破密分析-從古典密碼學到現代密碼學

資訊安全人才培育計畫 Hacking Weekend MyFirstCTF Training

古典密碼及其破密分析

Cryptanalysis

Kryptós + analýein

Security Mentors

臺灣好厲駭 讓你更厲害

資安實務導師培訓計畫

classical ciphers

古典密碼

Modern Cryptography

現代密碼

量子密碼

Quantum Cryptography

科技之巅2
《麻省理工科技评论》2017年10大全球突破性技术深度剖析
麻省理工科技评论◎著
10
Breakthrough Technologies
联合全球多领域行业专家，深度解读全球权威科技榜单
中国工信出版集团
人民邮电出版社

MIT Technology

Re

《麻省理工科技評論》2017

10大全球突破性技術

1. **Reinforcement Learning 強化學習**
2. The 360-Degree Selfie 360°自拍
3. Gene Therapy 2.0 基因療法2.0
4. Hot Solar Cells 太陽能熱光伏電池
5. The Cell Atlas 細胞圖譜
6. **Self-Driving Trucks自動駕駛貨車**
7. **Paying with Your Face刷臉支付**
8. **Practical Quantum Computers 實用型量子電腦**
9. Reversing Paralysis治癒癱瘓
10. Botnets of Things僵屍物聯網

無所不在的
密碼學

Cryptography

https://en.wikipedia.org/wiki/Cryptography

密碼學（Cryptography）可分為古典密碼學和現代密碼學。

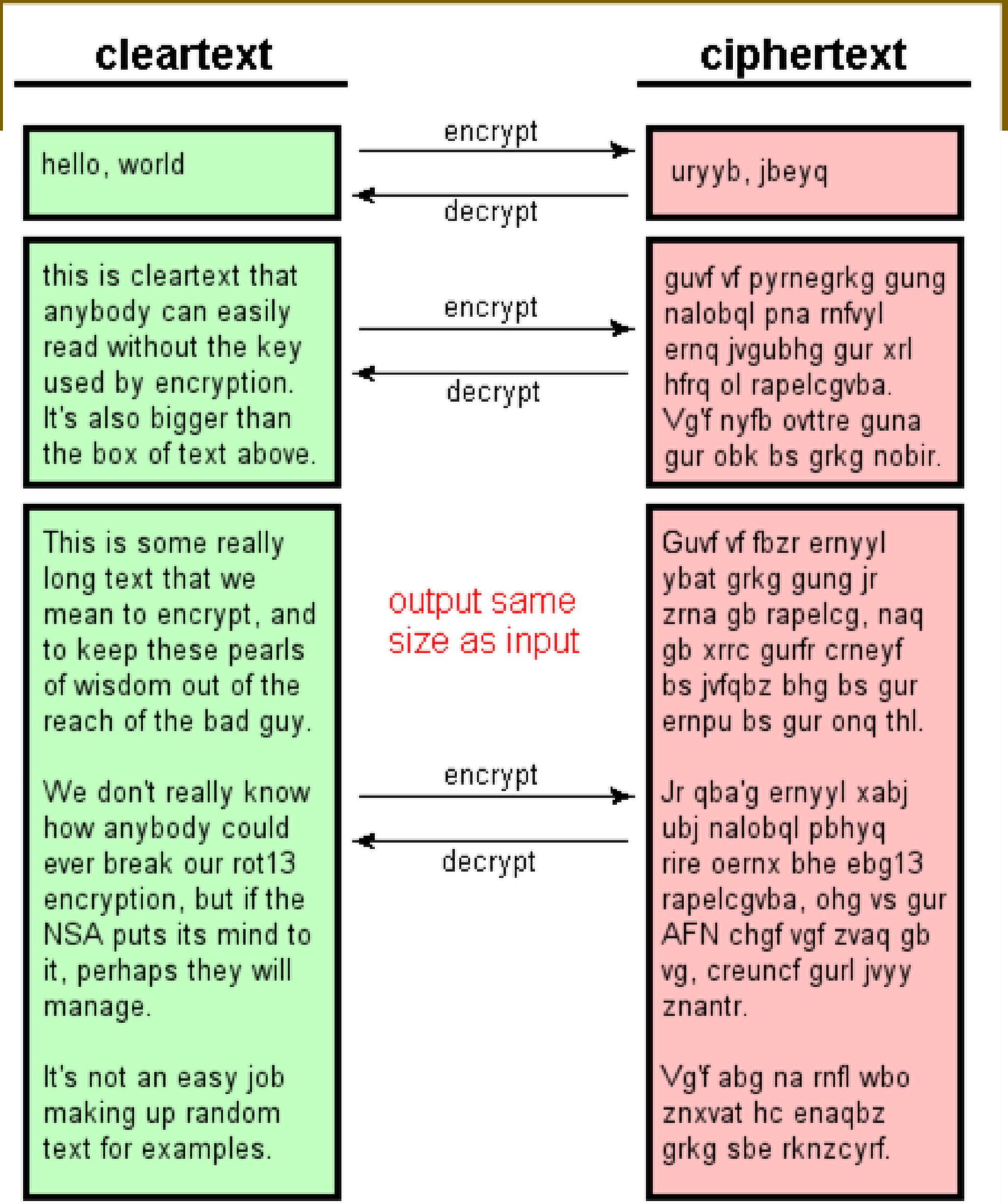
在西歐語文中，密碼學一詞源於希臘語kryptós「隱藏的」，和gráphein「書寫」。

古典密碼學主要關注資訊的保密書寫和傳遞，以及與其相對應的破譯方法。

而現代密碼學不只關注資訊保密問題，還同時涉及資訊完整性驗證（訊息驗證碼）、資訊發布的不可抵賴性（數位簽章）、以及在分散式計算中產生的來源於內部和外部的攻擊的所有資訊保安問題。

古典密碼學的編碼和破譯通常依賴於設計者和敵手的創造力與技巧，作為一種實用性藝術存在，並沒有對於密碼學原件的清晰定義。

現代密碼學則起源於20世紀末出現的大量相關理論，這些理論使得現代密碼學成為了一種可以系統而嚴格地學習的科學。



cleartext	ciphertext
hello, world	uryyb, jbeyq
this is cleartext that anybody can easily read without the key used by encryption. It's also bigger than the box of text above.	guvf vf pyrnegrkg gung nalobql pna rnfvyl ernq jvgubhg gur xrl hfrq ol rapelcgvba. Vg'f nyfb ovttre guna gur obk bs grkg nobir.
This is some really long text that we mean to encrypt, and to keep these pearls of wisdom out of the reach of the bad guy. We don't really know how anybody could ever break our rot13 encryption, but if the NSA puts its mind to it, perhaps they will manage. It's not an easy job making up random text for examples.	Guvf vf fbzr ernyyl ybat grkg gung jr zrna gb rapelcg, naq gb xrrc gurfr crneyf bs jvfqbz bhg bs gur ernpu bs gur onq thl. Jr qba'g ernyyl xabj ubj nalobql pbhyq rire oernx bhe ebg13 rapelcgvba, ohg vs gur AFN chgf vgf zvaq gb vg, creuncf gurl jvyy znantr. Vg'f abg na rnfl wbo znxvat hc enaqbz grkg sbe rknzcyrf.

http://www.unixwiz.net/techtips/iguide-crypto-hashes.html

Cryptanalysis

https://en.wikipedia.org/wiki/Cryptanalysis

密碼分析（英語：cryptanalysis，來源於希臘語kryptós，即「隱藏」，以及analýein，即「解開」），是一門研究在不知道通常解密所需要的秘密信息的情況下對加密的信息進行解密的學問。

通常，這需要尋找一個秘密的鑰匙。用不是很正規的話來說，這就是所謂的破解密碼。

密碼分析這個詞有時也被用來指廣義上的繞開某個密碼學算法或密碼協議的嘗試，而不僅僅是針對加密算法。

但是，密碼分析通常不包括並非主要針對密碼算法或協議的攻擊，如賄賂、拷打、入室搶劫、鍵盤記錄器，等等。

儘管這些攻擊方式是計算機安全領域裡的重要考慮因素，而且通常比傳統的密碼分析更加有效。

密碼分析又稱破密術。密碼分析的目的是發現密碼機制的弱點，從事者可能是意圖顛覆系統惡意的攻擊者或評估系統弱點的設計人。在現代，密碼演算法與協定必須被仔細檢查和測試，確定其保證的安全性。

大眾普遍誤解認為所有加密法都可以被破解。香農在二戰時的工作就已證明只要金鑰是完全隨機，不重覆使用，對外絕對保密，與訊息等長或比訊息更長的一次一密是不可能破解的。除了一次一密以外的多數加密法都可以以暴力攻擊法破解，但是破解所需的努力可能是金鑰長度的指數成長。

密碼分析的方式有很多，因此有數個分類。一個常見的分別法則是攻擊者知曉多少資訊。在唯密文攻擊中，密碼分析者只能存取密文，好的現代密碼系統對這種情況通常是免疫的。在已知明文攻擊中，密碼分析者可以存取多個明文、密文對。在選擇明文攻擊中，密碼分析者可以自選任意明文，並被賦予相對應的密文，例如二戰時布列顛所使用的園藝法。最後，選擇密文攻擊中，密碼分析者可以自選任意密文，並被賦予相對應的明文

classical ciphers
古典密碼
及其
破密分析

古典密碼

classical ciphers

https://en.wikipedia.org/wiki/Outline_of_cryptography

Substitution ciphers **替換加密**	https://en.wikipedia.org/wiki/Substitution_cipher
Monoalphabetic substitution	凱撒密碼**Caesar cipher(ROT13) [https://en.wikipedia.org/wiki/Caesar_cipher]**
	Affine cipher Atbash cipher Keyword cipher
Polyalphabetic substitution	**Vigenère cipher (https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher)** Autokey cipher Homophonic substitution cipher
Polygraphic substitution	Playfair cipher Hill cipher
Transposition ciphers 換位加密法	https://en.wikipedia.org/wiki/Transposition_cipher
	Rail Fence cipher Route cipher
	Scytale Grille Permutation cipher VIC cipher

凱撒密碼@替換式密碼

Caesar cipher(ROT13)

@Substitution cipher

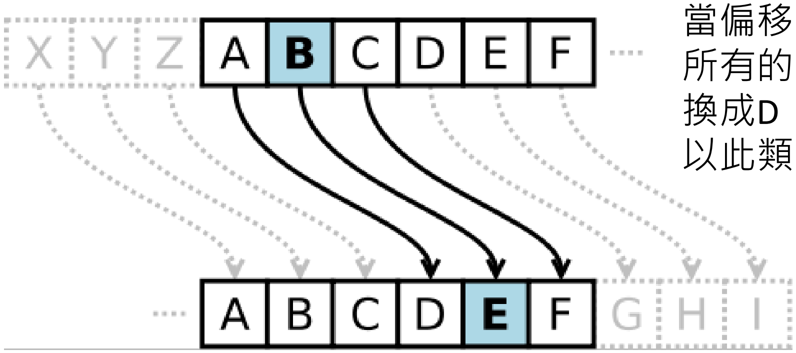
古典密碼のの凱撒密碼

classical ciphers||Caesar cipher(ROT13) [https://en.wikipedia.org/wiki/Caesar_cipher]

Gaius Julius Caesar

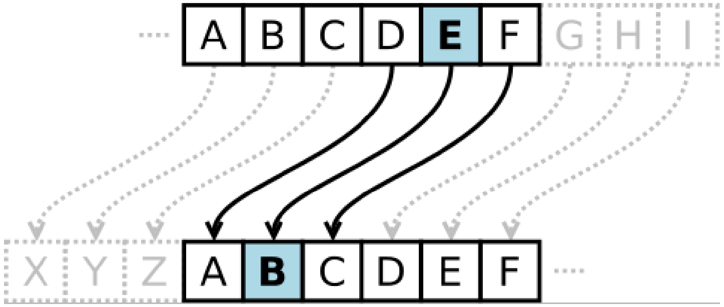
- ✓愷撒密碼是一種**替換加密**的技術
- ✓**明文中的所有字母都在字母表上向後（或向前）按照一個固定數目進行偏移後被替換成密文。**
- ✓這個加密方法是以羅馬共和時期愷撒的名字命名的，當年愷撒曾用此方法與其將軍們進行聯繫。
- ✓愷撒密碼非常容易被破解，而且在實際應用中也無法保證通信安全。

把字母往右或往左移動幾位



當偏移量是3的時候，所有的字母A將被替換成D，B變成E，以此類推。

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: XYZABCDEFGHIJKLMNOPQRSTUVW



