CTF-I春秋第二届春秋欢乐赛-CRYPTO-RSA256

原创

he110_Z 于 2020-06-01 22:13:19 发布 367 收藏

分类专栏： CTF python 文章标签： 安全 python git

本文链接：https://blog.csdn.net/weixin_43880435/article/details/105894458

CTF 同时被 2 个专栏收录

10 篇文章 0 订阅

订阅专栏

python

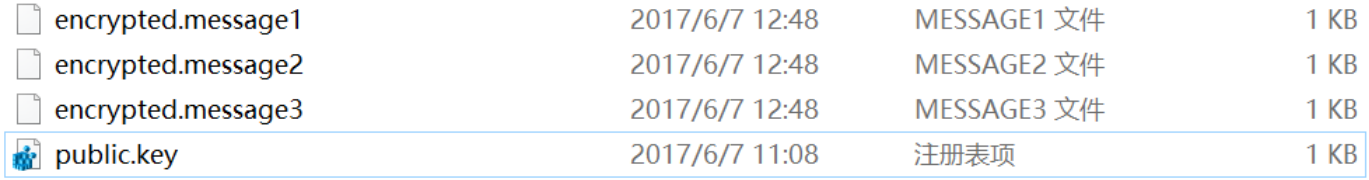
8 篇文章 0 订阅

订阅专栏

#CTF

试题 地址：https://www.ichunqiu.com/battalion?t=1&r=61107

2下载后有四个文件

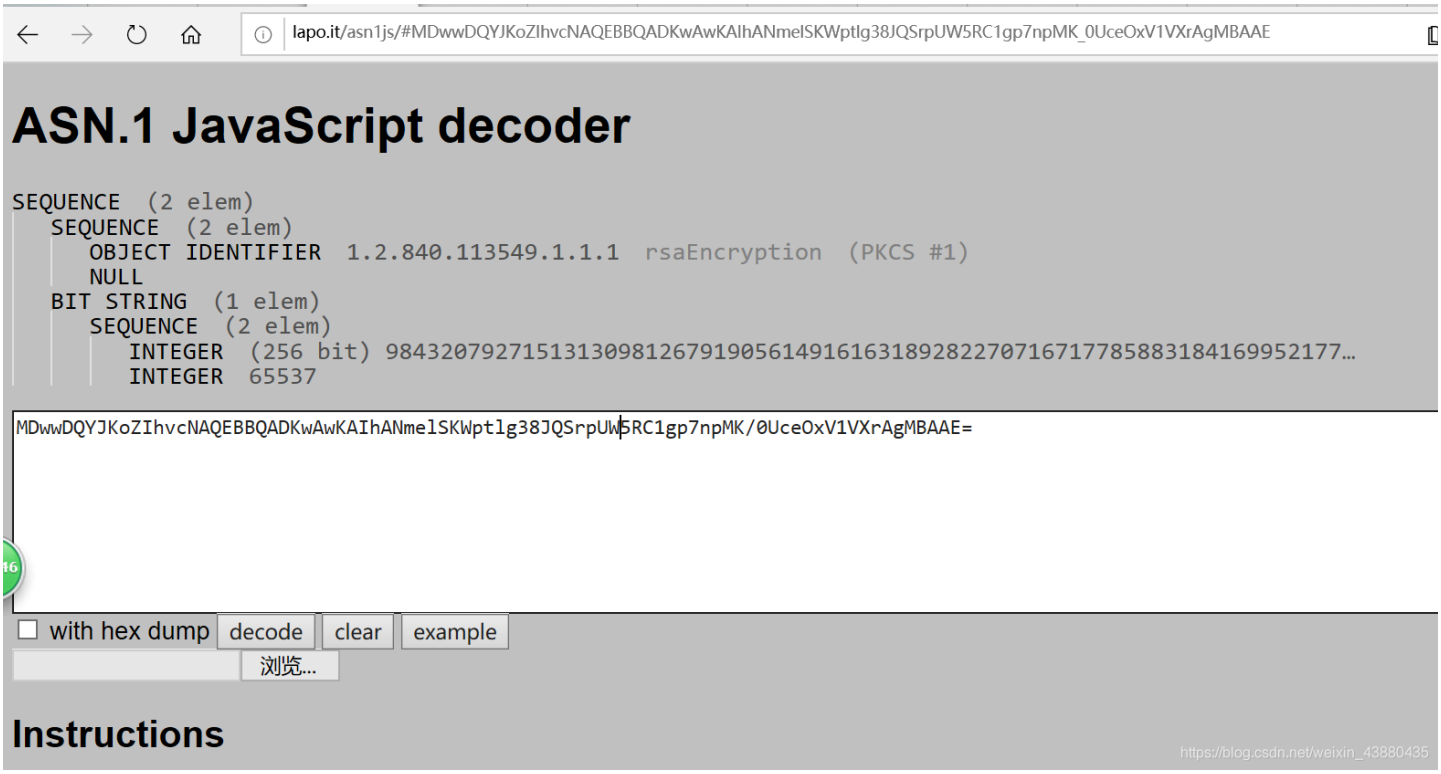


3、text打开public.key

```
-----BEGIN PUBLIC KEY-----
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhANmelSKWptlg38JQSrpUW5RC1gp7npMK
/0UceOxV1VXrAgMBAAE=
-----END PUBLIC KEY-----
```

