《现代密码学》第五讲

流密码（一）

《现代密码学》第五讲

RC4 算法简介

本章主要内容

- 流密码（序列密码）的思想起源
- 流密码技术的发展及分类
- 基于移位寄存器的流密码算法
- 其它流密码算法

RC4 算法

- RC4 是由 Rivest 于 1987 年开发的一种序列密码，它已被广泛应用于 Windows 、 Lotus Notes 和其它软件，还被用于安全套接字（ SSL ）和无线通信系统等。 RC4 算法最初没有被公布，但其源代码在 1994 年被人匿名发布，在这种情况下 RSA 数据公司于 1997 年公开了 RC4 算法 .
- RC4 不是基于 LFSR 的序列密码，它使用了一个 256 字节大小的非线性数据表（简称 S 表），依据表进行非线性变换，得到密钥流 . S 表的值 S_0 ， S_1 ，…， S_{255} 是数字 0 到 255 的一个排列， RC4 有两个计数器 I 和 J ，初值都为 0.
- RC4 的优点是算法简单、高效，特别适于软件实现，加密速度比 DES 大约快 10 倍 . RC4 可以支持不同密钥长度，美国政府特别限定，用于出口的 RC4 的密钥长度不得超过 40 位 .

RC4 算法

- RC4 首先进行 S 表的初始化，过程如下：
- 对 S 表进行填充： $S_i = i$ ， $0 \leqslant i < 255$ ；
- 用密钥填充另一个 256 字节的数组 K，如果密钥长度小于 256 字节，则依次重复填充，直至填满这个数组： K_0 ， K_1 ，…， K_{255} ；
- $J=0$ ；
- 对于 $I=0$ 到 255 重复以下步骤：
  - $J=J+ S_I+K_I$ （mod 256）；
  - 交换 S_I 和 S_J 。
- RC4 按下列步骤输出密钥流的一个字节 z ：
- $I=0$ ， $J=0$ ；
- $I = I + 1$ （mod 256）；
- $J = S_I + S_J$ （mod 256）；
- 交换 S_I 和 S_J ；
- $t=S_I+S_J$ （mod 256）；
- $z=S_t$ 。

RC4 算法

假如使用 3 位（从 0 到 7）的 RC4，其操作是对 8 取模（而不是对 256 取模）。数据表 S 只有 8 个元素，初始化为：

S	0	1	2	3	4	5	6	7
	0	1	2	3	4	5	6	7

选取一个密钥，该密钥是由 0 到 7 的数以任意顺序组成的。例如选取 5、6 和 7 作为密钥。该密钥如下填入密钥数据表中：

K	5	6	7	5	6	7	5	6
	0	1	2	3	4	5	6	7

RC4 算法

密钥调度算法 KSA

然后利用如下循环构建实际的 S 数据表：

```
j:=0;
for  i=0  to  7  do
     j:=(j+s(i)+k(i))  mod  8;
     swap(S(i),S(j));
```

该循环以 j=0 和 i=0 开始。使用更新公式后 j 为：

j=(0+S(0)+K(0)) mod 8=5

S 数据表的第一个操作是将 S(0) 与 S(5) 互换。

5	1	2	3	4	0	6	7
0	1	2	3	4	5	6	7

RC4 算法

索引 i 加 1 后， j 的下一个值为：

$$j=(5+S(1)+K(1)) \bmod 8=(5+1+6) \bmod 8=4$$

即将 S 数据表的 S(1) 和 S(4) 互换：

5	4	2	3	1	0	6	7
0	1	2	3	4	5	6	7

当该循环执行完后，数据表 S 就被随机化为：

5	4	0	7	1	6	3	2
0	1	2	3	4	5	6	7

RC4 算法

伪随机数生成算法 PRGA

这样数据表 S 就可以用来生成随机的密钥流序列。

从 j=0 和 i=0 开始， RC4 如下计算第一个密钥字：

i=(i+1) mod 8=(0+1) mod 8 =1

j=(j+s(i)) mod 8=(0+s(1)) mod 8=(0+4) mod 8=4

5	1	0	7	4	6	3	2
0	1	2	3	4	5	6	7

RC4 算法

然后如下计算 t 和 k:

5	1	0	7	4	6	3	2
0	1	2	3	4	5	6	7

t=(S(j)+S(i)) mod 8=(S(4)+S(1)) mod 8=(1+4) mod 8=5

k=S(t)=S(5)=6

第一个密钥字为 6，其二进制表示为 110 。反复进行

该过程，直到生成的二进制的数量等于明文位的数量。

本章主要内容

- 流密码（序列密码）的思想起源
- 流密码技术的发展及分类
- 基于移位寄存器的流密码算法
- RC4 算法

THE END !