第五章　RSA 密码体制与整数因子分解

张磊

华东师范大学 • 软件学院

本章内容

1. 公钥密码学简介
2. 更多数论知识
3. RSA 密码体制
4. 对 RSA 的攻击
5. Rabin 密码体制
6. RSA 的语义安全性

§5.1　公钥密码学简介

对称密码体制的特点

目前为止, 我们学习了以下密码体制:

1. 古典密码体制: 移位密码、代换密码、置换密码、仿射密码、维吉尼亚密码等
2. 现代密码体制: DES、AES、Hash 函数、MAC、HMAC 等

对称密码体制的特点

目前为止, 我们学习了以下密码体制:

1. 古典密码体制: 移位密码、代换密码、置换密码、仿射密码、维吉尼亚密码等
2. 现代密码体制: DES、AES、Hash 函数、MAC、HMAC 等

上述密码体制都属于对称密码体制, 具有以下特点:

1. 只使用一个密钥
2. 收发双方共享这个单一的密钥
3. 密钥是对称的，双方是对等的

对称密码体制的不足

1. 密钥分配问题: 通信双方要进行加密通信,首先需要通过秘密的安全信道协商密钥, 而这样的安全信道在现实中可能很难实现.
2. 密钥管理问题: 在有多个用户的系统中, 任何两个用户之间都需要有共享的秘密密钥. 如果用户个数为 n, 则系统总共需要

$$C_n^2 = \frac{n(n-1)}{2}$$

个密钥. 这使得用户量增大时, 密钥空间急剧增大.

3. 数字签名问题: 对称密码算法无法实现抗伪造和不可否认的需求, 数据发送方或接收方都可以否认他/她以前的某个操作.

公钥密码的起源

1. 1970 年, Ellis 在一篇题为“非秘密加密的可能性”非公开文献中, 就已经提出了公钥密码学的思想.
2. 1973 年, Cocks 发表了题为“关于非秘密加密的注释”的论文, 其中描述的公钥密码体制本质上与 RSA 一样. 这篇论文与上一篇论文都被列为绝密文件, 后在 1997 年 12 月才由英国政府通信司令部 (GCHQ) 正式解密公开.
3. 1976 年, Diffie 和 Hellman 在其“密码学新方向”一文中公开提出了公钥密码学的思想.
4. 1978 年, Rivest, Shamir 和 Adleman 提出了第一个公钥密码体制 RSA.

公钥密码体制简介

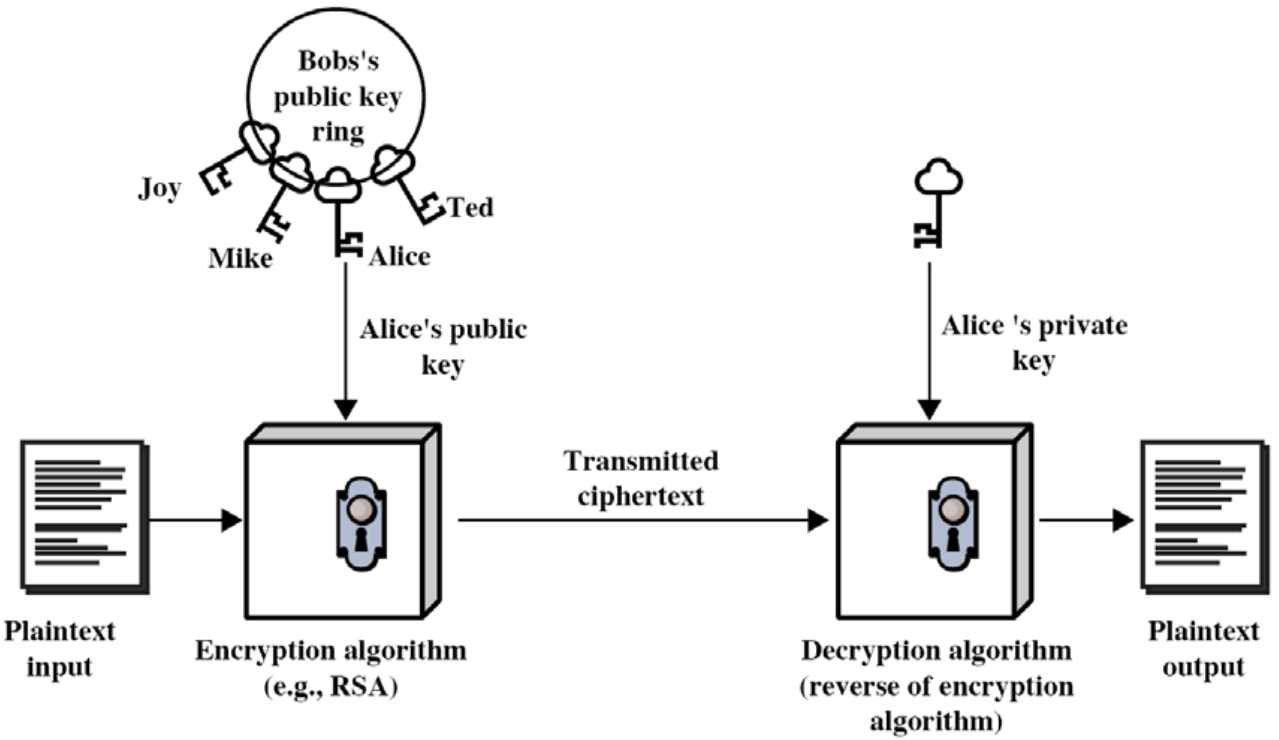
1. 密码学发展历史中最伟大的一次革命
2. 公钥/双钥/非对称密码都是指使用两个密钥：
   1. 公钥 (记为 pk)：可以公开的密钥，用于加密消息或验证签名
   2. 私钥 (记为 sk)：只能秘密保存，用于解密消息或计算签名
3. 两个密钥配对使用
   1. 公钥加密信息，私钥解密信息
   2. 私钥签名信息，公钥验证签名
   3. 参与方不对等，所以是非对称的
4. 基于数学函数而非基于代换和置换

公钥密码体制的主要应用

公钥密码体制主要三类应用:

1. 加密/解密 (提供保密性)
2. 数字签名 (提供认证)
3. 密钥交换 (生成会话密钥)

公钥密码体制之加密方案模型



公钥密码体制的要求

1. 产生用户的公-私密钥对 (pk, sk) 在计算上是容易的.
2. 加密运算和解密运算能够快速实现.

公钥密码体制的要求

1. 产生用户的公-私密钥对 (pk, sk) 在计算上是容易的.
2. 加密运算和解密运算能够快速实现.
3. 仅仅知道算法和公钥 pk，推导私钥 sk 计算上是不可行的. 这相当于已知加密函数 E_{pk}, 推导逆函数 D_{sk} 是困难的.

   满足上述性质 3 的函数称为单向函数 (即: 容易计算但难于求逆的函数). 尽管有很多单射函数被认为是单向的, 但目前还没有一个能被证明.

4. 如果知道私钥 sk (陷门), 则很容易得到逆函数.

   同时满足上述性质 3 和 4 的函数称为单向陷门函数, 它是公钥密码体制的一种抽象.

Examp-5-1-1: 单向函数

定义函数 f 为: $f(p,q) = pq$, 其中 p,q 是两个大素数. f 的逆函数其实就是大整数的因子分解, 目前还没有有效算法.

Example

已知 $f(p,q) = 32213114911055087$, 求 p,q.

Examp-5-1-1: 单向函数

定义函数 f 为: $f(p,q) = pq$, 其中 p,q 是两个大素数. f 的逆函数其实就是大整数的因子分解, 目前还没有有效算法.

Example

已知 $f(p,q) = 32213114911055087$, 求 p,q.

目前分解最大的整数为: RSA-768 (十进制 232 位, 09.12.12)

Examp-5-1-1: 单向函数

定义函数 f 为: $f(p,q) = pq$, 其中 p,q 是两个大素数. f 的逆函数其实就是大整数的因子分解, 目前还没有有效算法.

Example

已知 $f(p,q) = 32213114911055087$, 求 p,q.

目前分解最大的整数为: RSA-768 (十进制 232 位, 09.12.12)

123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3

Examp-5-1-1: 单向函数

定义函数 f 为: $f(p,q) = pq$, 其中 p,q 是两个大素数. f 的逆函数其实就是大整数的因子分解, 目前还没有有效算法.

Example

已知 $f(p,q) = 32213114911055087$, 求 p,q.

目前分解最大的整数为: RSA-768 (十进制 232 位, 09.12.12)

123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3

更多挑战数字见: http://www.rsa.com/rsalabs/node.asp?id=2093

Examp-5-1-2: 单向陷门函数 RSA

假设 $n = pq$, 其中 p, q 是两个大素数, b 为整数, 那么如下定义的函数 f 是单向陷门函数:

$$f(x) = x^b \bmod n.$$

Examp-5-1-2: 单向陷门函数 RSA

假设 $n = pq$, 其中 p, q 是两个大素数, b 为整数, 那么如下定义的函数 f 是单向陷门函数:

$$f(x) = x^b \bmod n.$$

如果知道 n 的因子分解, 那么就可以容易的求出 f 的逆:

$$f^{-1}(y) = y^a \bmod n,$$

其中 $a = b^{-1} \bmod \phi(n)$.

