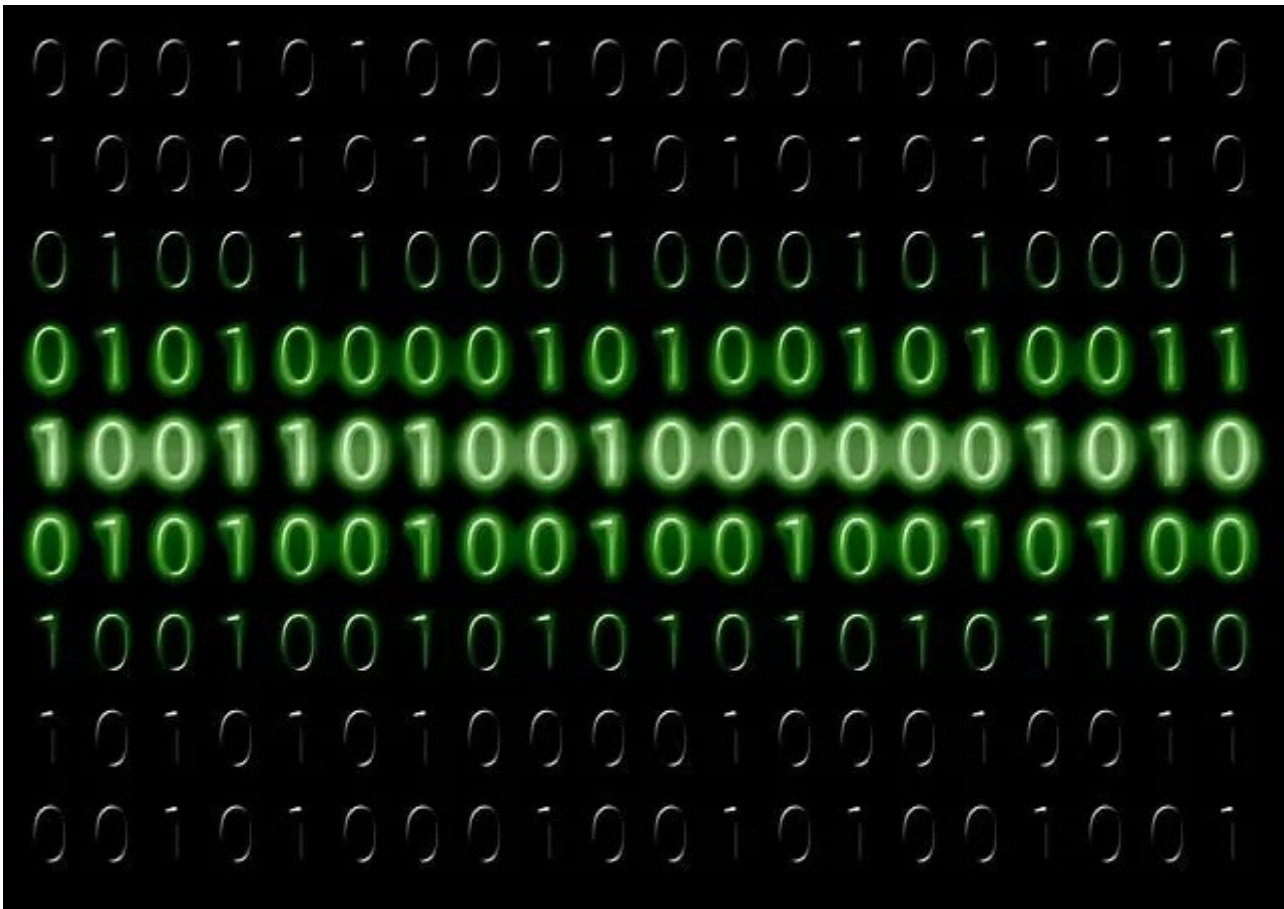
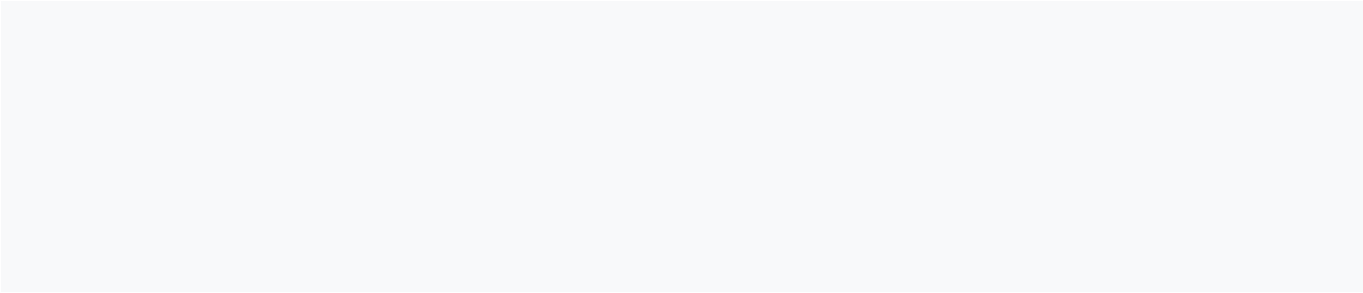


