

()

☒ AI - AI - () 2  - (),

	2026. 06. 23.
(/)	#include <string.h> - strlen(password); . - memcpy(key, initial, sizeof(initial)); 32 key . - memcmp(magic, expected_magic, sizeof(magic)) magic Gerbera . - strcmp() . - strcspn() . (): if (!fgets(mode, sizeof(mode), stdin)) return <u>1;</u> : if ; ; .
(2)	1

```

● temp: ./build/gerbera
Mode (encrypt/decrypt): encrypt
Input file: tests/test.png
Output file: test.png.gerbera
Password: mizuki
⊗ temp: ./build/gerbera
Mode (encrypt/decrypt): decrypt
Input file: test.png.gerbera
Output file: wow.png
Password: mizu
The password is incorrect or the file is corrupted.
● temp: ./build/gerbera
Mode (encrypt/decrypt): decrypt
Input file: test.png.gerbera
Output file: wow.png
Password: mizuki
○ temp: 
⊗ temp: ./build/gerbera --help
Usage:
./build/gerbera encrypt <input file> <output file> <password>
./build/gerbera decrypt <input file> <output file> <password>

```

2



<https://git.mizuki.guru/imnyang/Gerbera>

nonce `srand((unsigned)time(NULL) ^ (unsigned)clock());`

()

cpu clock time XOR

CSPRNG