

1. Mod 26

- Rot13 là xoay(dịch) mỗi ký tự đi 13 chữ cái trong bảng 26 chữ.
- Dùng web rot13.com để dịch lại xâu đê cho.

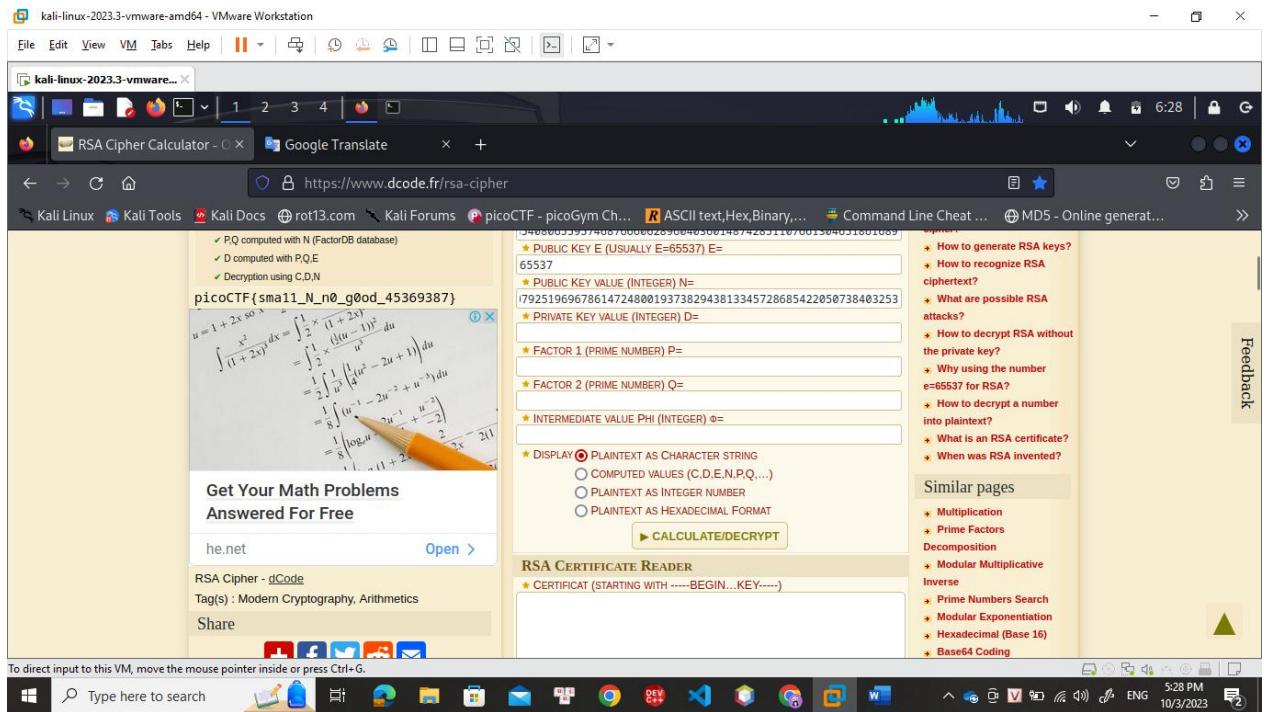
2. Mind your Ps and Qs

- Tìm hiểu về hệ mã hóa RSA:
 - + RSA là 1 hệ mã hóa bát đối xứng, tức là gồm 2 khóa: public key dùng để mã hóa và private key dùng để giải mã.
 - + Trong hệ mã hóa này, bất kỳ ai cũng có thể dùng public key để mã hóa nhưng chỉ người sở hữu private key mới có thể giải mã.
 - + Trong hệ mã hóa RSA, public key có thể chia sẻ công khai cho tất cả mọi người, hoạt động của RSA dựa trên 4 bước chính: sinh khóa, chia sẻ key, mã hóa và giải mã.
 - + Các ký hiệu trong hệ mã hóa RSA:
 - c: ciphertext (văn bản mã hóa)
 - n: modulus, là 1 số nguyên lớn được tạo thành bằng cách nhân 2 số nguyên tố lớn p, q lại với nhau.
 - e: public exponent (số mũ công khai)
 - p, q: 2 số nguyên tố lớn tạo ra n, 2 số này bí mật và không được công khai.
 - $\varphi(n)$: hàm euler phi, sử dụng để tính toán khóa công khai và khóa bí mật.
 - d: private exponent (số mũ bí mật), sử dụng trong quá trình giải mã ciphertext để khôi phục lại plaintext ban đầu.
 - m: plaintext (văn bản gốc)

```
n = p*q
φ(N) = (p-1)*(q-1)
d = e^-1 mod φ(N)
m = c^d mod n

find the factors of n to get p & q (http://factordb.com)
calculate φ(N) using p & q
calculate d using e and φ(N)
calculate m using c, d, n
```

- Lên google gõ rsa cipher decode, nhập các số đã biết rồi có thể tính các số còn lại hoặc tính luôn plaintext



