

CRYPTOGRAPHY

Mod 26

Mod 26

10 points

Tags: picoCTF 2021 Cryptography

AUTHOR: PANDU

Description

Cryptography can be easy, do you know what ROT13 is?
cvpbPGS{arkg_gvzr_V'yy_gel_2_ebhaqf_bs_ebg13_hyLicInt}

Hints

1

This can be solved online if you don't want to do it by hand!

155,048 solves / 159,475 users attempted (97%)

91% Liked

Submit Flag

Diberikan sebuah flag yang di enkripsi menggunakan ROT13:

cvpbPGS{arkg_gvzr_V'yy_gel_2_ebhaqf_bs_ebg13_hyLicInt}

Lalu saya coba decrypt menggunakan tools online, setelah saya coba maka terdapat flag sebenarnya:

picoCTF{next_time_I'll_try_2_rounds_of_rot13_ulYvpVag}

rot13.com

[About ROT13](#)

```
cvpbPGS{arkg_gvzr_V'yy_gel_2_ebhaqf_bs_ebg13_hyLicInt}
```

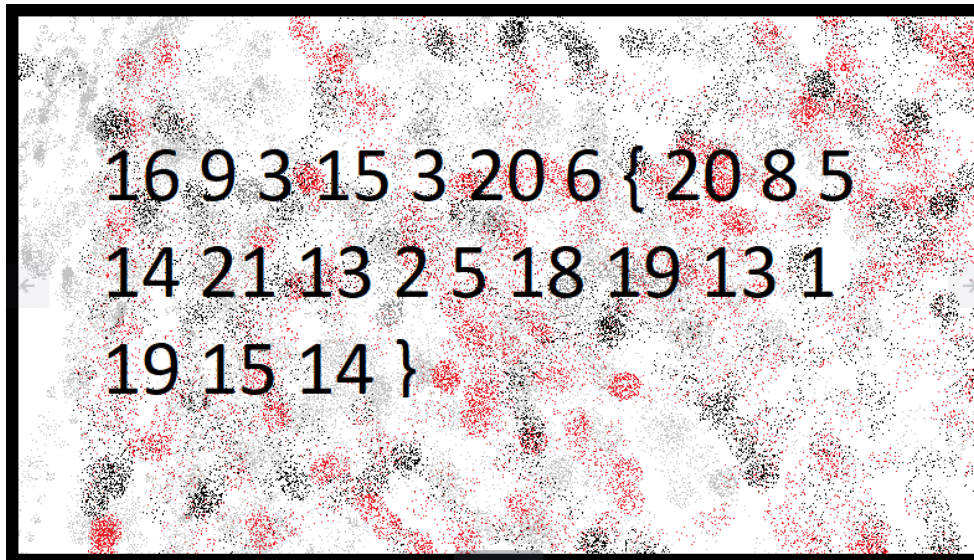


ROT13 ▾



```
picoCTF{next_time_I'll_try_2_rounds_of_rot13_ulYvpVag}
```

The Numbers



Diberikan sebuah serangkaian nomor yang berformat seperti flag picoCTF. Saat dicek ternyata nomor tersebut merupakan index dari huruf alphabet, 16 = "P", 9 = "I", dst. Maka saya buat script:

```
from string import ascii_uppercase as uppercase

num = [16, 9, 3, 15, 3, 20, 6, "{", 20, 8, 5, 14, 21, 13, 2, 5,
       18, 19, 13, 1, 19, 15, 14, "}"]

flag = []

for i in num:
    if(not isinstance(i, int)):
        flag.append(i)
    else:
        i = i - 1
        flag.append(uppercase[i])


print (''.join(flag))
```

Karena library `ascii_uppercase` menggunakan zero base alphabet maka setiap nomor harus dikurang 1 agar mendapatkan hasil yang diinginkan.

```
└─[$]> python3 numbers.py
PICOCTF{THENUMBERSMASON}
```

Maka flagnya adalah: **PICOCTF{THENUMBERSMASON}**

Easy1

Easy1 

 | 100 points 

Tags: picoCTF 2019 Cryptography

AUTHOR: ALEX FULTON/DANNY

Hints 


Description

1 2

The one time pad can be cryptographically secure, but not when you know the key. Can you solve this? We've given you the encrypted flag, key, and a table to help UFJKXQZQUNB with the key of SOLVECRYPTO. Can you use this [table](#) to solve it?