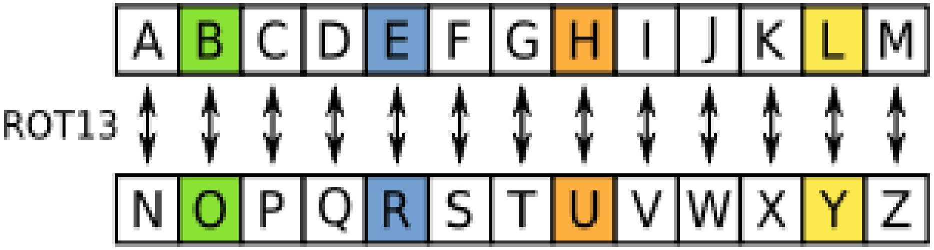
https://en.wikipedia.org/wiki/Julius_Caesar

凱撒密碼@替換式密碼

Caesar cipher(ROT13) @Substitution cipher

```
echo 'Funny{MyfirstCTF}' | tr xyza-w a-z
```

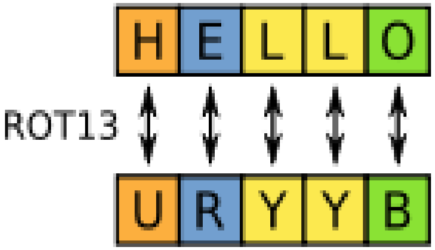
```
Fxqqb{MbiluvwCTF}
```



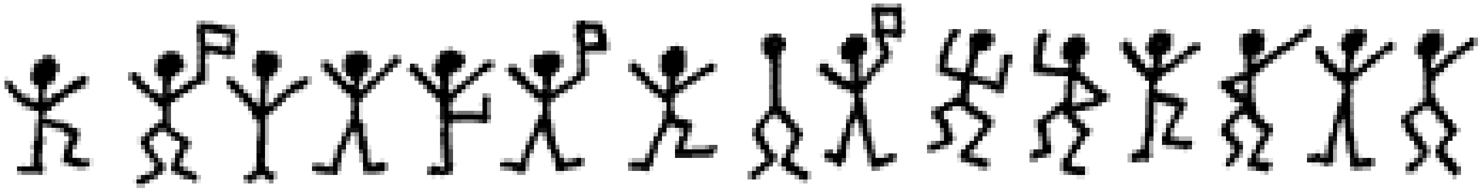
	A	B	C	D	E	F	G	H	I	J	K	L	M
ROT13	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

```
echo 'Fxqqb{MbiluvwCTF}' | tr  a-z xyza-w
```

```
Funny{MyfirstCTF}
```



	H	E	L	L	O
ROT13	↕	↕	↕	↕	↕
	U	R	Y	Y	B



tr --help

Usage: tr [OPTION]... SET1 [SET2]

Translate, squeeze, and/or delete characters from standard input,

writing to standard output.

```
  -c, -C, --complement    use the complement of SET1

  -d, --delete          delete characters in SET1, do not translate

  -s, --squeeze-repeats   replace each sequence of a repeated
character that is listed in the last specified SET, with a single
occurrence of that character

  -t, --truncate-set1     first truncate SET1 to length of SET2

      --help     display this help and exit

      --version  output version information and exit
```

SETs are specified as strings of characters.

Most represent themselves.

Interpreted sequences are:

```
\NNN         character with octal value NNN (1 to 3 octal digits)
\\           backslash
\a           audible BEL
\b           backspace
\f           form feed
\n           new line
\r           return
\t           horizontal tab
\v           vertical tab
```

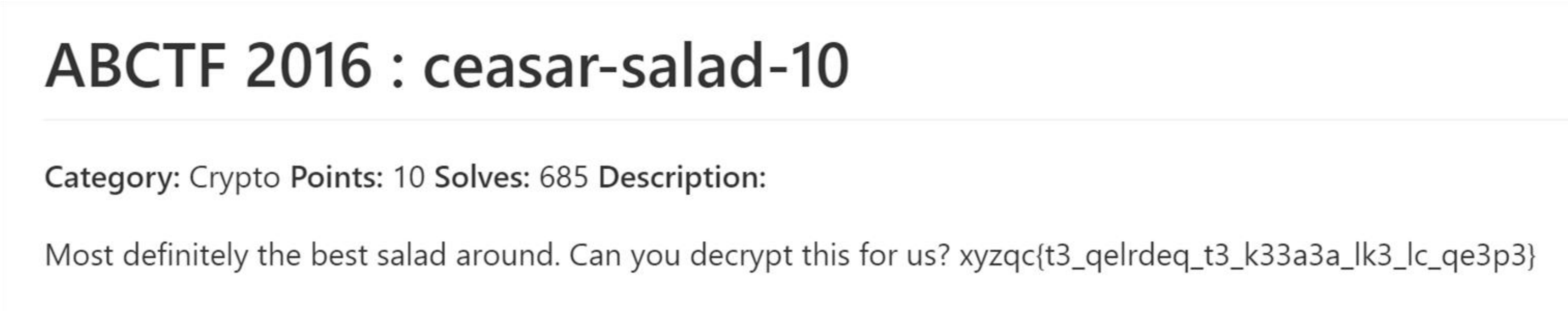
CHAR1-CHAR2   all characters from CHAR1 to CHAR2 in ascending order

```
[CHAR*]        in SET2, copies of CHAR until length of SET1
[CHAR*REPEAT]   REPEAT copies of CHAR, REPEAT octal if starting with 0
[:alnum:]      all letters and digits
[:alpha:]      all letters
[:blank:]      all horizontal whitespace
[:cntrl:]      all control characters
[:digit:]      all digits
[:graph:]      all printable characters, not including space
[:lower:]      all lower case letters
[:print:]      all printable characters, including space
[:punct:]      all punctuation characters
[:space:]      all horizontal or vertical whitespace
[:upper:]      all upper case letters
[:xdigit:]     all hexadecimal digits
[=CHAR=]       all characters which are equivalent to CHAR
```

CTF- cryptography

ABCTF 2016 : ceasar-salad-10

https://github.com/ctfs/write-ups-2016/tree/master/abctf-2016/crypto/ceasar-salad-10



ABCTF 2016 : ceasar-salad-10

Category: Crypto **Points:** 10 **Solves:** 685 **Description:**

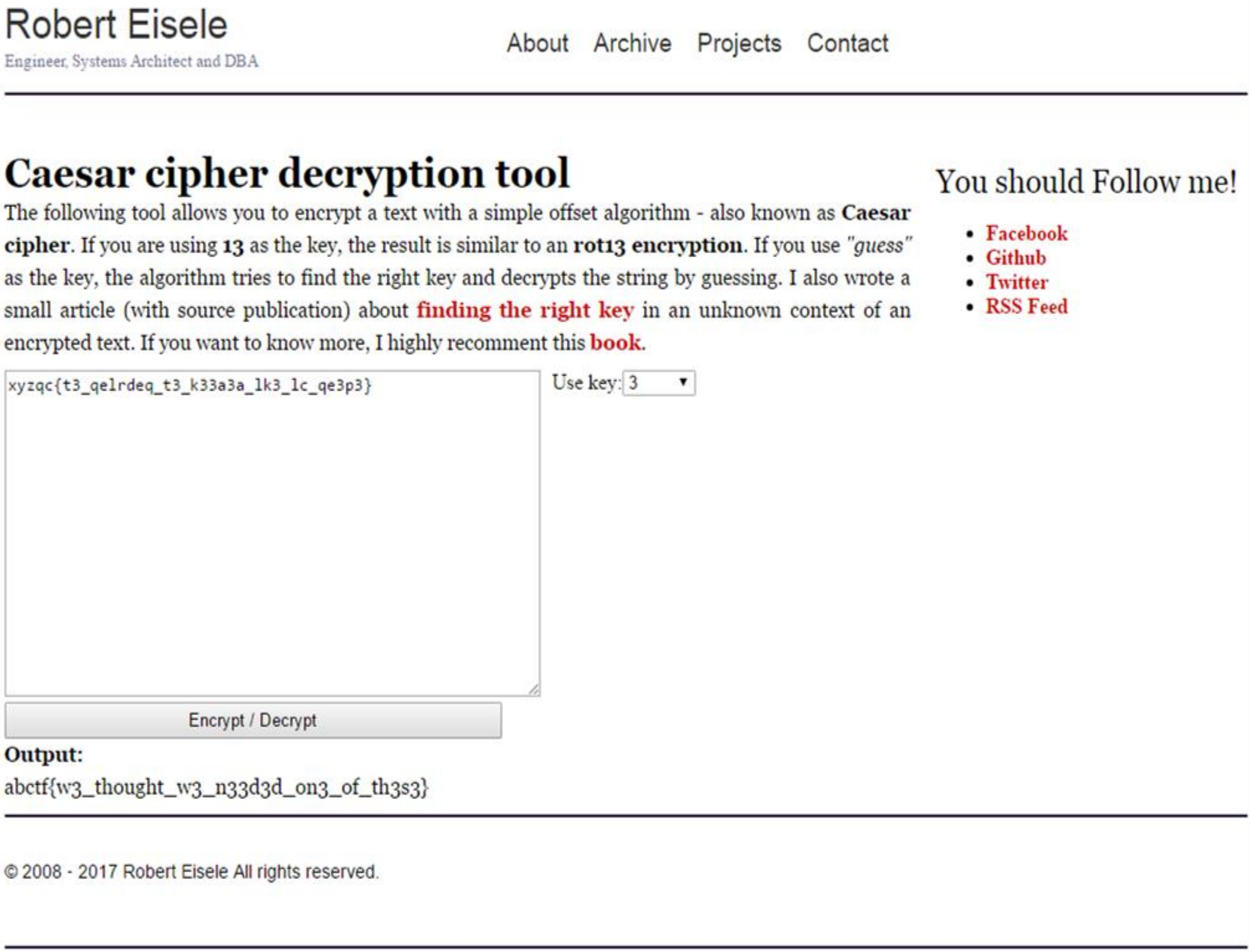
Most definitely the best salad around. Can you decrypt this for us? xyzqc{t3_qelrdeq_t3_k33a3a_lk3_lc_qe3p3}

ABCTF 2016 : ceasar-salad-10

Most definitely the best salad around. Can you decrypt this for us?

xyzqc{t3_qelrdeq_t3_k33a3a_lk3_lc_qe3p3}

解法一::使用線上工具:輸入看看
http://www.xarg.org/tools/caesar-cipher/



Caesar cipher decryption tool

The following tool allows you to encrypt a text with a simple offset algorithm - also known as **Caesar cipher**. If you are using **13** as the key, the result is similar to an **rot13 encryption**. If you use *"guess"* as the key, the algorithm tries to find the right key and decrypts the string by guessing. I also wrote a small article (with source publication) about **finding the right key** in an unknown context of an encrypted text. If you want to know more, I highly recomment this **book**.

```
xyzqc{t3_qelrdeq_t3_k33a3a_lk3_lc_qe3p3}
```

Use key: 3

Output:

