关于加密和安全

六旗工作室

关于加密和安全 V 0.94

作者： 舞飞的枫叶 & Banner

安全在计算机行业中可能会是个永久的话题。2004 年到 2005 年间，山东大学王小云教授攻破 MD5，降低了 SHA-1 的安全强度，这更是引起了大家的关注。并且，随着网络技术的发展和普及，大家的网络安全意识也越来越强。因此，在这里对加密和安全的基础知识做一点入门性质的介绍，以便大家能对这方面有更准确的了解和把握，能更好地保护自己重要数据的安全。

本文侧重密码方面的基础知识的介绍。本文一直在逐步修改和完善。 如果哪位朋友在安全方面存在疑惑和问题，欢迎提出来，我们将尽力帮忙寻求解答，并丰富本文的内容，以便能帮助更多的人。如果本文存在问题和错误，也欢迎诸位给予批评指正。

1. 请大家准备好，开工了

密码学的方法离我们并不遥远。它应用很广泛，在我们日常使用计算机的时候就会经常用到，只不过我们没有多加留意而已。比如我们启动 Windows 的时候，我们要输入口令，这个口令在系统中就是加密后保存的。在我们上网时，有些网站需要我们建立安全连接，这时也是在密码算法支持下进行的。在你的 IE 浏览器中，看一下工具->Internet 选项->内容->证书，会发现密码技术其实早已在后台默默地为我们工作了。

密码算法有很多种。包括对称算法、非对称算法、消息摘要算法等。对称加密算法包括 DES 和 AES 等；非对称加密算法包括 RSA、DSA、椭圆曲线算法等。

接下来将以逐条解释基本概念的形式对主要的密码安全技术做一个简单的介绍。

2. 朴素的密码

“天王盖地虎，宝塔镇河妖……”大家一定在电影里看过土匪对暗号的场面。其实，土匪口中的“黑话”就是一种最朴素的密码。只不过这种密码过于简单，经不起密码学家的分析，非常容易破译。

3. 凯撒密码

这是一个古老的加密方法，当年凯撒大帝行军打仗时用这种方法进行通信，因此得名。它的原理很简单，其实就是单字母的替换。让我们看一个简单的例子 ：“This is Caesar Code”。用凯撒密码加密后字符串变为“vjku ku Ecguct Eqfg”。看起来似乎加密得很“安全”。可是你可以尝试一下，把这段很难懂的东西每一个字母换为字母表中前移 2 位的字母……哦，结果出来了。

凯撒密码的字母对应关系：

A b c d e f g h i … x y z

C d e f g h I j k … z a b

4. rot13

ROT13 是网络上常见的一种简单的“加密”方式。它是用字母表里 a—m 的字符来代替 n—z，用 n—z 的字符来代替 a—m 字符。它的原理和凯撒密码非常类似。凯撒密码移了 2 位，而 ROT13 移了 13 位。ROT13 通常作为简单的手段使得我们的电子信件不能被直接识别和阅读，也不会被那些匹配程序用通常的方法直接找到。

如"V Ybir lbh!" 这个句子实际上是"I Love you!"。

ROT13 字母对应关系：

A b c d e f g h I … x y z

N o p q r s t u v … k l m

明白了吗？“解密”一下下面的内容：

jrypbxr gb jjj.syntjner.arg

5. 受限密码

上面讨论的“加密”是非常简单的，简单到不用计算机的帮助就能手工破译，简单到只能防止 3 岁的小妹妹偷看你的文件 **J**

我们可以把这些算法变得更复杂，引入更多的变换、更多的交叉和扩散 …… 这样也许会更难破译些。但是，在这个基础上变得再复杂，也还跳不出“受限密码”的范畴。所谓“受限密码”，是指算法的安全性是建立在算法保密的基础上的。一旦算法泄漏，所加密的内容也就完全没有安全性可言了。我们前面讨论的算法就是有这个特点的。

算法泄漏的问题使得这类算法的应用范围受到很大的限制。基本上，现在已经没人用了。

6. 现代密码技术的开始：密钥与算法分离

受限密码一旦泄漏了算法，那么所有加密的内容都会曝露在光天化日之下。使用这样的方法来保护重要信息是很危险的。因此，密码学家提出了算法和密钥分离的思想。这是密码学的一个里程碑。

它的思想是，密码的安全性取决于一个密钥，而不是取决于一个算法。每条消息用一个 Key 加密，只要 Key 不泄露，消息就是安全的。即使算法公开了，也威胁不到消息的安全性。现代的密码算法，如 3DES,AES 等，都是属于这一类。后面我们将会对这些算法做简要的介绍。

