23121677-范舒舰-6 月 11 日 crypto 作业 WP

Chal1. 套娃

第一题拿到”佛曰：”就知道要去网上找佛曰解码器

但是翻遍了百度，谷歌，github 都没找到配套的佛曰解码

于是直接使用搜索引擎第一个网站 https://pi.hahaka.com/开始观察文本

对文本直接加密可得

佛曰：楞……诃漫

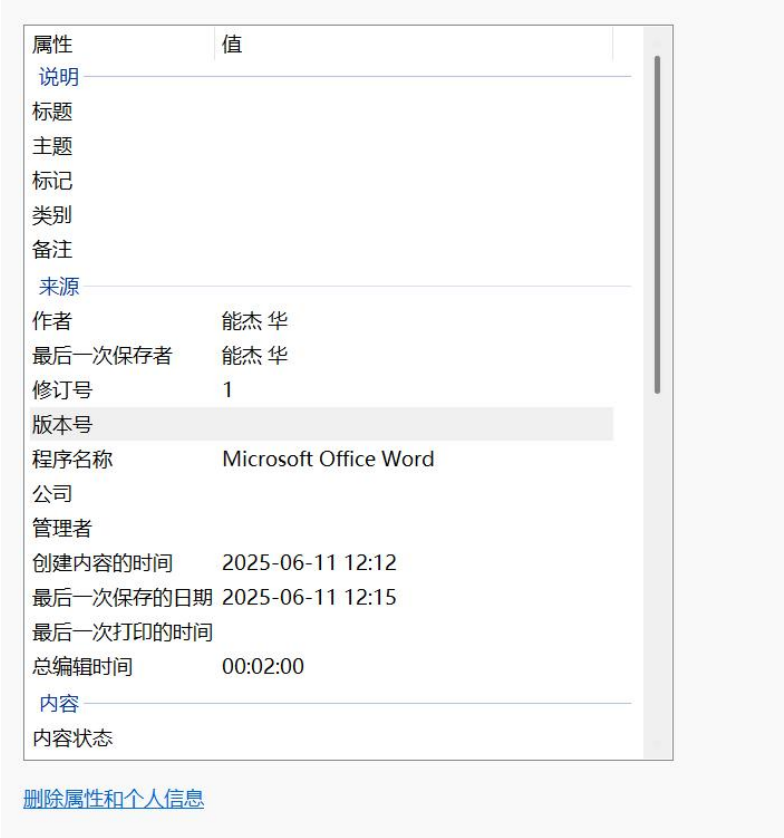
与原文

佛曰：楞……漫漫

有异曲同工之妙，所以**网站是找对了**

但是无法正确解密是为什么？是存在密钥吗？

Word 文档的属性中可能会藏着一些东西，但是查看属性后只能得到



华能杰使用了两分钟就出好了这一题，显然是没有太多时间去添加一些隐藏元素的

但是我不信邪又使用 kali 分析，还是得出**没有隐藏密钥**

那就再次观察原文：

好像有一些文字太复杂了？？比如最后的**蘇參輸**明显没有出现在二次加密的密文当中

一定是出题者使用了繁体字加密！

直接将原文放到网站上变成简体字

施主可曾记得此为哪位高僧所言？（佛语有误，请确定密钥正确并未被篡改）

呼尼謹阿他爍伊孕羯舍舍唵穆耶佛曳俱盧栗醯爍南怛哆吉俱羯度摩鉢羯唎舍蘇謹地帝他南寫閣盧
度提參墀耶穆提罰楞舍薩摩提埵唵輸輸孕蘇輸爍沙羯怛薩遮無地寫囉沙哆伽參地呼那參室阿他薩
佛無埵尼阿吉室數娑豆蒙菩蒙伊楞寫謹唎阿皤阿呼嚧楞蒙墀菩囉伽地佛遮俱嚧唵陀吉婆尼他薩穆
閣醯室帝陀埵提盧參嚧無爍唵耶悉南唵阿阿帝數爍謹摩閣唎阿皤薩蘇醯伽盧菩伽度馱唵訶南俱栗
吉吉遮參娑阿參鉢他地阿楞閣鉢俱蘇參輸地漫漫

