Features Business Explore Pricing

This repository Search

Sign in or Sign up

p4-team / ctf

Watch 79 Star 295 Fork 63

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

Branch: master ▾ ctf / 2016-01-29-nullcon / crypto_1 /

Create new file Find file History

Pharisaeus formatting fix for crypto 1 Latest commit `c8a082d` on 1 Feb 2016

..

Heart_clear.txt	crypto 1 writeup	a year ago
Heart_crypt.txt	crypto 1 writeup	a year ago
Mind_crypt.txt	crypto 1 writeup	a year ago
README.md	formatting fix for crypto 1	a year ago

README.md

##Xor with static key (Crypto, 500p)

```
You are in this GAME.
A critical mission, and you are surrounded by the beauties, ready to shed their slik gowns on your beck.
On onside your feelings are pulling you apart and another side you are called by the duty.
The biggiest question is seX OR success?
The signals of subconcious mind are not clear, cryptic.
You also have the message of heart which is clear and cryptic.
You just need to use three of them and find whats the clear message of your Mind...
What you must do?
```

###PL ENG

Dostajemy 3 pliki: plaintext 1, ciphertext 1, ciphertext 2

Na podstawie dwóch pierwszych plików należy ustalić algorytm szyfrowania a następnie zdekodować trzeci plik. Treść zadania sugeruje, że szyfrowanie to XOR. W związku z tym wyciągamy klucz szyfrowania korzystając a zależności:

`Plaintext xor Key = Ciphertex => Paintext xor Ciphertext = Key`

Zadanie rozwiązujemy prostym skryptem:

```
import codecs

name = "Heart_clear.txt"
name2 = "Heart_crypt.txt"
with codecs.open(name) as input_file:
    with codecs.open(name2) as input_file2:
        data = input_file.read()
        data2 = input_file2.read()
        xor_key = [(ord(x) ^ ord(y)) for (x, y) in zip(data, data2)]
        print(xor_key)
        print("".join([chr(x) for x in xor_key]))
    with codecs.open("Mind_crypt.txt") as crypto:
        data = crypto.read()
        print("".join(chr(xor_key[i] ^ ord(x)) for i, x in enumerate(data)))
```

Który daje nam klucz: `Its right there what you are looking for.` oraz link: https://play.google.com/store/apps/collection/promotion_3001629_watch_live_games?hl=en

Nie bardzo wiedzieliśmy co dalej zrobić, ponieważ link nie był flagą. W końcu wpadliśmy na to żeby wysłać tytuł "strony" `Never Miss a Game` i to okazało sie flagą.

###ENG version

We get 3 files: plaintext 1, ciphertext 1, ciphertext 2

Using the first two we are supposed to figure out the algorithm and then decode the third file. Task description suggests XOR encryption. Therefore we proceed to recoved XOR key using the fact that:

```
Plaintext xor Key = Ciphertex => Paintext xor Ciphertext = Key
```

We solve the task with simple script:

```python
import codecs

name = "Heart_clear.txt"
name2 = "Heart_crypt.txt"
with codecs.open(name) as input_file:
    with codecs.open(name2) as input_file2:
        data = input_file.read()
        data2 = input_file2.read()
        xor_key = [(ord(x) ^ ord(y)) for (x, y) in zip(data, data2)]
        print(xor_key)
        print("".join([chr(x) for x in xor_key]))
    with codecs.open("Mind_crypt.txt") as crypto:
        data = crypto.read()
        print("".join(chr(xor_key[i] ^ ord(x)) for i, x in enumerate(data)))
```

And we get the key: `Its right there what you are looking for.` and a link: https://play.google.com/store/apps/collection/promotion_3001629_watch_live_games?hl=en

At this point we were puzzled and didn't know how to proceed since the link was not a flag. However at some point we tried to send the "title" of the page as flag `Never Miss a Game` and it turned out to be ok.