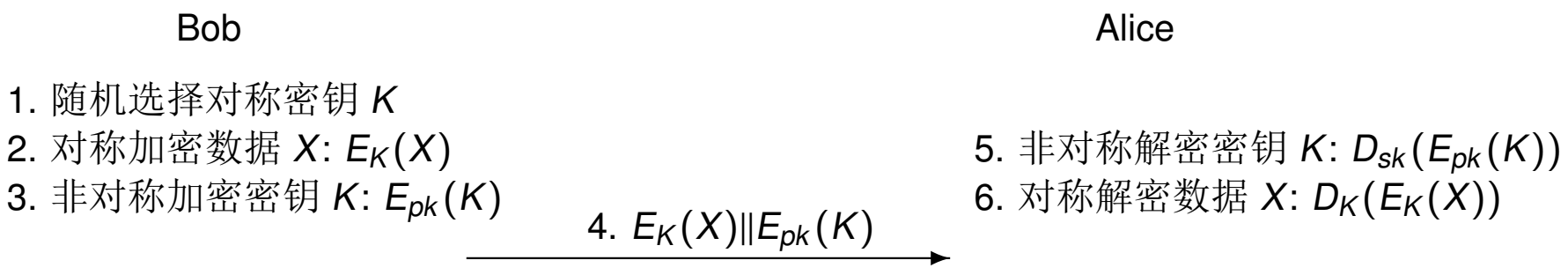
公钥密码体制的分类

根据其安全性所依赖的具体困难问题, 公钥密码体制可以分为以下几类:

1. 基于大整数分解困难性的 RSA 密码体制及其变体;
2. 基于离散对数问题困难性的 ElGamal 密码体制及其变体;
3. 其它类型的密码体制有: 基于背包问题的密码体制, 有限自动机密码体制.

公钥密码体制的缺点

1. 算法少, 被公认安全的实用算法更少—目前的公钥算法中只有 RSA 和椭圆曲线密码体制为人们普遍接受.
2. 速度慢, 无法用于大规模数据加密. 公钥密码一般和对称密码结合使用: 对称密码用来加密数据, 公钥密码用来加密对称密码所需的密钥 (见下图: 这里假设 Alice 的公-私密钥对为 (pk, sk), Bob 需发送数据 X 给她).



§5.2　更多数论知识

记号

1. (a, b) / $\gcd(a, b)$: 整数 a 和 b 的最大公因子;
2. $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$, 其上定义了加法和乘法;
3. $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n \mid (x, n) = 1\}$, 其元素个数为 $\phi(n)$.

记号

1. (a, b) / $\gcd(a, b)$: 整数 a 和 b 的最大公因子;
2. $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$, 其上定义了加法和乘法;
3. $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n \mid (x, n) = 1\}$, 其元素个数为 $\phi(n)$.

接下去的目的: 找出一个对 $\forall\, x \in \mathbb{Z}_n^*$, 有效计算

$$x^{-1} \bmod n$$

的方法.

Examp-5-2-1: 最大公因子

问题：如何有效计算两个整数 a, b 的最大公因子 (a, b)

Examp-5-2-1: 最大公因子

问题：如何有效计算两个整数 a, b 的最大公因子 (a, b)

Example

计算: $(99, 63)$

进行如下辗转相除过程:

$$\underline{99} \quad = \quad 1 \cdot \underline{63} + \underline{36} \quad \Rightarrow (99, 63) = (63, 36)$$

Examp-5-2-1: 最大公因子

问题：如何有效计算两个整数 a, b 的最大公因子 (a, b)

Example

计算: $(99, 63)$

进行如下辗转相除过程:

$$\underline{99} = 1 \cdot \underline{63} + \underline{36} \quad \Rightarrow (99, 63) = (63, 36)$$

$$\underline{63} = 1 \cdot \underline{36} + \underline{27} \quad \Rightarrow (63, 36) = (36, 27)$$

Examp-5-2-1: 最大公因子

问题：如何有效计算两个整数 a, b 的最大公因子 (a, b)

Example

计算: $(99, 63)$

进行如下辗转相除过程:

$$\begin{aligned} \underline{99} &= 1 \cdot \underline{63} + \underline{36} && \Rightarrow (99, 63) = (63, 36) \\ \underline{63} &= 1 \cdot \underline{36} + \underline{27} && \Rightarrow (63, 36) = (36, 27) \\ \underline{36} &= 1 \cdot \underline{27} + \underline{9} && \Rightarrow (36, 27) = (27, 9) \end{aligned}$$

Examp-5-2-1: 最大公因子

问题：如何有效计算两个整数 a, b 的最大公因子 (a, b)

Example

计算: $(99, 63)$

进行如下辗转相除过程:

$$
\begin{aligned}
\underline{99} &= 1 \cdot \underline{63} + \underline{36} && \Rightarrow (99, 63) = (63, 36) \\
\underline{63} &= 1 \cdot \underline{36} + \underline{27} && \Rightarrow (63, 36) = (36, 27) \\
\underline{36} &= 1 \cdot \underline{27} + \underline{9} && \Rightarrow (36, 27) = (27, 9) \\
\underline{27} &= 3 \cdot \underline{9} + \underline{0} && \Rightarrow (27, 9) = 9
\end{aligned}
$$

Examp-5-2-1: 最大公因子

问题：如何有效计算两个整数 a, b 的最大公因子 (a, b)

Example

计算: $(99, 63)$

进行如下辗转相除过程:

$$
\begin{aligned}
\underline{99} &= 1 \cdot \underline{63} + \underline{36} && \Rightarrow (99, 63) = (63, 36) \\
\underline{63} &= 1 \cdot \underline{36} + \underline{27} && \Rightarrow (63, 36) = (36, 27) \\
\underline{36} &= 1 \cdot \underline{27} + \underline{9} && \Rightarrow (36, 27) = (27, 9) \\
\underline{27} &= 3 \cdot \underline{9} + \underline{0} && \Rightarrow (27, 9) = 9
\end{aligned}
$$

因此, $(99, 63) = (63, 36) = (36, 27) = (27, 9) = 9$

欧式 (Euclidean) 算法

把上面的方法应用到更一般的情形，得到欧式算法：

基本原理: 如果 $a = qb + r\ (0 \le r < b)$, 那么 $(a, b) = (b, r)$.

基本过程: 先令 $r_0 = a$, $r_1 = b$, 后进行辗转相除, 直到余数为零：

$$\begin{array}{lcll} r_0 & = & q_1 r_1 + r_2 & 0 < r_2 < r_1 \\ r_1 & = & q_2 r_2 + r_3 & 0 < r_3 < r_2 \\ r_2 & = & q_3 r_3 + r_4 & 0 < r_4 < r_3 \\ \vdots & \vdots & \vdots & \vdots \\ r_{m-2} & = & q_{m-1} r_{m-1} + r_m & 0 < r_m < r_{m-1} \\ r_{m-1} & = & q_m r_m & \end{array}$$

那么

$$(a, b) = (r_1, r_2) = \cdots = (r_{m-2}, r_{m-1}) = (r_{m-1}, r_m) = r_m.$$

Euclidean Algorithm (a, b)

$r_0 \leftarrow a$

$r_1 \leftarrow b$

$m \leftarrow 1$

while $r_m \neq 0$

do $\begin{cases} q_m \leftarrow \lfloor \frac{r_{m-1}}{r_m} \rfloor \\ r_{m+1} \leftarrow r_{m-1} - q_m r_m \\ m \leftarrow m + 1 \end{cases}$

$m \leftarrow m - 1$

return $(q_1, q_2, \cdots, q_m; r_m)$

comment: $r_m = (a, b)$

Examp-5-2-2: 课堂练习

求整数 $a = 680261, b = 678709$ 的最大公因子.

Examp-5-2-2: 课堂练习

求整数 $a = 680261, b = 678709$ 的最大公因子.

解:

$$\begin{aligned} 680261 &= 1 \cdot 678709 + 1552 \\ 678709 &= 437 \cdot 1552 + 485 \\ 1552 &= 3 \cdot 485 + 97 \\ 485 &= 5 \cdot 97 \end{aligned}$$

$\therefore \quad q_1 = 1, q_2 = 437, q_3 = 3, q_4 = 5, r_4 = 97,$ 即有

$$(680261, 678709) = 97.$$

求模乘逆的思路

对任意整数 a, b, 我们现在探讨模乘逆 $b^{-1} \bmod a$ 的求法.

求模乘逆的思路

对任意整数 a, b, 我们现在探讨模乘逆 $b^{-1} \bmod a$ 的求法.