3. Easy peasy

- Tìm hiểu về hệ mã hóa one time pad (OTP)
- + Trên lý thuyết thì one time pad không thể bị phá vỡ.
- + Đây là 1 dạng mã hóa sử dụng key để mã hóa plaintext thành ciphertext.
- + Plaintext XOR key = cipher text
- + Plaintext = key XOR cipher text
- + key phải có độ dài \geq độ dài plaintext
- Ở bài này đe đã cho cipher text (sau khi netcat thì thấy cờ đã được mã hóa)
- Nhiệm vụ là phải tìm được key để thực hiện phép xor tìm ra plaintext. Key này phải là key gốc và được tạo từ key trung gian có độ dài bằng với độ dài ciphertext.
- Ta thấy rằng ciphertext có 64 ký tự hexa \Rightarrow độ dài 32 byte vì mỗi 1 byte trong hệ hexa tương ứng với 2 ký tự.
- Mà trong code đe cho thì KEY_LEN = 50000, đã mất 32 byte để mã dùng cho ciphertext, do đó khi tạo key thì phải bắt đầu trong 49968 byte còn lại và độ dài mỗi lần tạo là 32 byte.
- Sau khi tạo xong key trung gian từ 1 ký tự bất kỳ, phải lấy key đó xor với 32 byte ký tự đó theo mã hexa, kết quả là key gốc.
- Dem key gốc xor với cipher text sẽ ra được plain text cần tìm.

Chi tiết:

Ciphertext

```
kali@kali: ~/Downloads
$ cd Downloads
(kali㉿kali)-[~/Downloads]
$ ls
otp.py
(kali㉿kali)-[~/Downloads]
$ nc mercury.picoctf.net 36449
*****#Welcome to our OTP implementation!*****
This is the encrypted flag!
551257106e1a52095f654f510a6b4954026c1e0304394100043a1c5654505b6b
What data would you like to encrypt? ^C
```

Số ký tự trong ciphertext

```
kali@kali: ~/Downloads
$ cd Downloads
(kali㉿kali)-[~/Downloads]
$ ls
otp.py
(kali㉿kali)-[~/Downloads]
$ nc mercury.picoctf.net 36449
*****#Welcome to our OTP implementation!*****
This is the encrypted flag!
551257106e1a52095f654f510a6b4954026c1e0304394100043a1c5654505b6b
What data would you like to encrypt? ^C
(kali㉿kali)-[~/Downloads]
$ python -c "len('551257106e1a52095f654f510a6b4954026c1e0304394100043a1c5654505b6b')"
dquote>
(kali㉿kali)-[~/Downloads]
$ python -c "len('551257106e1a52095f654f510a6b4954026c1e0304394100043a1c5654505b6b')"
dquote>
(kali㉿kali)-[~/Downloads]
$ python
Python 3.11.4 (main, Jun 7 2023, 10:13:09) [GCC 12.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> len('551257106e1a52095f654f510a6b4954026c1e0304394100043a1c5654505b6b')
64
>>>
```

Có thẻ kiểm tra bằng lệnh

```
python -c
print(len('551257106e1a52095f654f510a6b4954026c1e03043941000
43a1c5654505b6b'))"
```

The screenshot shows a Kali Linux 2023.3 VM running in VMware Workstation. The terminal window displays a challenge from the Pwned challenge set. The user has run a command to calculate the length of a string, resulting in the value 64. The challenge interface shows the user has solved 64 out of 164 possible challenges.

Tạo key trung gian (cipher text của 1 ký tự bất kỳ)

Do sử dụng ký tự a tạo key trung gian nên plaintext của ký tự này là một chuỗi hexa gồm 32 số 61 (vì trong bảng ascii thì a có mã hexa là 61)

Đem xor plaintext của a với ciphertext của a để tìm key gốc.

Sử dụng cyberchef

From hex là ciphertext của a

Xor với key là plaintext

Kết quả (key gốc) là to hex

The screenshot shows the CyberChef interface with the following configuration:

- Input:** 034605413d190050083d1951533d1902053d1903003d1902553d190403500f3d
- From Hex:** Delimiter set to "Auto".
- XOR:** Key is 61616161616161... (partial key shown), Scheme is "Standard".
- To Hex:** Delimiter set to "None", Bytes per line set to 0.
- Output:** The resulting hex output is 622764205c786131695c7830325c7863645c7862615c7863345c786562316e5c.

At the bottom, there is a green button labeled "BAKE!" with a chef icon, and a checked checkbox for "Auto Bake".

Lấy key gốc xor với ciphertext của flag

The screenshot shows the CyberChef interface with the following details:

- Operations:** A sidebar on the left containing various conversion tools like "To HTML Entity", "To Hex", "PEM to Hex", "To Hexdump", "To Hex Content", "Object Identifier to Hex", "To Charcode", "Convert to NATO alphabet", "Split Colour Channels", "Image Hue/Saturation/Lightness", "HASS Client Fingerprint", "HASS Server Fingerprint", and "JA3 Fingerprint".
- Recipe:** The main workspace is titled "Recipe" and contains the following sections:
 - From Hex:** Set to "Auto" Delimiter.
 - XOR:** Key is "551257106e1a52...", Scheme is "Standard".
 - Null preserving is checked.
 - To Hex:** Delimiter is "None" and Bytes per line is "0".
- Input:** Hex value: 622764205c786131695c7830325c7863645c7862615c7863345c786562316e5d
- Output:** Hex value: 3735333032623338363937613837313766306661656539633066643336613537
- Buttons:** "BAKE!" and "Auto Bake".
- Bottom Navigation:** Buttons for "SMS", "Raw Bytes", and "LF".

