# RSA密码体制

# 素性检测

素数个数定理：设 $\pi(N)$ 为小于 $N$ 的素数个数，则

$$\pi(N) \approx N / \ln N$$

一个随机的512比特的整数是素数的概率为：

$$= \frac{\pi(2^{512}) - \pi(2^{511})}{2^{512} - 2^{511}} \approx \frac{\frac{2^{512}}{\ln 2^{512}} - \frac{2^{511}}{\ln 2^{511}}}{2^{511}} \approx$$

$$\frac{2}{\ln 2^{512}} - \frac{1}{\ln 2^{511}} \approx \frac{1}{\ln 2^{512}} \approx \frac{1}{335}$$

# 非确定性算法

- 概率算法（使用随机数或伪随机数）
  - 蒙特卡洛算法
    - 解不一定正确，但是一定可以得到解
  - 拉斯维加斯算法
    - 解一定正确，但不一定总能得到解

  - 偏是的蒙特卡洛算法
    - 当回答“是”时，总是正确的
    - 当回答“否”时，不一定正确

# 素性检测

- 合数（Composite）
  - 前提：对于一个不小于2的正整数a，
  - 问题：a是一个合数吗？

  - 对于偏“是”的蒙特卡洛算法，
    - 如何算法输出a是合数，那么a一定是合数
    - 如果算法输出a是素数，那么a可能是合数

- 构造一个安全参数多项式时间的算法，使得算法出错的概率可忽略。

# 素性检测

- 对奇素数p和整数a，a是模p的二次剩余，如果 $a \neq 0 \bmod p$ 且同余方程 $y^2 = a \bmod p$ 有一个解 $y \in Z_p$ 。

- 对奇素数p和整数a，a是模p的二次非剩余，如果 $a \neq 0 \bmod p$ 且a不是模p的二次剩余。

# 素性检测

- 在 $Z_{11}$ 中，1,3,4,5,9都是模11的二次剩余，2,6,7,8,10都是模11的二次非剩余。

$$1^2 = 1 \bmod 11 \qquad 5^2 = 3 \bmod 11$$
$$10^2 = 1 \bmod 11 \qquad 6^2 = 3 \bmod 11$$

$$2^2 = 4 \bmod 11 \qquad 4^2 = 5 \bmod 11 \qquad 3^2 = 9 \bmod 11$$
$$9^2 = 4 \bmod 11 \qquad 7^2 = 5 \bmod 11 \qquad 8^2 = 9 \bmod 11$$

# 素性检测

- 对奇素数p，若a是模p的二次剩余，那么存在 $y \in Z_p^*$，使得 $y^2 = a \bmod p$。
- 显然，$(-y)^2 = a \bmod p$
- 因为p是奇素数，所以 $-y \neq y \bmod p$
- 否则 $p = (2y) \bmod p$
- 对方程 $x^2 - a = 0 \bmod p$，可将方程因式分解为 $(x-y)(x+y) = 0 \bmod p$ 这等价于 $p \mid (x-y)(x+y)$
- 由于p是素数，故 $p \mid (x-y)$ 或 $p \mid (x+y)$
- 即 $x = \pm y \bmod p$ 为方程 $x^2 - a = 0 \bmod p$ 的解。

# 素性检测

**定理 5.9 (Euler 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

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

**证明** 首先，假定 $a \equiv y^2 \pmod{p}$。从推论 5.6 可知，如果 $p$ 是素数，那么 $a^{p-1} \equiv 1 \pmod{p}$ 对于任一 $a \not\equiv 0 \pmod{p}$ 成立。于是我们有

$$\begin{aligned} a^{(p-1)/2} &\equiv (y^2)^{(p-1)/2} \pmod{p} \\ &\equiv y^{p-1} \pmod{p} \\ &\equiv 1 \pmod{p} \end{aligned}$$

反过来，假定 $a^{p-1} \equiv 1 \pmod{p}$。设 $b$ 为一个模 $p$ 的本原元素。那么 $a \equiv b^i \pmod{p}$ 对于某个正整数 $i$，我们有

$$\begin{aligned} a^{(p-1)/2} &\equiv (b^i)^{(p-1)/2} \pmod{p} \\ &\equiv b^{i(p-1)/2} \pmod{p} \end{aligned}$$

由于 $b$ 的阶为 $p-1$，因此必有 $p-1$ 整除 $i(p-1)/2$。因此，$i$ 是偶数，于是 $a$ 的平方根为 $\pm b^{i/2} \bmod p$。

