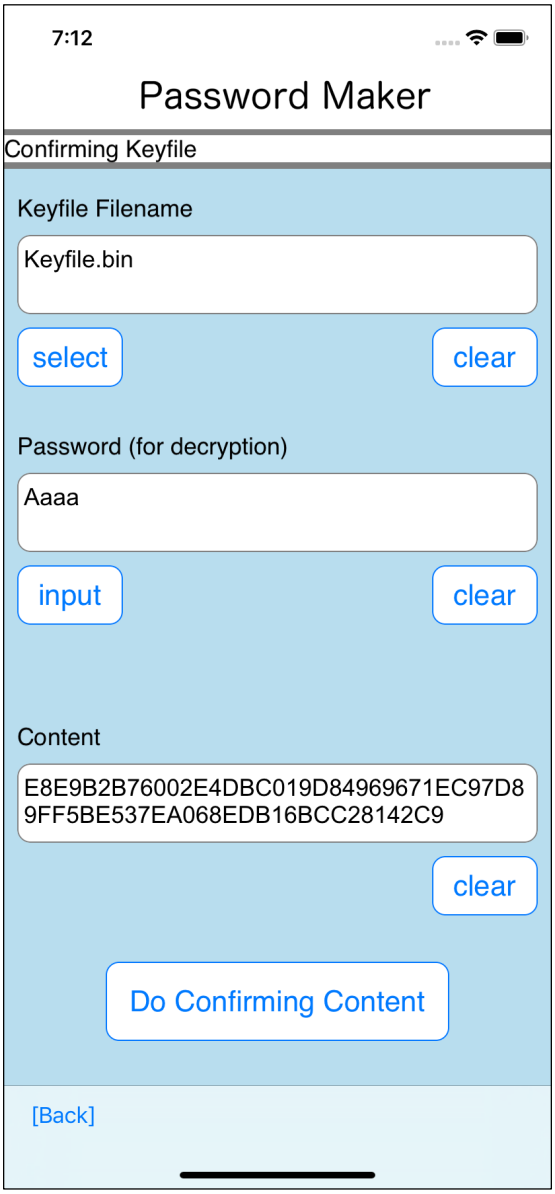
also participates in password generation.

As a result,

It is the person who have the key file can generate the password.

it will be like this.




The value in the key file Keyfile.bin used in this example is

E8E9B2B76002E4DBC019D84969671EC9
7D89FF5BE537EA068EDB16BCC28142C9

this 32-byte value.

This 32-byte value also participates in the generation of the password iYD9QF4wDGPNI0bi.

The password iYD9QF4wDGPNI0bi can only be generated by people who have this 32-byte value.

The key file Keyfile.bin is created in such ways:

32-byte value

E8E9B2B76002E4DBC019D84969671EC9
7D89FF5BE537EA068EDB16BCC28142C9

AES-256-Keywap is applied with this value and the wrapped value is encrypted with AES-256-GCM.

Cipher text created using AES-256-GCM can detect such things:

The decryption key is wrong.

Cipher text has been tampered with.

If this is detected,  password generation using a key file does not generate a password.