Kết quả đang ở dạng hex, cần chuyển sang mã ascii submit.

4. New Caesar:

- Bài này cờ (plaintext) được mã hóa như sau:

Xét từng ký tự trong plaintext, chuyển ký tự đó sang nhị phân (8 bit), chia đôi cụm nhị phân đó thành 2 phần mỗi phần 4 bit, với mỗi phần thì lại chuyển nó thành chữ (ASCII).

- Giải mã như sau: Xét cụm mã hóa ciphertext (cụm để bài cho)
- Mỗi ký tự của ciphertext giải mã bằng cách dịch chuyển theo key.
- Key trong bài này là ký tự thuộc từ a-p (16 chữ cái), giả sử dịch chuyển theo a tức là dịch đi 0 ký tự (giữ nguyên), theo b là dịch đi 1 ký tự => Tương tự phép Rot. Lưu ý rằng key này được sinh ngẫu nhiên trong 16 ký tự nên lúc in ra cờ thì phải tìm cờ đọc được để submit.
- Sau khi dịch xong từng ký tự trong ciphertext, ta được chuỗi plaintext đã dịch, tuy nhiên do cờ được mã hóa bằng cách chia đôi bit trong từng ký tự nên cần thêm hàm giải mã điều này.
- Duyệt cụm plaintext đã dịch với bước nhảy 2 (trong mỗi lần duyệt xét 2 ký tự). Tìm giá trị số nguyên của 2 ký tự rồi lấy t1 dịch trái 4 bit (thêm 4 bit 0 ở cuối) cộng với t2, mục đích là để tạo thành chuỗi 8 bit. Sau đó chuyển nó sang mã ASCII.
- Chi tiết

Hàm mã hóa:

```
def bi6_encode(plain):  
    enc = ""  
    for c in plain:  
        binary = "{0:08b}".format(ord(c))  
        enc += ALPHABET[int(binary[:4], 2)]  
        enc += ALPHABET[int(binary[4:], 2)]  
    return enc
```

Hàm dịch theo key:

```
def shift(c, k):  
    t1 = ord(c) - LOWERCASE_OFFSET  
    t2 = ord(k) - LOWERCASE_OFFSET  
    return ALPHABET[(t1 + t2) % len(ALPHABET)]
```

Hàm giải mã:

```

def decode(plaintext_shifted):
    dec = ""
    for i in range(0, len(plaintext_shifted), 2): # duyệt cờ mã hóa với bước nhảy là 2
        t1 = ord(plaintext_shifted[i]) - LOWERCASE_OFFSET      # tính giá trị số nguyên của t1
        t2 = ord(plaintext_shifted[i+1]) - LOWERCASE_OFFSET    # tính giá trị số nguyên của t2
        dec += chr((t1<<4)+t2)    # chuyển sang mã ASCII, lưu ý rằng t1 phải dịch trái 4 bit
                                    # (thêm 4 bit 0 ở cuối) để cộng được với t2 thành dây đủ 8 bit
    return dec

```

1 usage

Full code:

Code để cho

```

Project Files
  C:\Users\Truong Son\Pyc
    > .idea
    > venv
    Caesar_decode.py
    main.py

main.py
9     binary = "{0:08b}".format(ord(c))
10    enc += ALPHABET[int(binary[:4], 2)]
11    enc += ALPHABET[int(binary[4:], 2)]
12
13
14 def shift(c, k):
15     t1 = ord(c) - LOWERCASE_OFFSET
16     t2 = ord(k) - LOWERCASE_OFFSET
17     return ALPHABET[(t1 + t2) % len(ALPHABET)]
18
19 flag = "redacted"
20 key = "redacted"
21 #assert all([k in ALPHABET for k in key])
22 #assert len(key) == 1
23
24 b16 = b16_encode(flag)
25 enc = ""
26 for i, c in enumerate(b16):
27     enc += shift(c, key[i % len(key)])
28 print(enc)
29

b16_encode() > for c in plain

```

Type here to search 11:52 CRLF UTF-8 8 spaces* Python 3.11 (NewCaesar_PicoCTF) 6:00 PM 10/4/2023

Code giải mã

```

Project Files
  C:\Users\Truong Son\Pycf
    idea
    venv
      Caesar_decode.py
      main.py

main.py Caesar_decode.py

1 import string
2
3 LOWERCASE_OFFSET = ord("a") # 97
4 ALPHABET = string.ascii_lowercase[16:] # a-p
5
6 usage
7 def decode(plaintext_shifted):
8     dec=""
9     for i in range(0, len(plaintext_shifted), 2): # duyệt cờ mã hóa với bước nhảy là 2
10        t1 = ord(plaintext_shifted[i]) - LOWERCASE_OFFSET # tính giá trị số nguyên của t1
11        t2 = ord(plaintext_shifted[i+1]) - LOWERCASE_OFFSET # tính giá trị số nguyên của t2
12        dec += chr((t1<=4)+t2) # chuyển sang mã ASCII, lưu ý rằng t1 phải dịch trái 4 bit
13        # (thêm 4 bit 0 ở cuối) để cộng được với t2 thành đầy đủ 8 bit
14
15    return dec
16
17 usage
18 def shift(c, k):
19     t1 = ord(c) - LOWERCASE_OFFSET
20     t2 = ord(k) - LOWERCASE_OFFSET
21     return ALPHABET[(t1 + t2) % len(ALPHABET)]
22
23 enc_flag = "mlnklnknljflfjljnjjjjmmjkmljnjhmhjgjnjjjmkkjijhmkjhpkmkmkljkijnjpmhmjjgjj"
24
25 for key in ALPHABET: # duyệt key trong 16 chữ cái từ a-p, phép dịch dựa vào key
26     plaintext="" # chuỗi ký tự sau khi dịch theo key
27     for i, c in enumerate(enc_flag): # duyệt trên cờ mã hóa, với i là index và c là giá trị của từng ký tự
28         plaintext += shift(c, key[i % len(key)]) # tiến hành dịch từng ký tự dựa vào key và cộng vào plaintext
29
30 flag = decode(plaintext) # giải mã plaintext
31 print("This is flag:", flag)