4、分析密钥

方法一：key的格式是ASN.1 在线解析网站http://lapo.it/asn1js/



方法二：kali linux

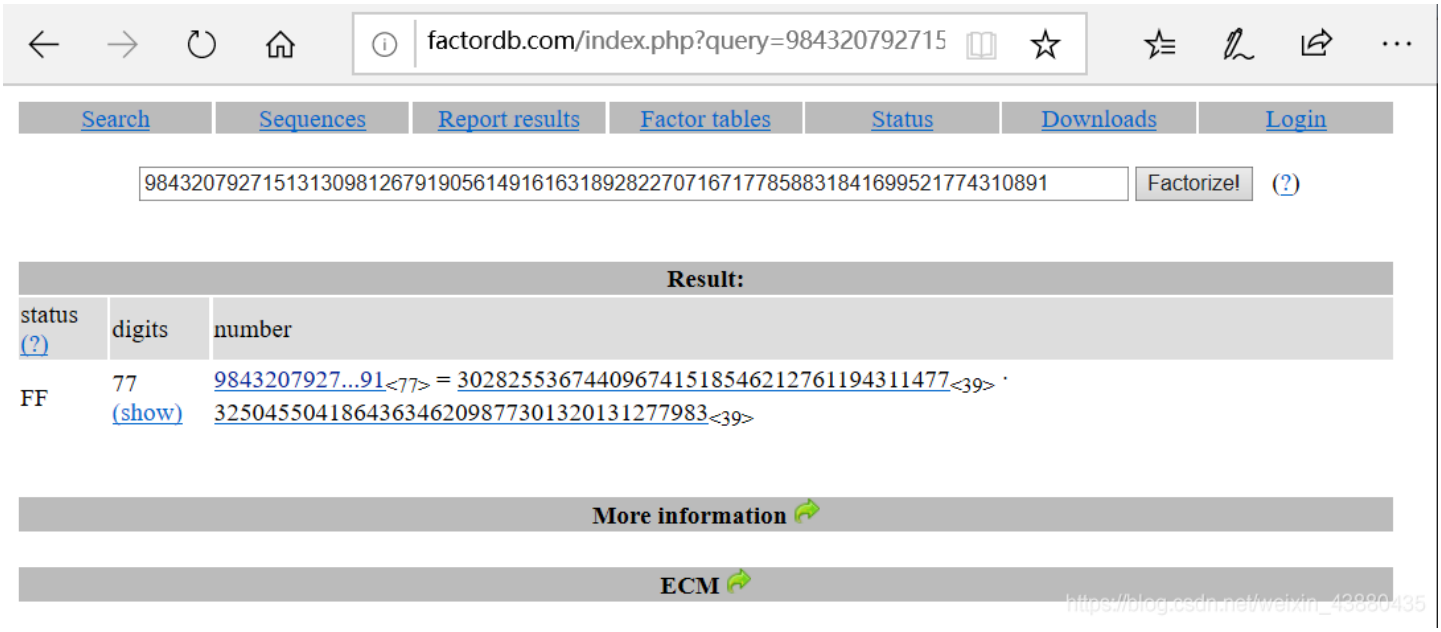
```
root@kali:/mnt/hgfs/CTF/Crypto/fujian_C74892BD664A142AF1F7F85F55754BCF/fujian# openssl rsa -pubin -text -modulus
 -in ./public.key
RSA Public-Key: (256 bit)
Modulus:
    00:d9:9e:95:22:96:a6:d9:60:df:c2:50:4a:ba:54:
    5b:94:42:d6:0a:7b:9e:93:0a:ff:45:1c:78:ec:55:
    d5:55:eb
Exponent: 65537 (0x10001)
Modulus=D99E952296A6D960DFC2504ABA545B9442D60A7B9E930AFF451C78EC55D555EB
writing RSA key
-----BEGIN PUBLIC KEY-----
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhANmelSKWptlg38JQSrpUW5RC1gp7npMK
/0UceOxV1VXrAgMBAAE=
-----END PUBLIC KEY-----
```

获取到数据如下：

(十制)N=98432079271513130981267919056149161631892822707167177858831841699521774310891 E=65537要想解密数据需要私钥D,要计算私钥D，则需要分解N，得到素数P，Q。

5、在线分解大数地址

http://factordb.com/



分解之后：P=3028255367440967415185462127611943114773

Q=3250455041864363462098773013201312779833

6、使用python解密得

```
#!/usr/bin/env python
# -*- coding:utf-8 -*-
#python3.7
import gmpy2
import rsa
p = 3028255367440967415185462127611943114773
q = 3250455041864363462098773013201312779833
n = 98432079271513130981267919056149161631892822707167177858831841699521774310891
e = 65537
d = int(gmpy2.invert(e , (p-1) * (q-1)))
key = rsa.PrivateKey(n , e , d , p , q)
with open("encrypted.message1" , "rb") as f1:
    str1=rsa.decrypt(f1.read(), key).decode()
with open("encrypted.message2" , "rb") as f2:
    str2=rsa.decrypt(f2.read(), key).decode()
with open("encrypted.message3" , "rb") as f3:
    str3=rsa.decrypt(f3.read(), key).decode()
print(str1+str2+str3)
```

得到flag{3b6d3806-4b2b-11e7-95a0-000c29d7e93d}