密码学导论

Introduction to Cryptography

密码导学团队

北京理工大学网络空间安全学院

17 octobre 2023

第六章（下） RSA和Rabin密码体制

素数有多少个?

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：

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

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

素数有多少个?

n-比特素数分布

对任意$n > 1$，n-比特整数为素数的概率至少为$\frac{1}{3n}$。

随机产生$t = 3n^2$个n-比特整数，不能得到一个素数的概率为

$$(1 - \frac{1}{3n})^t = ((1 - \frac{1}{3n})^{3n})^n \leq (e^{-1})^n = e^{-n},$$

是关于n的可忽略函数。所以运行n的多项式次能以很高概率得到一个素数。那么怎样判断一个整数是不是素数?

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
  算法不一定正确，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
  - 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，
    - 如果算法输出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。

二次剩余

二次剩余

- 对奇素数p和整数a，a是模p的二次剩余，如果$a \neq 0 \mod p$且同余方程$y^2 = a \mod p$有一个解$y \in \mathbb{Z}_p^*$。
- 对奇素数p和整数a，a是模p的二次非剩余，如果$a \neq 0 \mod p$且a不是模p的二次剩余。

- 在$\mathbb{Z}_{11}^*$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。

$$
\begin{aligned}
1^2 &= 1 \mod 11 \qquad & 10^2 &= 1 \mod 11 \\
2^2 &= 4 \mod 11 \qquad & 9^2 &= 4 \mod 11 \\
3^2 &= 9 \mod 11 \qquad & 8^2 &= 9 \mod 11 \\
4^2 &= 5 \mod 11 \qquad & 7^2 &= 5 \mod 11 \\
5^2 &= 3 \mod 11 \qquad & 6^2 &= 3 \mod 11
\end{aligned}
$$

二次剩余

同余方程$x^2 - a \equiv 0(\text{mod} p)$模$p$意义下恰好有两个解，且这两个解模$p$互为相反数。

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

二次剩余

定理(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

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

二次剩余

定理(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

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

证明 首先，假定$a \equiv y^2 \pmod p$。从推论1(Lagrange定理的推论)可知，如果p是素数，那么$a^{p-1} \equiv 1 \pmod p$对与任一$a \not\equiv 0 \pmod p$成立。于是我们有

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

二次剩余

定理(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

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

证明 首先，假定$a \equiv y^2 \pmod p$。从推论1(Lagrange定理的推论)可知，如果p是素数，那么$a^{p-1} \equiv 1 \pmod p$对与任一$a \not\equiv 0 \pmod p$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$a^{(p-1)/2} \equiv 1 \pmod p$。设$b$为$\mathbb{Z}_p^*$的生成元。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$\pm b^{i/2} \mod p$。

Miller-Rabin算法

算法6.3 Miller-Rabin(n) 判断n是合数还是素数：
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$1\le a\le n-1$

$b \leftarrow a^m \bmod n$
if $b \equiv 1 \bmod n$ **then**
  return ("n is prime")
endif
for $i \leftarrow 0$ **to** $k-1$ **do**
  if $b \equiv -1 \bmod n$ **then**
    return ("n is prime")
  else
    $b \leftarrow b^2 \bmod n$
  endif
endfor
return ("n is composite")（此时a是n为合数的一个"见证"。）

素性检测

定理

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

素性检测

定理

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。假设算法6.3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$a^m \not\equiv 1 (\bmod n)$。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$0 \leq i \leq k-1$，有：

$$a^{2^i m} \not\equiv -1 (\bmod n)$$

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

$$a^{2^k m} \equiv 1 (\bmod n)$$

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$\pm 1 \mod n$。我们有：

$$a^{2^{k-1}m} \not\equiv -1 (\bmod n),$$

素性检测

定理

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。

素性检测

Miller-Rabin算法正确性分析

- 如果n是素数，则Miller-Rabin算法总是将其判定为素数。
- 如果n是合数，执行t次Miller-Rabin算法（注意每次随机选取整数a），只要有一次输出为“合数"则判定其为合数。则t次执行判定其为合数的概率$\geq 1-2^{-t}$。

证明思路：

假设n是合数：

随机选择的a不是一个“见证"的概率$\leq \frac{1}{2}$

证明至少存在一个"见证"

证明“非见证"构成一个子群

子群的阶整除群的阶，所以“非见证"比例$\leq \frac{1}{2}$。

t次选择的a都是“非见证"的概率$\leq \frac{1}{2^t}$。

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?