```

```

Project Files
  C:\Users\Truong Son\Pycf
    idea
    venv
      Caesar_decode.py
      main.py

main.py Caesar_decode.py

1 for i in range(0, len(plaintext_shifted), 2): # duyệt cờ mã hóa với bước nhảy là 2
2     t1 = ord(plaintext_shifted[i]) - LOWERCASE_OFFSET # tính giá trị số nguyên của t1
3     t2 = ord(plaintext_shifted[i+1]) - LOWERCASE_OFFSET # tính giá trị số nguyên của t2
4     dec += chr((t1<=4)+t2) # chuyển sang mã ASCII, lưu ý rằng t1 phải dịch trái 4 bit
5     # (thêm 4 bit 0 ở cuối) để cộng được với t2 thành đầy đủ 8 bit
6
7 return dec
8
9 usage
10 def shift(c, k):
11     t1 = ord(c) - LOWERCASE_OFFSET
12     t2 = ord(k) - LOWERCASE_OFFSET
13     return ALPHABET[(t1 + t2) % len(ALPHABET)]
14
15 enc_flag = "mlnklnknljflfjljnjjjjmmjkmljnjhmhjgjnjjjmkkjijhmkjhpkmkmkljkijnjpmhmjjgjj"
16
17 for key in ALPHABET: # duyệt key trong 16 chữ cái từ a-p, phép dịch dựa vào key
18     plaintext="" # chuỗi ký tự sau khi dịch theo key
19     for i, c in enumerate(enc_flag): # duyệt trên cờ mã hóa, với i là index và c là giá trị của từng ký tự
20         plaintext += shift(c, key[i % len(key)]) # tiến hành dịch từng ký tự dựa vào key và cộng vào plaintext
21     flag = decode(plaintext) # giải mã plaintext
22     print("This is flag:", flag)

```

5. The Numbers

Chuyển số sang chữ (bảng chữ cái tiếng Anh)

6. Easy!

Table cho ta biết đây là Vigenere Cipher

Vigenere Cipher (Dạng bảng): Sẽ cho 1 ciphertext, 1 key và 1 table. Cách giải mã là dùng table để ánh xạ từng chữ cái. Với từng ký tự ciphertext ta

nhìn vào hàng của ký tự đó, còn với từng ký tự của key ta nhìn vào cột, giao nhau tại đâu thì đó chính là ký tự được giải mã.

Có thể dùng web Vigenera Cipher decode để giải mã.

7. 13

Rot13

8. caesar

Lên web caesar decode để giải mã bằng cách brute force tất cả các trường hợp của ciphertext (tìm cụm từ có nghĩa rồi submit)

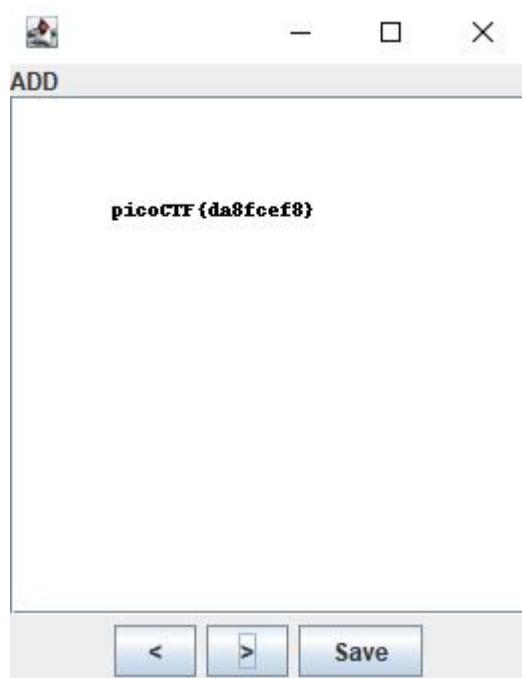
9. Pixelated

Kỹ thuật mã hóa dùng trong bài này là tách plaintext ra rồi đặt trong 2 ảnh khác nhau.

Do đó để giải mã thì cần xếp chồng 2 ảnh lên nhau.

Dùng Stegsolve để giải quyết bài này.

Mở stegsolve -> File -> Open -> chọn ảnh 1 -> Analyze -> image combiner -> chọn ảnh 2



10.spelling-quiz

Kỹ thuật mã hóa dùng trong bài này là dịch chuyển ký tự, khá giống mật mã caesar nhưng bài này có key để giải mã.

