CTF密码学练习

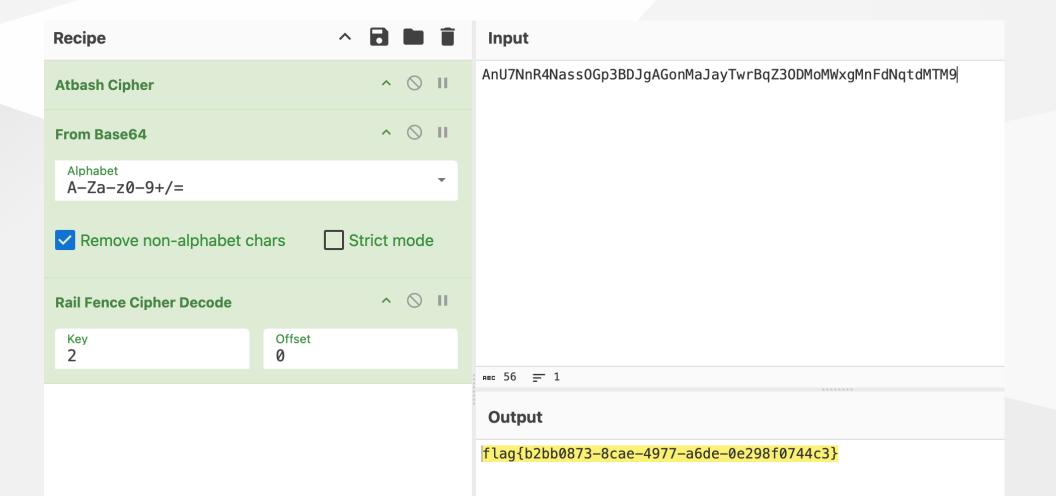
陈张萌 2024/7/3

推荐安装

pip3 install pycryptodome factordb.com

古典密码

AtBash密码+base64解密(经常跟密码学混在一起)+栅栏密码



rsa-factor

直接丢到factordb里面就可以解出来

rsa-m3

$$c1 = pow(m,e,n)$$
 $c2 = pow(m+1,e,n)$

又因为e=3

因此有

$$c1 = m^3 \mod n$$
 $c2 = (m^3 + 3m^2 + 3m + 1) \mod n$

rsa-m3

因此有

$$c2-c1-1=3(m^2+m) \mod n$$
 $c2+c1=(2m+1)(m^2+m+1) \mod n$

因此可以得到2m+1的值,进而求出m

rsa-fragile

可以发现p,ra,a,q,rb,b之间存在一定的关系:

$$p = a^8 + ra$$
 $q = b^8 + rb$

ra_的作用是使得p不一定是大于 a^8 的第一个质数。然后我们会发现:

$$n = p * q = (a^8 + ra) * (b^8 + rb)$$

rsa-fragile

再根据:

这些约束关系,我们可以发现ra和rb都很小。这样的话,对n开8次跟号,取整数部分,发现这就是ab。因为 $(a+1)^8b^8$ 和 $a^8(b+1)^8$ 都小于n。

rsa-fragile

发现n开8次跟号后很小,已经可以直接进行质因数分解了。分解结果:

nbs=[2,2,2,7,17,17,23,144680046702678787996517557250872603,2112824752321302638932489226261448911]

然后观察题目中的约束条件,发现a和b都是128位,p和q都是1024位,而且a<b<2a。因此,对上面的质因数进行排列组合后,计算出符合约束条件的a和b

得到满足条件的a和b,进而就可以直接计算得到p,q,进而得到n的分解。然后就可以求出phi和d,由密文算出明文。

rsa-easy

$$egin{aligned} n1 &= p1*q1 \ n2 &= p2*q2 \ n &= p1*q2*r \end{aligned}$$

那么

$$q2=\gcd(n2,n)$$

$$p1 = \gcd(n1, n)$$

而且题目里面已知r是500以内的素数,因此将500以内的素数遍历一下即可得到r,进而得到n的质因数分解

Thanks!