在公钥密钥学中EAV和CPA攻击的强度是相同的，因为加密密钥是公开的。
RSA算法需要引入随机数，才能实现CCA安全。

实际中，采用Optimal Asymmetric Encryption Padding (OAEP) 填充的RSA能够抵抗CCA攻击。
OAEP 由 Mihir Bellare 和 Phillip Rogaway提出，随后在 PKCS1 v2 和 RFC 2437中被标准化。

Optimal Asymmetric Encryption Padding, OAEP

- 1994年, Bellare 和 Rogaway 提出：由单向陷门置换构造公钥加密体制的通用方法.
- RSA-OAEP是基于RSA的OAEP，已被嵌入安全电子交易系统（Secure Electronic Transaction System，SET），并成为新的RSA 加密标准PKCS#1 v2.0。
- 2001年, Shoup 的贡献：
  - 如果存在异或扩张的置换生成器, 则存在单向陷门置换生成器, 使得基于该置换生成器的 OAEP不是IND-CCA2安全的.
    (异或扩张：存在有效算法 U 能够 $(f_0, f_0(t), \Delta) \Rightarrow f_0(t \oplus \Delta)$, 这里 f_0 为置换生成器生成的任意置换.)
  - 给出了OAEP的改进版本：OAEP+
- 2001年，Fujisaki等：在ROM下，若置换是局部单向的，则OAEP是ind-cca2的。
  (推论：RSA-OAEP是ind-cca2安全的，因为RSA的局部单向性等价于其单向性。)

OAEP vs. OAEP+

设 f 是单向陷门置换, H, G, H' 均为哈希函数(ROM模型).
公钥：f, 私钥：$g \triangleq f^{-1}$

OAEP：

$$
\begin{aligned}
s &= G(r) \oplus (x||0^{k_1}) \\
t &= H(s) \oplus r \\
w &= s||t \\
y &= f(w)
\end{aligned}
$$

OAEP+：

$$
\begin{aligned}
s &= (G(r) \oplus x)||H'(r||x) \\
t &= H(s) \oplus r \\
w &= s||t \\
y &= f(w)
\end{aligned}
$$

其中，x, y, r分别表示明文、密文和加密中引入的随机数。

课堂思考：如何解密？如何验证密文完整性？

实际中RSA_OAEP标准详见https ://www.rfc-editor.org/rfc/pdfrfc/rfc8017.txt.pdf

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

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。

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

已知挑战密文$c = m^e \mod n$

查询$\hat{c}$的明文$\hat{c}^d \mod n$

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

$$m = (\hat{c})^d(\frac{c}{\hat{c}})^d = c^d \mod n$$

对RSA的攻击

选择密文攻击

已知挑战密文$c = m^e \mod n$

查询$\hat{c}$的明文$\hat{c}^d \mod n$

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

$m = (\hat{c})^d (\frac{c}{\hat{c}})^d = c^d \mod n$

低加密指数攻击

$c_1 = m^3 \mod n_1$

$c_2 = m^3 \mod n_2$

$c_3 = m^3 \mod n_3$

$c = m^3 \mod n_1 n_2 n_3$

$m^3 \leq n_1 n_2 n_3$

对RSA的攻击

选择密文攻击

已知挑战密文$c = m^e \mod n$

查询$\hat{c}$的明文$\hat{c}^d \mod n$

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

$m = (\hat{c})^d (\frac{c}{\hat{c}})^d = c^d \mod n$

低加密指数攻击

$c_1 = m^3 \mod n_1$

$c_2 = m^3 \mod n_2$

$c_3 = m^3 \mod n_3$

$c = m^3 \mod n_1 n_2 n_3$

$m^3 \leq n_1 n_2 n_3$

公共模数攻击

$c_1 = m^{e_1} \mod n$
$c_2 = m^{e_2} \mod n$

$$\begin{cases} \mathsf{gcd}(e_1, e_2) = 1 \\ \mathsf{gcd}(c_1, n) = 1 \end{cases}$$

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

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

中国剩余定理

中国南北朝时期（公元5世纪）的数学著作《孙子算经》卷下第二十六题，叫做“物不知数”问题，原文如下：

- 有物不知其数，三三数之剩二，五五数之剩三，七七数之剩五。问物几何?

