维吉尼亚密码 ctf

原创

husb-052 于 2021-10-27 14:36:44 发布 2194 收藏

分类专栏： 古典密码 文章标签： 密码学 安全

本文链接：https://blog.csdn.net/weixin_49298265/article/details/120992475

维吉尼亚密码

> BUUCTF-Crypto-[BJDCTF 2nd]燕言燕语-y1ng
> 小燕子，穿花衣，年年春天来这里，我问燕子你为啥来，燕子说:
> 79616E7A69205A4A517B78696C7A765F6971737375686F635F73757A6A677D20
> 转字符串得 yanzi ZJQ{xilzv_iqssuhoc_suzjg}

原理

维吉尼亚密码（又译维热纳尔密码）是使用一系列凯撒密码组成密码字母表的加密算法，属于多表密码的一种简单形式。

加密步骤

①当明文为ATTACKATDAWN

②选择某一关键词并重复而得到密钥，如关键词为LEMON时，密钥为：LEMONLEMONLE

③对于明文的第一个字母A，对应密钥的第一个字母L，于是使用表格中L行字母表进行加密，得到密文第一个字母L。类似地，明文第二个字母为T，在表格中使用对应的E行进行加密，得到密文第二个字母X。以此类推，可以得到：

明文：ATTACKATDAWN

密钥：LEMONLEMONLE

密文：LXFOPVEFRNHR

分析

yanzi 为密钥，使用脚本逆向解密。

脚本

```
s = 'ZJQ{xilzv_iqssuhoc_suzjg}'
key = 'yanzi'
flag = ''
k = 0
for i in s:
    if i >= "A" and i <= "Z" or i >= "a" and i <= "z":
        x = ord(i) - (ord(key[k%5]) - 97)
        if i >= "A" and i <= "Z" and x < 65:
            x += 26
        if i >= "a" and i <= "z" and x < 97:
            x += 26
        flag += chr(x)
        k += 1
    else:
        flag += i
print(flag)
```

5. 答案

BJD{yanzi_jiushige_shabi}