

(-)

: 10 104 :

1. : / /

C () / /

<https://www.hanbit.co.kr/books/%ED%98%BC%EC%9E%90-%EA%B3%B5%EB%B6%80%ED%95%98%EB%8A%94-C-%EC%96%B8%EC%96%B4%26%2340%3B%EA%B0%9C%EC%A0%95%ED%8C%90%26%2341%3B?code=E3773573071>

2. 1

```
1      C      XOR      nonce
      , magic(10 ), nonce(16 ), (8 ), (tag, 16 )
magic      , nonce
      ,
      C      . string.h strlen()      , memcpy()
      , memcmp()      magic
strcmp() strcspn()
      , 0x00      strlen()
stddef.h      size_t      . size_t sizeof      ,
      . int      ,
      .
      XOR . XOR A ^ B ^ B = A      XOR
      XOR      . C ^      , cipher_apply()
      . XOR
      , nonce
      ,
      . , 256 , nonce,
      . auth_update()
      , auth_finish()      . cipher_apply(), auth_update(), auth_finish()
      , , ,
```

3. 1 2 - -

C

```

,
C ( ) . C ,
.
XOR . XOR 1 0 , .
^
. A ^ B ^ B = A , cipher_apply()
.
XOR , . char
strlen()
0x00 . memcpy()
memcmp() . sizeof size_t
.
. magic, nonce, , , magic
, nonce , , .
.
, nonce, XOR , auth_update() auth_finish()
.
. XOR , XOR
nonce ,
.
, , magic, nonce , ChaCha20-Poly1305
. size_t, , ,
.
C ( ) ,
XOR ,
,
,

```