为什么还是错的？！

因为出题者没有考虑到佛曰加密的文字本身存在繁体字！导致无法从繁简混合->繁体->繁简混合，只能繁简混合->繁体->简体(实际上只有嚧被替换成了)

明白了存在一次些繁体转简体后，就开始尝试还原成原文：

遍历原文取出不重复的单个字再按拼音排序进入文件：(python 实现)

```
pip install pypinyin
```

```
import os
import pypinyin

def is_chinese(char):
    """判断是否为汉字"""
    return '\u4e00' <= char <= '\u9fff'

def read_unique_chars_by_order(file_path):
    unique_chars = []
    seen_chars = set()

    with open(file_path, 'r', encoding='utf-8') as f:
        while True:
            char = f.read(1)
            if not char:
                break
            if is_chinese(char) and char not in seen_chars:
                seen_chars.add(char)
                unique_chars.append(char)

    return unique_chars
```

```
def sort_by_pinyin(chars):
    return sorted(chars, key=lambda c: pypinyin.lazy_pinyin(c)[0])

def write_to_file(chars, output_path):
    with open(output_path, 'w', encoding='utf-8') as f:
        for c in chars:
            f.write(c + '\n')

if __name__ == "__main__":
    input_file = "input.txt"            # 输入文件路径
    output_file = "output.txt"          # 输出文件路径

    unique_chars = read_unique_chars_by_order(input_file)
    sorted_chars = sort_by_pinyin(unique_chars)

    write_to_file(sorted_chars, output_file)
```

然后将原文和加密两次后的原文(保证文本够长覆盖所有字)分别输出对比

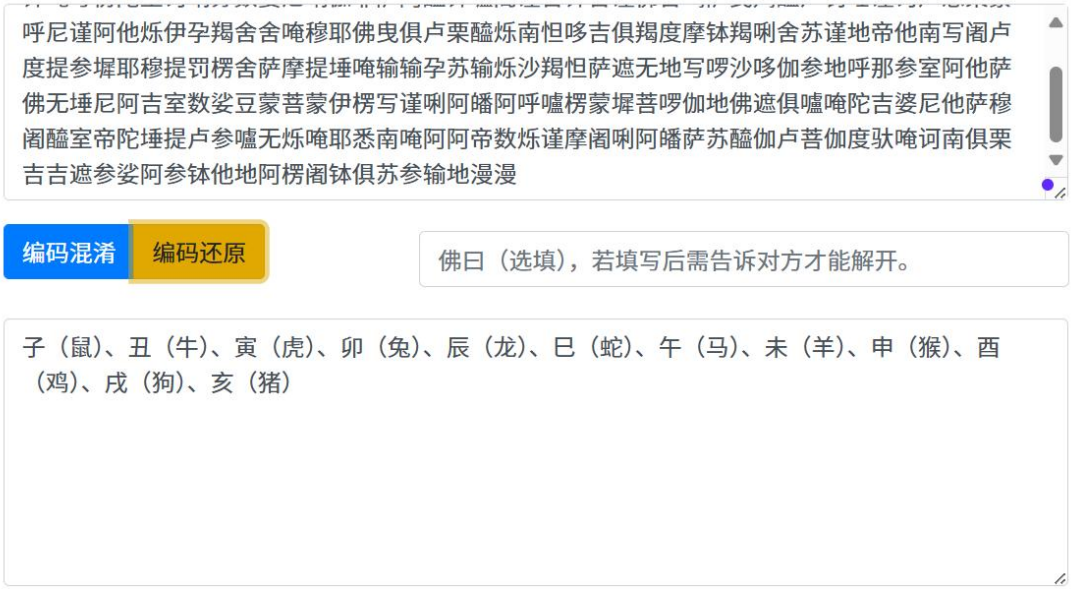
繁体	简体	繁体	简体	繁体	简体	繁体	简体
阿	阿	喝	喝	摩	摩	他	他
唵	唵	呼	呼	穆	穆	提	提
鉢	钵	吉	吉	那	那	陀	陀
參	参		迦	南	南	馱	驮
墀	墀	羯	羯	尼	尼	無	无
怛	怛	謹	谨	婆	婆	醯	醯
地	地	俱	俱	皤	皤	悉	悉
帝	帝	楞	楞	菩	菩	寫	写
豆	豆	栗	栗	薩	萨	曳	曳
闍	阇	利	利	沙	沙	夜	夜
度	度	唎	唎	舍	舍	耶	耶
埵	埵	嚧	嚧	室	室	伊	伊
哆	哆	盧	卢	數	数	曰	曰
罰	罚	囉	啰	輸	输	孕	孕
佛	佛	漫	漫	爍	烁	遮	遮
伽	伽	蒙	蒙	蘇	苏		
訶	诃	咩	咩	娑	娑		

