public-key cryptography

1.简介

公开密钥加密（英语：public-key cryptography，又译为公开密钥加密），也称为非对称加密（asymmetric cryptography），一种[密码学](https://zh.wikipedia.org/wiki/%E5%AF%86%E7%A2%BC%E5%AD%B8" \o "密码学)[算法](https://zh.wikipedia.org/wiki/%E6%BC%94%E7%AE%97%E6%B3%95" \o "算法)类型，在这种密码学方法中，需要一对密钥，一个是私人密钥，另一个则是公开密钥。这两个密钥是数学相关，用某用户密钥加密后所得的信息，只能用该用户的解密密钥才能解密。如果知道了其中一个，并不能计算出另外一个。因此如果公开了一对密钥中的一个，并不会危害到另外一个的秘密性质。称公开的密钥为公钥；不公开的密钥为私钥。

如果加密密钥是公开的，这用于客户给私钥所有者上传加密的数据，这被称作为公开密钥加密（狭义）。例如，网络银行的客户发给银行网站的账户操作的加密数据。

如果解密密钥是公开的，用私钥加密的信息，可以用公钥对其解密，用于客户验证持有私钥一方发布的数据或文件是完整准确的，接收者由此可知这条信息确实来自于拥有私钥的某人，这被称作[数字签名](https://zh.wikipedia.org/wiki/%E6%95%B0%E5%AD%97%E7%AD%BE%E5%90%8D" \o "数字签名)，公钥的形式就是[数字证书](https://zh.wikipedia.org/wiki/%E6%95%B0%E5%AD%97%E8%AF%81%E4%B9%A6" \o "数字证书)。

RSA

RSA加密算法是一种[非对称加密算法](https://zh.wikipedia.org/wiki/%E9%9D%9E%E5%AF%B9%E7%A7%B0%E5%8A%A0%E5%AF%86%E6%BC%94%E7%AE%97%E6%B3%95" \o "非对称加密算法)。在[公开密钥加密](https://zh.wikipedia.org/wiki/%E5%85%AC%E5%BC%80%E5%AF%86%E9%92%A5%E5%8A%A0%E5%AF%86" \o "公开密钥加密)和[电子商业](https://zh.wikipedia.org/wiki/%E7%94%B5%E5%AD%90%E5%95%86%E4%B8%9A" \o "电子商业)中RSA被广泛使用。比起[DES](https://zh.wikipedia.org/wiki/DES" \o "DES)和其它[对称算法](https://zh.wikipedia.org/w/index.php?title=%E5%AF%B9%E7%A7%B0%E7%AE%97%E6%B3%95&action=edit&redlink=1" \o "对称算法（页面不存在）)来说，RSA要慢得多。

Diffie–Hellman

迪菲-赫尔曼密钥交换（英语：Diffie–Hellman key exchange，缩写为D-H） 是一种[安全协议](https://zh.wikipedia.org/wiki/%E5%AE%89%E5%85%A8%E5%8D%8F%E8%AE%AE" \o "安全协议)。它可以让双方在完全没有对方任何预先信息的条件下通过不安全[信道](https://zh.wikipedia.org/wiki/%E4%BF%A1%E9%81%93" \o "信道)创建起一个[密钥](https://zh.wikipedia.org/wiki/%E5%AF%86%E9%92%A5" \o "密钥)。这个密钥可以在后续的通讯中作为[对称密钥](https://zh.wikipedia.org/wiki/%E5%AF%B9%E7%A7%B0%E5%AF%86%E9%92%A5" \o "对称密钥)来[加密](https://zh.wikipedia.org/wiki/%E5%8A%A0%E5%AF%86" \o "加密)通讯内容，迪菲－赫尔曼密钥交换本身并没有提供通讯双方的[身份验证](https://zh.wikipedia.org/wiki/%E8%BA%AB%E4%BB%BD%E9%AA%8C%E8%AF%81" \o "身份验证)服务，因此它很容易受到[中间人攻击](https://zh.wikipedia.org/wiki/%E4%B8%AD%E9%97%B4%E4%BA%BA%E6%94%BB%E5%87%BB" \o "中间人攻击)。