# Miller-Rabin算法

**算法 5.7** Miller-Rabin ( $n$ )

把 $n-1$ 写成 $n-1=2^k m$，其中 $m$ 是一个奇数

选取随机整数 $a$，使得 $1 \leqslant a \leqslant n-1$

$b \leftarrow a^m \pmod{n}$

**if** $b \equiv 1 \pmod{n}$

**then return** ("$n$ is prime")

**for** $i \leftarrow 0$ **to** $k-1$

**do** $\begin{cases} \textbf{if } b \equiv -1 \pmod{n} \\ \quad \textbf{then return } (\text{“}n \text{ is prime”}) \\ \quad \textbf{else } b \leftarrow b^2 \pmod{n} \end{cases}$

**return** ("$n$ is composite")

$O((\log n)^3)$

# 素性检测

**定理 5.11** Miller-Rabin 算法对于合数问题是一个偏是的 Monte Carlo 算法。

**证明** 我们用反证法。先假定算法 5.7 对于某个素数 $n$ 回答了"$n$ 为合数"，然后推出矛盾。由于算法回答"$n$ 为合数"，必有 $a^m \not\equiv 1 \pmod{n}$。现在考虑在算法中检测的 $b$ 的序列。由于 $b$ 在 for 循环的每一步中都做平方运算，我们测试的值为 $a^m, a^{2m}, \cdots, a^{2^{k-1}m}$。由于算法回答"$n$ 为合数"，我们可知对于 $0 \leqslant i \leqslant k-1$，有：

$$a^{2^i m} \not\equiv -1 \pmod{n}$$

现在，利用 $n$ 为素数的假定，由于 $n-1=2^k m$，由 Fermat 定理(参见推论 5.6)知：

$$a^{2^k m} \equiv 1 \pmod{n}$$

那么 $a^{2^{k-1}m}$ 是模 $n$ 的 1 的平方根。由于 $n$ 为素数，仅有两个模 $n$ 的 1 的平方根，即 $\pm 1 \bmod n$。我们有：

$$a^{2^{k-1}m} \not\equiv -1 \pmod{n}$$

# 素性检测

**定理 5.11** Miller-Rabin 算法对于合数问题是一个偏是的 Monte Carlo 算法。

由此得出

$$a^{2^{k-1}m} \equiv 1 \pmod{n}$$

那么 $a^{2^{k-2}m}$一定是模 $n$ 的 1 的平方根。基于相同的理由，

$$a^{2^{k-2}m} \equiv 1 \pmod{n}$$

重复上述过程，我们最后得到：

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

但是在这种情形下，算法会回答"$n$ 为素数"，推出矛盾。

# RSA算法

- 1. RSA算法是CCA安全的加密算法吗？
- 2. RSA算法是CPA安全的加密算法吗？
- 3. RSA算法是EAV安全的加密算法吗？

- $r$, RSA$(x,r) \oplus k$ ?

# 对RSA的攻击

如果一个密码分析者能够求出 $\phi(n)$ 的值，他就能分解$n$ ，进而攻破系统，也就是说计算 $\phi(n)$ 并不比分解 $n$ 容易

例：假定 $n = 84773093$ ，$\phi(n) = 84754668$，求 $n$ 的因子

# 对RSA的攻击

计算 $\phi(n)$

可以看到，计算 $\phi(n)$ 并不比因式分解 $n$ 容易

因为如果 $\phi(n)$ 以及 $n$ 已知，那么就可以容易地分解 $n$

# 对RSA的攻击

## 选择密文攻击

已知$c = m^e \bmod n$

查询$\frown{c}$的明文$\frown{c}^d \bmod n$

查询$\frac{c}{\frown{c}}$的明文$(\frac{c}{\frown{c}})^d$

$$m = (\frown{c})^d (\frac{c}{\frown{c}})^d = c^d \bmod n$$

# 对RSA的攻击

低加密指数攻击(e很小)

$$c_1 = m^3 \bmod n_1 \qquad c_2 = m^3 \bmod n_2$$

$$c = m^3 \bmod n_1 n_2$$

$$m^3 \le n_1 n_2$$

# 对RSA的攻击

## 公共模数攻击

$$c_1 = m^{e_1} \bmod n \qquad c_2 = m^{e_2} \bmod n \qquad \gcd(e_1, e_2) = 1$$

$$\gcd(e_1, e_2) = 1 \Rightarrow re_1 + se_2 = 1$$

$$(c_1^{-1})^{-r}(c_2)^s = m \bmod n$$

# 中国剩余定理

- 将军点兵,三三数余2,五五数余3,七七数余5问兵几何?

