RSA:由p,q,dp,dq,c求明文的算法

转载

暮w光 于 2021-12-16 23:11:00 发布 184 收藏 2

分类专栏： # 密码学 文章标签： 算法

原文链接：https://blog.csdn.net/MikeCoke/article/details/105959599

密码学 专栏收录该内容

13 篇文章 1 订阅

订阅专栏

1.例题：【BUUCTF】RSA1

2.例题writeup

3.

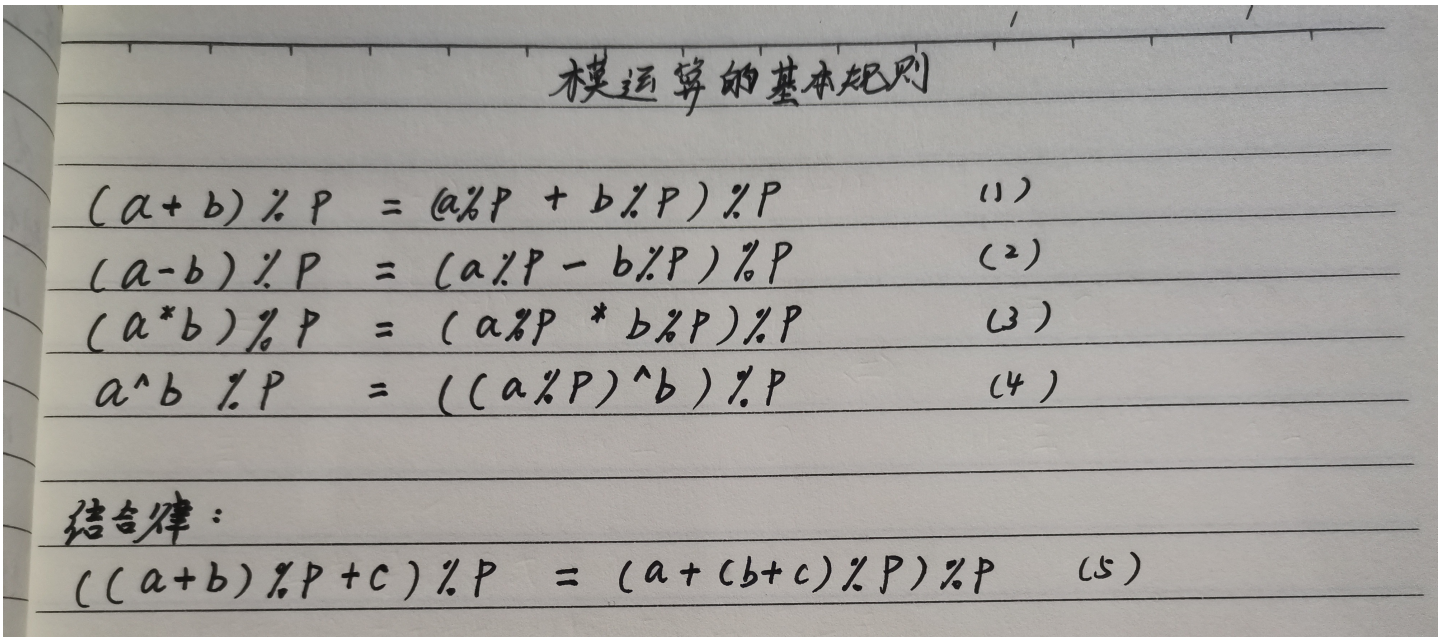
python解密：

```
import gmpy2
I = gmpy2.invert(q,p)
mp = pow(c,dp,p)
mq = pow(c,dq,q)                #求幂取模运算

m = (((mp-mq)*I)%p)*q+mq        #求明文公式

print(hex(m))           #转为十六进制
```

3.数学原理分析：



$((a*b)\%P*c)\%P = (a*(b*c)\%P)\%P$ (6)

交换律

$(a+b)\%P = (b+a)\%P$ (7)

$(a*b)\%P = (b*a)\%P$ (8)

$(a*b)\%P = (b*a)\%P$ (8)

分配律：

$(a+b)\%P = (a\%P + b\%P)\%P$ (9)

$((a+b)\%P*c)\%P = ((a*c)\%P + (b*c)\%P)\%P$ (10)

重要定理：

若 $a \equiv b (\%P)$，对任意的 C，都有 $(a+c) \equiv (b+c)(\%P)$ (11)

