# 加密算法简介

## 加密算法分类

加密算法整体可以分为：**可逆加密**和**不可逆加密**，可逆加密又可以分为：**对称加密**和**非对称加密**。

**不可逆加密算法** ：指不可以从密文中推算出明文的加密算法；

**不可逆加密算法** ：指不可以从密文中推算出明文的加密算法

**对称加密** ：在数据加密和解密的时用的都是同一个密钥；

**非对称加密**：非对称加密算法有两个密钥，这两个密钥完全不同但又完全匹配。只有使用匹配的一对公钥和私钥，才能完成对明文的加密和解密过程。

## 不可逆算法

**不可逆加密算法** ：指不可以从密文中推算出明文的加密算法（MD5、HMAC、SHA1、SHA-224、SHA-256、SHA-384、SHA-512等）

**MD5算法特点：**

1. 压缩性：无论数据长度是多少，计算出来的MD5值长度相同  
   2、容易计算性：由原数据容易计算出MD5值  
   3、抗修改性：即便修改一个字节，计算出来的MD5值也会巨大差异  
   4、抗碰撞性：知道数据和MD5值，很小概率找到相同MD5值相同的原数据。

## 可逆算法

### 对称加密（DES、AES、Blowfish、twofish ）

**对称加密** 对称加密算法是应用比较早的算法，在数据加密和解密的时用的都是同一个密钥。

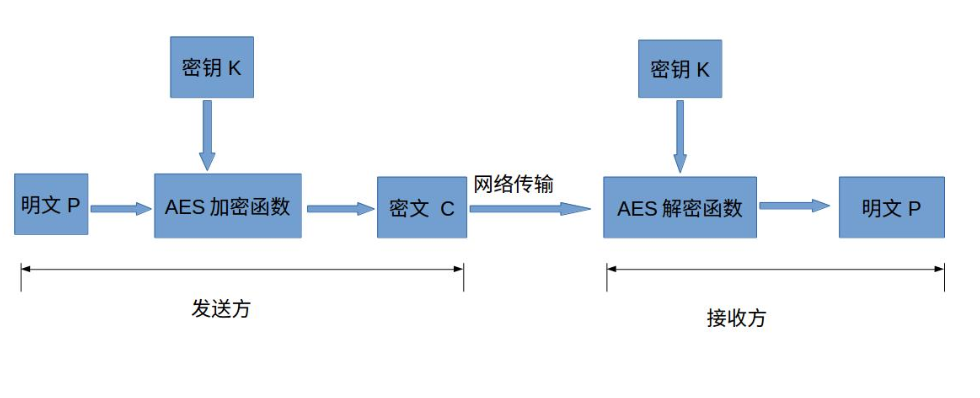
**优缺点：**

密钥管理：比较难，不适合互联网，一般用于内部系统

安全性：中

加密速度：加密速度快，适合大数据量的加解密处理

AES算法图：



### 非对称加密 （RSA、SM2、ECC等）

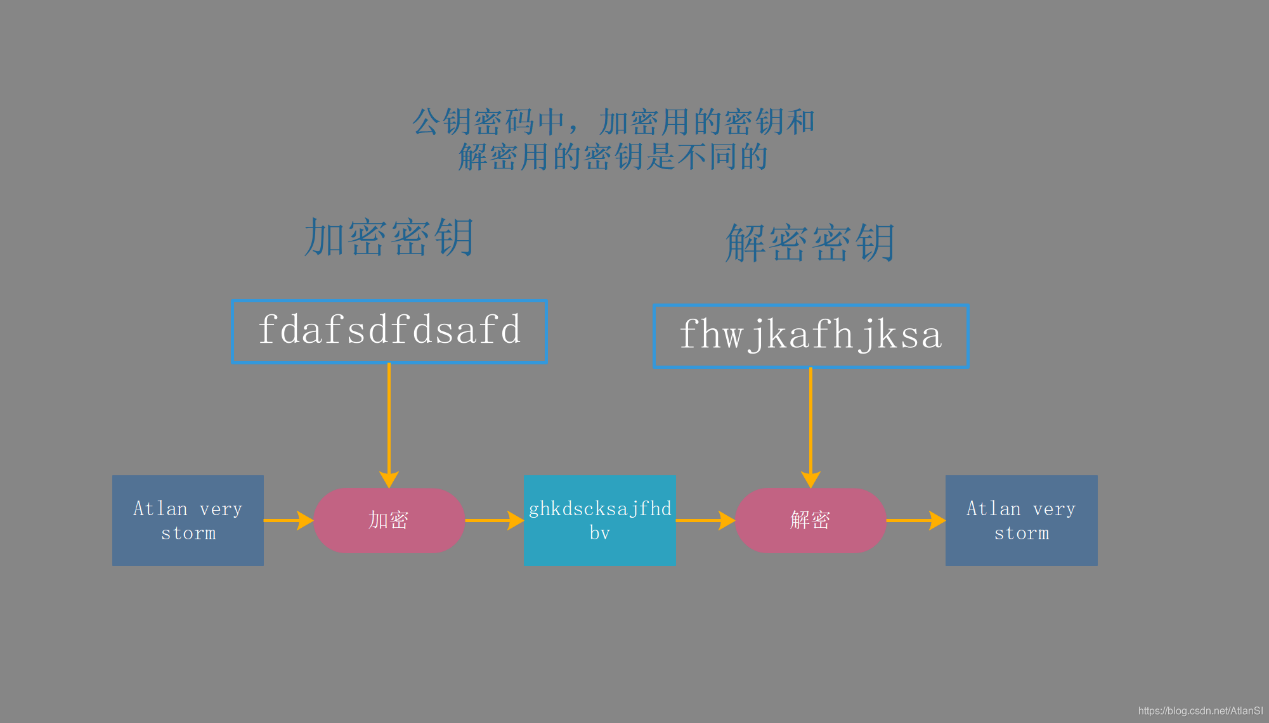
非对称加密算法有两个密钥，这两个密钥完全不同但又完全匹配。只有使用匹配的一对公钥和私钥，才能完成对明文的加密和解密过程。

优缺点：

密钥管理：密钥容易管理

安全性：高

加密速度：比较慢，适合 小数据量 加解密或数据签名



## 加密盐

加密盐也是比较常听到的一个概念，盐就是一个随机字符串用来和我们的加密串拼接后进行加密。加盐主要是为了提供加密字符串的安全性。