28,488 solves / 33,173 users attempted (86%)

 55% Liked 

 picoCTF{FLAG}

Submit Flag

Diberikan encrypted flag, key, dan sebuah table.

Encrypted flag = UFJKXQZQUNB

Key = SOLVECRYPTO

Table =

```
L[$]> cat table.txt
 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
+-----+
A | A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B | B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C | C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D | D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
E | E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F | F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G | G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H | H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I | I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J | J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K | K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L | L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M | M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N | N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O | O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P | P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q | Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R | R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
S | S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T | T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U | U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V | V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
W | W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
X | X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y | Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z | Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
```

Setelah di cek ini merupakan sebuah Vigenère cipher. Lalu saya coba decrypt menggunakan CyberChef

Recipe

Vigenère Decode

Key
SOLVECRYPTO

Input

UFJKXQZQUNB

abc 11 1

Output

CRYPTOISFUN

Maka flagnya adalah: **PICOCTF{CRYPTOISFUN}**

Easy Peasy

Easy Peasy

40 points

Tags: picoCTF 2021 Cryptography

AUTHOR: MADSTACKS

Description

A one-time pad is unbreakable, but can you manage to recover the flag? (Wrap with picoCTF{}) nc mercury.picoctf.net 36981 otp.py

6,843 solves / 11,648 users attempted (59%)

49% Liked

picoCTF{FLAG}

Submit Flag

Diberikan sebuah alamat host dan port nya, serta sebuah file python yang merupakan source code dari program yang ada di host. Lalu, saya coba jalankan alamat yang diberikan tadi maka tampil seperti berikut:

```
*****Welcome to our OTP implementation!*****
This is the encrypted flag!
5541103a246e415e036c4c5f0e3d415a513e4a560050644859536b4f57003d4c

What data would you like to encrypt? abc
Here ya go!
50035d
```

Disini terlihat program bisa mengenkripsi inputan dari user. Lalu saya periksa flagnya menggunakan pyhon.

```
Python 3.9.2 (default, Feb 28 2021, 17:03:44)
[GCC 10.2.1 20210110] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> len("5541103a246e415e036c4c5f0e3d415a513e4a560050644859536b4f57003d4c")
64
```

Berdasarkan screenshot diatas, bisa diketahui bahwa flag tersebut merupakan bilangan desimal 32 bit.

```
KEY_FILE = "key"
KEY_LEN = 50000
FLAG_FILE = "flag"

def startup(key_location):
    flag = open(FLAG_FILE).read()
    kf = open(KEY_FILE, "rb").read()

    start = key_location
    stop = key_location + len(flag)
```

```
    if stop >= KEY_LEN:
        stop = stop % KEY_LEN
        key = kf[start:] + kf[:stop]
    else:
        key = kf[start:stop]
    key_location = stop
```

Setelah saya memeriksa source code nya saya menemukan bagian looping perkondisian dimana jika inputan user melebihi **KEY_LEN** / panjang key(di source

code tertulis 50000) maka posisi key yang digunakan untuk dienkripsi akan kembali dari awal. Posisi key bertambah seiring ada inputan dari user, posisi key dimulai dari 0 namun diawal saat memulai program sudah terpakai sebanyak 32 byte untuk mengenkripsi flag. Jadi jika kita mengirim kembali 32 byte bilangan desimal contohnya "0" disaat posisi key dimulai dari awal, lalu hasilnya di XOR dengan flag yang kita dapat maka akan dapat kunci aslinya

```
└─[$]> python3 -c "print('\x00'*(50000-32)+'\n'+'\x00'*32)" | nc mercury.picoctf.net
36981
*****Welcome to our OTP implementation!*****
This is the encrypted flag!
5541103a246e415e036c4c5f0e3d415a513e4a560050644859536b4f57003d4c
```

```
What data would you like to encrypt? Here ya go!
6227295e455c7838375c7866375c7862355c786430635c7838665c7863365c78
```

