week1 whritup

Easy RSA

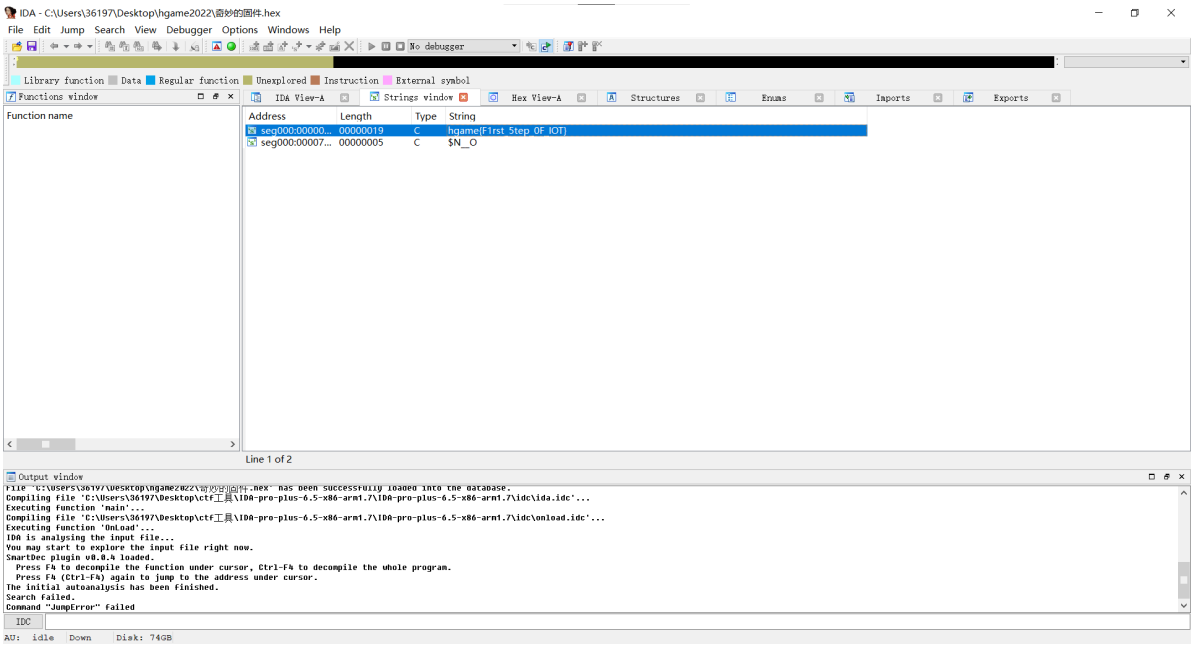
```
import libnum
from Crypto.Util.number import long_to_bytes

for e, p, q, c in [(12433, 149, 197, 104), (8147, 131, 167, 6633), (10687, 211,
197, 35594),
                       (19681, 131, 211, 15710), (33577, 251, 211, 38798),
(30241, 157, 251, 35973),
                       (293, 211, 157, 31548), (26459, 179, 149, 4778), (27479,
149, 223, 32728),
                       (9029, 223, 137, 20696), (4649, 149, 151, 13418), (11783,
223, 251, 14239),
                       (13537, 179, 137, 11702), (3835, 167, 139, 20051),
(30983, 149, 227, 23928),
                       (17581, 157, 131, 5855), (35381, 223, 179, 37774), (2357,
151, 223, 1849),
                       (22649, 211, 229, 7348), (1151, 179, 223, 17982), (8431,
251, 163, 30226),
                       (38501, 193, 211, 30559), (14549, 211, 151, 21143),
(24781, 239, 241, 45604),
                       (8051, 179, 131, 7994), (863, 181, 131, 11493), (1117,
239, 157, 12579),
                        (7561, 149, 199, 8960),
                       (19813, 239, 229, 53463), (4943, 131, 157, 14606),
(29077, 191, 181, 33446),
                       (18583, 211, 163, 31800), (30643, 173, 191, 27293),
(11617, 223, 251, 13448),
                       (19051, 191, 151, 21676), (18367, 179, 157, 14139),
(18861, 149, 191, 5139),
                       (9581, 211, 193, 25595)]:
    # c = 0x6cd55a2bbb49dfd2831e34b76cb5bdfad34418a4be96180b618581e9b6319f86
    n = p * q
    # n = int("",16)
    # e = 65537
    # e = int("",16)
    # q = 333360321402603178263879595968004169219
    # p = 325593180411801742356727264127253758939

    d = libnum.invmod(e, (p - 1) * (q - 1))
    m = pow(c, d, n)  # m 的十进制形式
    string = long_to_bytes(m)  # m明文
    print(string)  # 结果为 b‘ m ’ 的形式
```

饭卡的uno

用IDA打开hex文件，架构用ARM，shift+f12即可得到字符串



欢迎欢迎！热烈欢迎！

关注公众号即可