abctf{w3_thought_w3_n33d3d_on3_of_th3s3}

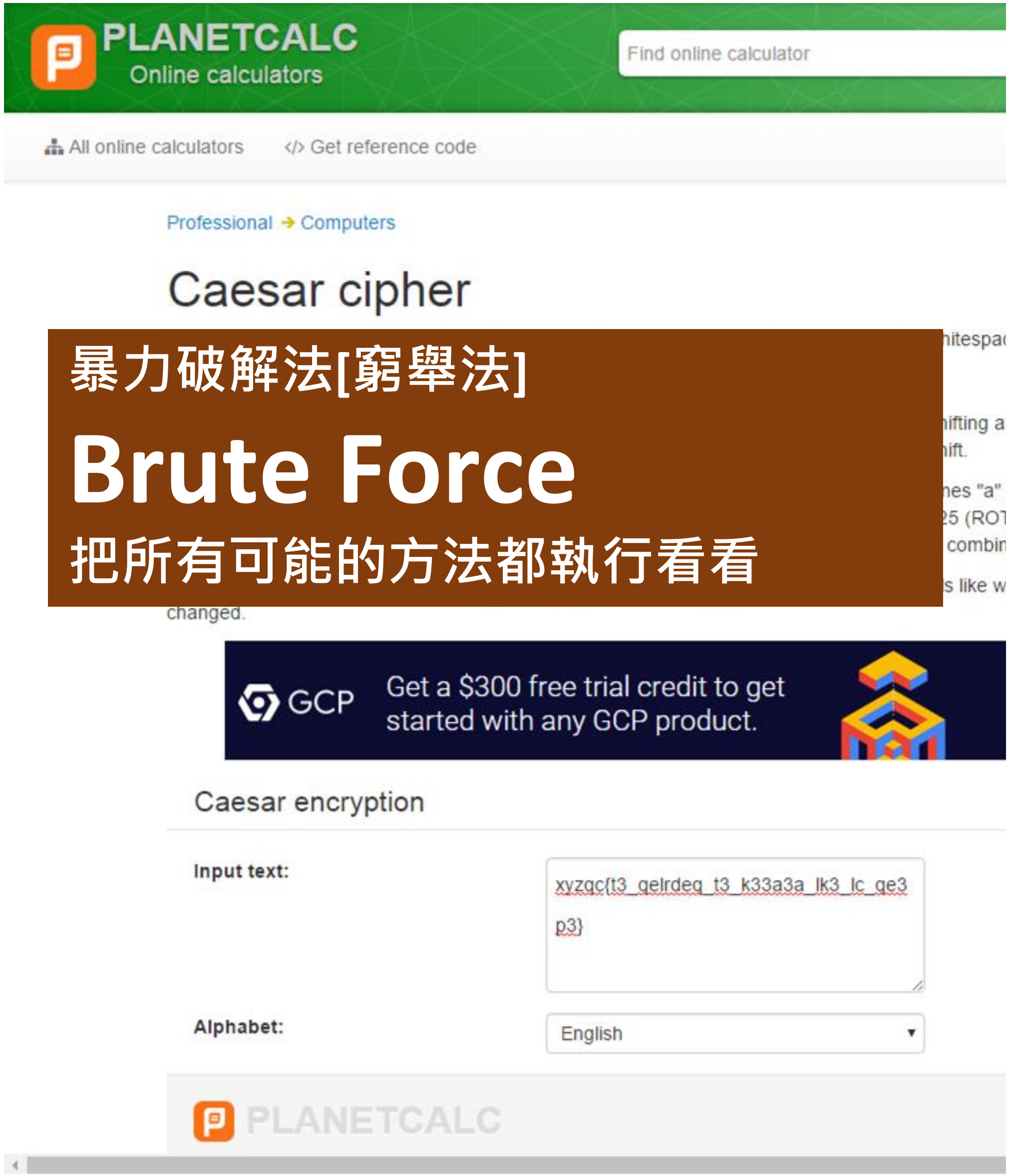
You should Follow me!

- **Facebook**
- **Github**
- **Twitter**
- **RSS Feed**

© 2008 - 2017 Robert Eisele All rights reserved.

解法二::暴力破解法

https://planetcalc.com/1434/



PLANETCALC Online calculators

Professional → Computers

Caesar cipher

暴力破解法[窮舉法]

Brute Force

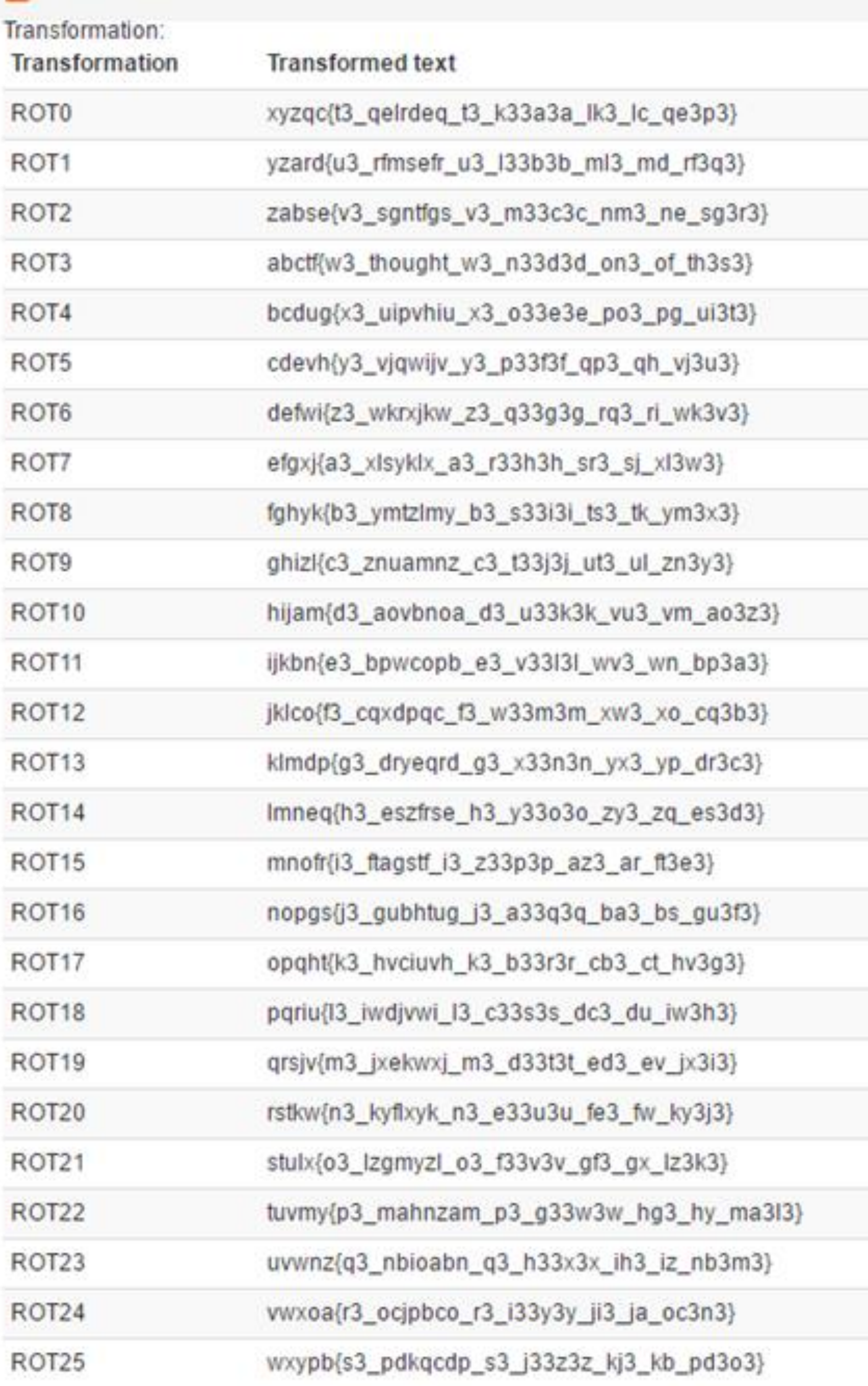
把所有可能的方法都執行看看

changed.

Caesar encryption

Input text: xyzqc{t3_qelrdeq_t3_k33a3a_lk3_lc_qe3p3}

Alphabet: English



Transformation:

Transformation	Transformed text
ROT0	xyzqc{t3_qelrdeq_t3_k33a3a_lk3_lc_qe3p3}
ROT1	yzard{u3_rfmsefr_u3_l33b3b_ml3_md_rf3q3}
ROT2	zabse{v3_sgntfgs_v3_m33c3c_nm3_ne_sg3r3}
ROT3	abctf{w3_thought_w3_n33d3d_on3_of_th3s3}
ROT4	bcdug{x3_uipvhiu_x3_o33e3e_po3_pg_ui3t3}
ROT5	cdevh{y3_vjqwijv_y3_p33f3f_qp3_qh_vj3u3}
ROT6	defwi{z3_wkrxjkw_z3_q33g3g_rq3_ri_wk3v3}
ROT7	efgxj{a3_xlsyklx_a3_r33h3h_sr3_sj_xl3w3}
ROT8	fghyk{b3_ymtzlmy_b3_s33i3i_ts3_tk_ym3x3}
ROT9	ghizl{c3_znuamnz_c3_t33j3j_ut3_ul_zn3y3}
ROT10	hijam{d3_aovbnoa_d3_u33k3k_vu3_vm_ao3z3}
ROT11	ijkbn{e3_bpwcopb_e3_v33l3l_wv3_wn_bp3a3}
ROT12	jklco{f3_cqxdpqc_f3_w33m3m_xw3_xo_cq3b3}
ROT13	klmdp{g3_dryeqrd_g3_x33n3n_yx3_yp_dr3c3}
ROT14	lmneq{h3_eszfrse_h3_y33o3o_zy3_zq_es3d3}
ROT15	mnofr{i3_ftagstf_i3_z33p3p_az3_ar_ft3e3}
ROT16	nopgs{j3_gubhtug_j3_a33q3q_ba3_bs_gu3f3}
ROT17	opqht{k3_hvciuvh_k3_b33r3r_cb3_ct_hv3g3}
ROT18	pqriu{l3_iwdjvwi_l3_c33s3s_dc3_du_iw3h3}
ROT19	qrsjv{m3_jxekwxj_m3_d33t3t_ed3_ev_jx3i3}
ROT20	rstkw{n3_kyflxyk_n3_e33u3u_fe3_fw_ky3j3}
ROT21	stulx{o3_lzgmyzl_o3_f33v3v_gf3_gx_lz3k3}
ROT22	tuvmy{p3_mahnzam_p3_g33w3w_hg3_hy_ma3l3}
ROT23	uvwnz{q3_nbioabn_q3_h33x3x_ih3_iz_nb3m3}
ROT24	vwxoa{r3_ocjpbco_r3_i33y3y_ji3_ja_oc3n3}
ROT25	wxypb{s3_pdkqcdp_s3_j33z3z_kj3_kb_pd3o3}

解法三::直覺法

xyzqc{t3_qelrdeq_t3_k33a3a_lk3_lc_qe3p3}

↕

abctf{FLAG}

https://kimiyuki.net/blog/2016/07/23/abctf-2016/

xyzqc

↕

abctf

Caesar cipher

ROT-
3

t3_qelrdeq_t3_k33a3a_lk3_lc_qe3p3

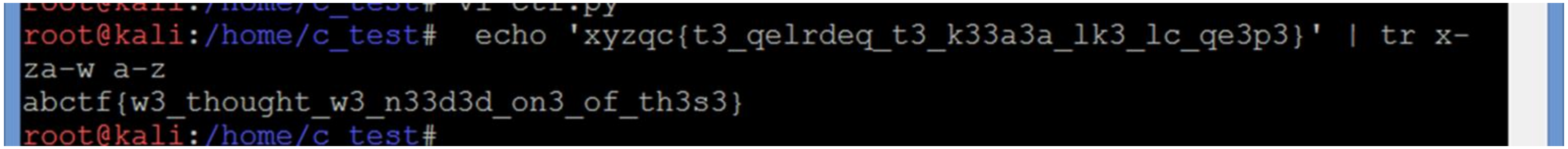
↓

w3_thought_w3_n33d3d_on3_of_th3s3

https://en.wikipedia.org/wiki/Caesar_cipher

解法四::使用tr指令

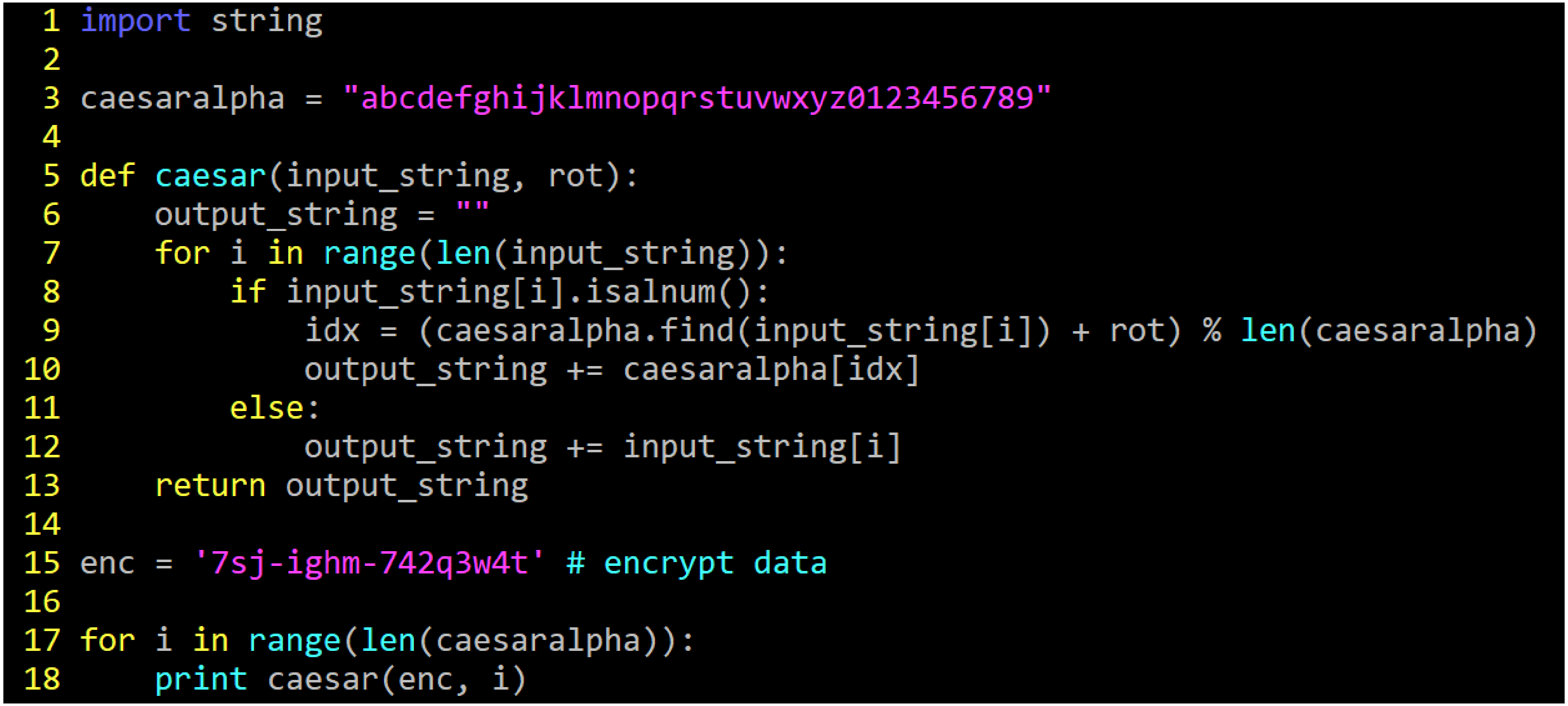
```
echo 'xyzqc{t3_qelrdeq_t3_k33a3a_lk3_lc_qe3p3}' | tr x-za-w a-z
```



```
root@kali:/home/c_test# vi ctf.py
root@kali:/home/c_test#  echo 'xyzqc{t3_qelrdeq_t3_k33a3a_lk3_lc_qe3p3}' | tr x-
za-w a-z
abctf{w3_thought_w3_n33d3d_on3_of_th3s3}
root@kali:/home/c_test#
```

