

Migdalo / writeups

Watch 1 Star 2 Fork 0

<> Code 0 Issues 0 0 Pull requests 0 0 Projects 0 Pulse Graphs

Branch: master writeups / qiwi-ctf-2016 / crypto100\_1 / Create new file Find file History

Migdalo committed on GitHub spelling Latest commit ddce3d9 on 21 Nov 2016

README.md spelling 4 months ago

README.md

# Crypto 100\_1

Ciphertext:

```
52112515_4535_331534
442315_321144422453_231143_543445
213431313452_442315_5223244415_411112122444
2533341325_2533341325_331534
442315_21311122_2443_442315_4423244214_31243315
```

We got a cipher text that was five lines long and consisted of underscores and numbers from 1 to 5. With this information I was able to identify the cipher to have been created with [Polybius square](#).

The original square [according to Wikipedia](#) is as follows:

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i/j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Each character is presented with two numbers. The first number shows the row and the second number shows the column of the character.

I wrote the following Python script to decipher the ciphertext:

```
ciphers = ['52112515_4535_331534',
           '442315_321144422453_231143_543445',
           '213431313452_442315_5223244415_411112122444',
           '2533341325_2533341325_331534',
           '442315_21311122_2443_442315_4423244214_31243315']

matrix = [['a', 'b', 'c', 'd', 'e'],
          ['f', 'g', 'h', 'i', 'k'],
          ['l', 'm', 'n', 'o', 'p'],
          ['q', 'r', 's', 't', 'u'],
          ['v', 'w', 'x', 'y', 'z']]

plain = []

for c in ciphers:
    words = c.split('_')
    for word in words:
        for num in range(0, len(word), 2):
            y = int(word[num])
```

```
x = int(word[num + 1])
plain.append(matrix[y - 1][x - 1])

plain.append('_')
plain[len(plain) - 1] = '\n'

print ''.join(plain)
```

The script printed the following plaintext:

```
wake_up_neo
the_matrix_has_you
follow_the_white_qabbit
knock_knock_neo
the_flag_is_the_third_line
```

Despite the printed text claiming that the flag is 'follow\_the\_white\_qabbit', the real flag didn't have a typo. The flag accepted by the site was 'follow\_the\_white\_rabbit'.

