

rsa

发表于 2021-01-04 更新于 2021-02-05 分类于 [Challenge](#) , [2019](#) , [湖湘杯](#) , [Crypto Challenge](#) | [2019](#) | [湖湘杯](#) | [Crypto](#) | [rsa](#)

[点击此处](#) 获得更好的阅读体验

题目考点

- RSA加密

解题过程

目是一个RSA加密，已知 n, e, dp, c , 求 m , 推理过程可以参考[RSA之拒绝套路\(1\)](#)

dp 的意思为: $dp \equiv d \pmod{p-1}$

故此可以得到 $k_2 * (p-1) * (q-1) + 1 = k_1 * (p-1) + dp * e * k_2 * (p-1) * (q-1) + 1 = k_1 * (p-1) + dp * e$

变换一下 $(p-1) * [k_2 * (q-1) - k_1] + 1 = dp * e * (p-1) * [k_2 * (q-1) - k_1] + 1 = dp * e$

因为 $dp < p-1$ 且 $dp < p-1$ 可以得到 $e > k_2 * (q-1) - k_1$ 且 $e > k_2 * (q-1) - k_1$

我们假设 $x = k_2 * (q-1) - k_1$ 且 $x = k_2 * (q-1) - k_1$ 可以得到 x 的范围为 $(0, e)$ $(0, e)$

因此有 $x * (p-1) + 1 = dp * ex * (p-1) + 1 = dp * e$

那么我们可以遍历 $x \in (0, e)$ $x \in (0, e)$ 求出 $p-1$ ，求的方法也很简单，遍历 65537 种可能

其中肯定有一个 p 可以被 n 整除那么求出 p 和 q

即可利用 $\phi(n) = (p-1) * (q-1)$ $d * e \equiv 1 \pmod{\phi(n)}$ $\phi(n) \phi(n) = (p-1) * (q-1)$ $d * e \equiv 1 \pmod{\phi(n)}$

推出 $d \equiv 1 * e^{-1} \pmod{\phi(n)}$ $d \equiv 1 * e^{-1} \pmod{\phi(n)}$

```
1 import gmpy2
2 import libnum
3 n = 2200059656985608536262301957399524014372089038067858129941121368885758461295301412287999580881687222103280573415134345892171933436019402489037707552168039967853365511
4 e = 65537
5 dp = 84373069210173690047629226878686144017052129353931011112880892379361035492516066159394115482289291025932915787077633999791002846189004408043685986856359812230222331
6 c = 1487427106466991858117806604720749555157042157526029811603886387742449950062692085586326119426416985067820660414431431817182936757568872659332386314566424118916782099
7 for i in range(1, 65538):
8     if (dp * e - 1) % i == 0:
9         if n % ((dp * e - 1) / i + 1) == 0:
10             p = ((dp * e - 1) / i) + 1
11             q = n / ((dp * e - 1) / i + 1)
12             phi = (p - 1) * (q - 1)
13             d = gmpy2.invert(e, phi) % phi
14             print libnum.n2s(pow(c, d, n))
```

FLAG

```
1 flag{d90a4bb43f64275794522dffdb4bd78b}
```

- 本文作者: CTFHub
- 本文链接: <https://writeup.ctfhub.com/Challenge/2019/湖湘杯/Crypto/iMNiefMznNyhSqcxjUosk5.html>
- 版权声明: 本博客所有文章除特别声明外，均采用 [BY-NC-SA](#) 许可协议。转载请注明出处！

[#Challenge #2019 #Crypto #湖湘杯](#)
[give me your passport](#)
[argument](#)