$$X \bmod 3 = 2$$
$$X \bmod 5 = 3$$
$$X \bmod 7 = 5$$

# 中国剩余定理

- 将军点兵, 三三数余2, 五五数余3, 七七数余5, 问兵几何?

$$X \bmod 3 = 2 \qquad 35 \quad 35*\left(35^{-1} \bmod 3\right) \quad \left(35*(-1)\right)*2$$

$$X \bmod 5 = 3 \qquad 21 \quad 21*\left(21^{-1} \bmod 5\right) \quad \left(21*1\right)*3$$

$$X \bmod 7 = 5 \qquad 15 \quad 15*\left(15^{-1} \bmod 7\right) \quad \left(15*1\right)*5$$

$$\left(35*(-1)\right)*2+\left(21*1\right)*3+\left(15*1\right)*5 \bmod 3*5*7$$

$$=68$$

# Rabin密码体制

## 中国剩余定理

中国剩余定理是求解某类特定同余方程组的一个好方法。

假定 $m_1, \ldots, m_r$ 为两两互素的正整数，即

$$i \neq j, \gcd(m_i, m_j) = 1$$

假定 $a_1, \ldots, a_r$ 是整数，考虑如下的同余方程组

$$x \equiv a_1 \pmod{m_1} \qquad x \equiv a_{r-1} \pmod{m_{r-1}}$$
$$x \equiv a_2 \pmod{m_2} \qquad x \equiv a_r \pmod{m_r}$$

# Rabin密码体制

中国剩余定理断言上页方程组有模 $M = m_1 \times m_2 \times ... \times m_r$ 的唯一解。

这里将给出证明，并给出求解这种类型的同余方程组的有效算法。

为方便起见，我们研究函数 $\chi : Z_M \to Z_{m1} \times ... \times Z_{mr}$ 按如下定义：$\chi(x) = \left(x \bmod m_1, ..., x \bmod m_r\right)$

# Rabin密码体制

例5.2 假定 $m_1=5, m_2=3$ 那么 $M = 15$ 函数 $\chi$ 取值如下：

| | | |
|---|---|---|
| $\chi(0) = (0,0)$ | $\chi(1) = (1,1)$ | $\chi(2) = (2,2)$ |
| $\chi(3) = (3,0)$ | $\chi(4) = (4,1)$ | $\chi(5) = (0,2)$ |
| $\chi(6) = (1,0)$ | $\chi(7) = (2,1)$ | $\chi(8) = (3,2)$ |
| $\chi(9) = (4,0)$ | $\chi(10) = (0,1)$ | $\chi(11) = (1,2)$ |
| $\chi(12) = (2,0)$ | $\chi(13) = (3,1)$ | $\chi(14) = (4,2)$ |

# Rabin密码体制

证明中国剩余定理就等于证明函数 $\chi$ 是一个双射。在例5.2中容易看到是一个双射。事实上，我们可以给出逆函数 $\chi^{-1}$ 的显式公式。

对于 $1 \le i \le r$ ，定义 $M_i = \frac{M}{m_i}$ 那么，容易看到

$$\gcd(M_i, m_i) = 1$$

下一步，对于 $1 \le i \le r$ ，定义 $y_i = M_i^{-1} \bmod m_i$

(逆存在是因为 $\gcd(M_i, m_i) = 1$ ）

注意到 $M_i y_i \equiv 1 \pmod{m_i}$ $1 \le i \le r$

# Rabin密码体制

现在，定义一个函数 $\rho : Z_{m1} \times \ldots \times Z_{mr} \rightarrow Z_M$

$$\rho(a_1, \ldots, a_r) = \sum_{i=1}^{r} a_i M_i y_i \bmod M$$

现在证明函数 $\rho = \chi^{-1}$，即它提供了一个求解原来的同余方程组的显式公式。

记 $X = \rho(a_1, \ldots, a_r)$，令$1 \leq j \leq r$，考虑上面和式中的项 $a_i M_i y_i$模 $m_j$ 的约化：

# Rabin密码体制

如果 $i = j$，由于 $M_i y_i \equiv 1 \pmod{m_i}$

所以 $a_i M_i y_i \equiv a_i \pmod{m_i}$

如果 $i \neq j$，由于 $m_j \mid M_j$

所以 $a_i M_i y_i \equiv 0 \pmod{m_i}$

$$X \equiv \sum_{i=1}^{r} a_i M_i y_i \pmod{m_j} \equiv a_j \pmod{m_j}$$

由于上式对所有的 $j$，$1 \leq j \leq r$ 都成立

所以 $X$ 是同余方程组的一个解

# Rabin密码体制

函数 $\chi$ 是从基数为M的定义域到基数为M的值域的映射，现在已经证明 $\chi$ 是一个满射。因此，$\chi$ 必须是单射，由于定义域和值域有相同的基数，所以 $\chi$ 是一个双射，且 $\chi^{-1} = \rho$

