# RC4算法

RC4算法是一种在电子信息领域加密的技术手段，用于无线通信领域。和DES算法一样，它是一种对称加密算法，也就是说使用的密钥为私钥。

不同于DES的是，RC4不是对明文进行分组处理，而是以字节流的形式加密每一个字节，解密的时候也是依次对密文中的每一个字节执行解密。

## 关键变量

密钥流

RC4算法的关键是根据明文和密钥生成相应的密钥流，密钥流的长度和明文的长度是对应的，也就是说明文的长度是500字节，那么密钥流也是500字节。当然，加密生成的密文也是500字节，因为密文第i字节=明文第i字节^密钥流第i字节；

状态向量S

长度为256，S[0],S[1].....S[255]。每个单元都是一个字节，算法运行的任何时候，S都包括0-255的8比特数的排列组合，只不过值的位置发生了变换；

临时向量T

长度也为256，每个单元也是一个字节。如果密钥的长度是256字节，就直接把密钥的值赋给T，否则，轮转地将密钥的每个字节赋给T；

密钥K

长度为1-256字节，注意密钥的长度 keylen 与明文长度、密钥流的长度没有必然关系，通常密钥的长度取值为16字节（128比特）。

## 算法原理

1、初始化S和T

for i=0 to 255 do

S[i] =i;

T[i]=K[ imodkeylen ];

2、初始排列S

for i=0 to 255 do

j= ( j+S[i]+T[i])mod256;

swap(S[i],S[j]);

3、产生密钥流

for r=0 to len do //r为明文长度，r字节

i=(i+1) mod 256;

j=(j+S[i])mod 256;

swap(S[i],S[j]);

t=(S[i]+S[j])mod 256;

k[r]=S[t];