18 July 2020

Modern Clueless Child

by anishbadhri

'I was surfing the crimson wave and oh my gosh I was totally bugging. I also tried out the lilac hair trend but it didn't work out. That's not to say you are any better, you are a snob and a half. But let's get back to the main question here- Who am I? (You don't know my name)'

Ciphertext = "52f41f58f51f47f57f49f48f5df46f6ef53f43f57f6cf50f6df53f53f40f58f51f6ef42f56f43f41f5ef5cf4e"

(hex) Key = "12123"

Solution

This question needs a number of observations.

First, it can be seen that `f` occurs after every 2 characters. Splitting the ciphertext on `f` yields an array of bytes.

It is known that the flag starts with `csictf{`. When represented in bytes, this results in an array, `63 73 69 63 74 66 7b`. On taking an xor of this array with the first 7 elements of the ciphertext, we get a bytearray, `31 32 31 32 33 31 32`. It can be seen that the unit digit of this bytearray is key.

Hence, taking each element of the key and prepending `3` before it gives an array of bytes. Taking the xor of this key with the ciphertext returns the flag.

Solution Script:

```python
import base64

cipher = "52f41f58f51f47f57f49f48f5df46f6ef53f43f57f6cf50f6df53f53f40f58f51f6ef42f56f43f41f5ef5cf4e".sp
key = ['3' + i for i in "12123"]

res = []
for i, n in enumerate(cipher):
        x = int(n, 16)
        y = int(key[i % len(key)], 16)
        res.append(hex(x ^ y)[2:])

res = "".join(res)
print(bytes.fromhex(res).decode())
```

Flag

```
csictf{you_are_a_basic_person}
```

tags: *Crypto*