tr -help

解法四::使用Python解解看



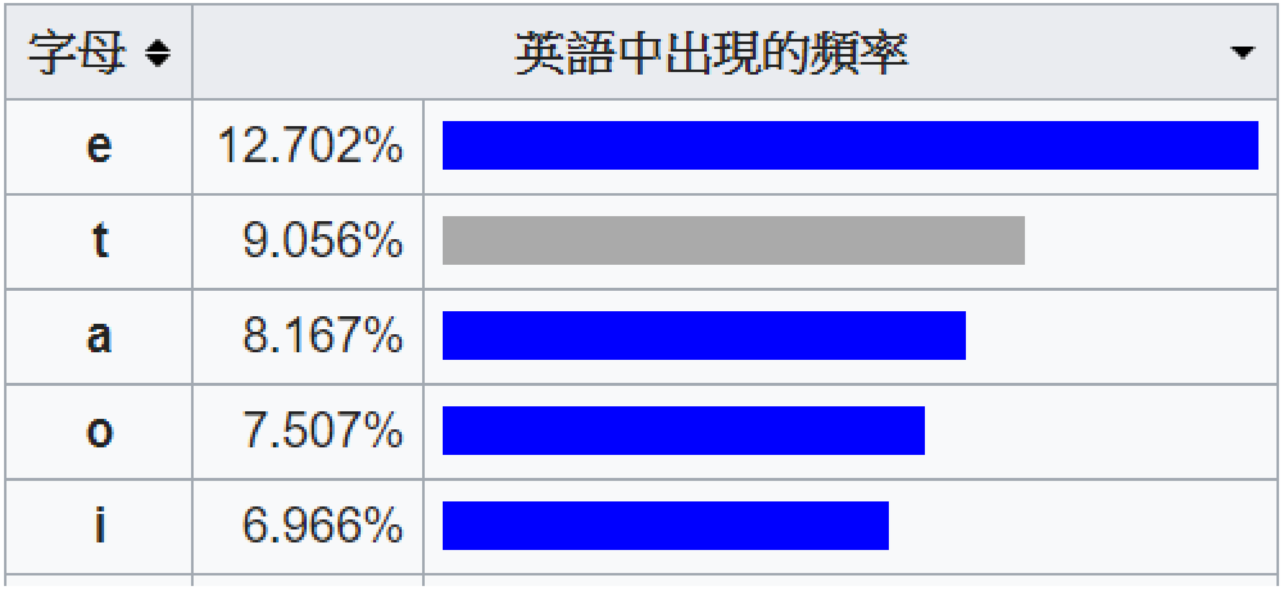
```python
import string

caesaralpha = "abcdefghijklmnopqrstuvwxyz0123456789"

def caesar(input_string, rot):
    output_string = ""
    for i in range(len(input_string)):
        if input_string[i].isalnum():
            idx = (caesaralpha.find(input_string[i]) + rot) % len(caesaralpha)
            output_string += caesaralpha[idx]
        else:
            output_string += input_string[i]
    return output_string

enc = '7sj-ighm-742q3w4t' # encrypt data

for i in range(len(caesaralpha)):
    print caesar(enc, i)
```

```
import string

caesaralpha = "abcdefghijklmnopqrstuvwxyz0123456789"

def caesar(input_string, rot):
    output_string = ""
    for i in range(len(input_string)):
        if input_string[i].isalnum():
            idx = (caesaralpha.find(input_string[i]) + rot) % len(caesaralpha)
            output_string += caesaralpha[idx]
        else:
            output_string += input_string[i]
    return output_string

enc = '7sj-ighm-742q3w4t' # encrypt data

for i in range(len(caesaralpha)):
    print caesar(enc, i)
```

替換式密碼の頻率分析法
Substitution cipher

https://zh.wikipedia.org/wiki/%E9%A2%91%E7%8E%87%E5%88%86%E6%9E%90

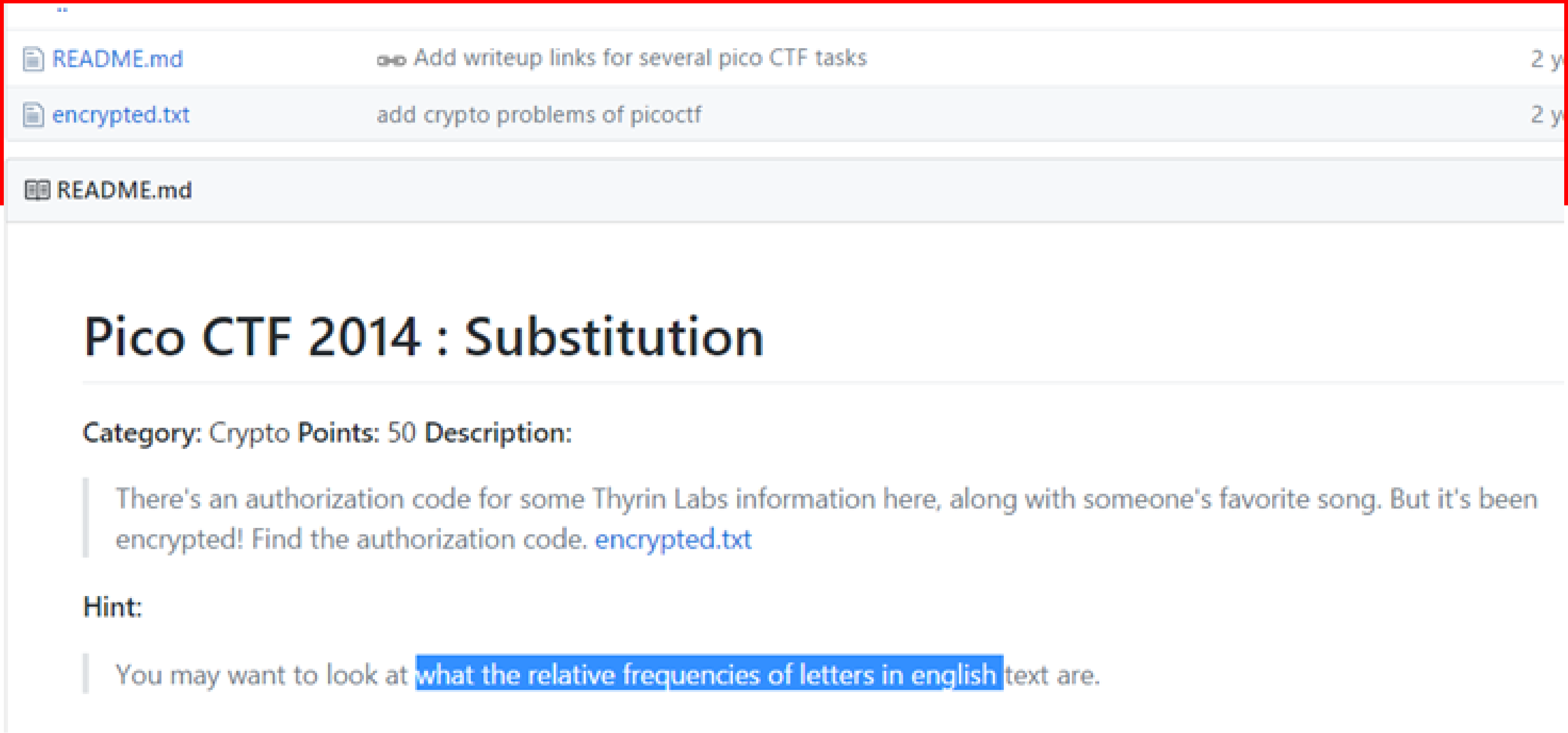
英文字母頻率



字母 ⬍	英語中出現的頻率 ▾	
e	12.702%	
t	9.056%	
a	8.167%	
o	7.507%	
i	6.966%	

Pico CTF 2014 : Substitution

https://github.com/VulnHub/ctf-writeups/blob/master/2014/picoctf/substitution.md



..

README.md	Add writeup links for several pico CTF tasks	2 y
encrypted.txt	add crypto problems of picoctf	2 y

README.md

Pico CTF 2014 : Substitution

Category: Crypto **Points:** 50 **Description:**

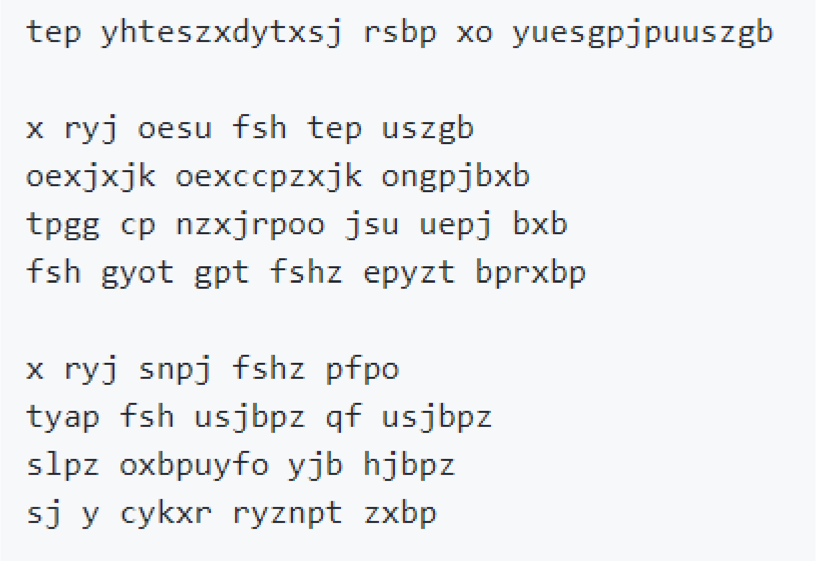
> There's an authorization code for some Thyrin Labs information here, along with someone's favorite song. But it's been encrypted! Find the authorization code. encrypted.txt

Hint:

> You may want to look at what the relative frequencies of letters in english text are.