Lên google gõ cipher decode rồi vào Boxentriq. com, vào Cipher Identifier tools cop ciphertext vào để nhận diện là kiểu mã hóa nào. => monoalpha...

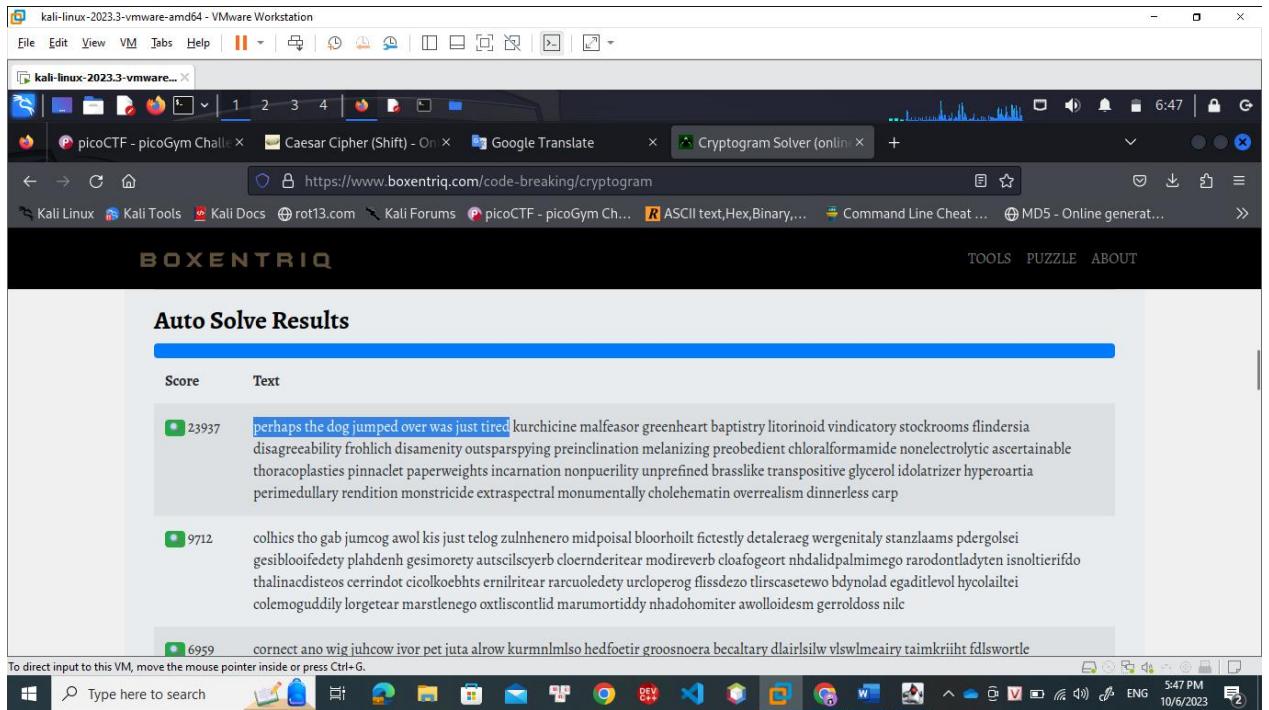
Cop cả ciphertext và studyguide vào rồi autosolve, cụm từ có khả năng là plaintext sẽ xuất hiện ở đầu.

The screenshot shows a Kali Linux VM running in VMware Workstation. The browser window is displaying the Boxentriq website. The URL in the address bar is <https://www.boxentriq.com/code-breaking/cipher-identifier>. The page content includes:

- Analysis Results**
- Ciphertext: brcfxba_vfr_mid_hosbrm_iprc_exa_hoav_vwcrm
- Your ciphertext is likely of this type: **Monoalphabetic Substitution Cipher (click to read more)**
- A sidebar titled "Votes" lists:
 - 1. BEST CRYPTOS TO BUY NOW
 - 2. CARTES BANCAIRES SANS FRAIS
 - 3. CRYPTOCURRENCIES TO BUY IN 2023
 - 4. FREE ROBUX CODES

The screenshot shows a Kali Linux VM running in VMware Workstation. The browser window is displaying the Boxentriq website. The URL in the address bar is <https://www.boxentriq.com/code-breaking/cryptogram>. The page content includes:

- Substitution Cipher Solver Tool**
- Ciphertext input field: brcfxba_vfr_mid_hosbrm_iprc_exa_hoav_vwcrm
- Action buttons: Copy, Paste, Text Options..., Start Manual Solving, Auto Solve
- Language dropdown: English



Thêm dấu _ giữa các từ rồi cho vào picoCTF{}

11. basic-mod1

```

1 x=[128, 322, 353, 235, 336, 73, 198, 332, 202, 285, 57, 87, 262, 221, 218, 405, 335, 101, 256, 227, 112, 140]
2 for i in range(len(x)):
3     x[i]%=37
4     print(x)
5     s=""
6     for i in range(len(x)):
7         if (x[i]<26):           #nếu x[i]<26 thi in ra ký tự hoa
8             s+=chr(ord('A')+x[i])
9         elif (x[i]<36):        #in ra số dạng thập phân
10            s+=chr(ord('0')+(x[i]-26))
11        else:
12            s+=" "
13     print(s)

```

12. basic-mod2

Cop đoạn mã để cho rồi decode theo modular 41 inverse

Python giải quyết yêu cầu đề bài

```

x=[28, 14, 22, 30, 18, 32, 30, 12, 25, 37, 8, 31, 18, 4, 37, 3, 33, 35, 27, 2, 4, 3, 28]
s=""
for i in range(len(x)):
    if (x[i]<=26):
        s+=chr(ord('A'))+(x[i]-1)
    elif (x[i]<=36):
        s+=chr(ord('0'))+(x[i]-27)
    else:
        s+= "-"
print(s)

```

Chú ý ở bài trước là 0-25 thì in ra ký tự, còn ở bài này là 1-26, do đó phải lấy `ord('A')+(x[i]-1)`, trường hợp in ra số cũng tương tự.

