


Stream Cipher

Website: <http://rc4.online-domain-tools.com/>

加密

RC4 – Symmetric Ciphers Online

Check all your site's rankings in 640+ search engines

 Rank Tracker [Check](#)

Input type:

Input text:
(plain)



☒ Plaintext ☐ Hex Autodetect: **ON** | OFF

Function:

Mode:

Key:
(plain)

☒ Plaintext ☐ Hex


[> Encrypt!](#) [> Decrypt!](#)  

Encrypted text:

e3 71 8a 7f c6 6f 21 59 3d 58 9d e8 25 69 6f db | ä q . Æ o ! Y = X è % i o Û
[\[Download as a binary file\] \[?\]](#) Inactive

解密

Check all your site's rankings in 640+ search engines

 Rank Tracker [Check](#)

Input type:



File: [Browse](#)

Function:

Mode:

Key:
(plain)

☒ Plaintext ☐ Hex

[> Encrypt!](#) [> Decrypt!](#)  

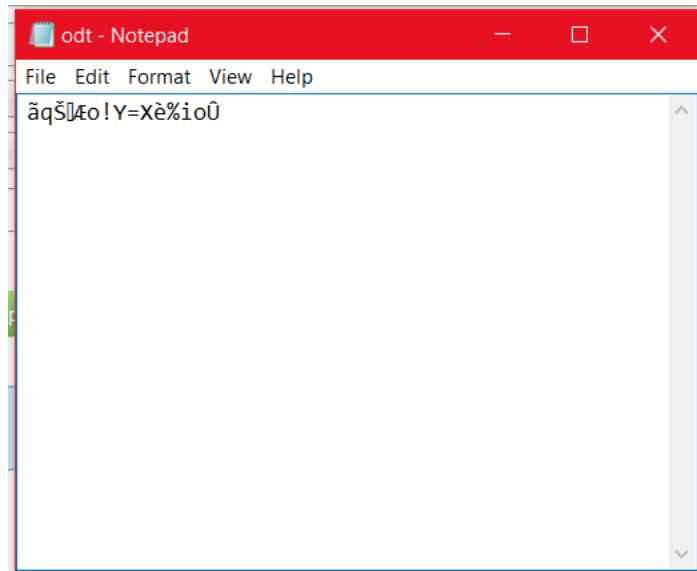
100%

File was uploaded.

Decrypted text:

4c 69 6f 77 4c 69 6f 77 4b 65 65 69 59 61 6e 6e | L i o w L i o w K e e i Y a n n
[\[Download as a binary file\] \[?\]](#) Inactive

解密的圖我用.dat 檔上傳



明文：LiowLiowKeeiYann

金鑰：cayon

加密方式：RC4

初始化長度為 256 的 S 盒。第一個循環將 0 到 255 的互不重複的元素裝入 S 盒。第二個循環根據密鑰打亂 S 盒

```
for (int i=0;i<256;i++)
{
    S[i] = i;
}
int j = 0;
for(int i=0 ; i<256 ; i++)
{
    j = (j + S[i] + key[i mod keylength]) % 256;
    swap values of S[i] and S[j];
}
```

下面 i , j 是兩個指針。通過一定的算法（（**a**），（**b**））定位 **S** 盒中的一個元素，並與輸入字節異或，得到 **k**。循環中還改變了 **S** 盒（（**c**））。如果輸入的是明文，輸出的就是密文；如果輸入的是密文，輸出的就是明文

```
Int i = 0;
Int j = 0;
While( GeneratingOutput)
{
    i = (i + 1) mod 256; //a
    j = (j + S[i]) mod 256; //b
    swap values of S[i] and S[j]; //c
    int k := inputByte ^ S[(S[i] + S[j]) % 256];
    printf("%d",k);
}
```

Reference language using: C++