最近有一位之前找过的用户问了我们小编的一个问题，我相信这也是很多币圈朋友经常会疑惑的问题：加密技术相关问题，加密技术名词解释相关问题，带着这一个问题，让专业的小编告诉您原因。

加密技术是最常用的安全保密手段，利用技术手段把重要的数据变为乱码（加密）传送，到达目的地后再用相同或不同的手段还原（解密）。

加密技术包括两个元素：算法和密钥。算法是将普通的信息或者可以理解的信息与一串数字（密钥）结合，产生不可理解的密文的步骤，密钥是用来对数据进行编码和解密的一种算法。在安全保密中，可通过适当的钥加密技术和管理机制来保证网络的信息通信安全。

数据加密技术可以从以下三个方面来看：

(1)加、解密的处理效率

比如DES算法只有56位密钥，加解密速度快，保密度高，可实现高速处理。而RSA算法需进行多位整数乘幂和求模等多倍字长处理，运算量大且复杂，加密和解密数据的速率较低，不适于对较长明文加密。

(2)算法的安全性与保密性

比如DES算法采用单密钥安全性全靠密钥的保密，易受穷举强力攻击。RSA算法采用双密钥产生密钥较麻烦，安全性依赖于大数分解的困难性。

(3)密钥的分配与管理

比如DES算法必须在通信前对密钥进行秘密分配，人多时密钥数量大，由此密钥的定期更换很困难，而RSA算法只对自己的秘密密钥进行保密管理就行了，不需要秘密通道或复杂协议来传送密钥，更换密钥也方便。

加密技术是最常用的安全保密手段，利用技术手段把重要的数据变为乱码（加密）传送，到达目的地后再用相同或不同的手段还原（解密）。

加密技术包括两个元素：算法和密钥。算法是将普通的信息或者可以理解的信息与一串数字（密钥）结合，产生不可理解的密文的步骤，密钥是用来对数据进行编码和解密的一种算法。在安全保密中，可通过适当的钥加密技术和管理机制来保证网络的信息通信安全。

加密技术分为：

1、对称加密

对称加密采用了对称密码编码技术，它的特点是文件加密和解密使用相同的密钥，即加密密钥也可以用作解密密钥，这种方法在密码学中叫做对称加密算法，对称加密算法使用起来简单快捷，密钥较短，且破译困难

2、非对称

1976年，美国学者Dime和Henman为解决信息公开传送和密钥管理问题，提出一种新的密钥交换协议，允许在不安全的媒体上的通讯双方交换信息，安全地达成一致的密钥，这就是“公开密钥系统”。

加密技术的功能：

原有的单密钥加密技术采用特定加密密钥加密数据，而解密时用于解密的密钥与加密密钥相同，这称之为对称型加密算法。采用此加密技术的理论基础的加密方法如果用于网络传输数据加密，则不可避免地出现安全漏洞。

区别于原有的单密钥加密技术，PKI采用非对称的加密算法，即由原文加密成密文的密钥不同于由密文解密为原文的密钥，以避免第三方获取密钥后将密文解密。

以上内容参考：百度百科—加密技术

对称密码是一种用相同的密钥进行加密和解密的技术，用于确保消息的机密性。在对称密码的算法方面，目前主要使用的是 AES。尽管对称密码能够确保消息的机密性，但需要解决将解密密钥配送给接受者的密钥配送问题。

主要算法

DES

数据加密标准（英语：Data Encryption Standard，缩写为 DES）是一种对称密钥加密块密码算法，1976年被美国联邦政府的国家标准局确定为联邦资料处理标准（FIPS），随后在国际上广泛流传开来。它基于使用56位密钥的对称算法。

DES现在已经不是一种安全的加密方法，主要因为它使用的56位密钥过短。

原理请参考： 加密技术01-对称加密-DES原理

3DES

三重数据加密算法（英语：Triple Data Encryption Algorithm，缩写为TDEA，Triple DEA），或称3DES（Triple DES），是一种对称密钥加密块密码，相当于是对每个数据块应用三次DES算法。由于计算机运算能力的增强，原版DES由于密钥长度过低容易被暴力破解；3DES即是设计用来提供一种相对简单的方法，即通过增加DES的密钥长度来避免类似的攻击，而不是设计一种全新的块密码算法。

注意：有3个独立密钥的3DES的密钥安全性为168位，但由于中途相遇攻击（知道明文和密文），它的有效安全性仅为112位。

3DES使用“密钥包”，其包含3个DES密钥，K1，K2和K3，均为56位（除去奇偶校验位）。

密文 = E k3 (D k2 (E k1 (明文)))

而解密则为其反过程：

明文 = D k3 (E k2 (D k1 (密文)))