Recipe	Input
<div><div>From Hex</div><div>Delimiter Auto</div></div>	5541103a246e415e036c4c5f0e3d415a513e4a560050644859536b4f57003d4c
<div><div>XOR</div><div>Key 1665c7863365c78 HEX ▾</div><div>Scheme Standard</div><div><input type="checkbox"/> Null preserving</div></div>	
	<div>Output</div> <div>7f9da29f40499a98db220380a57746a4</div>

Maka flagnya adalah: **picoCTF{7f9da29f40499a98db220380a57746a4}**

Caesar

caesar

100 points

Tags: picoCTF 2019 Cryptography

AUTHOR: SANJAY C/DANIEL TUNITIS

Description

Decrypt this [message](#).

Hints ?

1

caesar cipher tutorial

32,864 solves / 37,783 users attempted (87%)

58% Liked

picoCTF{FLAG}

Submit Flag

Diberikan sebuah ciphertext yang berisi:

picoCTF{ynkooejcpdanqxeykjrbdofgkq}

Berdasarkan dari hint jenis enkripsi yang digunakan adalah caesar cipher jadi saya mencari tools yang tersedia di online, lalu mencoba mendekripsi nya

VIEW

Ciphertext

ynkooejcpdanqxeykjrbdofgkq

ENCODE DECODE

Caesar cipher

SHIFT 48 a→W

ALPHABET abcdefghijklmnopqrstuvwxyz

CASE STRATEGY Maintain case

FOREIGN CHARS Include Ignore

Decoded 26 chars

VIEW

Plaintext

crossingtherubiconvfhsjkou

Setelah mencari, saya menemukan kata yang tidak acak yang kemungkinan adalah flagnya, dan ternyata benar.

Maka flagnya adalah: **picoCTF{crossingtherubiconvfhsjkou}**

13

13

100 points

Tags: picoCTF 2019 Cryptography

AUTHOR: ALEX FULTON/DANIEL TUNITIS

Description

Cryptography can be easy, do you know what ROT13 is?
cvpbPGS{abg_gbb_onq_bs_n_ceboyzz}

Hints ?

1

This can be solved online if you don't want to do it by hand!

38,803 solves / 39,067 users attempted (99%)

86% Liked

picoCTF{FLAG}

Submit Flag

Diberikan sebuah flag yang dienkripsi menggunakan ROT13:

cvpbPGS{abg_gbb_onq_bs_n_ceboyzz}

Karena sudah mengetahui jenis enkripsinya saya menggunakan cyberchef untuk mendekripsinya

Caesar Box Cipher

Box Height
1

ROT13

☒ Rotate lower case chars

☒ Rotate upper case chars

☐ Rotate numbers

Amount
13

cvpbPGS{abg_gbb_onq_bs_n_ceboyzz}

33 1

Output

picoCTF{not_too_bad_of_a_problem}

Maka flagnya adalah: **picoCTF{not_too_bad_of_a_problem}**

Pixelated

Pixelated 

 | 100 points 

Tags: picoCTF 2021 Cryptography

AUTHOR: SARA

Description

I have these 2 images, can you make a flag out of them? [scrambled1.png](#)
[scrambled2.png](#)