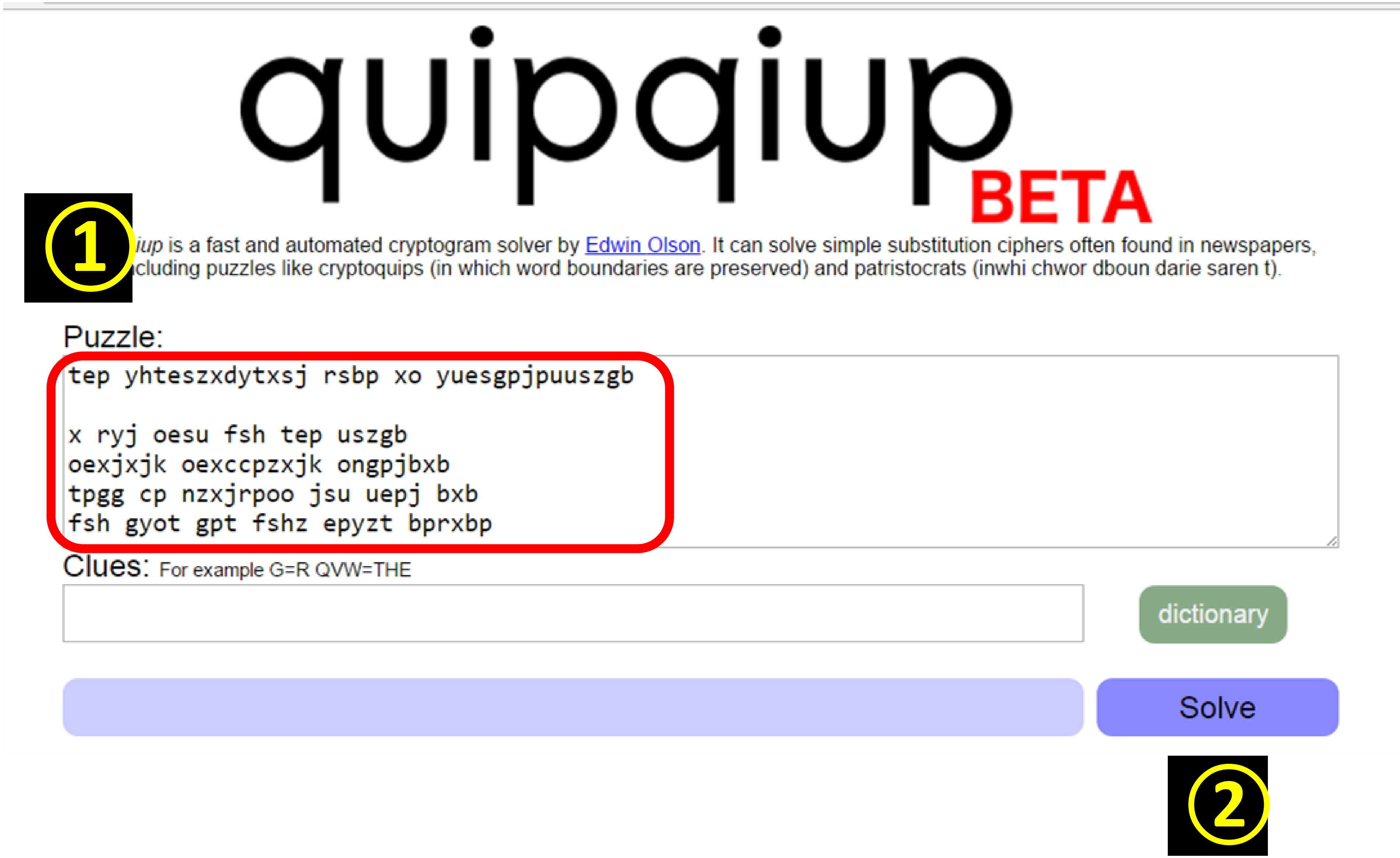
Pico CTF 2014 : Substitution

There's an authorization code for some Thyrin Labs information here, along with someone's favorite song. But it's been encrypted! Find the authorization code



```
tep yhteszxdytxsj rsbp xo yuesgpjpuuszgb

x ryj oesu fsh tep uszgb
oexjxjk oexccpzxjk ongpjbxb
tpgg cp nzxjrpoo jsu uepj bxb
fsh gyot gpt fshz epyzt bprxbp

x ryj snpj fshz pfpo
tyap fsh usjbpz qf usjbpz
slpz oxbpuyfo yjb hjbpz
sj y cykxr ryznpt zxbp
```

解法一:使用線上工具http://www.dcode.fr/scytale-cipher



iup is a fast and automated cryptogram solver by Edwin Olson. It can solve simple substitution ciphers often found in newspapers,
cluding puzzles like cryptoquips (in which word boundaries are preserved) and patristocrats (inwhi chwor dboun darie saren t).

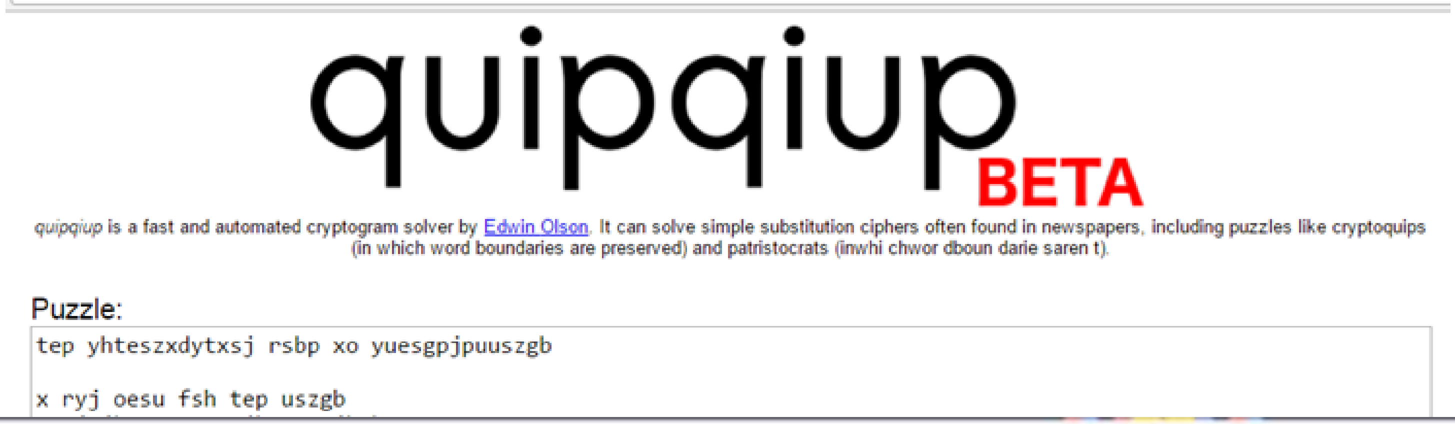
Puzzle:

```
tep yhteszxdytxsj rsbp xo yuesgpjpuuszgb

x ryj oesu fsh tep uszgb
oexjxjk oexccpzxjk ongpjbxb
tpgg cp nzxjrpoo jsu uepj bxb
fsh gyot gpt fshz epyzt bprxbp
```

Clues: For example G=R QVW=THE

解法一:使用線上工具

http://quipqiup.com/

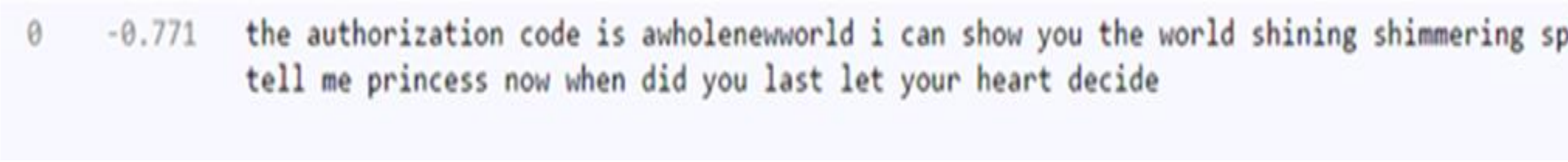


quipqiup BETA

quipqiup is a fast and automated cryptogram solver by Edwin Olson. It can solve simple substitution ciphers often found in newspapers, including puzzles like cryptoquips (in which word boundaries are preserved) and patristocrats (inwhi chwor dboun darie saren t).

Puzzle:

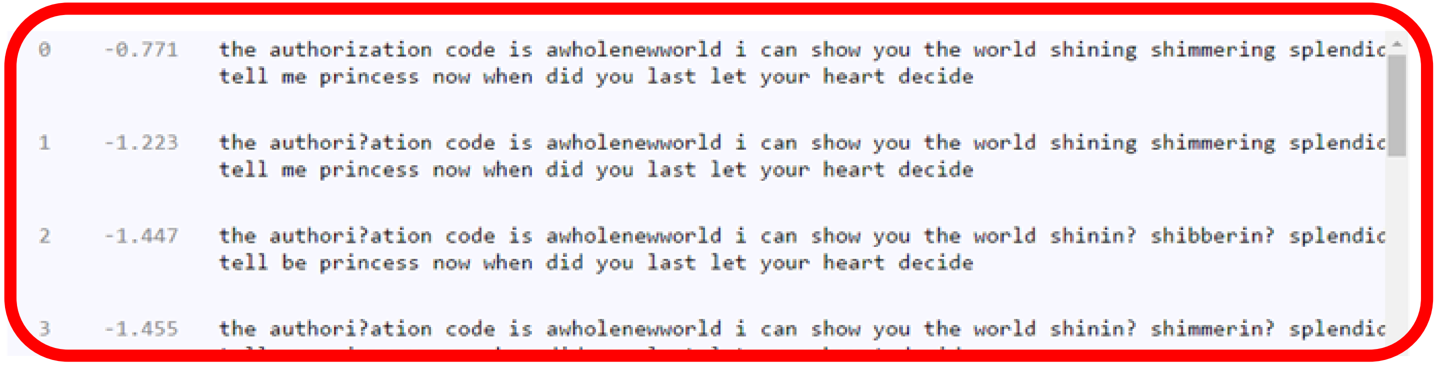
```
tep yhteszxdytxsj rsbp xo yuesgpjpuuszgb

x ryj oesu fsh tep uszgb
```



```
0    -0.771   the authorization code is awholenewworld i can show you the world shining shimmering sp
              tell me princess now when did you last let your heart decide
```

③

答案



```
0    -0.771   the authorization code is awholenewworld i can show you the world shining shimmering splendic
              tell me princess now when did you last let your heart decide

1    -1.223   the authori?ation code is awholenewworld i can show you the world shining shimmering splendic
              tell me princess now when did you last let your heart decide

2    -1.447   the authori?ation code is awholenewworld i can show you the world shinin? shibberin? splendic
              tell be princess now when did you last let your heart decide

3    -1.455   the authori?ation code is awholenewworld i can show you the world shinin? shimmerin? splendic
```

換位加密法
Transposition cipher

換位加密法 Transposition cipher

https://en.wikipedia.org/wiki/Transposition_cipher

- In cryptography, a transposition cipher is a method of encryption by which **the positions held by units of plaintext** (which are commonly characters or groups of characters) are shifted according to **a regular system**, so that the ciphertext constitutes a permutation of the plaintext.
- That is, the order of the units is changed (the plaintext is reordered). Mathematically a bijective function is used on the characters' positions to encrypt and an inverse function to decrypt.

Rail Fence cipher

Route cipher

Columnar transposition

Double transposition

Myszkowski transposition(1902)

Disrupted transposition

Grille (cryptography)

換位加密法の籬笆密碼法

Transposition cipher

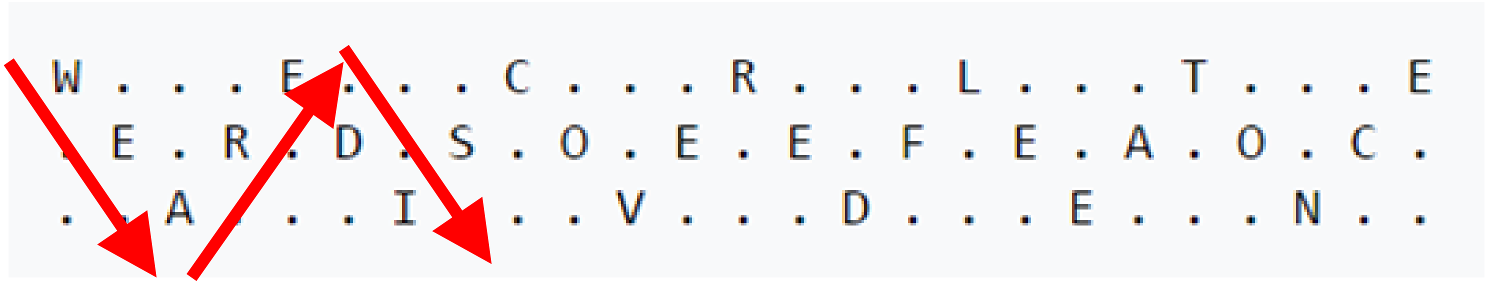
Rail fence cipher

Rail fence cipher::加密方法

https://en.wikipedia.org/wiki/Rail_fence_cipher

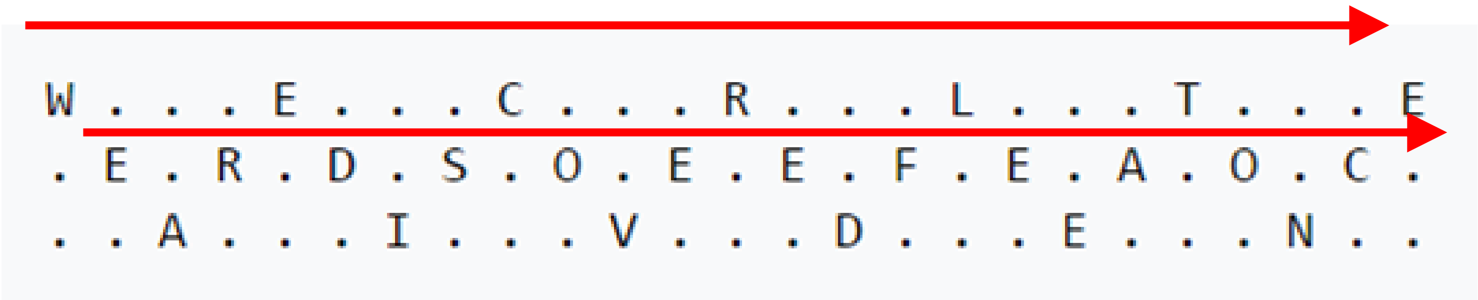
明文 'WE ARE DISCOVERED. FLEE AT ONCE'