若 $a \equiv b (\%P)$，$\forall C$，有：$(a*c) \equiv (b*c)(\%P)$ (12)

若 $a \equiv b (\%P)$（$\forall C$，有），$c \equiv d (\%P)$，

则 $(a+c) \equiv (b+d)(\%P)$，$(a-c) \equiv (b-d)(\%P)$

$(a*c) \equiv (b*d)(\%P)$

RSA

已知 P、Q、dp、dq、C

公式：

1. $m_1 = C^{dp} \bmod p$
2. $m_2 = C^{dq} \bmod q$

3. $m = (((m_1 - m_2) * I) \bmod p) * q + m_2$ #求明文

4. I：乘法逆元

已知条件：

$C \equiv m^e \bmod n$ #加密

$m \equiv C^d \bmod n$ #解密

$\varphi(n) = (p-1)(q-1)$ #欧拉定理

$d \cdot e \equiv 1 \bmod \varphi(n)$ #欧拉定理与模反元素

$dp \equiv d \bmod (p-1)$

$dq \equiv d \bmod (q-1)$

$dq \equiv d \bmod (q-1)$

利用中国剩余定理，可得到：

$m_1 \equiv C^d \bmod p$ ，$m_2 \equiv C^d \bmod q$

证明过程：

由 $m \equiv C^d \bmod n$

可得：$m = C^d + k*n$

$\because n = p*q$

$\therefore m = C^d + k*p*q$

上述式子，同时取余 q 和 p，可分别得到：

$m_1 = C^d \bmod p$ ，$m_2 = C^d \bmod q$

$\Rightarrow C^d = kp + m_1$

代入 $m_2 = C^d \bmod q$ 得：

$m_2 \equiv (kp + m_1) \bmod q$

等式两边同时减去 m_1，可以得到：

$(m_2 - m_1) \equiv kp \bmod q$

这里因为 $gcd(p, q) = 1$

$\therefore$ 可求 p 的逆元，得：

$(m_2 - m_1) * p^{-1} \equiv k \bmod q$

$\Rightarrow k \equiv (m_2 - m_1) * p^{-1} \bmod q$

$$\begin{cases} k \equiv (m_2 - m_1) * p^{-1} \bmod q \\ C^d = kp + m_1 \end{cases}$$

$\Rightarrow C^d = ((m_2 - m_1) * p^{-1} \bmod q) * p + m_1$

代入 $m \equiv C^d \bmod n$

得 $m \equiv (((m_2 - m_1) * p^{-1} \bmod q) * p + m_1) \bmod n$

现在，只要求 m_1 和 m_2 了：

∵ $d \equiv dp \bmod (p-1)$, $d \equiv dq \bmod (q-1)$

分别代入 m_1, m_2 有：

$m_1 \equiv c^{dp \bmod (p-1)} \bmod p$ ①　　$m_1 \equiv c^{dp} \bmod p$

⇔

$m_2 \equiv c^{dq \bmod (q-1)} \bmod q$ ②　　$m_2 \equiv c^{dq} \bmod q$

用费马小定理推导①②式：

gcd(a,b) # 求最大公约数，欧几里德算法

假如 p 是质数，且 gcd(k,p)=1，则：$k^{(p-1)} \equiv 1 \bmod p$

∴ 如果有等式 $d = dp + k*(p-1)$

代入 $m_1 \equiv c^d \bmod p$

得：$m_1 \equiv c^{dp+k*(p-1)} \bmod p$

用费马小定理推导①②式：

gcd(a,b) # 求最大公约数，欧几里德算法

假如 p 是质数，且 gcd(k,p)=1，则：$k^{(p-1)} \equiv 1 \bmod p$

∴ 如果有等式 $d = dp + k*(p-1)$

代入 $m_1 \equiv c^d \bmod p$

得：$m_1 \equiv c^{dp+k*(p-1)} \bmod p$

⇒ $m_1 \equiv c^{dp} \cdot c^{k*(p-1)} \bmod p$

由费马小定理：

$c^{k*(p-1)} \bmod p = (c^{(p-1)} \bmod p)^k = 1^k = 1$

∴ $m_1 \equiv c^{dp} \bmod p$ ☆☆

同理 $m_2 \equiv c^{dq} \bmod q$ ☆☆