Hints 

1 2

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

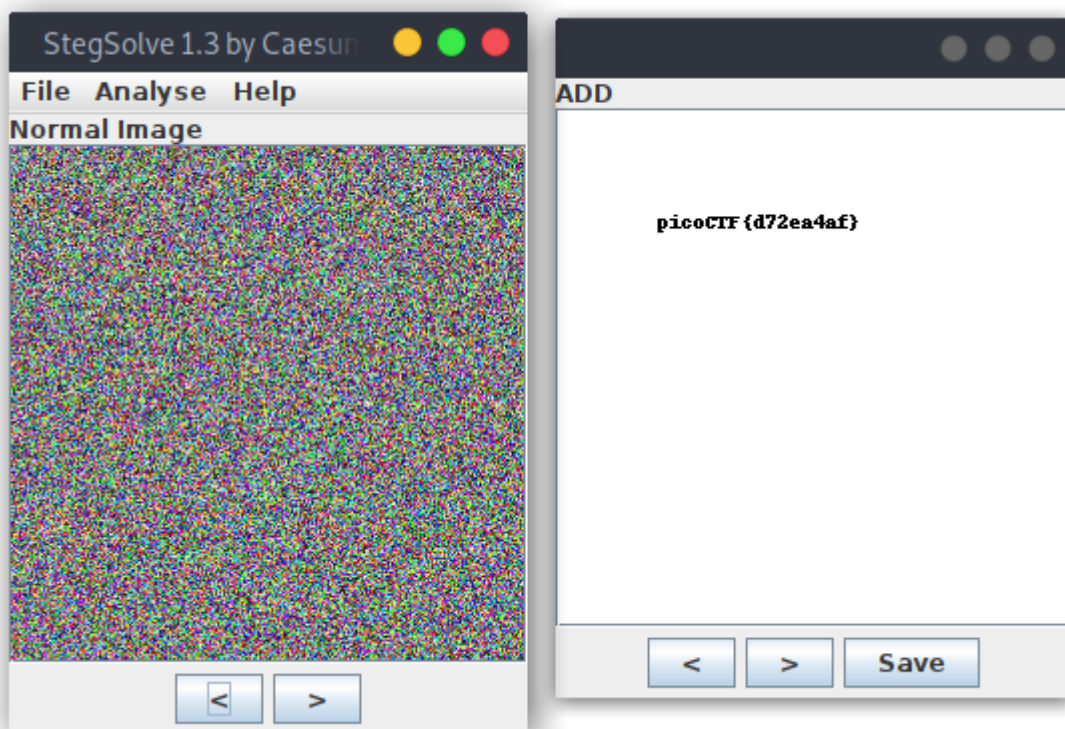
4,781 solves / 5,977 users attempted (80%)

 70% Liked 

 picoCTF{FLAG}


Submit Flag



Diberikan 2 buah gambar yang diacak, saya coba memeriksanya dengan stegsolve image combiner, dan ternyata benar, ada flag didalamnya



Maka flagnya adalah: **picoCTF{d72ea4af}**

Vigenere

Vigenere 

 | 100 points 

Tags: picoCTF 2022 Cryptography

AUTHOR: MUBARAK MIKAIL

Hints 

Description

1

Can you decrypt this message?


Decrypt this [message](#) using this key "CYLAB".

11,814 solves / 12,266 users attempted (96%)



89% Liked



 picoCTF{FLAG}

Submit Flag

Diberikan sebuah pesan yang dienkripsi, dari judul saya langsung mengetahui bahwa itu adalah vigenere cipher, lalu langsung saja saya eksekusi menggunakan cyberchef

Vigenère Decode

Key

CYLAB

rgnoDVD{00NU_WQ3_G1G303T3_A1AH3S_2951c89f}

sec 42 1

Output

picoCTF{D0NT_US3_V1G3N3R3_C1PH3R_2951a89h}

Maka flagnya adalah: **picoCTF{D0NT_US3_V1G3N3R3_C1PH3R_2951a89h}**

Morse-Code

morse-code

100 points

picoCTF 2022

Cryptography

morse_code

AUTHOR: WILL HONG

Description

Morse code is well known. Can you decrypt this?
Download the file [here](#).
Wrap your answer with picoCTF{}, put underscores in place of pauses, and use all lowercase.