步驟一 明文由上至下順序寫上，當到達最低部時，再回頭向上，一直重複直至整篇明文寫完為止



```
W . . . E . . . C . . . R . . . L . . . T . . . E
. E . R . D . S . O . E . E . F . E . A . O . C .
. . A . . . I . . . V . . . D . . . E . . . N . .
```

步驟二 產生密文:往右順序抄寫一次



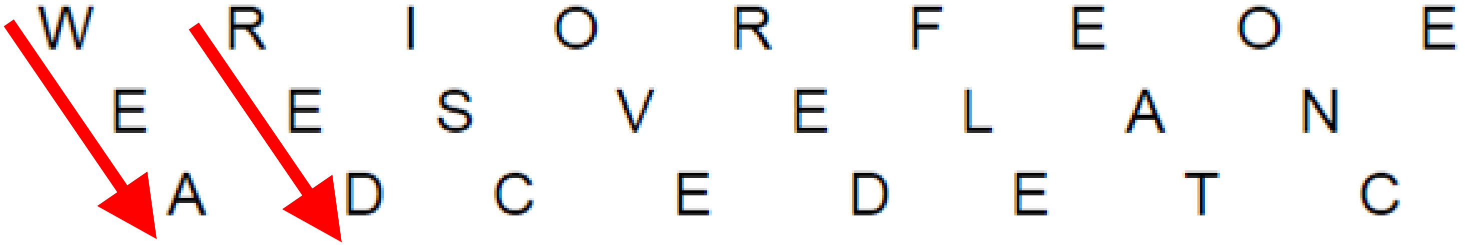
```
W . . . E . . . C . . . R . . . L . . . T . . . E
. E . R . D . S . O . E . E . F . E . A . O . C .
. . A . . . I . . . V . . . D . . . E . . . N . .
```

密文 WECRLTEERDSOEEFEAOCAIVDEN

如果改成下列規則,如何解密?

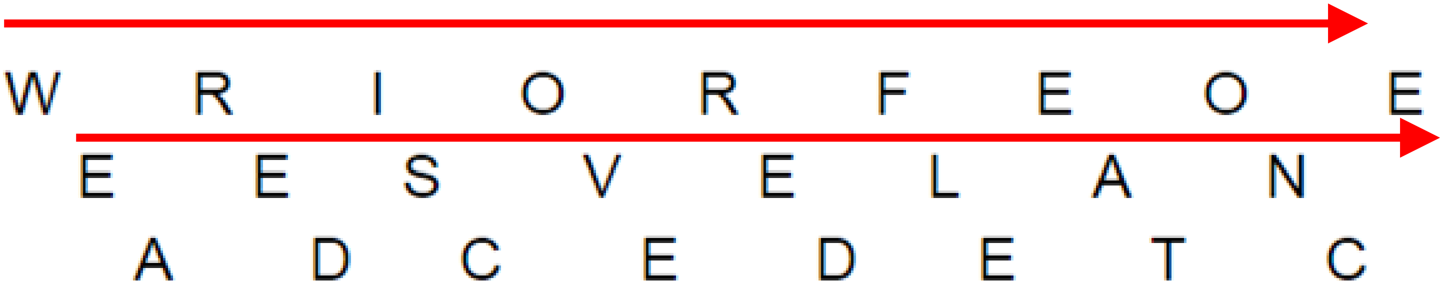
明文 'WE ARE DISCOVERED. FLEE AT ONCE'

步驟一 明文由上至下順序寫上，當到達最低部時，再回頭向上，一直重複直至整篇明文寫完為止



```
W   R   I   O   R   F   E   O   E
  E   E   S   V   E   L   A   N
    A   D   C   E   D   E   T   C
```

步驟二 產生密文:往右順序抄寫一次



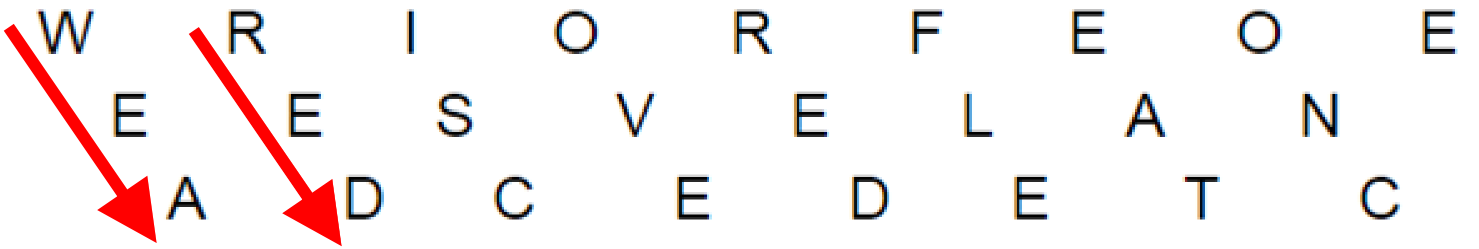
```
W   R   I   O   R   F   E   O   E
  E   E   S   V   E   L   A   N
    A   D   C   E   D   E   T   C
```

密文

Route cipher→如何解密?

明文 'WE ARE DISCOVERED. FLEE AT ONCE'

步驟一 明文由上至下順序寫上，當到達最低部時，再回頭向上，一直重複直至整篇明文寫完為止

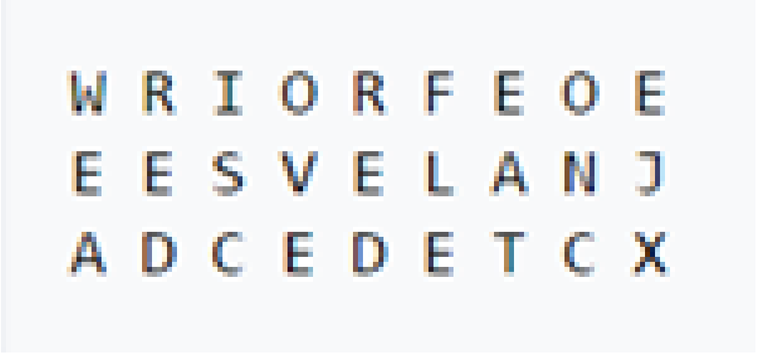


W R I O R F E O E

E E S V E L A N

A D C E D E T C

步驟二 產生密文:



W R I O R F E O E

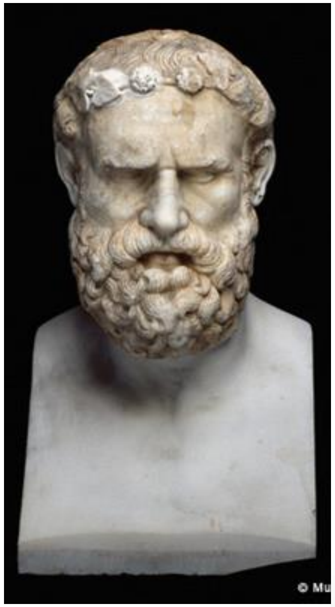
E E S V E L A N J

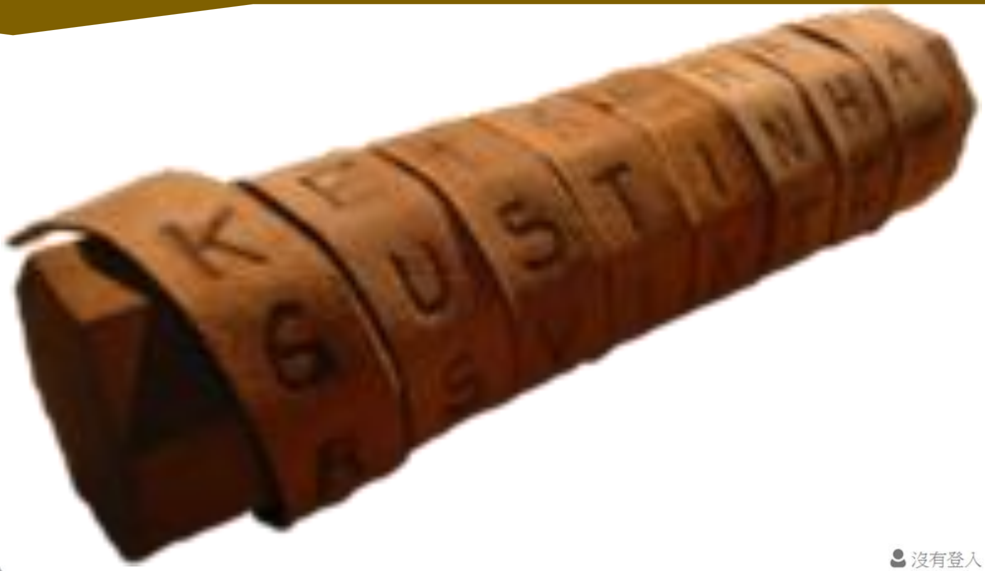
A D C E D E T C X

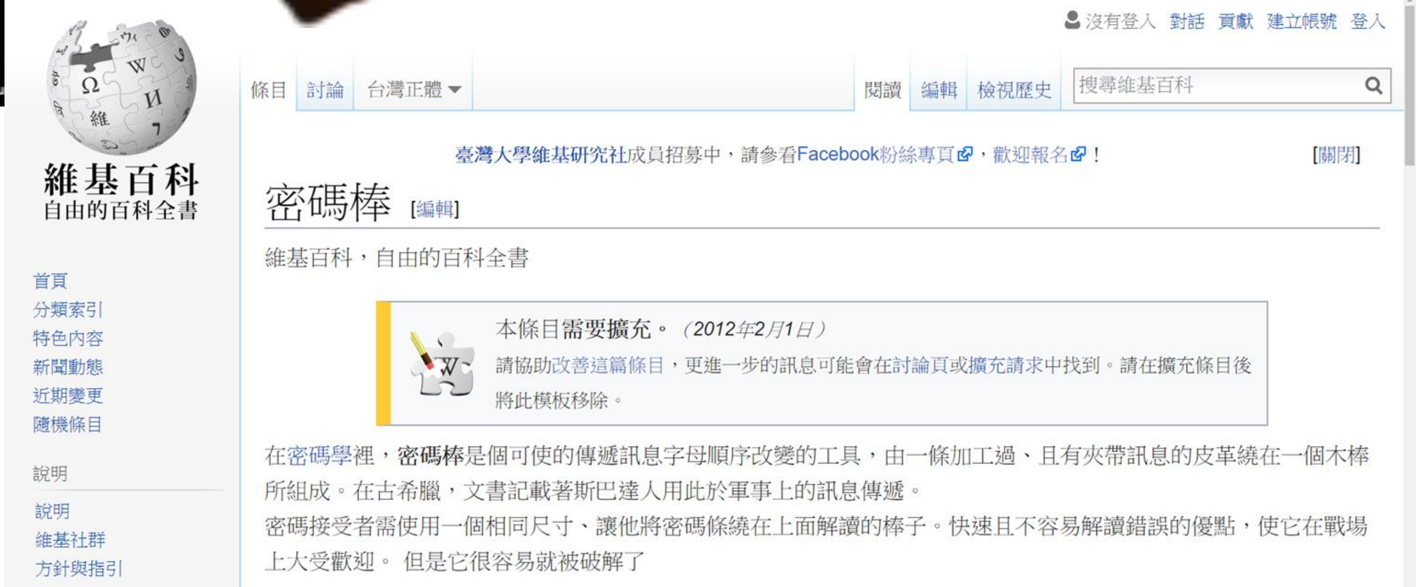
密文 WRIORFEOEEESVELANADCEDETC

Scytale cipher
密碼棒

西元前7世紀的希臘詩人 Archilochus







臺灣大學維基研究社成員招募中，請參看Facebook粉絲專頁，歡迎報名！ [關閉]

密碼棒 [編輯]