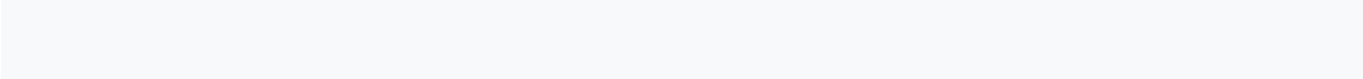
: 1



:	
:	
:	10104
:	
:	2026. 06. 25.



- 1.
- 2.
- 3.
 - 3-1.
 - 3-2. :
 - 3-3. (notion).....
- 4.
- 5.
- 6.



1.

C , 4096

2.

, XOR ,

3.

3-1.

2-a-i. string.h

string.h

strlen(password);

memcpy(key, initial, sizeof(initial)); 32 key

memcmp(magic, expected_magic, sizeof(magic)) magic Gerbera

strcmp()

strcspn()

2-a-ii. XOR

, XOR

XOR

$A \oplus B \oplus B = A$

XOR

A B A ^ B

0 0 0

0 1 1

1 0 1

1 1 0

C **XOR** ^ .

```
#include <stdio.h>
```

```
int main() {  
    int a = 5;  
    int b = 3;  
  
    int c = a ^ b;  
  
    printf("%d\n", c);  
  
    return 0;  
}
```

5 = 0101

3 = 0011

^ = 0110 = 6

XOR 1 XOR , 0 XOR .

```
#include <stdio.h>
```

```
int main() {  
    unsigned char x = 0b10101010;  
  
    x ^= 0b00001111;  
  
    printf("%u\n", x);  
}
```

10101010

00001111

10100101

C .

```
struct Student {
```

```

+ nonce
→ 32
→ 256
→
→ XOR
→
→

```

nonce 16 . nonce ,

magic(10) + nonce(16) + (8) + + tag(16)

magic Gerbera .

{'M', 'I', 'Z', 'U', 'K', 'I', 0xF0, 0x9F, 0x8E, 0x80}

gerbera_cipher_apply() . XOR . XOR

gerbera_auth_update() gerbera_auth_finish() .

3-3. (notion)

<https://akiyama-mizuki.notion.site/2026-1-programming-project>

4.

5.

nonce , . GUI

6.

[Stream cipher - Wikipedia](#)

[Keystream - Wikipedia](#)

[XOR cipher - Wikipedia](#)

[RC4 - Wikipedia](#)

[RFC 8439 - ChaCha20 and Poly1305 for IETF Protocols](#)

[SP 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode \(GCM\) and](#)

[GMAC | CSRC](#)

[SP 800-132, Recommendation for Password-Based Key Derivation: Part 1: Storage Applications | CSRC](#)

[rand - cppreference.com](#)

[CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator \(PRNG\)](#)