13. credstuff:

- Giải nén file tải về, thấy có 2 file txt là user và password.
- Mỗi user tương ứng với 1 password.
- Tìm pass ứng với user cultiris.
- Thử decode theo caesar cipher thì thấy cờ pico xuất hiện

CAESAR CIPHER DECODER

★ CAESAR SHIFTED CIPHERTEXT [?](#)
CVpDPGS{P7eL5_54I35_71Z3}

Test all possible shifts (26-letter alphabet A-Z) [DECRYPT \(BRUTEFORCE\)](#)

MANUAL DECRYPTION AND PARAMETERS

★ SHIFT/KEY NUMBER: 10

(●) USE THE ENGLISH ALPHABET (26 LETTERS FROM A TO Z)
 ○ USE THE ENGLISH ALPHABET AND ALSO SHIFT THE DIGITS 0-9
 ○ USE THE LATIN ALPHABET IN THE TIME OF CAESAR (23 LETTERS, NO J, U OR W)
 ○ USE THE ASCII TABLE (0-127) AS ALPHABET
 ○ USE A CUSTOM ALPHABET (A-Z/0-9 CHARS ONLY)
 0123456789ABCDEFHJKLMNOPQRSTUVWXYZ

[DECRYPT](#)

See also: ROT Cipher – Shift Cipher

CAESAR ENCODER

★ CAESAR CODE PLAIN TEXT [?](#)
dcode Caesar

★ SHIFT/KEY NUMBER: 3

(●) USE THE ENGLISH ALPHABET (26 LETTERS FROM A TO Z)
 ○ USE THE ENGLISH ALPHABET AND ALSO SHIFT THE DIGITS 0-9

Similar pages

- ★ ROT Cipher
- ★ Shift Cipher
- ★ Vigenere Cipher
- ★ Keyboard Shift Cipher
- ★ ROT1 Cipher
- ★ ROT-13 Cipher
- ★ ROT-47 Cipher

14. Morse code:

Chuyển mã Morse dạng audio sang text.

15. Rail fence:

Mật mã rail fence (mã hóa theo kiểu hàng rào)

Giải mã cipher text với 4 rail

16. Substitution 0

Gõ cipher analyzer để xem đây là loại thay thế nào thì thấy là mono...

Gõ mono... decode, cop ciphertext và key vào rồi decode

MONO-ALPHABETIC SUBSTITUTION

Cryptography - Substitution Cipher - Mono-alphabetic Substitution

MONOALPHABETIC SUBSTITUTION DECODER

★ MONOALPHABETIC SUBSTITUTION CIPHERTEXT
R Z O T H D N B V S X K F C A P Y W H Q E I G L U J
⇒ OHNFUMwSVZLXEGCPtAjDyIRkOB (Original Encryption Alphabet)
⇒ RZOTMDNBVSVXKFCAPYwHQEIGLUJ (Reciprocal Decryption Alphabet)

| | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S | U | A | Y | P | C | G | X | U | W | A | O | G | F | D | A | C | J | U | R | V |
| H | E | R | E | U | P | O | N | L | E | G | R | A | N | T | I | Z | W | I | K | B |
| D | S | O | W | A | O | I | U | O | G | F | J | D | O | U | X | Q | O | V | A | T |
| T | H | A | G | R | A | V | E | A | N | S | U | S | D | U | H | U | D | X | Y | W |
| A | N | D | B | R | O | G | H | C | A | Y | W | S | D | E | T | L | T | Z | Y | Z |
| U | M | A | C | E | O | W | X | O | J | V | R | S | V | F | U | W | U | Y | W | U |
| E | F | R | O | M | A | G | L | A | S | C | E | I | N | W | H | I | Y | U | U | U |
| N | S | V | D | R | O | J | U | G | N | X | C | J | U | F | V | D | R | O | V | Y |
| C | H | I | T | W | A | S | E | N | C | L | O | S | E | D | I | T | W | A | S | Y |
| O | U | H | O | Y | D | V | M | Y | J | N | O | A | H | O | U | Y | J | O | Y | Z |
| A | B | E | A | U | T | I | F | U | S | C | A | R | B | A | E | U | S | A | Y | Z |
| G | F | , | O | D | D | S | O | D | E | V | U | , | Y | G | L | G | R | G | Y | Z |
| N | D | , | A | T | T | H | A | T | T | H | E | , | U | N | K | N | O | W | Y | Z |
| D | C | , | G | O | D | Y | A | O | X | V | J | D | , | C | M | N | C | Y | A | Z |
| T | O | , | N | A | T | N | R | A | L | I | S | T | , | - | O | F | C | O | R | U |
| A | G | , | W | A | U | O | D | P | A | V | B | U | V | 0 | J | N | V | U | G | D |
| M | V | , | P | C | V | G | D | C | M | I | V | U | R | , | D | S | U | A | R | Y |

Similar pages

- ★ Word Desubstitution
- ★ Caesar Cipher
- ★ Word Substitution
- ★ Deranged Alphabet Generator
- ★ Transposition Cipher
- ★ Columnar Transposition Cipher
- ★ Word letter Change

17. Substitution 1:

Quipquip: công cụ giải mã các mật mã chuyển vị thông qua phân tích tần suất xuất hiện của các ký tự trong ciphertext, càng dài thì càng dễ decode.