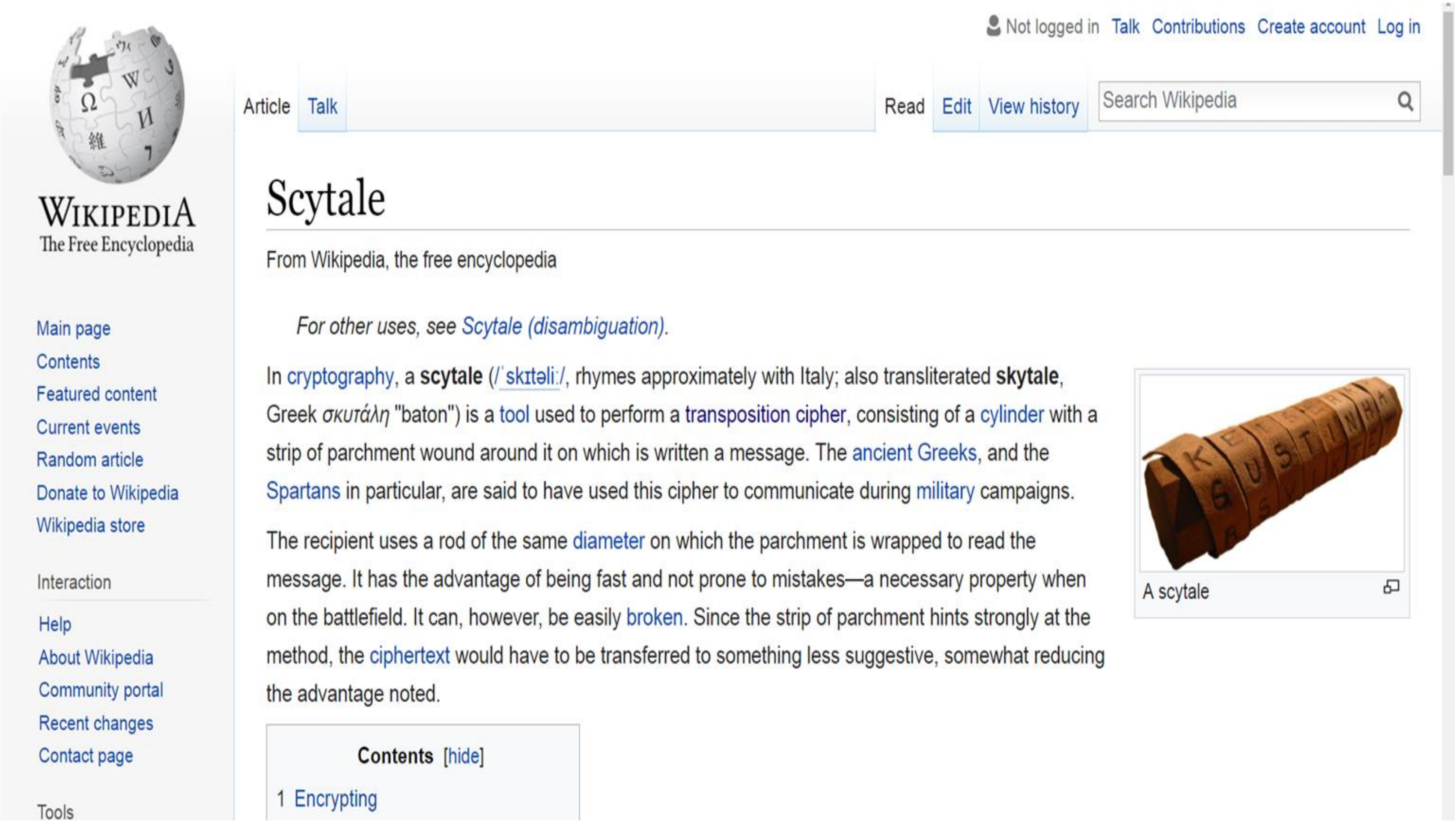
維基百科，自由的百科全書

本條目需要擴充。（2012年2月1日）
請協助改善這篇條目，更進一步的訊息可能會在討論頁或擴充請求中找到。請在擴充條目後將此模板移除。

在密碼學裡，**密碼棒**是個可使的傳遞訊息字母順序改變的工具，由一條加工過、且有夾帶訊息的皮革繞在一個木棒所組成。在古希臘，文書記載著斯巴達人用此於軍事上的訊息傳遞。
密碼接受者需使用一個相同尺寸、讓他將密碼條繞在上面解讀的棒子。快速且不容易解讀錯誤的優點，使它在戰場上大受歡迎。 但是它很容易就被破解了

Scytale cipher

https://en.wikipedia.org/wiki/Scytale



Scytale

From Wikipedia, the free encyclopedia

For other uses, see Scytale (disambiguation).

In cryptography, a **scytale** (/ˈskɪtəliː/, rhymes approximately with Italy; also transliterated **skytale**, Greek *σκυτάλη* "baton") is a tool used to perform a transposition cipher, consisting of a cylinder with a strip of parchment wound around it on which is written a message. The ancient Greeks, and the Spartans in particular, are said to have used this cipher to communicate during military campaigns.

A scytale

The recipient uses a rod of the same diameter on which the parchment is wrapped to read the message. It has the advantage of being fast and not prone to mistakes—a necessary property when on the battlefield. It can, however, be easily broken. Since the strip of parchment hints strongly at the method, the ciphertext would have to be transferred to something less suggestive, somewhat reducing the advantage noted.

Contents [hide]

Scytale cipher::加密方法

https://en.wikipedia.org/wiki/Scytale

假設那棒可寫下四個字母使之圍繞
成圓圈且5個字母可連成一線。

範例文字："Help me I am under attack".

H E L P M
E I A M U
N D E R A
T T A C K

"HENTEIDTLAEAPMRCMUAK"

Scytale cipher::解密方法

https://en.wikipedia.org/wiki/Scytale

假設那棒可寫下四個字母使之圍繞成圓圈且5個字母可連成一線。

範例文字："Help me I am under attack".

H E L P M
E I A M U
N D E R A
T T A C K

"HENTEIDTLAEAPMRCMUAK"

解密方法

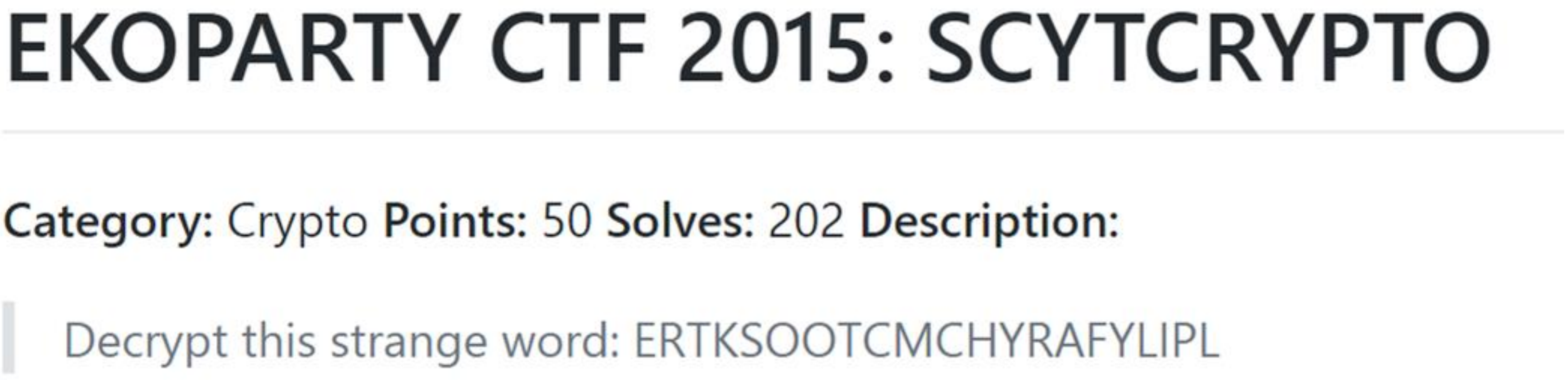
"HENTEIDTLAEAPMRCMUAK"

H	E	N	T
E	I	D	T
L	A	E	A
P	M	R	C
M	U	A	K

HELPMEIAMUNDERATTACK

EKOPARTY CTF 2015: SCYTCRYPTO

https://github.com/ctfs/write-ups-2015/tree/master/ekoparty-ctf-2015/crypto/cry50



EKOPARTY CTF 2015: SCYTCRYPTO

Category: Crypto **Points:** 50 **Solves:** 202 **Description:**

> Decrypt this strange word: ERTKSOOTCMCHYRAFYLIPL

答案格式:EKO{XXXXXXXXXXXXXXXXXXXXX}

神猜法

EKOPARTY CTF 2015: SCYTCRYPTO

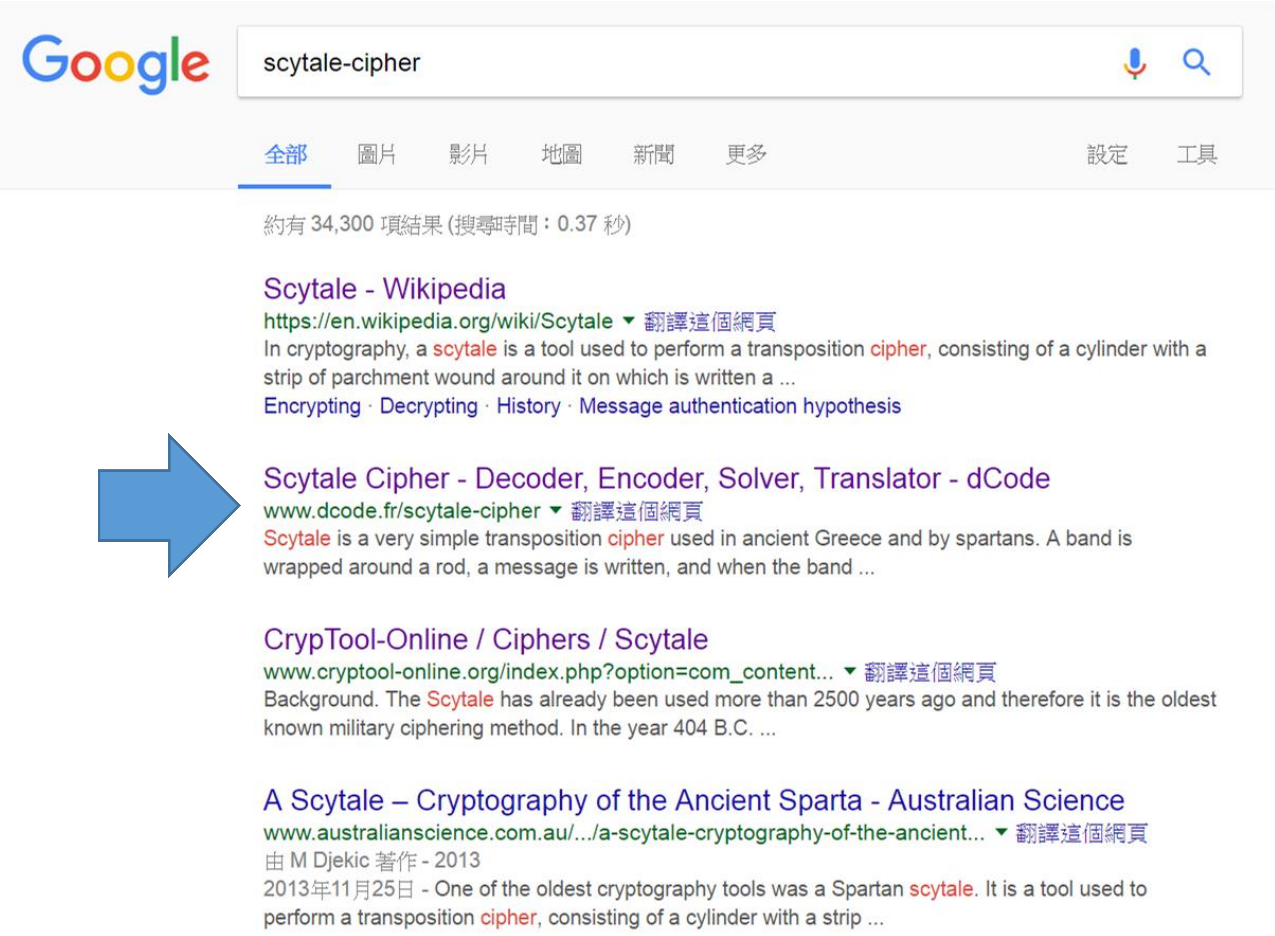
題目告訴你 → **SCYT**Crypto

題目又是密碼問題 ↓

scytale-cipher

www.dcode.fr/scytale-cipher

善用Google
看看



scytale-cipher

約有 34,300 項結果 (搜尋時間：0.37 秒)