考虑更一般情形:

1. 是否存在整数 s, t, 使得 $sa + tb = (a, b)$?
2. 如果存在这样的 s, t 的话, 且 $(a, b) = 1$, 则有

$$sa + tb = 1.$$

等式两边模 a 之后, 得到 $tb \equiv 1 \pmod{a}$, 即有

$$t = b^{-1} \bmod a.$$

s, t 的存在性

从欧式算法可知有关系式:

$$
\begin{aligned}
r_0 &= q_1 r_1 + r_2 && 0 < r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3 && 0 < r_3 < r_2 \\
&\vdots \quad \vdots \quad \vdots && \vdots \\
r_{m-2} &= q_{m-1} r_{m-1} + r_m && 0 < r_m < r_{m-1} \\
r_{m-1} &= q_m r_m
\end{aligned}
$$

$$
\begin{aligned}
\therefore (a, b) &= r_m = r_{m-2} - q_{m-1} r_{m-1} \\
&= r_{m-2} - q_{m-1}(r_{m-3} - q_{m-2} r_{m-2}) \\
&= (1 + q_{m-1} q_{m-2}) r_{m-2} - q_{m-1} r_{m-3} \\
&= \cdots \\
&= f(q_1, q_2, \cdots, q_m) r_0 + g(q_1, q_2, \cdots, q_m) r_1 \\
&= sa + tb
\end{aligned}
$$

s, t 的快速计算—扩展欧式算法

如下定义两个数列 $t_0, t_1, \cdots, t_m$ 和 $s_0, s_1, \cdots, s_m$:

$$t_j = \begin{cases} 0, & j = 0; \\ 1, & j = 1; \\ t_{j-2} - q_{j-1} t_{j-1}, & j \geq 2. \end{cases} \quad s_j = \begin{cases} 1, & j = 0; \\ 0, & j = 1; \\ s_{j-2} - q_{j-1} s_{j-1}, & j \geq 2. \end{cases}$$

Theorem

对于如上定义的 s_j 和 t_j, 有关系式

$$r_j = s_j r_0 + t_j r_1, \ 0 \leq j \leq m.$$

特别地, 我们有

$$(a, b) = r_m = s_m a + t_m b.$$

s, t 的快速计算—扩展欧式算法

如下定义两个数列 $t_0, t_1, \cdots, t_m$ 和 $s_0, s_1, \cdots, s_m$:

$$t_j = \begin{cases} 0, & j = 0; \\ 1, & j = 1; \\ t_{j-2} - q_{j-1} t_{j-1}, & j \geq 2. \end{cases} \quad s_j = \begin{cases} 1, & j = 0; \\ 0, & j = 1; \\ s_{j-2} - q_{j-1} s_{j-1}, & j \geq 2. \end{cases}$$

Theorem

对于如上定义的 s_j 和 t_j, 有关系式

$$r_j = s_j r_0 + t_j r_1, \ 0 \leq j \leq m.$$

特别地, 我们有

$$(a, b) = r_m = s_m a + t_m b.$$

comment: 如果 $(a, b) = 1$, 则 $t_m = b^{-1} \bmod a$.

Examp-5-2-3: 计算 $28^{-1} \bmod 75$

根据扩展欧式算法, 我们做如下计算:

j	r_j	q_j	s_j	t_j
0	75		1	0
1	28	2	0	1
2	19	1	1	-2
3	9	2	-1	3
4	1	9	3	$\underline{-8}$

$\because\ m = 4, r_4 = 1, q_4 = 9, s_4 = 3, t_4 = -8,$

$\therefore$ 有等式 $(75, 28) = 1 = 3 \cdot 75 + (\underline{-8}) \cdot 28,$

最后得到: $28^{-1} \bmod 75 = \underline{-8} \bmod 75 = 67.$

计算 $b^{-1} \bmod a$ 的改进

1. 在上述求 $28^{-1} \bmod 75$ 的例子中, 其实我们只需最终得到整数 $t_4 = -8$, 它只与数列 t_3, t_2, t_1, t_0 相关, 故我们可以计算如下 (即删除了 s_j 列):

j	r_j	q_j	t_j
0	75		0
1	28	2	1
2	19	1	-2
3	9	2	3
4	1	9	$\underline{-8}$

同样得到 $t_4 = \underline{-8}$, 从而 $28^{-1} \bmod 75 = \underline{-8} \bmod 75 = 67$.

计算 $b^{-1} \bmod a$ 的改进

1. 在上述求 $28^{-1} \bmod 75$ 的例子中, 其实我们只需最终得到整数 $t_4 = -8$, 它只与数列 t_3, t_2, t_1, t_0 相关, 故我们可以计算如下 (即删除了 s_j 列):

j	r_j	q_j	t_j
0	75		0
1	28	2	1
2	19	1	−2
3	9	2	3
4	1	9	$\underline{-8}$

   同样得到 $t_4 = \underline{-8}$, 从而 $28^{-1} \bmod 75 = \underline{-8} \bmod 75 = 67$.

2. 同理, 在求 $b^{-1} \bmod a$ 的过程中也只需关注数列 $\{t_j\}$ 的运算, 所以我们可以删除扩展欧式算法中关于数列 $\{s_j\}$ 的计算部分, 得到如下的乘法逆算法.

Multiplicative Inverse (a, b)

$a_0 \leftarrow a$

$b_0 \leftarrow b$

$t_0 \leftarrow 0$

$t \leftarrow 1$

$q \leftarrow \lfloor \frac{a_0}{b_0} \rfloor$

$r \leftarrow a_0 - qb_0$

while $r > 0$

do
- temp $\leftarrow (t_0 - qt) \bmod a$
- $t_0 \leftarrow t$
- $t \leftarrow$ temp
- $a_0 \leftarrow b_0$
- $b_0 \leftarrow r$
- $q \leftarrow \lfloor \frac{a_0}{b_0} \rfloor$
- $r \leftarrow a_0 - qb_0$

if $b_0 \neq 1$

then b has no inverse modulo a

else return (t)

comment: $t = b^{-1} \bmod a$

关于中国剩余定理的典故:“物不知其数”问题

1. 《孙子算经》：今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？

关于中国剩余定理的典故:“物不知其数”问题

1. 《孙子算经》：今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？
2. 上述问题可抽象成以下同余方程组:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

关于中国剩余定理的典故:“物不知其数”问题

1. 《孙子算经》：今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？
2. 上述问题可抽象成以下同余方程组:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

3. 解决此类特定同余方程组的方法称为中国剩余定理或者孙子定理.

中国剩余定理

假定 $m_1, m_2, \cdots, m_r$ 为两两互素的正整数, 又假定 $a_1, a_2, \cdots, a_r$ 为整数, 那么同余方程组

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \quad \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

有模 $M = m_1 m_2 \cdots m_r$ 的唯一解, 此解由下式给出:

$$x = \sum_{i=1}^{r} a_i M_i y_i \bmod M,$$

其中 $M_i = \frac{M}{m_i}$, $y_i = M_i^{-1} \bmod m_i$, $1 \le i \le r$.

中国剩余定理证明

正确性: 注意到 $\begin{cases} a_i M_i y_i \equiv a_i \pmod{m_j}, & i = j; \\ a_i M_i y_i \equiv 0 \pmod{m_j}, & i \neq j. \end{cases}$ $\therefore\ \forall\ 1 \leq j \leq r$, 有

$$x = \sum_{i=1}^{r} a_i M_i y_i \bmod M \equiv (\sum_{i=j} + \sum_{i \neq j}) a_i M_i y_i \equiv a_j \pmod{m_j}.$$

中国剩余定理证明

正确性: 注意到 $\begin{cases} a_i M_i y_i \equiv a_i \pmod{m_j}, & i = j; \\ a_i M_i y_i \equiv 0 \pmod{m_j}, & i \neq j. \end{cases}$ $\therefore\ \forall\ 1 \leq j \leq r$, 有

$$x = \sum_{i=1}^{r} a_i M_i y_i \bmod M \equiv (\sum_{i=j} + \sum_{i \neq j}) a_i M_i y_i \equiv a_j \pmod{m_j}.$$

唯一性: (反证法) 假设有两个模 M 的不同解 x_1, x_2 满足同余方程组, 则有 $x_1 - x_2 \not\equiv 0 \pmod{M}$. 即存在 $s, 0 < t < M$, 使得

$$x_1 - x_2 = sM + t.$$

因为 $i \neq j$ 时有 $(m_i, m_j) = 1$, 所以必存在某一个 m_j 使得 $m_j \nmid t$, 也就是说, $x_1 - x_2 \equiv s m_1 m_2 \cdots m_r + t \equiv t \not\equiv 0 \pmod{m_j}$;

另一方面, $x_1 - x_2 \equiv a_j - a_j \equiv 0 \pmod{m_j}$. 矛盾!