AES

AES 全称 Advanced Encryption Standard（高级加密标准）。它的出现主要是为了取代 DES 加密算法的，因为 DES 算法的密钥长度是 56 位，因此算法的理论安全强度是 56 位。于是 1997 年 1 月 2 号，美国国家标准技术研究所宣布希望征集高级加密标准，用以取代 DES。AES 也得到了全世界很多密码工作者的响应，先后有很多人提交了自己设计的算法。最终有5个候选算法进入最后一轮：Rijndael，Serpent，Twofish，RC6 和 MARS。最终经过安全性分析、软硬件性能评估等严格的步骤，Rijndael 算法获胜。

AES 密码与分组密码 Rijndael 基本上完全一致，Rijndael 分组大小和密钥大小都可以为 128 位、192 位和 256 位。然而 AES 只要求分组大小为 128 位，因此只有分组长度为 128 位的 Rijndael 才称为 AES 算法。

本文 AES 默认是分组长度为 128 位的 Rijndael 算法

原理请参考： 加密技术02-对称加密-AES原理

算法对比

公钥密码是一种用不同的密钥进行加密和解密的技术，和对称密码一样用于确保消息的机密性。使用最广泛的一种公钥密码算法是 RAS。和对称密码相比，公钥密码的速度非常慢，因此一般都会和对称密码一起组成混合密码系统来使用。公钥密码能够解决对称密码中的密钥交换问题，但存在通过中间人攻击被伪装的风险，因此需要对带有数字签名的公钥进行认证。

公钥密码学的概念是为了解决对称密码学中最困难的两个问题而提出

应用场景

几个误解

主要算法

Diffie–Hellman 密钥交换

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。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创建起一个密钥。这个密钥可以在后续的通讯中作为对称密钥来加密通讯内容。公钥交换的概念最早由瑞夫·墨克（Ralph C.
Merkle）提出，而这个密钥交换方法，由惠特菲尔德·迪菲（Bailey Whitfield Diffie）和马丁·赫尔曼（Martin Edward
Hellman）在1976年发表，也是在公开文献中发布的第一个非对称方案。

Diffie–Hellman 算法的有效性是建立在计算离散对数很困难的基础上。简单地说，我们可如下定义离散对数。首先定义素数 p 的本原跟。素数 p
的本原根是一个整数，且其幂可以产生 1 到 p-1 之间所有整数，也就是说若 a 是素数 p 的本原根，则

a mod p, a 2 mod p,..., a p-1 mod p 各不相同，它是整数 1 到 p-1
的一个置换。

对任意整数 b 和素数 p 的本原跟 a，我们可以找到唯一的指数 i 使得

b ≡ a i (mod p) 其中 0 = i = p-1

其中 a, b, p 这些是公开的，i 是私有的，破解难度就是计算 i 的难度。

Elgamal

1985年，T.Elgamal 提出了一种基于离散对数的公开密钥体制，一种与 Diffie-Hellman 密钥分配体制密切相关。Elgamal
密码体系应用于一些技术标准中，如数字签名标准(DSS) 和 S/MIME
电子邮件标准。

基本原理就是利用 Diffie–Hellman 进行密钥交换，假设交换的密钥为 K，然后用 K 对要发送的消息 M，进行加密处理。

所以 Elgamal 的安全系数取决于 Diffie–Hellman 密钥交换。

另外 Elgamal 加密后消息发送的长度会增加一倍。

RSA

MIT 的罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）在 1977 年提出并于 1978 年首次发表的算法。RSA 是最早满足要求的公钥算法之一，自诞生日起就成为被广泛接受且被实现的通用的公钥加密方法。

RSA 算法的有效性主要依据是大数因式分解是很困难的。

原理请参考： 加密技术03-非对称加密-RSA原理

ECC

大多数使用公钥密码学进行加密和数字签名的产品和标准都使用 RSA 算法。我们知道，为了保证 RSA
使用的安全性，最近这些年来密钥的位数一直在增加，这对使用 RSA 的应用是很重的负担，对进行大量安全交易的电子商务更是如此。近来，出现的一种具有强大竞争力的椭圆曲线密码学（ECC）对 RSA
提出了挑战。在标准化过程中，如关于公钥密码学的 IEEE P1363
标准中，人们也已考虑了 ECC。

与 RSA 相比，ECC 的主要诱人之处在于，它可以使用比 RSA 短得多的密钥得到相同安全性，因此可以减少处理负荷。

ECC 比 RSA 或 Diffie-Hellman 原理复杂很多，本文就不多阐述了。

算法对比

公钥密码体制的应用

密码分析所需计算量（ NIST SP-800-57 ）

注：L=公钥的大小，N=私钥的大小

散列函数是一种将长消息转换为短散列值的技术，用于确保消息的完整性。在散列算法方面，SHA-1 曾被广泛使用，但由于人们已经发现了一些针对该算法理论上可行的攻击方式，因此该算法不应再被用于新的用途。今后我们应该主要使用的算法包括目前已经在广泛使用的 SHA-2，以及具有全新结构的 SHA-3 算法。散列函数可以单独使用，也可以作为消息认证、数字签名以及伪随机数生成器等技术的组成元素来使用。

