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$r \in Z, 0 \leq r < s$，使得$b^{2^r t} \equiv -1 \ (mod\ n)$，则$n$称为对于基$b$的强拟素数。

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

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

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

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

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$b, 2 \le b \le n-2$，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。

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$b, 2 \le b \le n-2$，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。

1.2 流密码

1.2.1 流密码的定义

- 将明文看作字符串或比特串，并逐字符或逐位进行加密。
- 为了防止密钥穷举，使用和明文信息一样长的密钥（无限）流$z=z_1z_2\ldots$进行加密。

$$y = y_1 y_2 \ldots = e_{z_1}(x_1)e_{z_2}(x_2)\ldots$$

- 这种密码体制称为流密码（或序列密码）

（1）可以使用非常简单的加密算法（如简单的异或运算）

（2）关键是如何生成密钥流

1.2.2 流密码的代表

- 弗纳姆（Vernam）密码

（1）1918年，Gillbert Vernam建议密钥与明文一样长并且没有统计关系的密钥内容，他采用的是二进制数据：

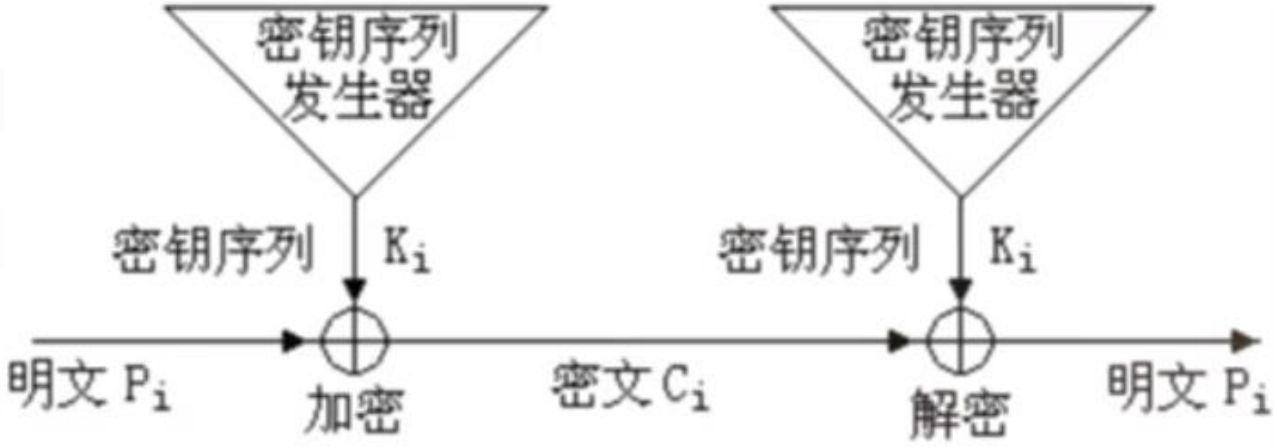
加密：$C_i = P_i \oplus K_i$

解密：$P_i = C_i \oplus K_i$

（2）关键：构造和消息一样长的随机密钥

1.2.3 流密码的特点

- 运算简单
- 实时性强
- 一次一密
- 安全性依赖于密钥流的产生



1.2.4 流密码的分类

- 按密钥的周期性分类

（1）周期流密码：存在某个固定的正整数r,使得密钥流每隔r个字符（或者比特）以后重复。

（2）非周期性密码：对任何正整数密钥流都不重复；如一次一密乱码本。

- 按密钥的产生方式分类

（1）同步流密码：密钥流的产生独立于消息流；如分组密码的OFB（输出反馈）模式。

（2）非周期性密码：每一个密钥字符是由前面n个明文或密文字符推导出来的，其中n为定值；例如分组密码的CFB（密码反馈）模式。

1.2.5 同步流密码

- 使用某种算法，由一个初始密钥变幻出和明文串相互独立的密钥流，定义如下：同步流密码是一个六元组（P, C, K, L, E, D）和一个函数g，且满足如下条件：

（1）P, C, K分别是明文、密文、密钥的有限集。

（2）L是密钥流字母表有限集。

（3）g是密钥流生成器，g使用密钥k∈K作为输入，产生无限长的密钥流$z=z_1z_2...$，其中zi∈L。

（4）对任意的z∈L，都有一个加密规则（函数）$e_z: P \longrightarrow C \in E$和相应的解密规则（函数）$d_z: C \longrightarrow P \in D$，并且对每个明文x∈P满足 $d_z(e_z(x)) = x$ 。

