About key file

The key file used by Password Maker is such a thing:

> "The cipher key used for the actual encryption. "

It is such a thing.

> Apply AES-256 Keywrap to a 256-bit (32-byte) cipher key.
>
> Encrypt the keywrapped key with AES-256-GCM.

In practice, when performing encryption and decryption, it is used as follows.

> Decrypt the key file and extract the contents (256-bit encryption key).
>
> Actual encryption and decryption are performed using the extracted cipher key.

AES-256-GCM decryption can detect such things:

> The key file has been tampered with (corrupted).
>
> The decryption password of the key file is incorrect.

When detected,

> Key file decryption
>
> Actual encryption, decryption

are not performed.

> Encryption is performed using a key that has never been used before.

That is the proper and ideal on cipher.

But actually doing this is too much.

However, password keys are too difficult to secure.

In terms of security, the key file is like the middle point between

> Random number generation key that has never been used for encryption and
>
> Password key.

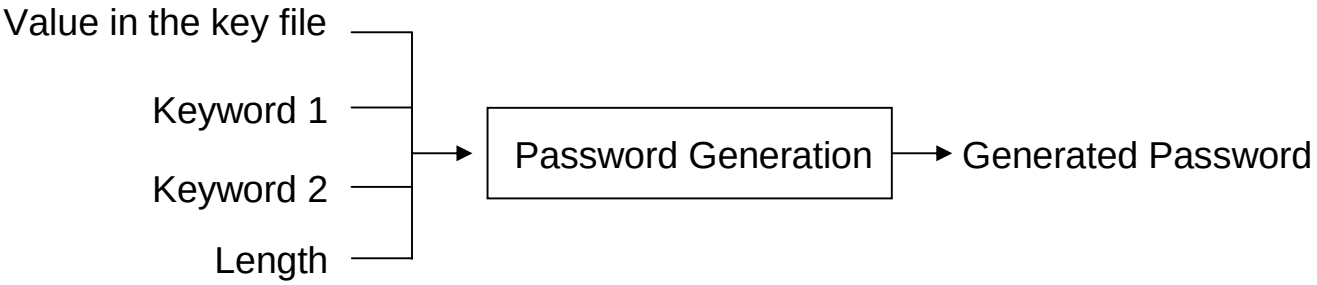
Although it is far from "random number generation key that has never been used for encryption", it is much better than "password key".

It is something like this.

If it is used for actual encryption and decryption, it will be like the one above.

Password Maker uses a key file for password generation rather than for encryption and decryption.

When generating a password, decrypt the key file and retrieve the contents value.



The 32-byte value extracted from the key file is thus involved in password generation.

32-byte value

E8E9B2B76002E4DBC019D84969671EC9
7D89FF5BE537EA068EDB16BCC28142C9

For example, if the 32-byte value in the key file is this value, the generated password will be a password that can be created only by those who have this 32-byte value.