第一章 大素数生成与流密码

1.1 大素数生成

- 非对称加密方案都需要用到一定长度（安全参数）大素数
- 如何有效地获得指定长度的大素数?

1.1.1 强拟素数

- 定义1.1.1 设$n > 1$为奇合数， $b \in Z, (b, n) = 1$，令$n = 2^s t + 1$，其中t为奇数，若$b^t \equiv 1 \ (mod\ n)$或存在$r \in Z, 0 \le r < s$，使得$b^{2^r t} \equiv -1 \ (mod\ n)$，则$n$称为对于基$b$的强拟素数。

1.1.1 强拟素数

- 定义1.1.1 设$n > 1$为奇合数， $b \in Z, (b, n) = 1$，令$n = 2^s t + 1$，其中t为奇数，若$b^t \equiv 1\ (mod\ n)$或存在$r \in Z, 0 \leq r < s$，使得$b^{2^r t} \equiv -1\ (mod\ n)$，则$n$称为对于基$b$的强拟素数。

- 设n为正奇数，$b \in Z, b > 1, s \in Z^+$，且$2^s|(n-1)$，令$t = \frac{n-1}{2^s} \in Z^+$，则$b^{n-1} - 1 = (b^{2^0 t} - 1)(b^{2^0 t} + 1)(b^{2^1 t} + 1) \cdots (b^{2^{s-1} t} + 1)$，因此若$n$为素数，则$b^{n-1} \equiv 1\ (mod\ n)$且$Z_n$无零因子，所以

$$b^{2^0 t} \equiv 1, b^{2^0 t} \equiv -1, b^{2^1 t} \equiv -1, \dots, b^{2^{s-1} t} \equiv -1$$

中必有一个成立。

1.1.1 强拟素数

- 定义1.1.1 设$n > 1$为奇合数， $b \in Z, (b, n) = 1$，令$n = 2^s t + 1$，其中t为奇数，若$b^t \equiv 1\ (mod\ n)$或存在$r \in Z, 0 \le r < s$，使得$b^{2^r t} \equiv -1\ (mod\ n)$，则$n$称为对于基$b$的强拟素数。

- 设n为正奇数，$b \in Z, b > 1, s \in Z^+$，且$2^s|(n-1)$，令$t = \frac{n-1}{2^s} \in Z^+$，则$b^{n-1} - 1 = (b^{2^0 t} - 1)(b^{2^0 t} + 1)(b^{2^1 t} + 1) \cdots (b^{2^{s-1} t} + 1)$，因此若$n$为素数，则$b^{n-1} \equiv 1\ (mod\ n)$且$Z_n$无零因子，所以
$$b^{2^0 t} \equiv 1, b^{2^0 t} \equiv -1, b^{2^1 t} \equiv -1, \dots, b^{2^{s-1} t} \equiv -1$$
中必有一个成立。

- 例$2047 = 23 \cdot 89$是对于基2的强拟素数。
事实上，$2047 - 1 = 2 \cdot 1023$，而
$2^{1023} = (2^{11})^{93} \equiv 1^{93} = 1\ (mod\ 2047)$，因此2047是对于基2的强拟素数。

1.1.1 强拟素数

- 定理1.1.1 存在无穷多个对于基2的强拟素数。

- 定理1.1.2 设n是奇合数，$b \in Z, 1 \leq b < n$，那么n是对于基b的强拟素数的概率不超过$\frac{1}{4}$。

1.1.2 Miller-Rabin素性检验

- 算法1.1.1（Miller-Rabin素性检验）给定正奇数n 和参数$t \in Z^+$，令$n = 2^s k + 1$，其中k为正奇数，

(i) 若已选过t个b，则判断n是素数，算法终止；

(ii) 随机选取整数$b, 2 \leq b \leq n-2$，令$i = 0$，计算$r_i = b^k \pmod n$，如果$r_i = 1$或$n-1$，则返回至(i)；

(iii) 若$i < s-1$，令$i = i+1$，计算$r_i = r_{i-1}^2 \pmod n$，如果$r_i = n-1$，则返回至(i)；

(iv) 判断n是合数，算法终止。

1.2 Miller-Rabin素性检验

- 算法1.2.1（Miller-Rabin素性检验）给定正奇数n 和参数$t \in Z^+$，令$n = 2^s k + 1$，其中k为正奇数，

(i) 若已选过t个b，则判断n是素数，算法终止；

(ii) 随机选取整数$b, 2 \leq b \leq n-2$，令$i = 0$，计算$r_i = b^k \ (mod\ n)$，如果$r_i = 1$或$n-1$，则返回至(i)；

(iii) 若$i < s-1$，令$i = i+1$，计算$r_i = r_{i-1}^2\ (mod\ n)$，如果$r_i = n-1$，则返回至$(i)$；

(iv) 判断n是合数，算法终止。

显然n是合数的可能性不超过$\frac{1}{4^t}$，即误判n是素数的概率不超过$\frac{1}{4^t}$。

问题：使用Miller-Rabin素性检验随机生成一个120比特的素数。