“物不知其数”问题的解

解: 因为 $a_1 = 2, a_2 = 3, a_3 = 2, m_1 = 3, m_2 = 5, m_3 = 7$, 故

$$M = 105,\ M_1 = 35,\ M_2 = 21,\ M_3 = 15$$

和

$$y_1 = M_1^{-1} \bmod m_1 = 2,\ y_2 = M_2^{-1} \bmod m_2 = 1,\ y_3 = M_3^{-1} \bmod m_3 = 1.$$

所以在 $\mathbb{Z}_{105}$ 内, 有

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \bmod M = 233 \bmod 105 = 23.$$

“物不知其数”问题的解

解: 因为 $a_1 = 2, a_2 = 3, a_3 = 2, m_1 = 3, m_2 = 5, m_3 = 7$, 故

$$M = 105,\ M_1 = 35,\ M_2 = 21,\ M_3 = 15$$

和

$$y_1 = M_1^{-1} \bmod m_1 = 2,\ y_2 = M_2^{-1} \bmod m_2 = 1,\ y_3 = M_3^{-1} \bmod m_3 = 1.$$

所以在 $\mathbb{Z}_{105}$ 内, 有

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \bmod M = 233 \bmod 105 = 23.$$

明朝大数学家程大位:

三人同行七十稀，五树梅花廿一枝，
七子团圆正半月，除百零五便得知。

阶、本原元 (素) 的概念

1. 整数 α 模 n 的阶定义为使得

$$\alpha^m \equiv 1 \pmod{n}$$

成立的最小正整数 m, 记为 $\mathrm{Ord}_n(\alpha)$.

阶、本原元 (素) 的概念

1. 整数 α 模 n 的阶定义为使得

$$\alpha^m \equiv 1 \pmod{n}$$

成立的最小正整数 m, 记为 $\mathrm{Ord}_n(\alpha)$.

Example

可以验证, 整数 5 模 7 的阶为 6:

$$5^1 \bmod 7 = 5, \quad 5^2 \bmod 7 = 4, \quad 5^3 \bmod 7 = 6,$$
$$5^4 \bmod 7 = 2, \quad 5^5 \bmod 7 = 3, \quad 5^6 \bmod 7 = 1.$$

阶、本原元 (素) 的概念

1. 整数 α 模 n 的阶定义为使得

$$\alpha^m \equiv 1 \pmod{n}$$

成立的最小正整数 m, 记为 $\mathrm{Ord}_n(\alpha)$.

Example

可以验证, 整数 5 模 7 的阶为 6:

$$5^1 \bmod 7 = 5, \quad 5^2 \bmod 7 = 4, \quad 5^3 \bmod 7 = 6,$$
$$5^4 \bmod 7 = 2, \quad 5^5 \bmod 7 = 3, \quad 5^6 \bmod 7 = 1.$$

2. 如果元素 α 模素数 p 的阶等于 $p-1$ (即 $\mathrm{Ord}_p(\alpha) = p-1$), 则称 α 是一个模 p (或 $\mathbb{Z}_p$) 的本原元 (素). 上例中, 5 就是模 7 的一个本原元素.

其它数论结果

1. 如果 $b \in \mathbb{Z}_n^*$, 则

$$b^{\phi(n)} \equiv 1 \pmod{n}.$$

其它数论结果

1. 如果 $b \in \mathbb{Z}_n^*$, 则

$$b^{\phi(n)} \equiv 1 \pmod{n}.$$

2. (Fermat 定理) 如果 p 是一个素数, 且 $b \in \mathbb{Z}_p$, 则

$$b^p \equiv b \pmod{p}.$$

其它数论结果

1. 如果 $b \in \mathbb{Z}_n^*$, 则

$$b^{\phi(n)} \equiv 1 \pmod{n}.$$

2. (Fermat 定理) 如果 p 是一个素数, 且 $b \in \mathbb{Z}_p$, 则

$$b^p \equiv b \pmod{p}.$$

3. 假定 $p > 2$ 是一个素数, 且 $\alpha \in \mathbb{Z}_p^*$. 那么 α 是一个模 p 的本原元素当且仅当

$$\alpha^{(p-1)/q} \not\equiv 1 \pmod{p}$$

对所有满足 $q|(p-1)$ 的素数 q 都成立.

§ 5.3　RSA 密码体制

RSA 密码体制

设 $n = pq$, 其中 p, q 是两个大素数. 设 $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$, 且定义

$$\mathcal{K} = \{(n, p, q, a, b) \mid ab \equiv 1 \pmod{\phi(n)}\}.$$

对于 $K = (n, p, q, a, b) \in \mathcal{K}$, 定义

$$E_K(x) = x^b \bmod n, \quad x \in \mathbb{Z}_n$$

和

$$D_K(y) = y^a \bmod n, \quad y \in \mathbb{Z}_n.$$

值 (n, b) 为公钥, 值 (p, q, a) 为私钥.

Examp-5-3-1: RSA 加密

假定 Bob 选取 $p = 101, q = 113$, 那么

$$n = pq = 11413, \quad \phi(n) = (p-1)(q-1) = 11200.$$

Bob 随机选择 $b = 3533$ 并通过欧式算法来验证 $(b, \phi(n)) = 1$, 然后计算秘密解密指数

$$a = b^{-1} \bmod 11200 = 6597.$$

公钥: $(n = 11413, b = 3533)$,

私钥: $(p = 101, q = 113, a = 6597)$.

Examp-5-3-1: RSA 加密

假定 Bob 选取 $p = 101, q = 113$, 那么

$$n = pq = 11413, \quad \phi(n) = (p-1)(q-1) = 11200.$$

Bob 随机选择 $b = 3533$ 并通过欧式算法来验证 $(b, \phi(n)) = 1$, 然后计算秘密解密指数

$$a = b^{-1} \bmod 11200 = 6597.$$

公钥: $(n = 11413, b = 3533)$,

私钥: $(p = 101, q = 113, a = 6597)$.

Alice 如果想加密明文 9726 发送给 Bob, 她使用 Bob 的公钥计算

$$E_K(9726) = 9726^{3533} \bmod 11413 = 5761,$$

然后把密文 5761 通过信道发送给 Bob.

Examp-5-3-1: RSA 加密

假定 Bob 选取 $p = 101, q = 113$, 那么

$$n = pq = 11413, \quad \phi(n) = (p-1)(q-1) = 11200.$$

Bob 随机选择 $b = 3533$ 并通过欧式算法来验证 $(b, \phi(n)) = 1$, 然后计算秘密解密指数

$$a = b^{-1} \bmod 11200 = 6597.$$

公钥: $(n = 11413, b = 3533)$,

私钥: $(p = 101, q = 113, a = 6597)$.

Alice 如果想加密明文 9726 发送给 Bob, 她使用 Bob 的公钥计算

$$E_K(9726) = 9726^{3533} \bmod 11413 = 5761,$$

然后把密文 5761 通过信道发送给 Bob.

Bob 收到密文之后, 使用秘密解密指数可计算出明文

$$D_K(5761) = 5761^{6597} \bmod 11413 = 9726.$$

实现 RSA 之: 参数生成

1. 生成两个大素数 p, q (使用素性测试算法, 为判定问题的随机算法)

实现 RSA 之: 参数生成

1. 生成两个大素数 p, q (使用素性测试算法, 为判定问题的随机算法)
2. $n \leftarrow pq$, 且 $\phi(n) \leftarrow (p-1)(q-1)$

实现 RSA 之: 参数生成

1. 生成两个大素数 p, q (使用素性测试算法, 为判定问题的随机算法)
2. $n \leftarrow pq$, 且 $\phi(n) \leftarrow (p-1)(q-1)$
3. 选择一个随机数 b $(1 < b < \phi(n))$, 使得 $(b, \phi(n)) = 1$ (使用欧式算法判断)

实现 RSA 之: 参数生成

1. 生成两个大素数 p, q (使用素性测试算法, 为判定问题的随机算法)
2. $n \leftarrow pq$, 且 $\phi(n) \leftarrow (p-1)(q-1)$
3. 选择一个随机数 b $(1 < b < \phi(n))$, 使得 $(b, \phi(n)) = 1$ (使用欧式算法判断)
4. $a \leftarrow b^{-1} \bmod \phi(n)$ (使用求逆算法)

实现 RSA 之: 参数生成

1. 生成两个大素数 p, q (使用素性测试算法, 为判定问题的随机算法)
2. $n \leftarrow pq$, 且 $\phi(n) \leftarrow (p-1)(q-1)$
3. 选择一个随机数 b $(1 < b < \phi(n))$, 使得 $(b, \phi(n)) = 1$ (使用欧式算法判断)
4. $a \leftarrow b^{-1} \bmod \phi(n)$ (使用求逆算法)
5. 公钥为 (n, b), 私钥为 (p, q, a)

实现 RSA 之: 平方-乘算法

考虑如何快速实现模指数运算?

Example

计算：3^9

方法一: 直接计算，需要 8 次乘法运算。

实现 RSA 之: 平方-乘算法

考虑如何快速实现模指数运算?