$$\begin{cases} X & \equiv 2 \mod 3 \\ X & \equiv 3 \mod 5 \\ X & \equiv 5 \mod 7 \end{cases}$$

中国剩余定理

中国南北朝时期（公元5世纪）的数学著作《孙子算经》卷下第二十六题，叫做“物不知数”问题，原文如下：

- 有物不知其数，三三数之剩二，五五数之剩三，七七数之剩五。问物几何？

$$\begin{cases} X & \equiv 2 \mod 3 \\ X & \equiv 3 \mod 5 \\ X & \equiv 5 \mod 7 \end{cases}$$

$$\begin{aligned} X &\equiv 2 \times 70 + 3 \times 21 + 5 \times 15 \mod 105 \\ &\equiv 68 \mod 105 \end{aligned}$$

最初对“物不知数”问题作出完整系统解答的是宋朝数学家秦九韶，载于1247年《数书九章》，从而使这一问题变为定理。明朝数学家程大位在《算法统宗》中将解法编成易于上口的《孙子歌诀》：

三人同行七十稀，
五树梅花廿一枝，
七子团圆月正半，
除百零五便得知。

《数书九章》在19世纪初被译为英文，而西方世界最早的完整系统解法由高斯在1801年提出。

中国剩余定理

中国南北朝时期（公元5世纪）的数学著作《孙子算经》卷下第二十六题，叫做“物不知数”问题，原文如下：

- 有物不知其数，三三数之剩二，五五数之剩三，七七数之剩五。问物几何?

$$\begin{cases} X & \equiv 2 \mod 3 \\ X & \equiv 3 \mod 5 \\ X & \equiv 5 \mod 7 \end{cases}$$

$$\begin{aligned} X &\equiv 2 \times 70 + 3 \times 21 + 5 \times 15 \mod 105 \\ &\equiv 68 \mod 105 \end{aligned}$$

- 70，21，15，105这几个数怎么来的?

最初对“物不知数”问题作出完整系统解答的是宋朝数学家秦九韶，载于1247年《数书九章》，从而使这一问题变为定理。明朝数学家程大位在《算法统宗》中将解法编成易于上口的《孙子歌诀》：

三人同行七十稀，
五树梅花廿一枝，
七子团圆月正半，
除百零五便得知。

《数书九章》在19世纪初被译为英文，而西方世界最早的完整系统解法由高斯在1801年提出。

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$m_1, \cdots, m_r$为两两互素的正整数，即

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

假定$a_1, \cdots, a_r$是整数，考虑如下的同余方程组

$$\begin{cases} X & \equiv a_1 (\bmod\ m_1) \\ X & \equiv a_2 (\bmod\ m_2) \\ & \vdots \\ X & \equiv a_{r-1} (\bmod\ m_{r-1}) \\ X & \equiv a_r (\bmod\ m_r) \end{cases}$$

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$m_1, \cdots, m_r$为两两互素的正整数，即

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

假定$a_1, \cdots, a_r$是整数，考虑如下的同余方程组

$$\begin{cases} X & \equiv a_1 (\bmod\ m_1) \\ X & \equiv a_2 (\bmod\ m_2) \\ & \vdots \\ X & \equiv a_{r-1} (\bmod\ m_{r-1}) \\ X & \equiv a_r (\bmod\ m_r) \end{cases}$$

中国剩余定理断言该方程组有模$M = m_1 \times m_2 \times \cdots \times m_r$的唯一解，即在$\mathbb{Z}_M$中有且仅有一个元素满足该方程组。

这里将给出证明，并给出找到这个唯一元素的有效算法。

为了方便起见，我们研究函数χ按如下定义：

$$\chi: \mathbb{Z}_M \to \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$$
$$\chi(x) = (x \bmod\ m_1, \cdots, x \bmod\ m_r)$$

证明中国剩余定理就等于证明函数χ是一个双射。

中国剩余定理

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

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

中国剩余定理

证明中国剩余定理就等于证明函数χ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χ^{-1}的显示公式。

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$y_i = M_i^{-1} \mod m_i$, (逆存在是因为$\gcd(M_i, m_i) = 1$)

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

中国剩余定理

现在，定义一个函数ρ：$\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r} \to \mathbb{Z}_M$

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

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示公式。

记$X = \rho(a_1, \cdots, a_r)$，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：

- 如果$i = j$，由于$M_j y_j \equiv 1 \pmod{m_j}$，所以$a_j M_j y_j \equiv a_j \pmod{m_j}$.

