Copperstudy

发表于 2021-01-04 分类于 Challenge， 2019， 强网杯， Crypto
Challenge | 2019 | 强网杯 | Crypto | Copperstudy

点击此处获得更好的阅读体验

WP来源

https://www.anquanke.com/post/id/179386#h2-2

解题思路

Challenge 1

给出模N，加密指数e和明文m，明文512位，但低72位被隐藏，因此Stereotyped messages攻击，用sage求出明文低位。得出明文低72位为`190298140065006432965l`。再通过给出`m + 190298140065006432965l`，得出整个明文。

Challenge 2

知道p高位隐藏低128位，p高位攻击，sage求出最小根即是解。得出p的值后gmpy2.invert解出私钥d，即可解出c的明文m。

Challenge 3

已知私钥d 低512位，利用`Partial Key Exposure Attack`（部分密钥泄露攻击）可破解得出模因子p，再通过p求解出d，然后是常规解密。

Challenge 4

*加密指数e=3,三个模和三个密文[n1,n2,n3][c1,c2,c3],明显的广播攻击(Hastad's broadcast attack)，利用中国剩余定理解出M=m**3，再gmpy2.iroot(M,3)得出明文。*

Challenge 5

给出两个明文关系M = km + A，由此可知是相关明文攻击，Franklin-Reiter attack可解出明文m。

得出明文：

Challenge 6

从给出的已知条件，`d=N**0.27,(d<N**0.292)` 满足boneh_durfee attack条件，可利用该算法解出私钥d。

整理后各challenge输出的结果。

利用脚本提交各关m值，到第六关得出flag。

 # Challenge # 2019 # Crypto # 强网杯
大数据
JuseRe