1.2.5 同步流密码

密钥流的产生

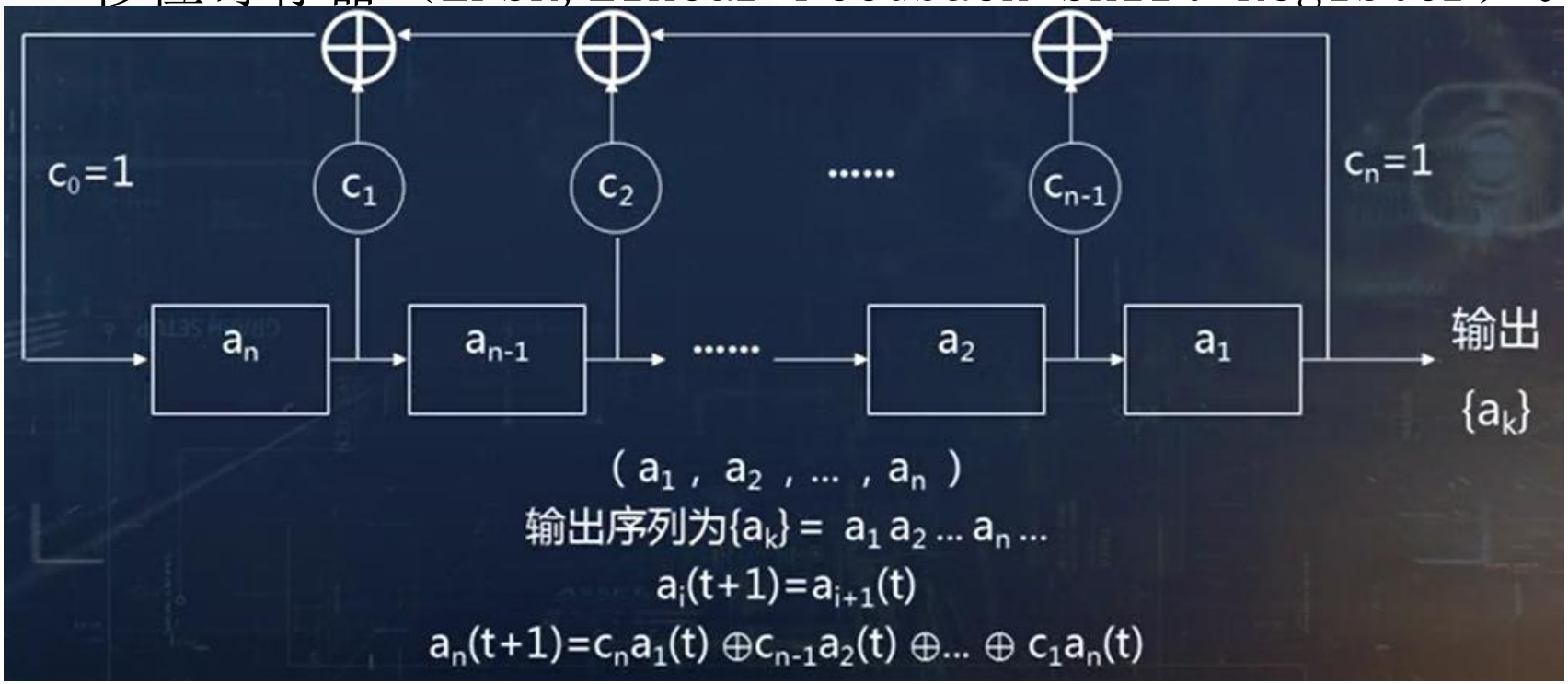
- 可用线性递推关系产生伪随机序列。
- 例如设m=4, (a_1, a_2, a_3, a_4)为(0, 0, 0, 1)密钥流按如下线性递推关系产生：$a_{i+4}=(a_i+a_{i+3}) \bmod 2$

产生的密钥序列为$a_1a_2a_3a_4\ldots$，即000111101011001 00011110...，周期为$2^4-1=15$，(a_1, a_2, a_3, a_4)通常被称为初始向量。

1.2.5 同步流密码

密钥流的产生

- 这种方式可以使用硬件有效实现，此硬件称为线性反馈移位寄存器（LFSR,Linear Feedback Shift Register）。



1.2.5 同步流密码

LFSR示例说明

- c_n=1的n级LFSR其输出序列为周期序列，且周期数r满足r≤2^n-1。
- 若n级LFSR其输出序列的周期达到最大2^n-1，则称之为m序列。
- $f(x)=c_0+c_1x+c_2x^2+...+c_nx^n$描述LFSR的反馈连接状态，称为特征多项式。
- 可以证明，一个n级LFSR能产生m序列的充要条件是它的特征多项式为一个n次本原多项式。

1.2.5 同步流密码

本原多项式

- 若一个n次多项式f(x)的阶为2^n-1，即满足条件：
  （1）f(x)为既约多项式
  （2）f(x)可整除（$x^{2^n-1}+1$）
  （3　f(x)不可整除（x^p+1），其中$p<2^n-1$