Example

计算：3^9

方法一: 直接计算，需要 8 次乘法运算。

方法二: 注意到

$$
\begin{aligned}
3^9 &= 3(3^4)^2 \\
&= 3((3^2)^2)^2 \\
&= 3((9)^2)^2 && \text{第 1 次乘法} \\
&= 3(81)^2 && \text{第 2 次乘法} \\
&= 3 \cdot 6561 && \text{第 3 次乘法} \\
&= 19683 && \text{第 4 次乘法}
\end{aligned}
$$

SquareMultiply (x, c, n)

假定: c 的二进制表示为 $c = \sum_{i=0}^{l-1} c_i 2^i$, $c_i \in \{0, 1\}$

$z \leftarrow 1$

for $i \leftarrow l - 1$ **downto** 0

do
- $z \leftarrow z^2 \bmod n$
- **if** $c_i = 1$
  - **then** $z \leftarrow (z \cdot x) \bmod n$

return (z)

comment: $z = x^c \bmod n$

作业 7 (共两大题)

1. 计算

   1. 利用求逆算法, 计算 $104729^{-1} \bmod 15485863$;
   2. (书上练习 5.6) 求解同余方程组

$$\begin{cases} x \equiv 12 \pmod{25} \\ x \equiv 9 \pmod{26} \\ x \equiv 23 \pmod{27} \end{cases}$$

   3. 证明 2 是模 11 的一个本原元素.

作业 7 (共两大题) 续

2. 下面数字序列给出的是一个用 RSA 加密的密文串, 你的任务是对它进行解密. 系统的公开参数为 $n = 31313, b = 4913$. 这可以按如下步骤完成: 首先分解 n (因为 n 较小，所以容易做到); 然后利用 $\phi(n)$ 计算解密指数 a; 最后解密密文. 利用平方乘算法来计算模 n 指数.

为了将明文变为通常的英文文字，你需要知道英文字母是如何在 $\mathbb{Z}_n$ 中"编码" 的. $\mathbb{Z}_n$ 中每一元素表示三个英文字母, 参见如下例子:

$$\begin{array}{lcll} \text{DOG} & \rightarrow & 3 \times 26^2 + 14 \times 26 + 6 & = & 2398 \\ \text{CAT} & \rightarrow & 2 \times 26^2 + 0 \times 26 + 19 & = & 1371 \\ \text{ZZZ} & \rightarrow & 25 \times 26^2 + 25 \times 26 + 25 & = & 17575 \end{array}$$

你需要在你的程序中最后一步完成这个过程的逆.

6340 8309 14010 8936 27358 25023 16481 25809 23614 7135 24996 30590 27570 26486 30388 9395 27584 14999

4517 12146 29421 26439 1606 17881 25774 7647 23901 7372 25774 18436 12056 13547 7908 8635 2149 1908 22076

7372 8686 1304 4082 11803 5314 107 7359 22470 7372 22827 15698 30317 4685 14696 30388 8671 29956 15705

1417 26905 25809 28347 26277 7897 20240 21519 12437 1108 27106 18743 24144 10685 25234 30155 23005 8267

9917 7994 9694 2149 10042 27705 15930 29748 8635 23645 11738 24591 20240 27212 27486 9741 2149 29329 2149

5501 14015 30155 18154 22319 27705 20321 23254 13624 3249 5443 2149 16975 16087 14600 27705 19386 7325

26277 19554 23614 7553 4734 8091 23973 14015 107 3183 17347 25234 4595 21498 6360 19837 8463 6000 31280

29413 2066 369 23204 8425 7792 25973 4477 30989

§ 5.4　对 RSA 的攻击

RSA 密码体制

设 $n = pq$, 其中 p, q 是两个大素数. 设 $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$, 且定义

$$\mathcal{K} = \{(n, p, q, a, b) \mid ab \equiv 1 \pmod{\phi(n)}\}.$$

对于$K = (n, p, q, a, b) \in \mathcal{K}$, 定义

$$E_K(x) = x^b \bmod n, \quad x \in \mathbb{Z}_n$$

和

$$D_K(y) = y^a \bmod n, \quad y \in \mathbb{Z}_n.$$

值 (n, b) 为公钥, 值 (p, q, a) 为私钥.

主要攻击形式

1. 分解模数 n
2. 计算 $\phi(n)$
3. 计算低解密指数
4. 其它类型攻击

分解模数 n

分解模数 n 方法有:

1. 二次筛法
2. 椭圆曲线分解算法
3. 数域筛法
4. 其它先驱算法: Pollard 的 ρ 方法和 $p-1$ 算法, William 的 $p+1$ 算法, 连分式算法, 试除法等.

实际中的分解因子算法

1. 二次筛法: 适合分解 $p \approx \sqrt{n}$ 型的整数, 是分解 RSA 模最常用的算法;
2. 椭圆曲线分解算法: 如果分解的整数 n 具有不同长度的素因子, 则此法更有效;
3. 数域筛法: 最近发展起来的算法, 其渐进运行时间比上述两种算法都少.

因子分解的里程碑事件

1. 1983 年，用二次筛法成功分解了一个 69 位的 10 进制数;

因子分解的里程碑事件

1. 1983 年，用二次筛法成功分解了一个 69 位的 10 进制数;
2. 1986 年，Lenstra 和 Manasse 利用二次筛法成功分解了一个 106 位的十进制整数;

因子分解的里程碑事件

1. 1983 年，用二次筛法成功分解了一个 69 位的 10 进制数;
2. 1986 年，Lenstra 和 Manasse 利用二次筛法成功分解了一个 106 位的十进制整数;
3. 2003 年 12 月, Franke 利用数域筛法分解了 RSA-576;

因子分解的里程碑事件

1. 1983 年，用二次筛法成功分解了一个 69 位的 10 进制数;
2. 1986 年，Lenstra 和 Manasse 利用二次筛法成功分解了一个 106 位的十进制整数;
3. 2003 年 12 月, Franke 利用数域筛法分解了 RSA-576;
4. 2009 年 12 月 12 日, RSA-768 被分解;

因子分解的里程碑事件

1. 1983 年，用二次筛法成功分解了一个 69 位的 10 进制数;
2. 1986 年，Lenstra 和 Manasse 利用二次筛法成功分解了一个 106 位的十进制整数;
3. 2003 年 12 月, Franke 利用数域筛法分解了 RSA-576;
4. 2009 年 12 月 12 日, RSA-768 被分解;

   12301866845301177551304949583849627207728535695953347921973224521517264005072636575187452021997864693899564749427740638459251925573263034537315482685079170261221429134616704292143116022212404792747377940806653514195974598569021434 13

因子分解的里程碑事件

1. 1983 年，用二次筛法成功分解了一个 69 位的 10 进制数;
2. 1986 年，Lenstra 和 Manasse 利用二次筛法成功分解了一个 106 位的十进制整数;
3. 2003 年 12 月, Franke 利用数域筛法分解了 RSA-576;
4. 2009 年 12 月 12 日, RSA-768 被分解;

123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3

33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489

367460436667995904282446337996279526322791581643430876426760322838157396665112792333734171433968102700927987363089 17

因子分解的里程碑事件

1. 1983 年，用二次筛法成功分解了一个 69 位的 10 进制数;
2. 1986 年，Lenstra 和 Manasse 利用二次筛法成功分解了一个 106 位的十进制整数;
3. 2003 年 12 月, Franke 利用数域筛法分解了 RSA-576;
4. 2009 年 12 月 12 日, RSA-768 被分解;

   12301866845301177551304949583849627207728535695953347921973224521517264005072636575187452021997864693899564749427740638459251925573263034537315482685079170261221429134616704292143116022212404792747377940806653514195974598569021434 13

   33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489

   36746043666799590428244633799627952632279158164343087642676032283815739666511279233373417143396810270092798736308917

5. 人们预计 1024 比特的模数将在 2018 年被分解.

计算 $\phi(n)$

1. 如果攻击者知道 $\phi(n)$, 那么他可由加密指数 b 计算出解密指数 $a = b^{-1} \bmod \phi(n)$.

计算 $\phi(n)$

1. 如果攻击者知道 $\phi(n)$, 那么他可由加密指数 b 计算出解密指数 $a = b^{-1} \bmod \phi(n)$.
2. 计算 $\phi(n)$ 并不比分解 n 容易: 如果知道 $n, \phi(n)$, 那么可以通过求解如下关于 p, q 的方程组来分解 n:

$$\begin{cases} n = pq \\ \phi(n) = (p-1)(q-1) \end{cases}$$

用 $q = n/p$ 代入第二个方程, 可得关于未知数 p 的二次方程:

$$p^2 - (n - \phi(n) + 1)p + n = 0,$$

其两个根就是 n 的两个因子 p, q. 因此一个攻击者如果能求出 $\phi(n)$, 他就能分解 n, 故计算 $\phi(n)$ 并不比分解 n 容易.

Examp-5-4-1: 由 $\phi(n)$ 分解 n

假定 $n = 84773093$，且攻击者已经得到 $\phi(n) = 84754668$，那么他可以获得如下关于 p 的方程:

$$p^2 - 18426 \cdot p + 84773093 = 0,$$

求解此方程, 可以得到两个根 9539 和 8887, 他们就是 n 的两个素因子:

$$n = 84773093 = 9539 \times 8887.$$

计算低解密指数

M. Wiener 提出的一种攻击. 假定 RSA 的解密指数 a 和模数素因子 p, q 满足如下条件:

$$3a < n^{1/4} \quad \text{且} \quad q < p < 2q,$$

那么可以有效计算出 a.