18. Substitution 2:

Cipher analyzer để xem là loại mã hóa gì => mono...

Google mono... decode, cop vào rồi decode

The result is a draft that should allow you to perform the decryption manually by indicating letters in each cell.

THESEXISTSEVERALOTHERWELLESTABLISHEDHIGHSCHOOLCOMPUTERSECURITYCOMPETITIONSINCLUDINGCYBERPRACTICANDUSCYSCHALLENGE THESECOMPETITIONSFORUSPRIMARILYSYSTEMSADMINISTRATIONFUNDAMENTALSWITCHAREVERYUSEFULANDMARKETABLESKILLSHOWEREVERBELIEVETHEPROPERPURPOSEOFAHIGHSCHOOLCOMPUTERSECURITYCOMPETITIONISNOTONLYTOTEACHVALUABLESKILLSBUTALSO TOGETSTUDENTSINTERESTEDINANDEXCITEDABOUTCOMPUTERSENCEDEFENSIVECOMPETITIONSAREOFENLABORIOUSAFFAIRSANDCODEDOWNTORUNNINGCHECKLISTSANDEXECUTINGCONFISCTIONSOFENSENTHEOTHERHANDISHEAVILYFOCUSDEXPLORATIONANDIMPROVATIONANDTENHAISELEMENTSOFPAYWEBELIEVEACOMPETITIONTOUCHINGONTHESEELEMENTSOFCOMPUTERSECURITYISTHEREFOREABETTERVHICLEFORTECHENGANGLISMSTOSTUDENTSINAMERICANHIGHSCHOOLSPURTHEREWEELIEVETHATANUNDERSTANDINGOFOFFENSIVETECHNIQUESISSESSENTIALFORMOUNTINGANEFFECTIVEDEFENSANDTHATTHETOOLSANDCONFIGURATIONFOCUSCOUNCETOKEKNOWTHEIRENEMYASFFECTIVELYATEACHINGTHEMTOACTIVELYTHINKLIKEANATTACKERPICTFISANOFFENSIVELYORIENTEDHIGHSCHOOLCOMPUTERSECURITYCOMPETITIONTHATSEEKS TOGENERATEINTERESTINCOMPUTERSCIENCEAMONGHIGHSCHOOLERSTEACHINGTHEMENOUGHABOUTCOMPUTERSECURITYTOPIZZETHEIRCURIOSITYMOTIVATINTHEMTOEXPLOREONTHEIROWNENABLEDTHENTOBETTERDEFENDTHEIRMACHINESTHEFLAGIS PICOCTF{NGRAM4_N41Y515_15_730105_8E1BF803}

1 TK2BFVRA 2 QSYENWUMOH 3 HDKJSEMYZQBNWTKLOGPAVUIRC

Feedback

(mono-)alphabetic substitution? (Definition)

- How to encrypt using an alphabetical substitution?
- How to decrypt using an alphabetical substitution?
- How to recognize a mono alphabetical substituted text?
- How to decipher a substitution without the alphabet?
- What are the variants of the substitution cipher?

Similar pages

- Word Substitution
- Caesar Cipher
- Word Substitution
- Deranged Alphabet Generator
- Transposition Cipher
- Columnar Transposition Cipher
- Word Letter Change
- DCODE'S TOOLS LIST

Support

- Paypal
- Patreon
- More

Forum/Help

DISCORD

19. Transposition-trial

This is a little tool to help decrypt transposition ciphers in the horizontal column switching format. Obviously this tool wont just solve your cipher for you, you will have to work for it. Luckily for you though, its very simple. Firstly, Enter your cipher text in the textarea below, pick a period (any number) and press (re)load table.

hefl g as iicpTo({74NRP051N5_16_35P3X51N3_V9AAB1F8})7

Proposed Key length: [3] (re)load table

Now try to arrange these to form words (by clicking and dragging the table numbers). The text box below shows the output if you tried to decrypt with this key. If you think the period is wrong simply change the number, and press reload.

| | | |
|---|---|---|
| 2 | 0 | 1 |
| T | h | e |
| f | 1 | |
| a | g | |
| i | s | |
| p | i | c |
| o | C | T |
| F | { | 7 |
| R | 4 | N |
| S | P | 0 |
| 5 | 1 | N |
| 6 | _ | 1 |
| 5 | _ | 3 |
| Y | D | 3 |

Proposed Key length: [3] (re)load table

Now try to arrange these to form words (by clicking and dragging the table numbers). The text box below shows the output if you tried to decrypt with this key. If you think the period is wrong simply change the number, and press reload.

