**密码学笔记**

作者： [阮一峰](http://www.ruanyifeng.com/)

日期： [2006年12月10日](http://www.ruanyifeng.com/blog/2006/12/)

1.

加密方法可以分为两大类。一类是单钥加密（private key cryptography），还有一类叫做双钥加密（public key cryptography）。前者的加密和解密过程都用同一套密码，后者的加密和解密过程用的是两套密码。

历史上，人类传统的加密方法都是前一种，比如二战期间德军用的Enigma电报密码。莫尔斯电码也可以看作是一种私钥加密方法。

2.

在单钥加密的情况下，密钥只有一把，所以密钥的保存变得很重要。一旦密钥泄漏，密码也就被破解。

3.

在双钥加密的情况下，密钥有两把，一把是公开的公钥，还有一把是不公开的私钥。

双钥加密的原理如下：

a) 公钥和私钥是一一对应的关系，有一把公钥就必然有一把与之对应的、独一无二的私钥，反之亦成立。

b) 所有的（公钥, 私钥）对都是不同的。

c) 用公钥可以解开私钥加密的信息，反之亦成立。

d) 同时生成公钥和私钥应该相对比较容易，但是从公钥推算出私钥，应该是很困难或者是不可能的。

4.

目前，通用的单钥加密算法为DES（Data Encryption Standard），通用的双钥加密算法为RSA（ Rivest-Shamir-Adleman），都产生于上个世纪70年代。

5.

在双钥体系中，**公钥用来加密信息，私钥用来数字签名**。

6.

因为任何人都可以生成自己的（公钥，私钥）对，所以为了防止有人散布伪造的公钥骗取信任，就需要一个可靠的第三方机构来生成经过认证的（公钥，私钥）对。目前，世界上最主要的数字服务认证商是位于美国加州的[Verisign](http://www.verisign.com/)公司，它的主要业务就是分发RSA数字证书。

（完）