2.密码散列函数（英语：Cryptographic hash function），又译为加密散列函数、密码散列函数、加密散列函数，是[散列函数](https://zh.wikipedia.org/wiki/%E6%95%A3%E5%88%97%E5%87%BD%E6%95%B8" \o "散列函数)的一种。它被认为是一种[单向函数](https://zh.wikipedia.org/wiki/%E5%96%AE%E5%90%91%E5%87%BD%E6%95%B8" \o "单向函数)，也就是说极其难以由散列函数输出的结果，回推输入的数据是什么。这样的单向函数被称为“现代密码学的驮马”。这种散列函数的输入数据，通常被称为消息（message），而它的输出结果，经常被称为消息摘要（message digest）或摘要（digest）。一个理想的密码散列函数应该有四个主要的特性：

(1)对于任何一个给定的消息，它都很容易就能运算出散列数值

(2)[难以](https://zh.wikipedia.org/wiki/%E8%A8%88%E7%AE%97%E8%A4%87%E9%9B%9C%E6%80%A7%E7%90%86%E8%AB%96" \o "计算复杂性理论)由一个已知的散列数值，去推算出原始的消息

(3)在不更动散列数值的前提下，修改消息内容是不可行的

(4)对于两个不同的消息，它不能给与相同的散列数值

MD5

MD5消息摘要算法（英语：MD5 Message-Digest Algorithm），一种被广泛使用的[密码散列函数](https://zh.wikipedia.org/wiki/%E5%AF%86%E7%A2%BC%E9%9B%9C%E6%B9%8A%E5%87%BD%E6%95%B8" \o "密码散列函数)，可以产生出一个128位（16[字节](https://zh.wikipedia.org/wiki/%E5%AD%97%E8%8A%82" \o "字节)）的散列值（hash value），用于确保信息传输完整一致。1996年后被证实存在弱点，可以被加以破解，对于需要高度安全性的数据，专家一般建议改用其他算法，如[SHA-1](https://zh.wikipedia.org/wiki/SHA-1" \o "SHA-1)。2004年，证实MD5算法无法防止碰撞，因此无法适用于安全性认证，如[SSL](https://zh.wikipedia.org/wiki/SSL" \o "SSL)[公开密钥认证](https://zh.wikipedia.org/wiki/%E5%85%AC%E9%96%8B%E9%87%91%E9%91%B0%E8%AA%8D%E8%AD%89" \o "公开密钥认证)或是[数字签名](https://zh.wikipedia.org/wiki/%E6%95%B8%E4%BD%8D%E7%B0%BD%E7%AB%A0" \o "数字签名)等用途。

SHA-1

SHA-1（英语：Secure Hash Algorithm 1，中文名：安全散列算法1）是一种[密码散列函数](https://zh.wikipedia.org/wiki/%E5%AF%86%E7%A0%81%E6%95%A3%E5%88%97%E5%87%BD%E6%95%B0" \o "密码散列函数)，[美国国家安全局](https://zh.wikipedia.org/wiki/%E7%BE%8E%E5%9B%BD%E5%9B%BD%E5%AE%B6%E5%AE%89%E5%85%A8%E5%B1%80" \o "美国国家安全局)设计，并由美国[国家标准技术研究所](https://zh.wikipedia.org/wiki/%E5%9C%8B%E5%AE%B6%E6%A8%99%E6%BA%96%E6%8A%80%E8%A1%93%E7%A0%94%E7%A9%B6%E6%89%80" \o "国家标准技术研究所)（NIST）发布为[联邦数据处理标准](https://zh.wikipedia.org/wiki/%E8%81%AF%E9%82%A6%E8%B3%87%E6%96%99%E8%99%95%E7%90%86%E6%A8%99%E6%BA%96" \o "联邦数据处理标准)（FIPS）。SHA-1可以生成一个被称为消息摘要的160[位](https://zh.wikipedia.org/wiki/%E4%BD%8D" \o "位)（20[字节](https://zh.wikipedia.org/wiki/%E5%AD%97%E8%8A%82" \o "字节)）散列值，散列值通常的呈现形式为40个[十六进制](https://zh.wikipedia.org/wiki/%E5%8D%81%E5%85%AD%E8%BF%9B%E5%88%B6" \o "十六进制)数。2005年，密码分析人员发现了对SHA-1的有效攻击方法，这表明该算法可能不够安全，不能继续使用

