# Modern Clueless Child

*发表于 2021-01-08 更新于 2021-01-21 分类于 Challenge， 2020， CSICTF， Crypto*
*Challenge | 2020 | CSICTF | Crypto | Modern Clueless Child*

*点击此处获得更好的阅读体验*

---

## *WriteUp来源*

*https://dunsp4rce.github.io/csictf-2020/crypto/2020/07/18/Modern-Clueless-Child.html*

*by* `anishbadhri`

## *题目描述*

> *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"`

## *题目考点*

## *解题思路*

*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.*

```
1  import base64
2  cipher = "52f41f58f51f47f57f49f48f5df46f6ef53f43f57f6cf50f6df53f53f40f58f51f6ef42f56f43f41f5ef5cf4e".split('f')
3  key = ['3' + i for i in "12123"]
4  res = []
5  for i, n in enumerate(cipher):
6    x = int(n, 16)
7    y = int(key[i % len(key)], 16)
8    res.append(hex(x ^ y)[2:])
9  res = "".join(res)
10 print(bytes.fromhex(res).decode())
```

## *Flag*

```
1 csictf{you_are_a_basic_person}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/CSICTF/Crypto/tgGcJBgNzLkru7brJzXVDf.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

*# Challenge # 2020 # Crypto # CSICTF*
*Rivest Shamir Adleman*
*Mein Kampf*