古典密码

ABCDEFG~

编写python脚本

```
from string import ascii_uppercase
flag =[18,24,26,13,8,18,13,20,26,15,11,19,26,25,22,7,8,12,13,20]
for i in flag:
    print(ascii_uppercase[::-1][i-1],end="")
```

小小凯撒

字母表中既有大写又有小写，编写脚本爆破

```
from string import ascii_letters

key = iter([1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25])
for j in range(26):
    for i in "kqEftuEUEftqOADDqoFRxmsOAzsDmFGxmFuAzE":
        print((ascii_letters)[(ascii_letters.find(i))-j],end="")
    print()
```

凯撒变异了

和小小凯撒差不多，就是多了个 114514 的key，每一位按照对应偏移量往回偏移即可

```
from string import ascii_letters, ascii_lowercase,ascii_uppercase
import itertools

pw = itertools.cycle('114514')
for i in "ZpyLfxGmelDeftewJwFbwDGsszszbliileadaa":
        print((ascii_letters)[(ascii_letters.find(i))-int(next(pw))],end="")
```

Vigenere

在浏览ctf-wiki时看到了爆破的在线工具，未知密钥

工具 ¶

- 已知密钥
  - Python 的 pycipher 库
  - 在线解密 Vigenère cipher
  - CAP4
- 未知密钥
  - Vigenère Cipher Codebreaker
  - Vigenere Solver ， 不够完善。

得到

Message

```
-- MESSAGE w/Key #1 = 'tfdvsjuz' ----------------
information security, sometimes shortened to infosec, is the practice of protecting information by mitigating
information risks. it is part of information risk management. it typically involves preventing or reducing the
probability of unauthorized/inappropriate access to data, or the unlawful use, disclosure, disruption, deletion,
corruption, modification, inspection, recording, or devaluation of information. it also involves actions intended
to reduce the adverse impacts of such incidents. protected information may take any form, e.g. electronic or
physical, tangible (e.g. paperwork) or intangible (e.g. knowledge). information security's primary focus is the
balanced protection of the confidentiality, integrity, and availability of data (also known as the cia triad)
while maintaining a focus on efficient policy implementation, all without hampering organization productivity.
this is largely achieved through a structured risk management process that involves:1. identifying information and
related assets, plus potential threats, vulnerabilities, and impacts;2. evaluating the risks3. deciding how to
address or treat the risks i.e. to avoid, mitigate, share or accept them4. where risk mitigation is required,
selecting or designing appropriate security controls and implementing them5. monitoring the activities, making
adjustments as necessary to address any issues, changes and improvement opportunities6. i won't tell you that the
flag is moectf attacking the vigenere cipher is interestingto standardize this discipline, academics and
professionals collaborate to offer guidance, policies, and industry standards on password, antivirus software,
firewall, encryption software, legal liability, security awareness and training, and so forth. this
standardization may be further driven by a wide variety of laws and regulations that affect how data is accessed,
processed, stored, transferred and destroyed. however, the implementation of any standards and guidance within an
entity may have limited effect if a culture of continual improvement isn't adopted.
```

现代密码

密码学之入门指北