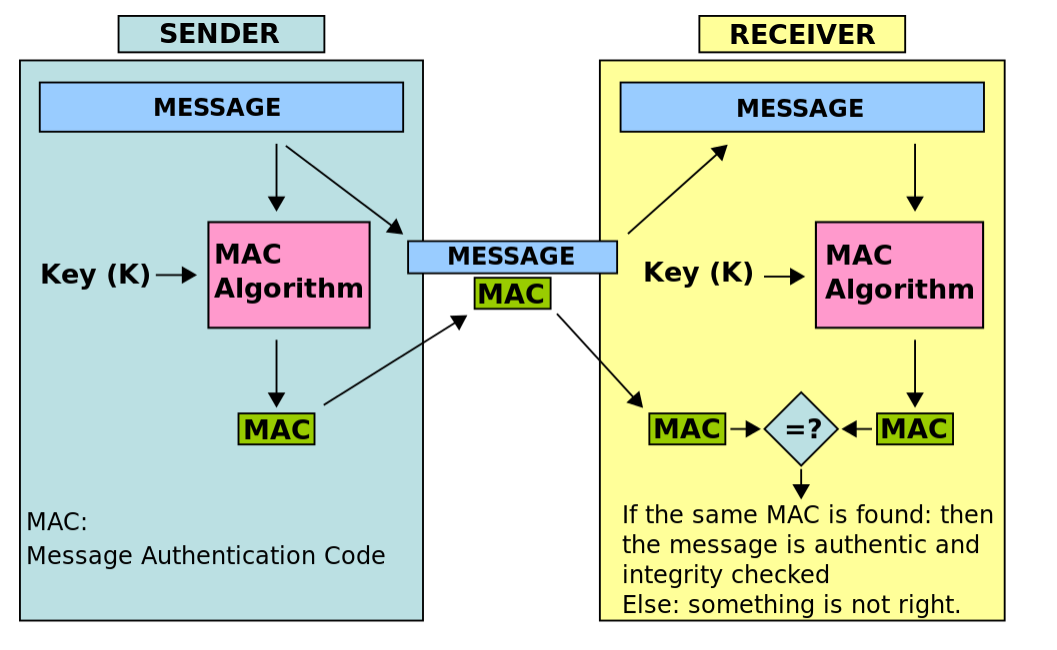
SHA-2

SHA-2，名称来自于安全散列算法2（英语：Secure Hash Algorithm 2）的缩写，一种[密码散列函数](https://zh.wikipedia.org/wiki/%E5%AF%86%E7%A2%BC%E9%9B%9C%E6%B9%8A%E5%87%BD%E6%95%B8" \o "密码散列函数)算法标准，由[美国国家安全局](https://zh.wikipedia.org/wiki/%E7%BE%8E%E5%9C%8B%E5%9C%8B%E5%AE%B6%E5%AE%89%E5%85%A8%E5%B1%80" \o "美国国家安全局)研发，由[美国国家标准与技术研究院](https://zh.wikipedia.org/wiki/%E7%BE%8E%E5%9B%BD%E5%9B%BD%E5%AE%B6%E6%A0%87%E5%87%86%E4%B8%8E%E6%8A%80%E6%9C%AF%E7%A0%94%E7%A9%B6%E9%99%A2" \o "美国国家标准与技术研究院)（NIST）在2001年发布。属于[SHA算法](https://zh.wikipedia.org/wiki/SHA%E5%AE%B6%E6%97%8F" \o "SHA家族)之一，是[SHA-1](https://zh.wikipedia.org/wiki/SHA-1" \o "SHA-1)的后继者。其下又可再分为六个不同的算法标准，包括了：SHA-224、SHA-256、SHA-384、SHA-512、SHA-512/224、SHA-512/256。