Scytale - Wikipedia
https://en.wikipedia.org/wiki/Scytale ▾ 翻譯這個網頁
In cryptography, a scytale is a tool used to perform a transposition cipher, consisting of a cylinder with a strip of parchment wound around it on which is written a ...
Encrypting · Decrypting · History · Message authentication hypothesis

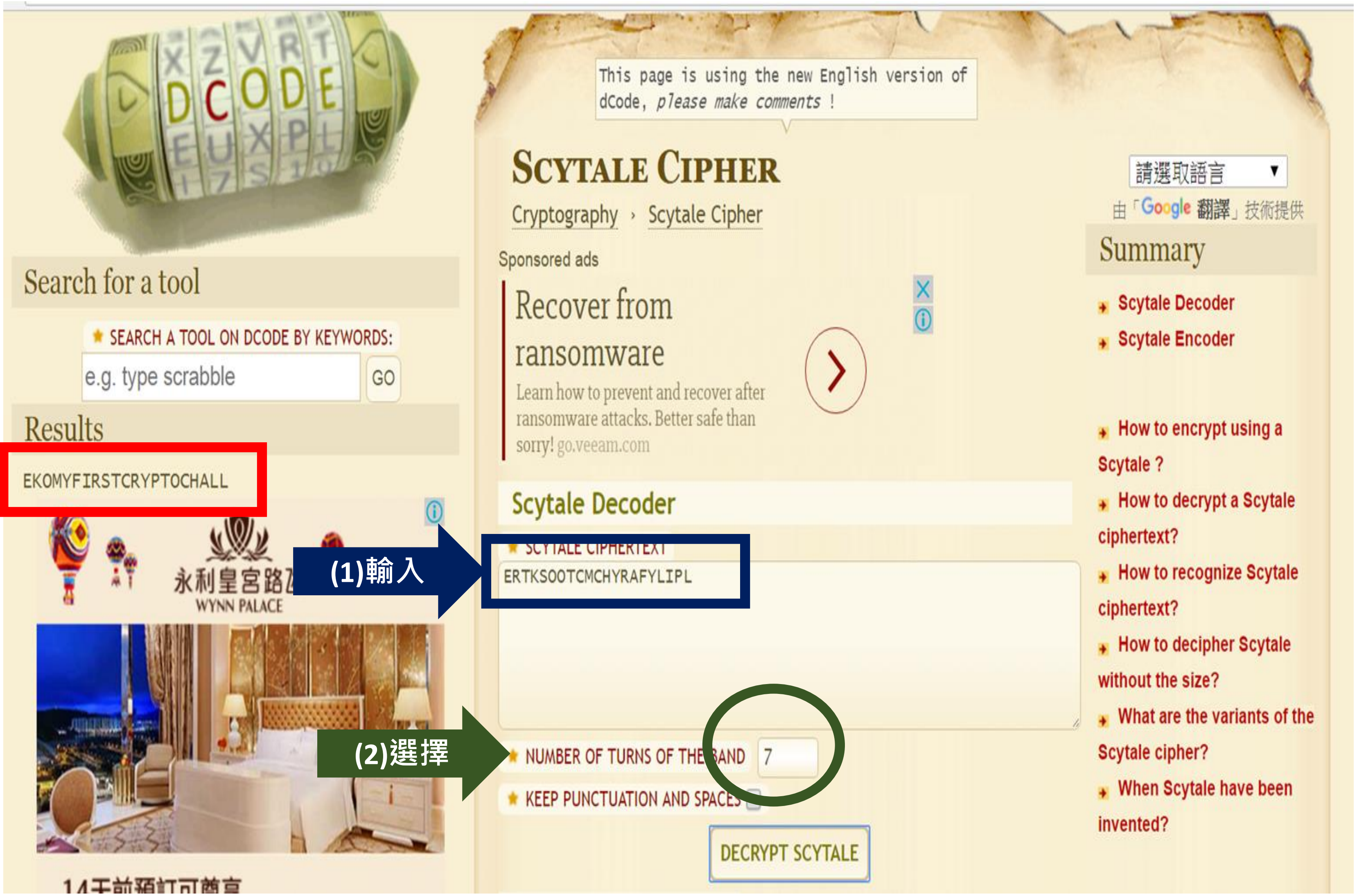
Scytale Cipher - Decoder, Encoder, Solver, Translator - dCode
www.dcode.fr/scytale-cipher ▾ 翻譯這個網頁
Scytale is a very simple transposition cipher used in ancient Greece and by spartans. A band is wrapped around a rod, a message is written, and when the band ...

CrypTool-Online / Ciphers / Scytale
www.cryptool-online.org/index.php?option=com_content... ▾ 翻譯這個網頁
Background. The Scytale has already been used more than 2500 years ago and therefore it is the oldest known military ciphering method. In the year 404 B.C. ...

A Scytale – Cryptography of the Ancient Sparta - Australian Science
www.australianscience.com.au/.../a-scytale-cryptography-of-the-ancient... ▾ 翻譯這個網頁
由 M Djekic 著作 - 2013
2013年11月25日 - One of the oldest cryptography tools was a Spartan scytale. It is a tool used to perform a transposition cipher, consisting of a cylinder with a strip ...

解法一:使用線上工具

http://www.dcode.fr/scytale-cipher


Search for a tool
★ SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type scrabble
GO
Results

EKOMYFIRSTCRYPTOCHALL

This page is using the new English version of dCode, *please make comments* !

Scytale Cipher

Cryptography › Scytale Cipher
Sponsored ads

Scytale Decoder

★ SCYTALE CIPHERTEXT

ERTKSOOTCMCHYRAFYLIPL

★ NUMBER OF TURNS OF THE BAND 7

★ KEEP PUNCTUATION AND SPACES □

DECRYPT SCYTALE
請選取語言 ▼
由「Google 翻譯」技術提供
Summary
Scytale Decoder
Scytale Encoder
How to encrypt using a Scytale ?
How to decrypt a Scytale ciphertext?
How to recognize Scytale ciphertext?
How to decipher Scytale without the size?
What are the variants of the Scytale cipher?
When Scytale have been invented?

(1)輸入

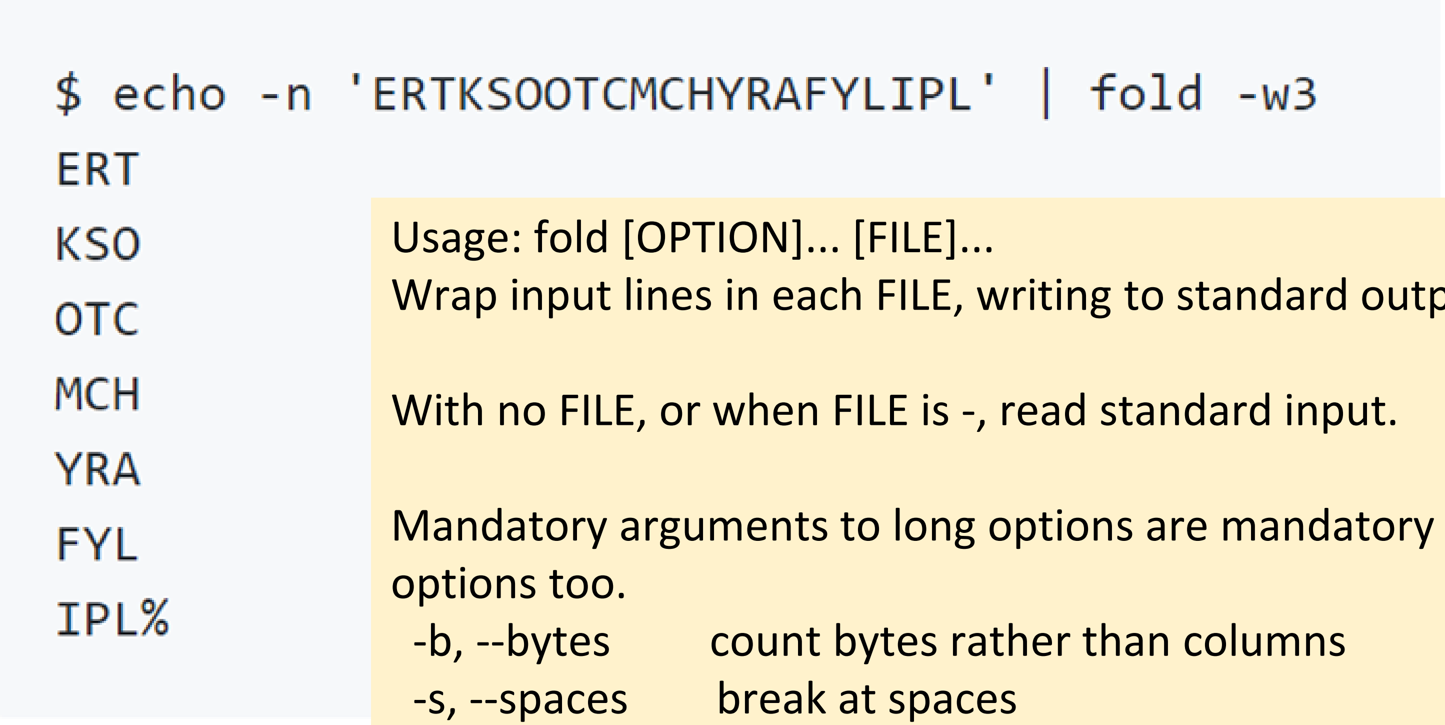
(2)選擇

(3)解答在此

解法二:使用linux command

EKO{MYFIRSTCRYPTOCHALL}

ERTKSOOTCMCHYRAFYLIPL



```
$ echo -n 'ERTKSOOTCMCHYRAFYLIPL' | fold -w3
ERT
KSO
OTC
MCH
YRA
FYL
IPL%
```

```
Usage: fold [OPTION]... [FILE]...
Wrap input lines in each FILE, writing to standard output.

With no FILE, or when FILE is -, read standard input.

Mandatory arguments to long options are mandatory for short
options too.
  -b, --bytes        count bytes rather than columns
  -s, --spaces        break at spaces
  -w, --width=WIDTH   use WIDTH columns instead of 80
  --help     display this help and exit
  --version  output version information and exit
```

crypto@CTF

AlexCTF Fore1-Hit_the_core

https://github.com/R3dCr3sc3nt/AlexCTF/blob/master/Fore1-Hit_the_core/README.md

fore1.core

解法

```
file fore1.core
```

```
strings fore1.core
```

```
cvqAeqacLtqazEigwiXobxrCrtuiTzahfFreqc{bnjrKwgk83kgd43j8
5ePgb_e_rwqr7fvbmHjklo3tews_hmkogooyf0vbnk0ii87Drfgh_
n kiwutfb0ghk9ro987k5tfb_hjiouo087ptfcv}
```

cvq**A**eqac**L**tqaz**E**igwi**X**obxrCrtuiTzahfFreqc{bnjrKwgk83kgd43
j85ePgb_e_rwqr7fvbmHjklo3tews_hmkogooyf0vbnk0ii87Drf
gh_n kiwutfb0ghk9ro987k5tfb_hjiouo087ptfcv}

解法

cvq**A**eqac**L**tqaz**E**igwi**X**obxrCrtuiTzahfFreqc{bnjrKwgk83kgd43j85ePgb_e_rwqr7fvbmHjklo3tews_hmkogooyf0vbnk0ii87Drfgh_n kiwutfb0ghk9ro987k5tfb_hjiouo087ptfcv}

```
cipher='cvqAeqacLtqazEigwiXobxrCrtuiTzahfFreqc{bnjrKwgk83kgd43j85ePgb_e_rwqr7fvbmHjklo3tews_hmkogooyf0vbnk0ii87Drfgh_n kiwutfb0ghk9ro987k5tfb_hjiouo087ptfcv}'


cipher=cipher[3:]
flag = ''
for x in range(0,len(cipher),1):
    if x%5==0:
        flag+=cipher[x]
print flag
```

```
python sol.py
```

```
ALEXCTF{K33P_7H3_g00D_w0rk_up}
```

解法

cvq**A**eqac**L**tqaz**E**igwi**X**obxrCrtuiTzahfFreqc{bnjrKwgk83kgd43j85ePgb_e_rwqr7fvbmHjklo3tews_hmkogooyf0vbnk0ii87Drfgh_n kiwutfb0ghk9ro987k5tfb_hjiouo087ptfcv}

```
cipher='cvqAeqacLtqazEigwiXobxrCrtuiTzahfFreqc{bnjrKwgk83kgd43j85ePgb_e_rwqr7fvbmHjklo3tews_hmkogooyf0vbnk0ii87Drfgh_n kiwutfb0ghk9ro987k5tfb_hjiouo087ptfcv}'

‘’.join(cipher[3 : : 5])
```

```
python sol.py
```

```
ALEXCTF{K33P_7H3_g00D_w0rk_up}
```