- 例：n=4时,周期为$2^4-1=15$，其特征多项式是能整除（$x^{15}+1$）的4次本原多项式。

$$x^{15}+1=(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$$

由于$(x^4+x^3+x^2+x+1)\mid x^5+1$，所以本原多项式为，$x^4+x+1$和$x^4+x^3+1$，选择$f(x)=x^4+x+1$,即$c_4=c_1=c_0=1$

1.2.5 同步流密码

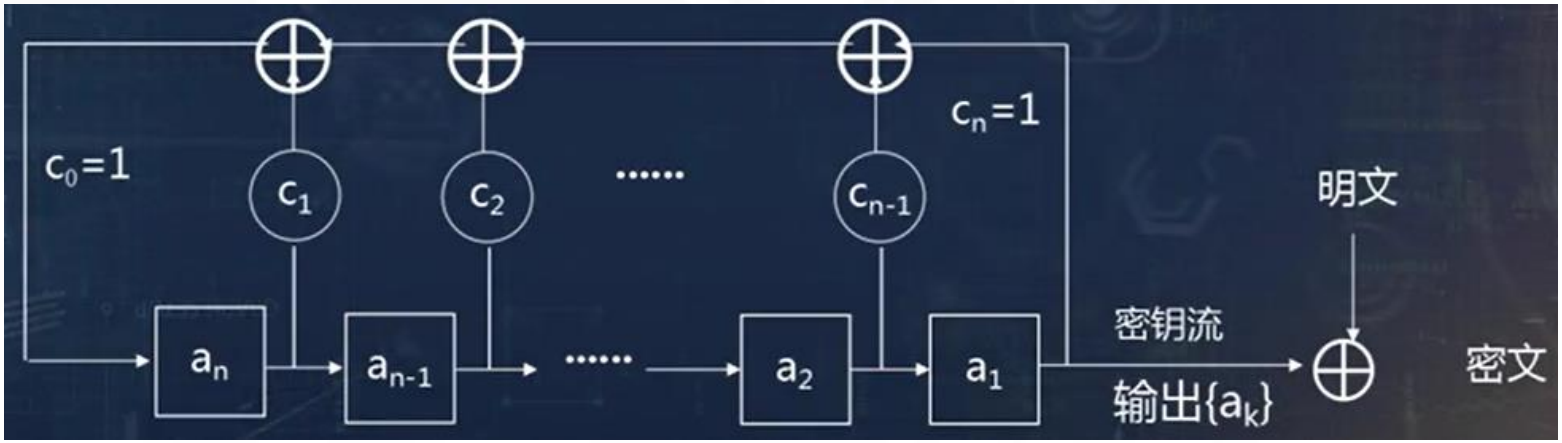
本原多项式

n	2^n-1	λ(n)	n	2^n-1	λ(n)
1	1	1	11	2047	176
2	3	1	12	4095	144
3	7	2	13	8191	630
4	15	2	14	16383	756
5	31	6	15	32767	1800
6	63	6	16	65535	2048
7	127	18	17	131071	7710
8	255	16	18	262143	7776
9	511	48	19	524287	27594
10	1023	60	20	1048575	24000

n级的LFSR可以产生$\lambda(n)*2^n-1$种密钥流

1.2.5 同步流密码

利用LFSR设计加密算法的同步序列密码实现



1.2.6 异步流密码

- 同步流密码存在周期问题。
- 异步流密码思路：密钥流z的产生不但与密钥k有关，还与明文元素或密文元素有关。
- 自动密钥密码：通过K和明文产生密钥流。

1.2.6 异步流密码

自动密钥密码

- 例：自动密钥密码是一个六元组（P,C,K,L,E,D），且满足如下条件：

（1）$P=C=K=L=Z_{26}$

（2）密钥流定义：$z_1=k\in K$，$z_i=x_{i-1}$ $i\geq 2$

（3）对任意的$z\in K$，$x,y\in Z_{26}$，定义

$$e_z(x)=(x+z)\bmod 26$$

$$d_z(y)=(y-z)\bmod 26$$

1.2.6 异步流密码

自动密钥密码

- 假设k=8, 明文为rendezvous
- 加密过程如下：

首先将明文转换为整数序列：　17 4　13 3 4 25 21 14 20 18

根据$z_1=k=8, z_i=x_{i-1}$得到密钥流为：8 17　4 13 3 4 25 21 14 20

将对应的元素相加并模26得到：　25 21 17 16 7 3 20 9 8 12

字母形式的密文为：ZVRQHDUJIM

问题：实现同步流序列密码的加解密系统，其中特征多项式 $f(x)=x^4+x+1$。