中国剩余定理

现在，定义一个函数ρ：$\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r} \to \mathbb{Z}_M$

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

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示公式。

记$X = \rho(a_1, \cdots, a_r)$，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：

- 如果$i = j$，由于$M_j y_j \equiv 1 (\bmod m_j)$，所以$a_j M_j y_j \equiv a_j (\bmod m_j)$.
- 如果$i \neq j$，由于$m_j | M_i$，所以$a_i M_i y_i \equiv 0 (\bmod m_j)$。

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

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。

函数χ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χ是一个满射。因此，χ必须是单射，由于定义域和值域有相同的基数，所以χ是一个双射，且$\chi^{-1} = \rho$。

中国剩余定理

定理（中国剩余定理）

假定$m_1,\cdots,m_r$为两两互素的正整数，又假定$a_1,\cdots,a_r$为整数，那么同余方程组$X\equiv a_i(\bmod\ m_i)$，$(1\le i\le r)$有模$M=m_1\times m_2\times\cdots\times m_r$的唯一解：

$$X\equiv\sum_{i=1}^{r}a_iM_iy_i \mod M$$

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

$$\begin{cases} X & \equiv 2 \mod 3\\ X & \equiv 3 \mod 5\\ X & \equiv 5 \mod 7\end{cases}$$

$$35\times(35^{-1} \mod 3)=35\times 2=70$$
$$21\times(21^{-1} \mod 5)=21\times 1=21$$
$$15\times(15^{-1} \mod 7)=15\times 1=15$$
$$X\equiv(70\times 2+21\times 3+15\times 5) \mod 3\times 5\times 7\equiv 68 \mod 105$$

Garner公式

这是中国剩余定理的用途之一：用一组较小的素数作为混合基底表示一个很大的整数。

原理：给定一组素数$p_1, p_2, \cdots, p_k$，若整数$a < \prod_{i=1}^{k} p_i$ 满足 $a \equiv a_i \pmod{p_i}, i = 1, \cdots, k$，则有

$$a = x_1 + x_2 p_1 + x_3 p_1 p_2 + \cdots + x_k p_1 p_2 \cdots p_{k-1}$$

其中，$x_1, \cdots, x_k$ 按如下方式确定：

1. 令 $r_{i,j} = p_i^{-1} \bmod p_j, (i < j, j = 2, \cdots, k)$
2. $a \bmod p_1 \rightarrow x_1 \equiv a_1 \pmod{p_1}$
3. $a \bmod p_2 \rightarrow x_1 + x_2 p_1 \equiv a_2 \pmod{p_2} \rightarrow x_2 \equiv (a_2 - x_1) r_{1,2} \pmod{p_2}$
4. ...
5. $a \bmod p_k \rightarrow x_1 + x_2 p_1 + x_3 p_1 p_2 + \cdots + x_k p_1 p_2 \cdots p_{k-1} \equiv a_k \pmod{p_k}$
   $\rightarrow x_k \equiv (\cdots((a_k - x_1) r_{1,k} - x_2) r_{2,k} - \cdots) r_{k-1,k} \pmod{p_k}$

CRT-RSA

利用中国剩余定理可以加速RSA的解密运算。实际中，加密密钥e往往选择比特'1'的个数尽量少的数，如$3, 17, 65537(=2^{16}+1)$，导致解密密钥d的长度与n的长度k相当，且大约一半比特为'1'，解密复杂度约为$\mathcal{O}(k^3)$，因此需要更高效地进行解密运算。

原理：利用中国剩余定理（Garner公式）更高效地计算$m = c^d \mod n$。

1. 首先计算
$$m_p = c^d \bmod p = c^{d \bmod p-1} \bmod p \quad \text{and} \quad m_q = c^d \bmod q = c^{d \bmod q-1} \bmod q$$
2. 再计算 $T = p^{-1} \bmod q$
3. 然后令：
$$h = (m_q - m_p) \cdot T \bmod q \quad \text{and} \quad m = m_p + h \cdot p$$

* 套用Garner公式（$k=2$），令$p_1 = p, p_2 = q, x_1 = a_1 = m_p, a_2 = m_q, r_{1,2} = T, x_2 = h$ 即得。

