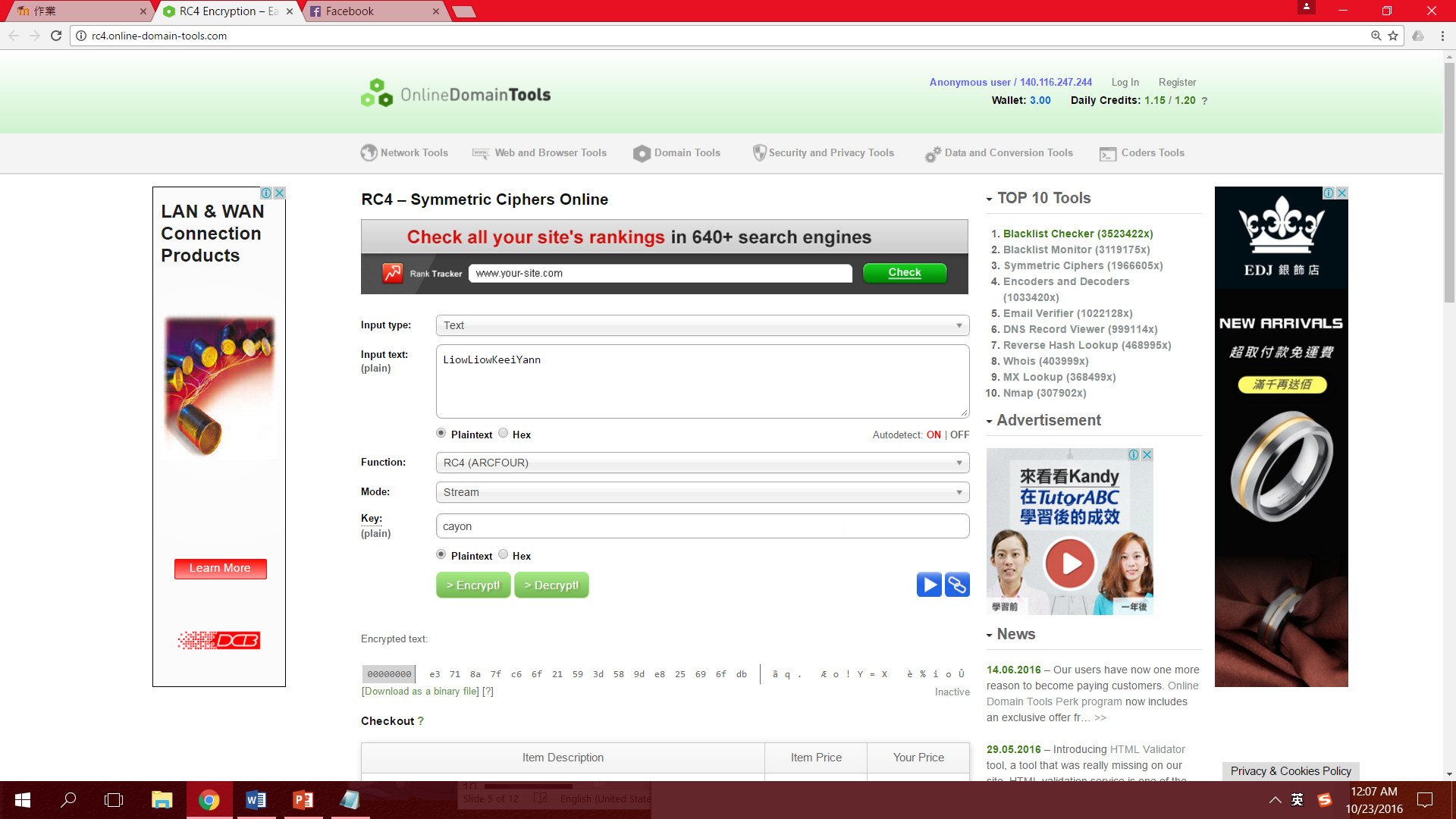
**資訊安全**

F74045018

資訊108

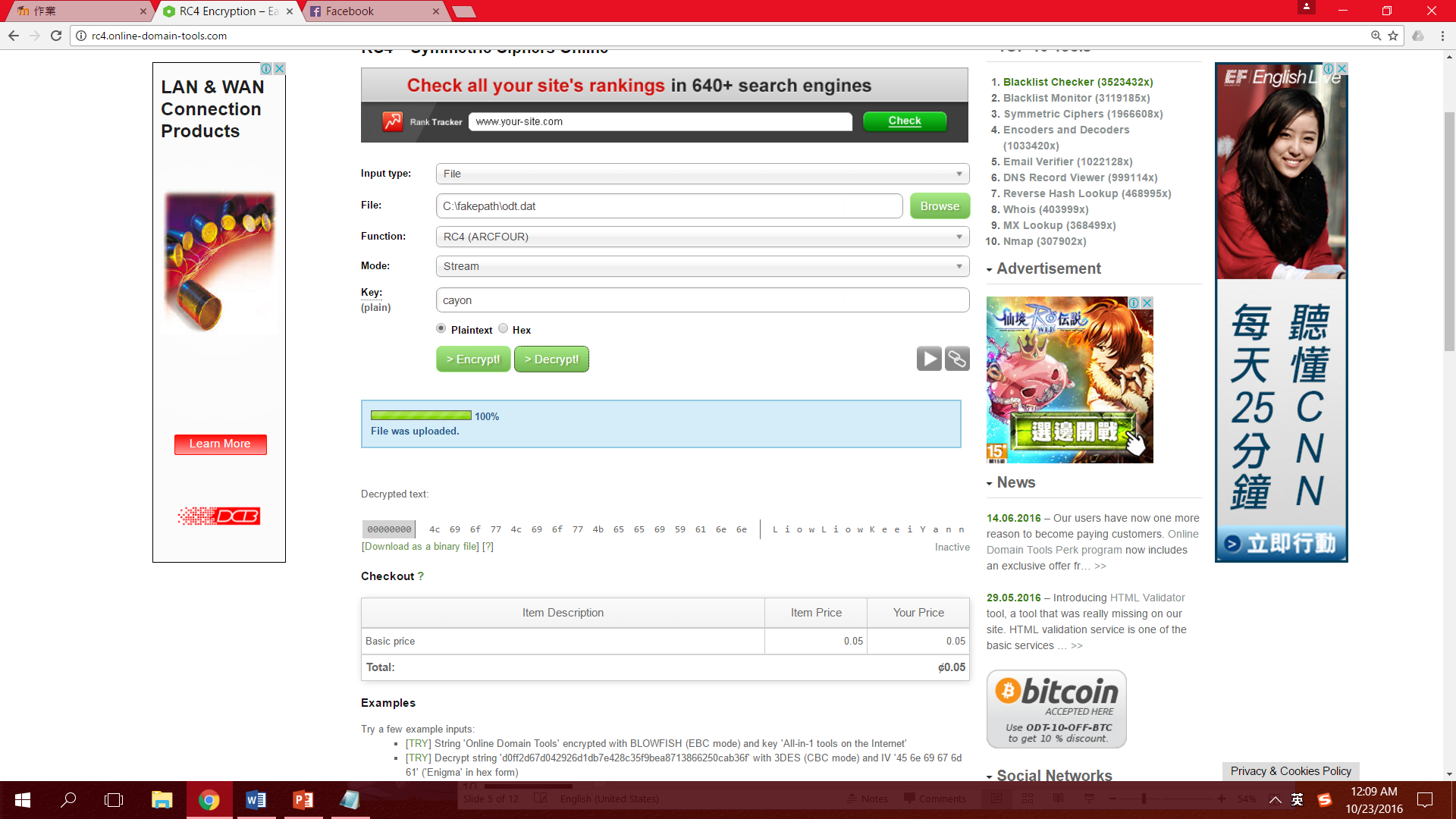
