# 单向加密

单向加密又称为不可逆加密算法，其密钥是由加密散列函数生成的。单向散列函数一般用于产生消息摘要，密钥加密等。

## 分类

常见的单向加密算法有：

MD5（Message Digest Algorithm 5）：是RSA数据安全公司开发的一种单向散列算法，非可逆，相同的明文产生相同的密文；

SHA（Secure Hash Algorithm）：可以对任意长度的数据运算生成一个160位的数值。其变种由SHA192，SHA256，SHA384等；

CRC-32，主要用于提供校验功能；

## 特征

1、输入一样，输出必然相同；

2、雪崩效应，输入的微小改变，将会引起结果的巨大变化；

3、定长输出，无论原始数据多大，结果大小都是相同的；

4、不可逆，无法根据特征码还原原来的数据。

# 对称加密

采用单钥密码系统的加密方法，同一个密钥可以同时用作信息的加密和解密，这种加密方法称为对称加密，也称为单密钥加密。

## 分类

## 特征

1、加密方和解密方使用同一个密钥；

2、加密解密的速度比较快，适合数据比较长时的使用；

3、密钥传输的过程不安全，且容易被破解，密钥管理也比较麻烦；

优点：对称加密算法的优点是算法公开、计算量小、加密速度快、加密效率高。

缺点：对称加密算法的缺点是在数据传送前，发送方和接收方必须商定好秘钥，然后使双方都能保存好秘钥。其次如果一方的秘钥被泄露，那么加密信息也就不安全了。

另外，每对用户每次使用对称加密算法时，都需要使用其他人不知道的唯一秘钥，这会使得收、发双方所拥有的钥匙数量巨大，密钥管理成为双方的负担。

# 非对称加密

非对称密钥加密也称为公钥加密，由一对公钥和私钥组成。公钥是从私钥提取出来的。可以用公钥加密，再用私钥解密，这种情形一般用于公钥加密，当然也可以用私钥加密，用公钥解密。常用于数字签名，因此非对称加密的主要功能就是加密和数字签名。

## 分类

RSA：由 RSA公司发明，是一个支持变长密钥的公共密钥算法，需要加密的文件块的长度也是可变的；既可以实现加密，又可以实现签名。

DSA（Digital Signature Algorithm）：数字签名算法，是一种标准的 DSS（数字签名标准）。

ECC（Elliptic Curves Cryptography）：椭圆曲线密码编

## 特征

1、秘钥对，公钥(public key)和私钥(secret key)

2、主要功能：加密和签名

发送方用对方的公钥加密，可以保证数据的机密性（公钥加密）。

发送方用自己的私钥加密，可以实现身份验证（数字签名）。

3、公钥加密算法很少用来加密数据，速度太慢，通常用来实现身份验证。

# 应用

## SSH

## git