最后替换原文中的字得到

佛曰：楞舍地呼栗耶啰南驮曳咩伽墀醯诃室度夜楞唵孕夜曳娑娑怛阇卢曳俱蒙婆耶喝罚菩卢利萨钵唵写楞陀室诃唎苏数婆尼唎伽耶萨阿醯钵嚧阇谨舍钵舍谨佛舍喝萨曳羯醯卢罚埵谨诃卢悉栗蒙呼尼谨阿他烁伊孕羯舍舍唵穆耶佛曳俱卢栗醯烁南怛哆吉俱羯度摩钵羯唎舍苏

谨地帝他南写阁卢度提参墀耶穆提罚楞舍萨摩提埵唵输输孕苏输烁沙羯怛萨遮无地写啰沙哆伽参地呼那参室阿他萨佛无埵尼阿吉室数娑豆蒙菩蒙伊楞写谨唎阿皤阿呼嚧楞蒙墀菩啰伽地佛遮俱嚧唵陀吉婆尼他萨穆阁醢室帝陀埵提卢参嚧无烁唵耶悉南唵阿阿帝数烁谨摩阁唎阿皤萨苏醢伽卢菩伽度驮唵诃南俱栗吉吉遮参娑阿参钵他地阿楞阁钵俱苏参输地漫漫

解码得到：



子（鼠）、丑（牛）、寅（虎）、卯（兔）、辰（龙）、巳（蛇）、午（马）、未（羊）、申（猴）、酉（鸡）、戌（狗）、亥（猪）

Chal2.ezRSA

第二题直接给了源码

```
def gen_rsa_param() -> Tuple[int, int, int, int]:
    p = getPrime(256)
    q = p + 2
    while True:
        q += 2
        if is_prime(q):
            break
    assert p < q
```

明确了 p 与 q 的生成条件：

随机选择一个 256 位的大素数从 p+2 开始（确保比 p 大）

每次尝试 q += 2（保持奇数）

直到找到一个素数为止，设为 q

两个素数之间的平均间隔是大约 100 到几百左右；差值 q - p 很小。

$$n = p * q = (a - b)(a + b) = a^2 - b^2$$

只要从 $a = \sqrt{n}$开始

找到$b^2 = a^2 - n$ 就能求出 p，q

```
    import math
    from Crypto.Util.number import long_to_bytes, inverse
    c = 57967681486378874912555870 39....
    n = 79485122429858814337712032 81....
    e = 65537

    def fermat_factor(n, max_gap=10**6):
        a = math.isqrt(n)
        if a * a < n:
            a += 1
        for b in range(1, max_gap):
            b2 = a*a - n
            # 如果 a 大于根号 n，a+=1
            if b2 < 0:
                a += 1
                continue
            # 检查是否是完全平方
            b0 = math.isqrt(b2)
            if b0 * b0 == b2:
                p = a - b0
                q = a + b0
```

```
                return p, q
            a += 1
        return None, None

if __name__ == "__main__":
    p, q = fermat_factor(n, max_gap=10000)
    if p is None:
        print("FAIL")
        exit(1)
    print(f"p = {p}\nq = {q}")

    phi = (p - 1) * (q - 1)
    d = inverse(e, phi)

    m = pow(c, d, n)
    flag = long_to_bytes(m)
    print(flag.decode())
```

最后求解得出：

p = 89154429183220512803696196460918889761876688182000638400711407194300547854987

q = 89154429183220512803696196460918889761876688182000638400711407194300547855067

flag{you_have_learned_factor}