定理5.3（中国剩余定理）

假定 $m_1, \ldots, m_r$ 为两两互素的正整数，又假定 $a_1, \ldots, a_r$ 为整数，那么同余方程组 $x \equiv a_i \pmod{m_i} (1 \leq i \leq r)$

有模 $M = m_1 \times m_2 \times \ldots \times m_r$ 的唯一解，

# Rabin密码体制

定理5.3（中国剩余定理）

此解由下式给出：

$$X \equiv \sum_{i=1}^{r} a_i M_i y_i \bmod M$$

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

# Rabin密码体制

设 $n = pq$，其中 $p$ 和 $q$ 为素数，且 $p, q \equiv 3 \pmod 4$

设 $P = C = Z_n^*$，且定义 $K = \{(n, p, q)\}$，对 $k = (n, p, q)$

定义 $e_k(x) = x^2 \bmod n$，和 $d_k(y) = \sqrt{y} \bmod n$

$n$ 为公钥，$p$ 和 $q$ 为私钥

注：条件 $p, q \equiv 3 \pmod 4$ 可以省去，且如果 $P = C = Z_n$ 密码体制仍能工作。这里我们增加这两条的原因主要是简化许多方面的计算和密码体制的分析。

# Rabin密码体制

Rabin密码体制的一个缺点是加密函数 $e_K$ 并不是一个单射，所以解密不能以一种明显的方式完成，其证明如下：

假定 $y$ 是一个有效的密文，这意味着 $y = x^2 \bmod n$，对某一 $x \in Z_n^*$，定理证明了存在 $y$ 模 $n$ 的四个解，是对应于密文 $y$ 的四个可能的解。

显然，除非明文中包含足够的冗余信息，否则解密方不能区分这四个可能的明文中哪一个是正确的。

# Rabin密码体制

解密方得到一个密文 $y$，且想找出$x$，使得 $x^2 \equiv y \pmod{n}$

这是一个关于$Z_n$中未知元$x$ 的二次方程，解密需要求出模 $n$ 的平方根。这等价于求解两个同余方程 $x^2 \equiv y \pmod{p}$ 且 $x^2 \equiv y \pmod{q}$，可以利用Euler准则来判断 $y$ 是否为一个模 $p$ (或模$q$ )的二次剩余。但是Euler准则无法帮助我们找到 $y$ 的平方根。

# Rabin密码体制

当$p \equiv 3 \pmod 4$ 时，有如下公式：

$$\left(\pm\, y^{(p+1)/4}\right)^2$$

$$\equiv y^{(p+1)/2} \pmod p$$

$$\equiv y^{(p-1)/2} y \pmod p$$ 根据Euler准则 $y^{(p-1)/2} \equiv 1 \pmod p$

$$\equiv y \pmod p$$

因此，$y$ 模$p$的两个平方根为$\pm\, y^{(p+1)/4} \pmod p$

同理，$y$ 模 $q$的两个平方根为$\pm\, y^{(q+1)/4} \pmod q$

# Rabin密码体制

最后，利用中国剩余定理可以得到 $y$ 模 $n$ 的四个平方根。

例：假定 $n = 77 = 7 \times 11$，那么函数为

$e_k(x) \equiv x^2 \pmod{77}$，且解密函数为 $d_k(x) \equiv \sqrt{x} \pmod{77}$

求密文 $y = 23$ 对应的明文。(注意7和11都模4余3)

# Rabin密码体制

最后，利用中国剩余定理可以得到 $y$ 模 $n$ 的四个平方根。

例：假定 $n = 77 = 7 \times 11$，那么函数为

$e_k(x) \equiv x^2 \pmod{77}$，且解密函数为 $d_k(x) \equiv \sqrt{x} \pmod{77}$

求密文 $y = 23$ 对应的明文。(注意7和11都模4余3)

$$p = 7, q = 11$$

$$23^{(7+1)/4} \equiv 2^2 \equiv 4 \pmod{7}$$

$$23^{(11+1)/4} \equiv 1^3 \equiv 1 \pmod{13}$$

# Rabin密码体制

- 1. Rabin是否正确？
- 2. Rabin能否在多项式时间加密和解密？
- 3. Rabin是否安全（CCA,CPA）？