CTF之Crypto学习笔记（二）

原创

3tefanie丶zhou 于 2021-12-20 15:01:52 发布 52 收藏

分类专栏： CTF 文章标签： 安全

本文链接：https://blog.csdn.net/luochen2436/article/details/122041007


CTF 专栏收录该内容

18 篇文章 0 订阅

订阅专栏

目录

前言

上次gwb比赛碰到RSA共模攻击，套用网上的脚本发现解出来的是乱码，菜鸡表示百思不得其解。好在以前学过一点点密码学以及高数，向度娘取了点资料学习一下其原理，深入研究一波。

共模攻击原理

共模攻击即用两个及以上的公钥(n,e)来加密同一条信息m

已知有密文：

c1 = pow(m, e1, n)

c2 = pow(m, e2, n)

条件：

当e1，e2互质，则有gcd(e1,e2)=1

根据扩展欧几里德算法，对于不完全为 0 的整数 a，b，gcd（a，b）表示 a，b 的最大公约数。那么一定存在整数 x，y 使得 gcd（a，b）=ax+by

即可得到：

e1*s1*+*e2*s2 = 1

因为e1和e2为正整数，所以s1、s2皆为整数，但是一正一负，此时假设s1为正数,s2为负数

高数推导过程

我们假设e1,e2互质，即

```
gcd(e1,e2)=1
```

根据欧几里得算法可得

```
e1*s1+e2*s2=1
```

在e1*s1*+*e2*s2=1中，s1和s2为整数，但是一个为正数，一个为负数

通过欧几里得扩展算法，我们可以获得一组解（s1,s2）

模运算性质

(a * b) % n = (a % n * b % n) %n

a ^ b % n = ((a % n) ^ b) % n

c1 = (m^e1)%n

c2 = (m^e2)%n

```
证明：m=(c1^s1)*(c2^s2)

(c1^s1)*(c2^s2)%n = ((m^e1%n)^s1*(m^e2%n)^s2)%)n
根据模运算性质，化简为
(c1^s1)*(c2^s2)%n = ((m^e1)^s1*(m^e2)^s2)%n
根据幂运算性质化简，化简为
(c1^s1)*(c2^s2)%n = (m^(e1*s1)*m^(e2*s2))%n
合并同类项
(c1^s1)*(c2^s2)%n =  (m^(e1*s1+e2*s2))%n
又因为当e1,e2互质时有e1*s1+e2*s2=1，可得
(c1^s1)*(c2^s2)%n = (m^(1))%n
即，(c1^s1)*(c2^s2)%n = m %n
最后化简得到，(c1^s1)*(c2^s2)=m


特别注意：以上运算是在gcd(e1,e2)=1的前提下计算,得到m=(c1^s1)*(c2^s2)。
当出现e1,e2不互质的情况下,
即gcd(e1,e2)!=1,
根据化简的结果(c1^s1)*(c2^s2)%n =(m^(e1*s1+e2*s2))%n
左右换一下位置(数学强迫症，变量不在左边浑身不舒服)
m^(e1*s1+e2*s2) = (c1^s1)*(c2^s2)
根据欧几里得算法可得
m^gcd(e1,e2) = (c1^s1)*(c2^s2)
即最后 m 应为(c1^s1)*(c2^s2)得计算结果再开gcd(e1,e2)次方
```

代码实现

```
#coding:utf-8
#by  :3tefani丶zhou
from Crypto.Util.number import *
import gmpy2
def egcd(a, b):
  if a == 0:
    return (b, 0, 1)
  else:
    g, y, x = egcd(b % a, a)
    return (g, x - (b // a) * y, y)

def decode():
  n = 9301237994959667987401083652097246343815517596128327774351420387111432900804473550072644001246402914420481341390932238958596631342661148892729287431962806352600940514443660599638998597734028098346980341211945818504747525305963612655545155734816951497524971090189952697424613955973046154066099037503466904295 9
  c1 = 6590267857272772417917649657396899718271206331708228912045309406819932541998968838217780852904232221788733400508450479639722080485616725517641569021734825212609780913019520802069402625019404746058116502417835843430549536498383075655237933598539987652892207603059523267904694131078663726076499249937542146452 9
  c2 = 8580940367825015015329147118599980587085812300127303421258284773182529689101681087139754613411701219759965172940159098002002838288406851320175892641619221182192259368623247596780896400678607646016042863935315365832320811945305507019924329533052280497484933092650109143041977515567026430622296241328961695751 9
  e1 = 667430104865289
  e2 = 537409930523421
  s = egcd(e1, e2)
  s1 = s[1]
  s2 = s[2]
  if s1<0:
    s1 = - s1
    c1 = gmpy2.invert(c1, n)
  elif s2<0:
    s2 = - s2
    c2 = gmpy2.invert(c2, n)
  if gmpy2.gcd(e1,e2)==1:
      print("e1,e2互质")
      message = pow(c1, s1, n) * pow(c2, s2, n) % n
      flag = long_to_bytes(message)
      print(flag)
  elif gmpy2.gcd(e1,e2)!=1:
      message = pow(c1, s1, n) * pow(c2, s2, n) % n
      common_e = gmpy2.gcd(e1, e2)
      print("e1,e2不互质，且公约数为"+str(common_e))
      flag = long_to_bytes((gmpy2.iroot(message, common_e)[0]))
      print(flag)
if __name__ == '__main__':
    decode()
```

【违心的事情，不要做。发自本心的事情，但是有违江湖道义的事情，也不要做。今日做不成，未来有望做成的事情，切不可为达目的不择手段，不要着急去做。】