其它类型攻击

1. 基于 LLL 算法的攻击: 将求解同余方程 $x^b \equiv y \pmod{n}$ 转化为求解一个格代数结构中的最短向量问题;
2. 未公开的攻击.

§ 5.5　Rabin 密码体制

二次剩余

假设 p 是奇素数, a 为一个整数, 那么:

1. a 为模 p 的二次剩余: 若 $a \not\equiv 0 \pmod{p}$, 且同余方程

$$y^2 \equiv a \pmod{p}$$

有解 $y \in \mathbb{Z}_p$;

2. a 为模 p 的二次非剩余: 若 $a \not\equiv 0 \pmod{p}$, 且 a 不是模 p 的二次剩余.

二次剩余

假设 p 是奇素数, a 为一个整数, 那么:

1. a 为模 p 的二次剩余: 若 $a \not\equiv 0 \pmod{p}$, 且同余方程

$$y^2 \equiv a \pmod{p}$$

有解 $y \in \mathbb{Z}_p$;

2. a 为模 p 的二次非剩余: 若 $a \not\equiv 0 \pmod{p}$, 且 a 不是模 p 的二次剩余.

Theorem (欧拉准则)

设 p 为一个奇素数, a 为一个正整数. 那么 a 是一个模 p 二次剩余, 当且仅当

$$a^{(p-1)/2} \equiv 1 \ (mod\ p).$$

Legendre (勒让德) 符号

设 p 是一个奇素数. 对任意整数 a, 定义 Legendre 符号 $\left(\frac{a}{p}\right)$ 如下:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & a \equiv 0 \pmod{p}; \\ 1, & a \text{ 是一个模 } p \text{ 二次剩余}; \\ -1, & a \text{ 是一个模 } p \text{ 二次非剩余}. \end{cases}$$

Legendre (勒让德) 符号

设 p 是一个奇素数. 对任意整数 a, 定义 Legendre 符号 $\left(\frac{a}{p}\right)$ 如下:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & a \equiv 0 \pmod{p}; \\ 1, & a \text{ 是一个模 } p \text{ 二次剩余}; \\ -1, & a \text{ 是一个模 } p \text{ 二次非剩余}. \end{cases}$$

Theorem

设 p 是一个奇素数,则

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Jacobi (雅可比) 符号

设 n 是一个奇正整数, 且 n 的素数幂因子分解为

$$n = \prod_{i=1}^{k} p_i^{e_i}.$$

设 a 为一个整数, 则 Jacobi 符号 $\left(\frac{a}{n}\right)$ 定义为:

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}.$$

Jacobi 符号的性质

1. 如果 n 是一个正奇数, 且 $m_1 \equiv m_2 \pmod{n}$, 那么

$$\left(\frac{m_1}{n}\right) = \left(\frac{m_2}{n}\right).$$

2. 如果 n 是一个正奇数, 那么

$$\left(\frac{2}{n}\right) = \begin{cases} 1, & n \equiv \pm 1 \pmod{8}; \\ -1, & n \equiv \pm 3 \pmod{8}. \end{cases}$$

3. 如果 n 是一个正奇数, 那么

$$\left(\frac{m_1 m_2}{n}\right) = \left(\frac{m_1}{n}\right)\left(\frac{m_2}{n}\right).$$

特别地, 如果 $m = 2^k t$ 且 t 为一个奇数, 那么

$$\left(\frac{m}{n}\right) = \left(\frac{2}{n}\right)^k \left(\frac{t}{n}\right).$$

4. (二次互反律) 如果 m 和 n 都是正奇数, 那么

$$\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right), & m \equiv n \equiv 3 \pmod{4}; \\ \left(\frac{n}{m}\right), & \text{其它}. \end{cases}$$

Examp-5-5-1: 计算 Jacobi 符号

例: 计算 Jacobi 符号 $\left(\frac{7411}{9283}\right)$.

Examp-5-5-1: 计算 Jacobi 符号

例: 计算 Jacobi 符号 $\left(\frac{7411}{9283}\right)$.

解:

$$\left(\frac{7411}{9283}\right) \overset{4}{=} -\left(\frac{9283}{7411}\right) \quad // \overset{i}{=} \text{表示由性质 } i\ (1 \le i \le 4) \text{ 得到}$$

Examp-5-5-1: 计算 Jacobi 符号

例: 计算 Jacobi 符号 $\left(\frac{7411}{9283}\right)$.

解:

$$\begin{aligned}\left(\frac{7411}{9283}\right) &\overset{4}{=} -\left(\frac{9283}{7411}\right) \qquad // \ \overset{i}{=} \text{表示由性质 } i\ (1 \le i \le 4) \text{ 得到} \\ &\overset{1}{=} -\left(\frac{1872}{7411}\right)\end{aligned}$$

Examp-5-5-1: 计算 Jacobi 符号

例: 计算 Jacobi 符号 $\left(\frac{7411}{9283}\right)$.

解:

$$\begin{aligned}
\left(\frac{7411}{9283}\right) &\overset{4}{=} -\left(\frac{9283}{7411}\right) \qquad // \ \overset{i}{=} \text{表示由性质 } i\ (1 \le i \le 4) \text{ 得到} \\
&\overset{1}{=} -\left(\frac{1872}{7411}\right) \\
&\overset{3}{=} -\left(\frac{2}{7411}\right)^4 \left(\frac{117}{7411}\right)
\end{aligned}$$

Examp-5-5-1: 计算 Jacobi 符号

例: 计算 Jacobi 符号 $\left(\frac{7411}{9283}\right)$.

解:

$$\begin{aligned}
\left(\frac{7411}{9283}\right) &\overset{4}{=} -\left(\frac{9283}{7411}\right) \qquad // \ \overset{i}{=} \text{表示由性质 } i\ (1 \le i \le 4) \text{ 得到} \\
&\overset{1}{=} -\left(\frac{1872}{7411}\right) \\
&\overset{3}{=} -\left(\frac{2}{7411}\right)^4 \left(\frac{117}{7411}\right) \\
&\overset{2}{=} -\left(\frac{117}{7411}\right)
\end{aligned}$$

Examp-5-5-1: 计算 Jacobi 符号

例: 计算 Jacobi 符号 $\left(\frac{7411}{9283}\right)$.

解:

$$
\begin{aligned}
\left(\frac{7411}{9283}\right) &\overset{4}{=} -\left(\frac{9283}{7411}\right) \qquad // \quad \overset{i}{=} \text{表示由性质 } i\ (1 \le i \le 4) \text{ 得到} \\
&\overset{1}{=} -\left(\frac{1872}{7411}\right) \\
&\overset{3}{=} -\left(\frac{2}{7411}\right)^4 \left(\frac{117}{7411}\right) \\
&\overset{2}{=} -\left(\frac{117}{7411}\right) \\
&\overset{4}{=} -\left(\frac{7411}{117}\right)
\end{aligned}
$$

Examp-5-5-1: 计算 Jacobi 符号

例: 计算 Jacobi 符号 $\left(\frac{7411}{9283}\right)$.

解:

$$
\begin{aligned}
\left(\frac{7411}{9283}\right) &\overset{4}{=} -\left(\frac{9283}{7411}\right) \qquad // \quad \overset{i}{=} \text{表示由性质 } i\ (1 \le i \le 4) \text{ 得到} \\
&\overset{1}{=} -\left(\frac{1872}{7411}\right) \\
&\overset{3}{=} -\left(\frac{2}{7411}\right)^4 \left(\frac{117}{7411}\right) \\
&\overset{2}{=} -\left(\frac{117}{7411}\right) \\
&\overset{4}{=} -\left(\frac{7411}{117}\right) \\
&\overset{1}{=} -\left(\frac{40}{117}\right)
\end{aligned}
$$

Examp-5-5-1: 计算 Jacobi 符号

例: 计算 Jacobi 符号 $\left(\frac{7411}{9283}\right)$.

解:

$$
\begin{aligned}
\left(\frac{7411}{9283}\right) &\overset{4}{=} -\left(\frac{9283}{7411}\right) && // \quad \overset{i}{=} \text{表示由性质 } i\ (1 \le i \le 4) \text{ 得到} \\
&\overset{1}{=} -\left(\frac{1872}{7411}\right) \\
&\overset{3}{=} -\left(\frac{2}{7411}\right)^4 \left(\frac{117}{7411}\right) \\
&\overset{2}{=} -\left(\frac{117}{7411}\right) \\
&\overset{4}{=} -\left(\frac{7411}{117}\right) \\
&\overset{1}{=} -\left(\frac{40}{117}\right) \\
&\overset{3}{=} -\left(\frac{2}{117}\right)^3 \left(\frac{5}{117}\right)
\end{aligned}
$$

Examp-5-5-1: 计算 Jacobi 符号

例: 计算 Jacobi 符号 $\left(\frac{7411}{9283}\right)$.