SHA-3

SHA-3第三代安全散列算法(Secure Hash Algorithm 3)，之前名为Keccak算法，设计者宣称在 [Intel Core 2](https://zh.wikipedia.org/wiki/Intel_Core_2" \o "Intel Core 2) 的CPU上面，此算法的性能是12.5cpb([每字节周期数](https://zh.wikipedia.org/w/index.php?title=%E6%AF%8F%E4%BD%8D%E5%85%83%E7%B5%84%E5%91%A8%E6%9C%9F%E6%95%B8&action=edit&redlink=1" \o "每字节周期数（页面不存在）)，cycles per byte)。不过，在[硬件实做](https://zh.wikipedia.org/wiki/%E7%89%B9%E6%AE%8A%E6%87%89%E7%94%A8%E7%A9%8D%E9%AB%94%E9%9B%BB%E8%B7%AF" \o "特殊应用集成电路)上面，这个算法比起其他算法明显的快上很多。

3.消息认证码（英语：Message authentication code，缩写为MAC），又译为消息鉴别码、文件消息认证码、讯息鉴别码、信息认证码，是经过特定算法后产生的一小段信息，检查某段消息的[完整性](https://zh.wikipedia.org/wiki/%E5%AE%8C%E6%95%B4%E6%80%A7" \o "完整性)，以及作[身份验证](https://zh.wikipedia.org/wiki/%E8%BA%AB%E4%BB%BD%E9%AA%8C%E8%AF%81" \o "身份验证)。它可以用来检查在消息传递过程中，其内容是否被更改过，不管更改的原因是来自意外或是蓄意攻击。同时可以作为消息来源的[身份验证](https://zh.wikipedia.org/wiki/%E8%BA%AB%E4%BB%BD%E9%AA%8C%E8%AF%81" \o "身份验证)，确认消息的来源。信息鉴别码不能提供对信息的保密，若要同时实现保密认证，同时需要对信息进行加密

密钥散列消息认证码（英语：Keyed-hash message authentication code，缩写为HMAC），又称散列消息认证码（Hash-based message authentication code），是一种通过特别计算方式之后产生的[消息认证码](https://zh.wikipedia.org/wiki/%E8%A8%8A%E6%81%AF%E9%91%91%E5%88%A5%E7%A2%BC" \o "消息认证码)（MAC），使用[密码散列函数](https://zh.wikipedia.org/wiki/%E5%AF%86%E7%A2%BC%E9%9B%9C%E6%B9%8A%E5%87%BD%E6%95%B8" \o "密码散列函数)，同时结合一个加密密钥。它可以用来保证数据的完整性，同时可以用来作某个消息的[身份验证](https://zh.wikipedia.org/wiki/%E8%BA%AB%E4%BB%BD%E9%AA%8C%E8%AF%81" \o "身份验证)。

4.数字签名（又称公钥数字签名，英语：Digital Signature）是一种类似写在[纸](https://zh.wikipedia.org/wiki/%E7%BA%B8" \o "纸)上的普通的物理[签名](https://zh.wikipedia.org/wiki/%E7%AD%BE%E5%90%8D" \o "签名)，但是使用了[公钥加密](https://zh.wikipedia.org/wiki/%E5%85%AC%E9%92%A5%E5%8A%A0%E5%AF%86" \o "公钥加密)领域的技术实现，用于鉴别数字信息的方法。数位签名了的文件的完整性是很容易验证的，而且数位签名具有不可抵赖性。

