WhiteHat Challenge 03 - Crypto002 - Cryptography

Mark Kipyegon

Mon 08 May 2017

Category: CTF (./category/ctf.html)
Tags: Cryptography (./tag/cryptography.html)

WhiteHat Challenge 03 - Crypto001 - Cryptography

Problem

We have components of an RSA cryptosystem. Decrypt the cipher to get the flag.

RSA info:

- https://vi.wikipedia.org/wiki/RSA_(m%C3%A3_h%C3%B3a) Vietnamese
- https://en.wikipedia.org/wiki/RSA_(cryptosystem) English"

Download RSA-info file here: http://material.wargame.whitehat.vn/challenges/3/Crypto002_c576122a778397b48fa2d0368e2e02a14df1db41.zip Submit WhiteHat{sha1(flag)} Example: flag = Hello World sha1("Hello World") = 0a4d55a8d778e5022fab701977c5d840bbc486d0 You must submit: WhiteHat{0a4d55a8d778e5022fab701977c5d840bbc486d0} (all hash charactera in lowercase)

Solution

For this solution I borrowed a snippet of code from Ne0Lux-C1Ph3r (https://github.com/Ne0Lux-C1Ph3r/WRITE-UP/blob/master/EasyCTF/Cryptography/RSA_3.md)

```
#!/usr/bin/env python
import libnum

e = 65537
c = 126028558760741438230925566962334702896791270808414391828894437291120207835997354509410869568173448979784329516392078311028442458946906210498176026685581176779209904039179175088984829699783861789249260322822491502790157863487861171337660785254139478229397872969136220001367017765809130698515063339265165085655

p = 124766829607957797234199892873062396063313473106045538256052630288550864180510863000062788880498963757540968271631213066964173145316666706623416735117894 87
q = 106266084851859097391871266021835132042159554660328682685707823588200477517959823732528733332768438313835423602028746832626786649753808654150685549920904 83

n=p*q
phi=(p-1)*(q-1)
d = libnum.modular.invmod(e, phi)
print libnum.n2s(pow(c, d, n))
```

When executed this returns the plain text string ***simple_rsa_decryption***.

```
$ echo -n simple_rsa_decryption | shasum
```

FLAG: **WhiteHat{100be37579e0f27c314efcb68a773b31537b5118}**

Comments