解:

$$
\begin{aligned}
\left(\frac{7411}{9283}\right) &\overset{4}{=} -\left(\frac{9283}{7411}\right) && // \ \overset{i}{=} \text{表示由性质 } i\ (1 \le i \le 4) \text{ 得到} \\
&\overset{1}{=} -\left(\frac{1872}{7411}\right) \\
&\overset{3}{=} -\left(\frac{2}{7411}\right)^4 \left(\frac{117}{7411}\right) \\
&\overset{2}{=} -\left(\frac{117}{7411}\right) \\
&\overset{4}{=} -\left(\frac{7411}{117}\right) \\
&\overset{1}{=} -\left(\frac{40}{117}\right) \\
&\overset{3}{=} -\left(\frac{2}{117}\right)^3 \left(\frac{5}{117}\right) \\
&\overset{2}{=} \left(\frac{5}{117}\right)
\end{aligned}
$$

Examp-5-5-1: 计算 Jacobi 符号

例: 计算 Jacobi 符号 $\left(\frac{7411}{9283}\right)$.

解:

$$
\begin{aligned}
\left(\frac{7411}{9283}\right) &\overset{4}{=} -\left(\frac{9283}{7411}\right) && // \ \overset{i}{=} \text{表示由性质 } i\ (1 \le i \le 4) \text{ 得到} \\
&\overset{1}{=} -\left(\frac{1872}{7411}\right) \\
&\overset{3}{=} -\left(\frac{2}{7411}\right)^4 \left(\frac{117}{7411}\right) \\
&\overset{2}{=} -\left(\frac{117}{7411}\right) \\
&\overset{4}{=} -\left(\frac{7411}{117}\right) \\
&\overset{1}{=} -\left(\frac{40}{117}\right) \\
&\overset{3}{=} -\left(\frac{2}{117}\right)^3 \left(\frac{5}{117}\right) \\
&\overset{2}{=} \left(\frac{5}{117}\right) \\
&\overset{4}{=} \left(\frac{117}{5}\right)
\end{aligned}
$$

Examp-5-5-1: 计算 Jacobi 符号

例: 计算 Jacobi 符号 $\left(\frac{7411}{9283}\right)$.

解:

$$
\begin{aligned}
\left(\frac{7411}{9283}\right) &\overset{4}{=} -\left(\frac{9283}{7411}\right) && // \ \overset{i}{=} \text{表示由性质 } i\ (1 \le i \le 4) \text{ 得到} \\
&\overset{1}{=} -\left(\frac{1872}{7411}\right) \\
&\overset{3}{=} -\left(\frac{2}{7411}\right)^4 \left(\frac{117}{7411}\right) \\
&\overset{2}{=} -\left(\frac{117}{7411}\right) \\
&\overset{4}{=} -\left(\frac{7411}{117}\right) \\
&\overset{1}{=} -\left(\frac{40}{117}\right) \\
&\overset{3}{=} -\left(\frac{2}{117}\right)^3 \left(\frac{5}{117}\right) \\
&\overset{2}{=} \left(\frac{5}{117}\right) \\
&\overset{4}{=} \left(\frac{117}{5}\right) \\
&\overset{1}{=} \left(\frac{2}{5}\right)
\end{aligned}
$$

Examp-5-5-1: 计算 Jacobi 符号

例: 计算 Jacobi 符号 $\left(\frac{7411}{9283}\right)$.

解:

$$
\begin{aligned}
\left(\frac{7411}{9283}\right) &\overset{4}{=} -\left(\frac{9283}{7411}\right) && // \ \overset{i}{=} \text{表示由性质 } i\ (1 \le i \le 4) \text{ 得到} \\
&\overset{1}{=} -\left(\frac{1872}{7411}\right) \\
&\overset{3}{=} -\left(\frac{2}{7411}\right)^4 \left(\frac{117}{7411}\right) \\
&\overset{2}{=} -\left(\frac{117}{7411}\right) \\
&\overset{4}{=} -\left(\frac{7411}{117}\right) \\
&\overset{1}{=} -\left(\frac{40}{117}\right) \\
&\overset{3}{=} -\left(\frac{2}{117}\right)^3 \left(\frac{5}{117}\right) \\
&\overset{2}{=} \left(\frac{5}{117}\right) \\
&\overset{4}{=} \left(\frac{117}{5}\right) \\
&\overset{1}{=} \left(\frac{2}{5}\right) \\
&\overset{2}{=} -1
\end{aligned}
$$

模 n 的平方根

接下去考虑同余方程

$$x^2 \equiv a \pmod{n}, \quad (a, n) = 1$$

根的个数:

模 n 的平方根

接下去考虑同余方程

$$x^2 \equiv a \pmod{n}, \quad (a, n) = 1$$

根的个数:

1. 当 n 为奇素数时, 方程或者有两个不同解 (此时 $\left(\frac{a}{n}\right) = 1$), 或者没有解 (此时 $\left(\frac{a}{n}\right) = -1$);

模 n 的平方根

接下去考虑同余方程

$$x^2 \equiv a \pmod{n}, \quad (a, n) = 1$$

根的个数:

1. 当 n 为奇素数时, 方程或者有两个不同解 (此时 $\left(\frac{a}{n}\right) = 1$), 或者没有解 (此时 $\left(\frac{a}{n}\right) = -1$);
2. 当 $n = p^e$ $(e > 0)$ 为奇素数幂时, 方程或者有两个不同解 (此时 $\left(\frac{a}{n}\right) = 1$), 或者没有解 (此时 $\left(\frac{a}{n}\right) = -1$);

模 n 的平方根

接下去考虑同余方程

$$x^2 \equiv a \pmod{n}, \quad (a, n) = 1$$

根的个数:

1. 当 n 为奇素数时, 方程或者有两个不同解 (此时 $\left(\frac{a}{n}\right) = 1$), 或者没有解 (此时 $\left(\frac{a}{n}\right) = -1$);
2. 当 $n = p^e$ $(e > 0)$ 为奇素数幂时, 方程或者有两个不同解 (此时 $\left(\frac{a}{n}\right) = 1$), 或者没有解 (此时 $\left(\frac{a}{n}\right) = -1$);
3. 假设 $n = \prod_{i=1}^{l} p_i^{e_i}$, 这里 p_i 为不同奇素数, $e_i > 0$, 则方程当 $\left(\frac{a}{p_i}\right) = 1$, $\forall\, i \in \{1, 2, \cdots, l\}$ 成立时有 2^l 个解, 其它情形没有解.

Rabin 密码体制

设 $n = pq$, 其中 p, q 为素数, 且 $p, q \equiv 3 \pmod 4$. 设 $\mathcal{P} = C = \mathbb{Z}_n^*$, 且定义

$$\mathcal{K} = \{n, p, q\}.$$

对 $K = (n, p, q) \in \mathcal{K}$, 定义

$$E_K(x) = x^2 \bmod n$$

和

$$D_K(y) = \sqrt{y} \bmod n.$$

n 为公钥, (p, q) 为私钥.

解密函数的说明

1. Rabin 密码体制的加密函数不是一个单射, 所以解密不能以一种明显的方式完成.
2. 由前面讨论知道, 对任何一个合法密文 y, 同余方程组

$$x^2 \equiv y \pmod{n}$$

有四个解 x_1, x_2, x_3, x_4. 一般情形下, 解密者不能判断哪一个是“正确”的, 除非明文中包含足够的冗余信息来排除其中的三个.

3. 问题: 如何来确定上述的四个解?

Rabin 密码体制中密文 y 模 n 四个平方根的求法

解法主要基于如下事实:

$x_1 \equiv x_2 \pmod{pq}$ 当且仅当 $x_1 \equiv x_2 \pmod{p}$ 且 $x_1 \equiv x_2 \pmod{q}$.

Rabin 密码体制中密文 y 模 n 四个平方根的求法

解法主要基于如下事实:

$x_1 \equiv x_2 \pmod{pq}$ 当且仅当 $x_1 \equiv x_2 \pmod{p}$ 且 $x_1 \equiv x_2 \pmod{q}$.

1. 首先, 求解同余方程 $u^2 \equiv y \pmod{p}$, 得到两个不同解

$$u_{1,2} = \pm y^{(p+1)/4} \bmod p;$$

2. 其次, 求解同余方程 $v^2 \equiv y \pmod{q}$, 得到两个不同解

$$v_{1,2} = \pm y^{(q+1)/4} \bmod q;$$

3. 对每一组 (u_i, v_j) $(1 \le i, j \le 2)$, 由中国剩余定理解同余方程组

$$\begin{cases} x_{i,j} \equiv u_i \pmod{p} \\ x_{i,j} \equiv v_j \pmod{q}, \end{cases}$$

可得四个解 $x_{1,1}$, $x_{1,2}$, $x_{2,1}$, $x_{2,2}$.

Examp-5-5-2: 课堂练习

假设 Rabin 密码体制的模数 $n = 77 = 7 \times 11$, 解密密文 $y = 23$.

Examp-5-5-2: 课堂练习

假设 Rabin 密码体制的模数 $n = 77 = 7 \times 11$, 解密密文 $y = 23$.