廖其忻

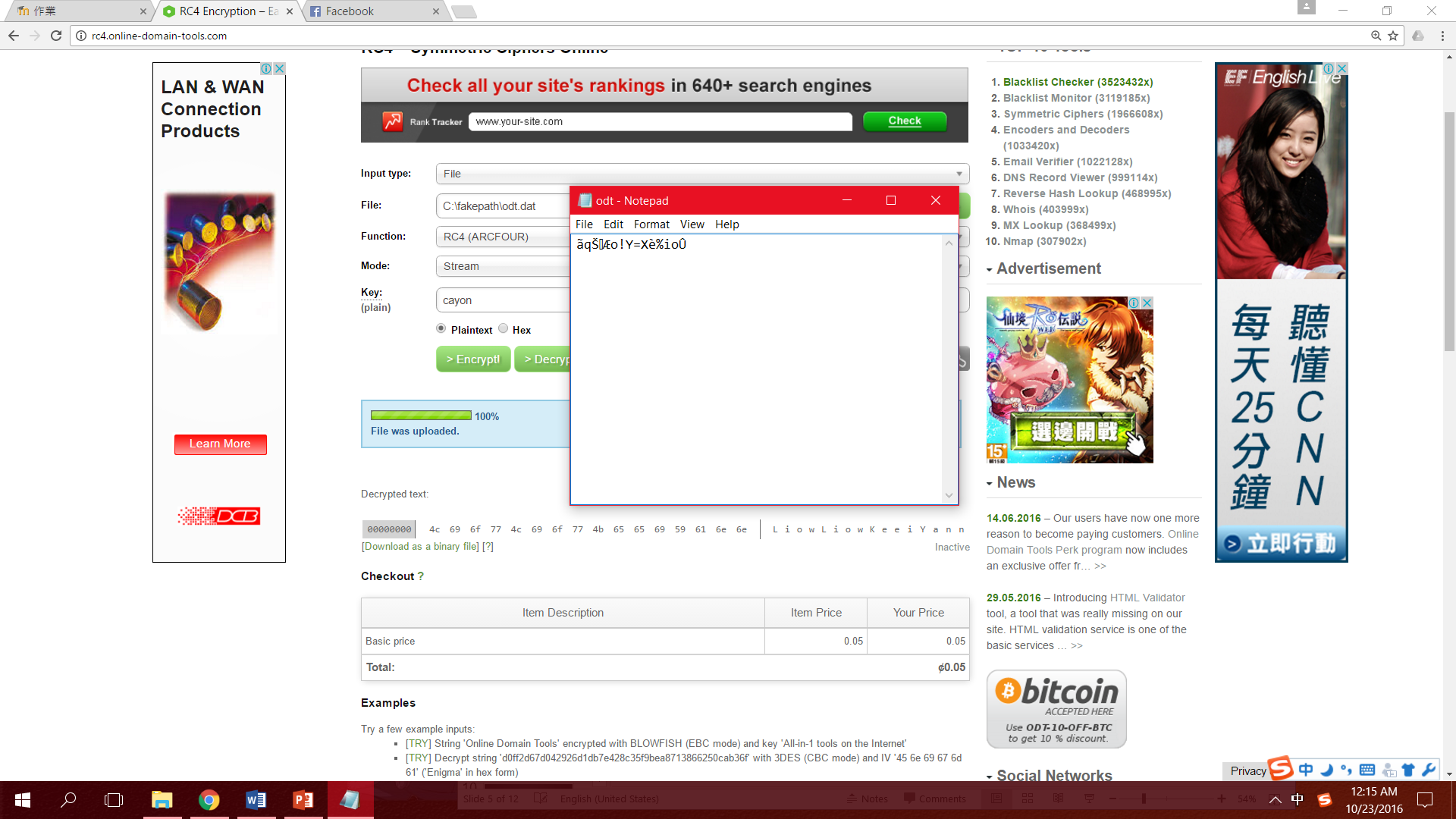
**Stream Cipher**

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

加密

解密



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++