主要应用

主要算法

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，可以产生出一个 128 位（ 16 字节，被表示为 32 位十六进制数字）的散列值（hash value），用于确保信息传输完整一致。MD5 由美国密码学家罗纳德·李维斯特（Ronald Linn Rivest）设计，于 1992 年公开，用以取代 MD4 算法。这套算法的程序在 RFC 1321 中被加以规范。

2009年，中国科学院的谢涛和冯登国仅用了 2 20.96 的碰撞算法复杂度，破解了MD5的碰撞抵抗，该攻击在普通计算机上运行只需要数秒钟。2011年，RFC 6151禁止MD5用作密钥散列消息认证码。

原理请参考： 加密技术04-哈希算法-MD5原理

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，美国国家安全局设计，并由美国国家标准技术研究所（NIST）发布为联邦资料处理标准（FIPS）。SHA-1可以生成一个被称为消息摘要的160位（20字节）散列值，散列值通常的呈现形式为40个十六进制数。

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，自2010年以来，许多组织建议用SHA-2或SHA-3来替换SHA-1。Microsoft、Google以及Mozilla都宣布，它们旗下的浏览器将在2017年停止接受使用SHA-1算法签名的SSL证书。

2017年2月23日，CWI Amsterdam与Google宣布了一个成功的SHA-1碰撞攻击，发布了两份内容不同但SHA-1散列值相同的PDF文件作为概念证明。

2020年，针对SHA-1的选择前缀冲突攻击已经实际可行。建议尽可能用SHA-2或SHA-3取代SHA-1。

原理请参考： 加密技术05-哈希算法-SHA系列原理

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，一种密码散列函数算法标准，由美国国家安全局研发，由美国国家标准与技术研究院（NIST）在2001年发布。属于SHA算法之一，是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-2 系列的算法主要思路和 SHA-1 基本一致

原理请参考： 加密技术05-哈希算法-SHA系列原理

SHA-3

SHA-3 第三代安全散列算法(Secure Hash Algorithm 3)，之前名为 Keccak 算法。

Keccak 是一个加密散列算法，由 Guido Bertoni，Joan Daemen，Micha?l Peeters，以及 Gilles Van Assche 在 RadioGatún 上设计。

2012年10月2日，Keccak 被选为 NIST 散列函数竞赛的胜利者。SHA-2
目前没有出现明显的弱点。由于对 MD5、SHA-0 和 SHA-1
出现成功的破解，NIST
感觉需要一个与之前算法不同的，可替换的加密散列算法，也就是现在的 SHA-3。

SHA-3 在2015年8月5日由 NIST 通过 FIPS 202 正式发表。

原理请参考： 加密技术05-哈希算法-SHA系列原理

算法对比

加密技术分为：

1、对称加密

对称加密采用了对称密码编码技术，它的特点是文件加密和解密使用相同的密钥，即加密密钥也可以用作解密密钥，这种方法在密码学中叫做对称加密算法，对称加密算法使用起来简单快捷，密钥较短，且破译困难

2、非对称

1976年，美国学者Dime和Henman为解决信息公开传送和密钥管理问题，提出一种新的密钥交换协议，允许在不安全的媒体上的通讯双方交换信息，安全地达成一致的密钥，这就是“公开密钥系统”。

相关信息：

目前主流的加密技术有对称加密例如DES，3DES和AES，然后还有非对称加密技术：例如RSA和椭圆加密算法。对称加密的话，就是用来加密和解密的密钥是一样的，非对称加密的话，加密的密钥和解密的密钥是不一样的，用加密的密钥加密以后，只有配对的另外一个密钥才能解开。

另外我们还可以常常看到MD5，SHA，SHA1之类的算法，其实他们不是加密算法，因为他们的结算结果不可逆，你没法从结果得到输入的数据是什么，他们的用途主要是为了防止泄密和修改数据，因为对于这些算法来说，每一个输入只能有一个输出，修改了输入就会使得输出变化很大，所以被人修改了数据的话通过这个算法就能知道了。

另外我校验密码的时候，如果只是通过这个计算结果来对比的话，其他人如果不知

道我的密码，即使他能解码我的程序也不行，因为程序里面只有结果，没有输入的密码。

以上就是小编对加密技术和加密技术名词解释的总结，更多加密技术名词解释方面的知识可以关注我们，在网站首页进行搜索你想知道的！