Rabin密码体制

Rabin密码体制

设$n = pq$，其中p和q为素数，且$p, q \equiv 3 \pmod 4$。设$\mathcal{P} = \mathcal{C} = \mathbb{Z}_n^*$，且定义$\mathcal{K} = \{(n, p, q)\}$。
对$k = (n, p, q)$，定义

- 加密：$e_k(x) = x^2 \mod n$，
- 解密：$d_k(y) = \sqrt{y} \mod n$，

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$\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$，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。

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$\mathbb{Z}_n$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：

$$\begin{aligned} &(\pm y^{(p+1)/4})^2 \\ \equiv & y^{(p+1)/2} \pmod{p} \\ \equiv & y^{(p-1)/2} y \pmod{p} \text{ 根据Euler准则 } y^{(p-1)/2} \equiv 1 \pmod{p} \\ \equiv & y \pmod{p} \end{aligned}$$

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$\pm y^{(q+1)/4} \pmod{q}$

最后，利用中国剩余定理可以得到y模n的四个平方根。

Rabin密码体制

例：假定$n = 77 = 7 \times 11$，那么加密函数为$y = e_k(x) \equiv x^2 \pmod{77}$，且解密函数为$d_k(y) \equiv \sqrt{y} \pmod{77}$。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

例：假定$n = 77 = 7 \times 11$，那么加密函数为$y = e_k(x) \equiv x^2 \pmod{77}$，且解密函数为$d_k(y) \equiv \sqrt{y} \pmod{77}$。求密文$y = 23$对应的明文。(注意7和11都模4余3)

$$y^{(p+1)/4} \bmod p = 23^{(7+1)/4} \bmod 7 = 23^2 \bmod 7 = 4$$
$$y^{(q+1)/4} \bmod q = 23^{(11+1)/4} \bmod 11 = 23^3 \bmod 11 = 1$$

	M_i	$y_i = M_i^{-1} \bmod n_i$	$M_i y_i$
$x \equiv \pm 4 \bmod 7$	11	$11^{-1} \bmod 7 = 2$	22
$x \equiv \pm 1 \bmod 11$	7	$7^{-1} \bmod 11 = 8$	56

a_1	a_2	$(a_1 \times 22 + a_2 \times 56) \bmod 77$
4	1	67
4	-1	32
-4	1	45
-4	-1	10

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：

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$y = x^2 \mod n$，对某一$x \in \mathbb{Z}_n^*$，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

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)?

小结

- RSA和Rabin加密算法
  - 公钥加密算法
  - 大整数因式分解难则Rabin算法安全
  - 大整数因式容易，RSA一定容易，反之未知
- CCA？
  - OAEP 和 OAEP+

- 为什么非对称加密算法比对称加密算法慢大概1000倍？
- 如何设计CPA安全而高效的加密算法呢？加密者与解密者没有预共享密钥
- 如何证明公钥是某个实体的？

本章作业

1. 在RSA公钥加密方案中，某用户选取了$p = 13, q = 17, n = pq = 221$，加密密钥$e_1 = 17$，

(1) 计算解密密钥d_1。

(2) 已知明文为$m = 16$，计算密文c。

(3) 已知密文为$c = 111$，计算明文m。

(4) （选择密文攻击）攻击者获得了挑战密文$c = 97$后，向解密应答器询问密文$\hat{c} = 3$，得到对应的明文为$\hat{m} = 139$。请再向解密应答器询问另一密文得到其对应明文，利用两次询问的明密文（和公钥）恢复挑战密文对应的明文。

(5) （共模攻击）有另一用户使用了相同的模数n，选取的加密和解密密钥分别为$e_2 = 25, d_2 = 169$。攻击者截获了同一明文m分别发送给两用户时的密文$c_1 = 192$和$c_2 = 199$。利用c_1, c_2（和公钥）求明文m。

2. （中国剩余定理）某用户将消息m广播给了三个用户，三个用户的加密密钥$e_1 = e_2 = e_3 = 3$，模数分别为$n_1 = 51, n_2 = 65, n_3 = 77$，攻击者截获了三个密文$c_1 = m^3 \mod 51 = 24, c_2 = m^3 \mod 65 = 27, c_3 = m^3 \mod 77 = 20$。在仅利用公钥的情况下求$m$。

Thank you for your attention !

Questions ?