babyre

发表于 2021-01-21 分类于 Challenge， 2017， HCTF， Bin
Challenge | 2017 | HCTF | Bin | babyre

点击此处获得更好的阅读体验

WriteUp 来源

https://xz.aliyun.com/t/1589

题目考点

解题思路

这个题目的难度其实处在第三层和第四层之间。当初把它放第四层其实有点犹豫，因为感觉会有老司机秒杀他。

这个题目说起来其实很简答，我写了一个蒙哥马利乘算法和一个大整数加减的库。熟悉密码学的大佬应该知道蒙哥马利乘运算的作用就是进行快速模幂运算，即RSA的核心算法。 有关蒙哥马利算法的文章网上其实有很多，我就不再赘述了。代码中只有e和n。将输入的flag转换成大数的形式，然后做en = pow(f,e,n)输出了大数en。这里用了一个非常大的e，使得可以用Wiener's attack来计算出d的值。然后用d即可解密出flag。

*之所以认为他简单，是因为即使不知道蒙哥马利乘运算也能够猜出是RSA。首先是因为大整数加减以及乘运算，这些大整数运算还是很容易就可以分辨的。一旦分辨出这些运算，应该就能联想到RSA。第二个就是模幂运算化简式子。对于一个D=C**E%N的大数运算，可以采用下面的化简式子。*

```
D=1
FOR i=n TO 0
    D=D*D % N
    IF E[i]=1
        D=D*C % N
RETURN D
```

能看出这个式子是模幂运算的化简式子，即使看不懂乘法函数是个什么鬼。应该也能猜到什么了。

Flag

```
无
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2017/HCTF/Bin/qqmCQdEnHXeZ7dQh95pmH9.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 # 2017 # HCTF # Bin
ippatsu-nyuukon
rroopp