1. 首先, 求解同余方程 $u^2 \equiv 23 \pmod 7$, 得到两个不同解
$$u_1 = 23^{(7+1)/4} \bmod 7 = 4, \ u_2 = -4 \bmod 7 = 3;$$
2. 其次, 求解同余方程 $v^2 \equiv 23 \pmod{11}$, 得到两个不同解
$$v_1 = \pm 23^{(11+1)/4} \bmod 11 = 1, \ v_2 = -1 \bmod 11 = 10;$$
3. 对 $(u_1, v_1) = (4, 1)$ 和 $(u_1, v_2) = (4, 10)$, 解同余方程组
$$\begin{array}{rcl} x_1 & \equiv & 4 \pmod 7 \\ x_1 & \equiv & 1 \pmod{11} \end{array} \quad \text{和} \quad \begin{array}{rcl} x_2 & \equiv & 4 \pmod 7 \\ x_2 & \equiv & 10 \pmod{11} \end{array}$$

可得两个解 $x_1 = 67$, $x_2 = 32$, 从而另外两个解为

$$x_3 = -x_1 \bmod n = 10, \quad x_4 = -x_2 \bmod n = 45.$$

Examp-5-5-2: 课堂练习

假设 Rabin 密码体制的模数 $n = 77 = 7 \times 11$, 解密密文 $y = 23$.

1. 首先, 求解同余方程 $u^2 \equiv 23 \pmod 7$, 得到两个不同解
$$u_1 = 23^{(7+1)/4} \bmod 7 = 4, \ u_2 = -4 \bmod 7 = 3;$$
2. 其次, 求解同余方程 $v^2 \equiv 23 \pmod{11}$, 得到两个不同解
$$v_1 = \pm 23^{(11+1)/4} \bmod 11 = 1, \ v_2 = -1 \bmod 11 = 10;$$
3. 对 $(u_1, v_1) = (4, 1)$ 和 $(u_1, v_2) = (4, 10)$, 解同余方程组
$$\begin{array}{rcl} x_1 & \equiv & 4 \pmod 7 \\ x_1 & \equiv & 1 \pmod{11} \end{array} \quad \text{和} \quad \begin{array}{rcl} x_2 & \equiv & 4 \pmod 7 \\ x_2 & \equiv & 10 \pmod{11} \end{array}$$
可得两个解 $x_1 = 67$, $x_2 = 32$, 从而另外两个解为
$$x_3 = -x_1 \bmod n = 10, \quad x_4 = -x_2 \bmod n = 45.$$

可以验证, $67, 32, 10, 45$ 平方后模 77 得到的值都是 23.

Rabin 密码体制的安全性

1. Rabin 密码体制在选择明文攻击下是可证计算安全的. 具体地, 如果一个攻击者能攻破 Rabin 密码体制的话, 他至少可以以 1/2 的概率分解模数 n.
2. 另一方面, Rabin 密码体制在选择密文攻击下是完全不安全的: 攻击者可以首先随机选择一个 r, 然后生成 $y = r^2 \bmod n$, 并将 y 提交给解密谕示器从而得到 x, 最后攻击者可以通过计算 $(x + r, n)$ 得到 n 的因子, 从而分解模数 n.

§ 5.6　RSA 的语义安全性

攻击者的目标

1. 完全攻破: 攻击者能够找出 Bob 的秘密密钥 (对称密码体制下的情形) 或者私钥 (公钥密码体制下的情形)。因此他能解密利用给定密钥加密的任意密文。
2. 部分攻破: 攻击者能以某一不可忽略的概率解密以前没有见过的密文 (无需知道密钥). 或者，攻击者能够对于给定的密文，得出明文的一些特定信息。
3. 密文识别: 攻击者能够以超过 1/2 的概率解决以下问题:

密文识别问题

实例: 一个加密函数 $f : X \to X$, 两个明文 $x_1, x_2 \in X$ 和一个密文 $y = f(x_i)$, 其中 $i \in \{1, 2\}$

问题: 是否 $i = 1$?

RSA 的部分攻破

假定攻击者获得密文 $y = x^b \bmod n$, 由于 $(b, \phi(n)) = 1$, 所以必然 b 为奇数. 因此 Jabobi 符号

$$\left(\frac{y}{n}\right) = \left(\frac{x}{n}\right)^b = \left(\frac{x}{n}\right).$$

上式表明, 给定密文 y, 任何人无需解密就可以有效计算 $\left(\frac{x}{n}\right)$. 也就是说, 一个 RSA 加密“泄漏”了一些明文信息, 即 Jacobi 符号 $\left(\frac{x}{n}\right)$ 的值.

RSA 的密文识别

显然, RSA 的加密函数是确定性的, 所以攻击者可以很容易解决密文识别问题: 只要计算 $f(x_1)$ 和 $f(x_2)$, 然后看哪一个等于 y, 就可以回答 i 是 1 还是 2.

语义安全定义

Definition

一个公钥密码体制称为语义安全的, 如果攻击者不能 (在多项式时间内) 进行密文识别.

语义安全定义

Definition

一个公钥密码体制称为语义安全的, 如果攻击者不能 (在多项式时间内) 进行密文识别.

1. 根据上面的定义和分析知, RSA 密码体制不是语义安全的;
2. 一个密码体制要满足语义安全性, 其加密函数必须是随机 (或者称为概率) 的.
3. 我们真正想要的是: 如何通过一个确定性的密码体制来构造一个语义安全的密码体制?

语义安全的公钥密码体制

假设函数 $f : X \to X$ 是一个陷门单向置换, 其逆置换记为 f^{-1}. f 是公钥密码体制的加密函数，f^{-1} 是解密函数。

语义安全的公钥密码体制

设 m, k 为正整数, $f : \{0,1\}^k \to \{0,1\}^k$ 为一陷门单向置换，$G : \{0,1\}^k \to \{0,1\}^m$ 为一个随机谕示器 (可理解为一个安全 Hash 函数). 令 $\mathcal{P} = \{0,1\}^m, C = \{0,1\}^k \times \{0,1\}^m$. 对密钥 $K = (f, f^{-1}, G)$, 随机选取 $r \in \{0,1\}^k$, 且定义

$$E_K(x) = (y_1, y_2) = (f(r), G(r) \oplus x),$$

其中 $y_1 \in \{0,1\}^k$, $x, y_2 \in \{0,1\}^m$. 进一步定义

$$D_K(y_1, y_2) = G(f^{-1}(y_1)) \oplus y_2.$$

函数 (f, g) 为公钥, 函数 f^{-1} 为私钥.

上述构造特点

1. 上述构造的密码体制是语义安全的: 可以把求函数 f 的逆函数 f^{-1} 问题规约到密文识别问题 (即如果密文识别问题可解, 则逆函数 f^{-1} 可求, 而这是假设不可能的).
2. 相对于底层的基于 f 的公钥密码体制而言, 上述构造只添加了很少的运算.
3. 上述构造主要缺点是数据扩展比较严重: m 比特明文被加密成 $k + m$ 比特密文. 如果上述 f 是 RSA 的加密函数, 为了使体制安全, $k \geq 1024$.

OAEP

我们可以由确定性公钥密码体制构造一个更有效的语义安全密码体制, 该密码体制称为最优非对称加密填充 (OAEP: Optimal Asymmetric Encryption Padding).

OAEP

设 m, k 为正整数且 $m < k$, $k_0 = k - m$. 令 $f : \{0,1\}^k \to \{0,1\}^k$ 为一单向陷门置换, $G : \{0,1\}^{k_0} \to \{0,1\}^m$, $H : \{0,1\}^m \to \{0,1\}^{k_0}$ 为两个随机函数. 定义 $\mathcal{P} = \{0,1\}^m$, $C = \{0,1\}^k$.

对任意密钥 $K = (f, f^{-1}, G, H)$, 设 $r \in \{0,1\}^{k_0}$ 为随机选择, 定义

$$E_K(x) = f(y_1 \| y_2),$$

其中 $y_1 = x \oplus G(r)$, $y_2 = r \oplus H(x \oplus G(r))$, $x, y_1 \in \{0,1\}^m$, $y_2 \in \{0,1\}^{k_0}$.

进一步定义

$$f^{-1}(y) = x_1 \| x_2, \quad r = x_2 \oplus H(x_1)$$

其中 $x_1 \in \{0,1\}^m$, $x_2 \in \{0,1\}^{k_0}$, 那么定义解密函数为

$$D_K(y) = G(r) \oplus x_1.$$

函数 (f, G, H) 为公钥, 函数 f^{-1} 为私钥.

OAEP 的特点

1. OAEP 也是可证明语义安全的公钥密码体制;
2. 密文长度 (k) 比明文长度 (m) 长出 $k_0 = k - m$ 比特. 如果上述 f 是 RSA 的加密函数, 为了使体制安全, $k_0 = 128$ 就够了. 这相比前一个构造的数据扩展少多了.

作业 8

1. (书上习题 5.33) 考虑 Rabin 密码体制的修改

$$E_K(x) = x(x + B) \bmod n,$$

其中 $B \in \mathbb{Z}_n$ 是公钥的一部分. 假定

$$p = 199, q = 211, n = pq, B = 1357,$$

试完成如下计算:

   1. 计算加密 $y = E_K(32767)$;
   2. 求出这个给定密文 y 的四个可能解密.