gcmc overview

gcmc is software that performs authentication encryption.

GCM mode of AES (AES-256-GCM) is used as a method.

If decryption of block ciphers has not been done by any means,

The encryption key (password) is incorrect.

The cipher text is broken (falsified).

In that case, it will not return to the original plain text.

Decryption in this case is something like "double encryption".

Then, that cipher text will be output as the decrypted text.

However, if you use a cipher with authentication function, you can see
"Is it back to plaintext as it was before encryption?"

Then, when it detects that "the plaintext as it is before encryption is not returned to plaintext", the decryption work is stopped and nothing is output.

If you use cipher with authentication function, you can almost certainly restore "just plaintext before encryption" without any problem.

You can not afford to use strange decrypting results.

If the cipher text is tampered with, it must be detected.

It is possible to realize something like this.

Also, gcmc can use following three types of encryption keys:

password key

key file

binary key