Hints ?

1

Audacity is a really good program to analyze morse code audio.

9,927 solves / 11,378 users attempted (87%)

60% Liked

picoCTF{FLAG}

Submit Flag

diberikan file .wav yang kemungkinan berupa kode morse, langsung saja saya cari decoder kode morse yang tersedia secara online

Audio Input

Microphone:

Listen

Stop

Pre-Recorded Audio File

Upload

Play

Stop

 File: "morse_chal.wav"

Received Data

WH47 H47H 90D W20U9H7

Clear message

Setelah mendapatkan pesannya, lalu saya sesuaikan dengan format yang ada dideskripsi.

Maka flagnya adalah: **picoCTF{wh47_h47h_90d_w20u9h7}**

Substitution0

substitution0 

 | 100 points 

Tags: picoCTF 2022 cryptology Substitution

AUTHOR: WILL HONG

Description

A message has come in but it seems to be all scrambled. Luckily it seems to have the key at the beginning. Can you crack this substitution cipher?

Download the message [here](#).

Hints

1

Try a frequency attack. An online tool might help.

10,814 solves / 11,544 users attempted (94%)

 86% Liked 

 picoCTF{FLAG}

Submit Flag

Diberikan sebuah pesan yang didekripsi, karena saya mengetahui bahwa pesan itu merupakan substitution cipher tapi tidak mengetahui jenis nya maka saya menggunakan cipher identifier tool yang tersedia secara online dan mendapatkan jenis nya yaitu Mono-alphabetic Substitution, lalu saya cari tool cipher solver yang tersedia secara online.



Search for a tool

★ SEARCH A TOOL ON DCode BY KEYWORDS:
e.g. type 'boolean'

★ BROWSE THE FULL DCode TOOLS' LIST

Results

dCode tried to find the correct alphabet and its substitution automatically.
The result is a draft that should allow you to perform the decryption manually by indicating letters in each cell.

ABCDEFGHIJKLMNOPQRSTUVWXYZ HEREUPON LEGRAND AROSE, WITH A GRAVE AND STATELY AIR, AND BROUGHT ME THE BEETLE FROM A GLASS CASE IN WHICH IT WAS ENCLOSED. IT WAS A BEAUTIFUL SCARABAEUS, AND, AT THAT TIME, UNKNOWN TO NATURALISTS--OF COURSE A GREAT PRIZE IN A SCIENTIFIC POINT OF VIEW. THERE WERE TWO ROUND BLACK SPOTS NEAR ONE EXTREMITY OF THE BACK, AND A LONG ONE NEAR THE OTHER. THE SCALES WERE EXCEEDINGLY HARD AND GLOSSY, WITH ALL THE APPEARANCE OF BURNISHED GOLD. THE WEIGHT OF THE INSECT WAS VERY REMARKABLE, AND, TAKING ALL THINGS INTO CONSIDERATION, I COULD HARDLY BLAME JUPITER FOR HIS OPINION RESPECTING IT. THE FLAG IS:
PICOCTF{5UB5717U710N_3V0LU710N_357BF9FF}%

1 ZGSOCPQUYHMILERVTBWNAFJDK
2 VSEYOWBKMXZNLUDGHPCRIQTFJA

Mono-alphabetic Substitution - dCode
Tag(s) : Substitution Cipher

MONO-ALPHABETIC SUBSTITUTION

Cryptology > Substitution Cipher > Mono-alphabetic Substitution

MONOALPHABETIC SUBSTITUTION DECODER

★ ALPHABETIC SUBSTITUTION CIPHERTEXT

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

→ ZGSOCPQUYHMILERVTBWNAFJDK (Original Encryption Alphabet)
→ VSEYOWBKMXZNLUDGHPCRIQTFJA (Reciprocal Decryption Alphabet)

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

Maka dapat flagnya.

Maka flagnya adalah: **PICOCTF{5UB5717U710N_3V0LU710N_357BF9FF}**