| | | |
|---|---|---|
| 2 | 0 | 1 |
| T | h | e |
| f | | 1 |
| a | g | |
| i | s | |
| p | i | c |
| o | C | T |
| F | { | 7 |
| R | 4 | N |
| S | P | O |
| S | 1 | N |
| 6 | | 1 |
| S | | 3 |
| X | P | 3 |
| N | 5 | 1 |
| V | 3 | |
| A | 9 | A |
| F | B | 1 |
| 7 | 8 | } |

The flag is picoCTF{7R4N5P051N6_15_3XP3N51V3_A9AFB178};

Transposition Cipher Solver v0.8 | Tim Holman | Using Draggable

20. Vigenere cipher:

Search for a tool

Results

Vigenere CYLAB (Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

picoCTF{DONT_US3_V1G3N3R3_C1PH3R_ae8272q}

VIGENERE CIPHER

Cryptography - Poly-Alphabetic Cipher - Vigenere Cipher

VIGENERE DECODER

VIGENERE CIPHERTEXT: rgnhDVO{D0NU_W3_1G1G03T3_A1AH35_cc82272b}

PARAMETERS

PLAINTEXT LANGUAGE: English

ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ

DECRIPTION METHOD

KNOWING THE KEY/PASSWORD: CYLAB

KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS: 3

KNOWING ONLY A PARTIAL KEY: KE?

KNOWING A PLAINTEXT WORD: CODE

VIGENERE CRYPTANALYSIS (KASISKI'S TEST)

DECRIPT

See also: Beaufort Cipher – Caesar Cipher

VIGENERE ENCODER

VIGENERE PLAIN TEXT: dcode Vigenere automatically

21. HideToSee

Atbash cipher: phương pháp mã hóa đơn giản bằng cách dùng các ký tự đối xứng. (a-z, b-y...)

Trong bài này, file tải về định dạng jpg là 1 file ảnh, để trích xuất nội dung 1 file ảnh có 2 cách:

- strings <tên file>
- steghide extract -sf <tên file>

dùng câu lệnh số 2 thì yêu cầu nhập mật khẩu (nếu cần), câu lệnh này sẽ trích xuất các thông tin ẩn trong 1 file ảnh hoặc âm thanh.

```

9Z]3[
]Rp8
73)/4
J'aZ
n@tI
/8?*T
4Q#
;MrK
\gn;
|^KG
YLx1+
0.5%
>&z,
p9ct
Qqa;
6W 5
,[kvwomf
Tlch%
9*20>
`ajQ0
;SUU
!.Ug
H^9
{:zY
q+aQK
=78
|w)W
h@Wv
9Q0L
#e(g
;k
[BM3Io
I#euWS
x)]H
800P
p)#
sonjulungul.picoctf@webshell:~$ steghide extract -sf atbash.jpg
Enter passphrase:
wrote extracted data to "encrypted.txt".
sonjulungul.picoctf@webshell:~$ cat encrypted.txt
krxTXGU(zgyzs_xizxp_7142uwv9}
sonjulungul.picoctf@webshell:~$ 

```

cat đọc dữ liệu đã được trích xuất trong file encrypted, decode dữ liệu đó bằng atbash cipher decode.

ATBASH CIPHER
Cryptography > Substitution Cipher > Atbash Cipher

ATBASH DECODER

ATBASH MIRRORED CIPHERTEXT [?](#)
krxTXGU(zgyzs_xizxp_7142uwv9}

ATBASH ENCODER

ATBASH PLAIN TEXT [?](#)
dcode decrypt Atbash

Similar pages

- Caesar Cipher
- Mono-alphabetic Substitution
- Affine Cipher
- ROT-13 Cipher
- Mirror Writing
- Writing in Reverse > esreveR
- Gravity Falls Cipher
- DCODE'S TOOLS LIST

22. ReadMyCert:

File .csr là 1 yêu cầu ký chứng chỉ số được tạo ra từ 1 bên yêu cầu (web server hoặc ứng dụng) và gửi đến 1 tổ chức chứng thực (Certificate Authority – CA) để nhận được chứng chỉ số cho việc xác thực và bảo mật trên mạng. (Sử dụng public và private key)

Ở bài này lên google gõ csr file decoder rồi decode.

The screenshot shows a web browser window with multiple tabs open. The active tab is 'certlogik.com/decoder/'. The page displays the 'CSR Summary' and 'CSR Detailed Information' for a certificate request. In the 'CSR Summary' section, under the 'Subject' tab, there is a table with two rows: 'Common Name (CN)' with value 'picoCTF(read_mycert_41d1c74c)' and 'name' with value 'ctfPlayer'. In the 'Properties' section, there is a table with several rows: 'Subject' (name = ctfPlayer, CN = picoCTF(read_mycert_41d1c74c)), 'Key Size' (2048 bits), 'Fingerprint (SHA-1)' (09:48:3E:37:CC:BA:5D:DS:7B:A5:92:11:3A:E9:C5:34:89:E4:D6:63), 'Fingerprint (MD5)' (92:4B:B7:C0:13:8C:BA:S1:F9:A2:20:CD:F6:6A:96:D1), and 'SANS' (empty). The 'CSR Detailed Information' section shows the 'Certificate Request' data, which includes the version (3 (0x0)) and the certificate data itself. The browser's address bar shows the URL 'certlogik.com/decoder/'.

23. rotation

Brute force caesar cipher