Mein Kampf

发表于 2021-01-08 分类于 Challenge， 2020， CSICTF， Crypto
Challenge | 2020 | CSICTF | Crypto | Mein Kampf

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/Mein-Kampf.html

by `raghul-rajasekar`

题目描述

题目考点

> *"We have intercepted the enemy's communications, but unfortunately, some data was corrupted during transmission. Can you recover the message?" M4 UKW $ Gamma 2 4 $ 5 9 $ 14 3 $ 5 20 fv cd hu ik es op yl wq jm "Ciphertext: zkrtwvvvnrkulxhoywoj" (Words in the flag are separated by underscores)*

解题思路

From the communication data format, it is clear that this challenge uses Enigma (the challenge title suggests the same too). However, there are dollar signs in a few places where we don't know the machine configuration. The only choice is to brute-force through all possibilities and see for which combination we get an output in the correct flag format. For automating this, I used the `py-enigma` *package in Python.*

```
from enigma.machine import EnigmaMachine
reflectors = ['B-Thin', 'C-Thin']
rotors = ['I', 'II', 'III', 'IV', 'V', 'VI', 'VII', 'VIII']
for r1 in rotors:
    for r2 in rotors:
        for r3 in rotors:
            for r in reflectors:
                machine = EnigmaMachine.from_key_sheet(
                   rotors=' '.join(['Gamma', r1, r2, r3]),
                   reflector=r,
                   ring_settings='D I C T',
                   plugboard_settings='fv cd hu ik es op yl wq jm'.upper())
                machine.set_display('BENE')
                temp = machine.process_text('zkrtwvvvnrkulxhoywoj')
                if 'CTF' in temp:
                    print(temp, r1, r2, r3, r)
```

The output is `CSICTFNOSHITSHERLOCK I IV VII B-Thin`.

Flag

```
csictf{no_shit_sherlock}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/CSICTF/Crypto/sTiiVPb8jnXQwoeq5FLcvF.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
Modern Clueless Child
unseen