7. 澄清一个观念：通常没有绝对的信息安全

在介绍现代的密码和信息安全技术之前，有必要澄清一个观念：密码技术里所提到的信息安全性通常不是绝对的，它是一个相对的范畴。

一位密码学家曾经这样评论：如果你想让你的信息绝对安全的话，你得把你要保密的信息写下来装在保险柜里，把保险柜焊死，到太平洋海底某个不为人知的角落挖坑深埋，这样也许会接近绝对的安全。可是这样的安全是没有用的，因为这并不能让需要信息的人得到它。所以，这种“安全”是没有用的。实际上，这不能叫做“信息安全”，把它叫做“信息隐藏”也许更为合适。

我们所讨论的信息安全，是有使用价值的信息安全。这种安全是相对的安全。

不过“相对安全”并不意味着不安全。我们日常生活中用的“锁”其实也是相对的安全。事实

上，密码算法的安全强度要比平常的锁的安全强度高出很多倍。

8. 相对的安全

在数学家香农（Claude E.Shanon）创立的信息论中，用严格的数学方法证明了这么一个结论：一切密码算法，除了一次一密以外，在理论上都是可以破解的。这些密码算法，包括现在的和过去的，已知的和未知的，不管它多么复杂、多么先进，只要有足够强大的计算机，有足够多的密文，一定可以破译。

那么就产生了这样一个问题：既然这样，那密码还有什么用呢？

这就是为什么我们要讨论相对安全的原因。

前面提到了，一切密码，理论上都是可以破译的。但是，只有在拥有足够强大的计算机的情况下才有可能破译。在实际上，也许并不存在这么强的计算机。如果破译一个算法需要现在最强的计算机运算几百年，那么这样的算法即使理论上可以破译，在实践中也还是有实用价值的。

因此，我们可以这样理解相对安全的观念：假如一条信息需要保密 10 年，如果要花 20 年的时间才能破解它，那么信息就是安全的。否则就不安全。

在现实中，能获得的计算能力在一定程度上与付出的经济代价成比例。因此，也可以从经济的角度来衡量安全程度。假如一条信息价值一百万元，如果需要要花 1000 万元的代价才能制造出足够强的计算机来破解它，那它就是安全的。但是，如果信息价值 1000 万，用 100 万元就能获得足够的计算能力来破解它，那么它就是不安全的。

9. 一次一密

前面提到除了一次一密以外，其它的密码理论上都是可以破解的。那么什么是一次一密呢？一次一密就是每一次加密都使用一个不同的密钥（废话，和没说一样**J**）。严格的说，满足以下条件的密码才是真正的一次一密：

a.密钥是随机产生的，并且必须是真随机数，而不是伪随机数；

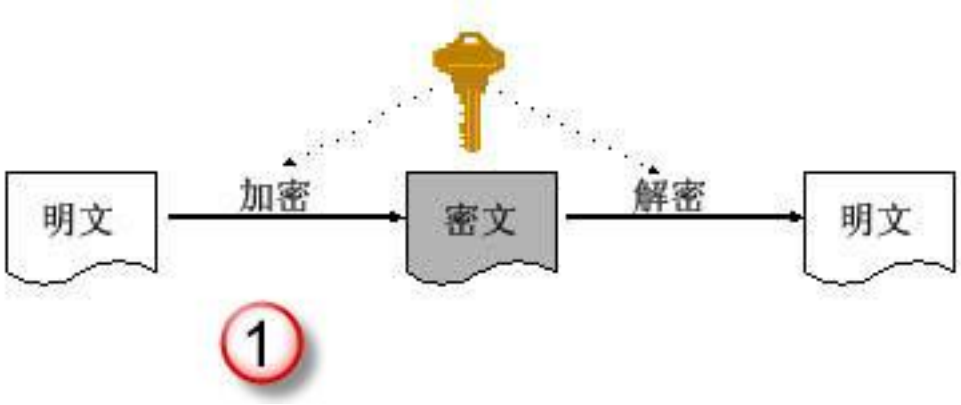
b.密钥不能重复使用；

c.密钥的有效长度不小于密文的长度。

一次一密是最安全的加密算法，双方一旦安全交换了密钥，之后交换信息的过程就是安全的。这种算法一直在一些要求高度机密的场合使用，据说美国和前苏联之间的热线电话、前苏联的间谍都是使用一次一密的方式加密的。不管有多强的超级计算机，不管超级计算机工作多久，也不管多少人，用什么方法和技术，具有多大的计算能力，都不可能破解用一次一密方法加密的信息，除非回到那个时代拿到他用过的密码本（也就是密钥）。前苏联间谍用一次一密方法加密过的信息将成为永久的谜。

10. 对称算法的概念

所谓对称算法就是指加密和解密过程均采用同一把密钥。如 DES,3DES,AES 等算法都属于对称算法。下面会对这几种有代表性的算法一一做介绍。

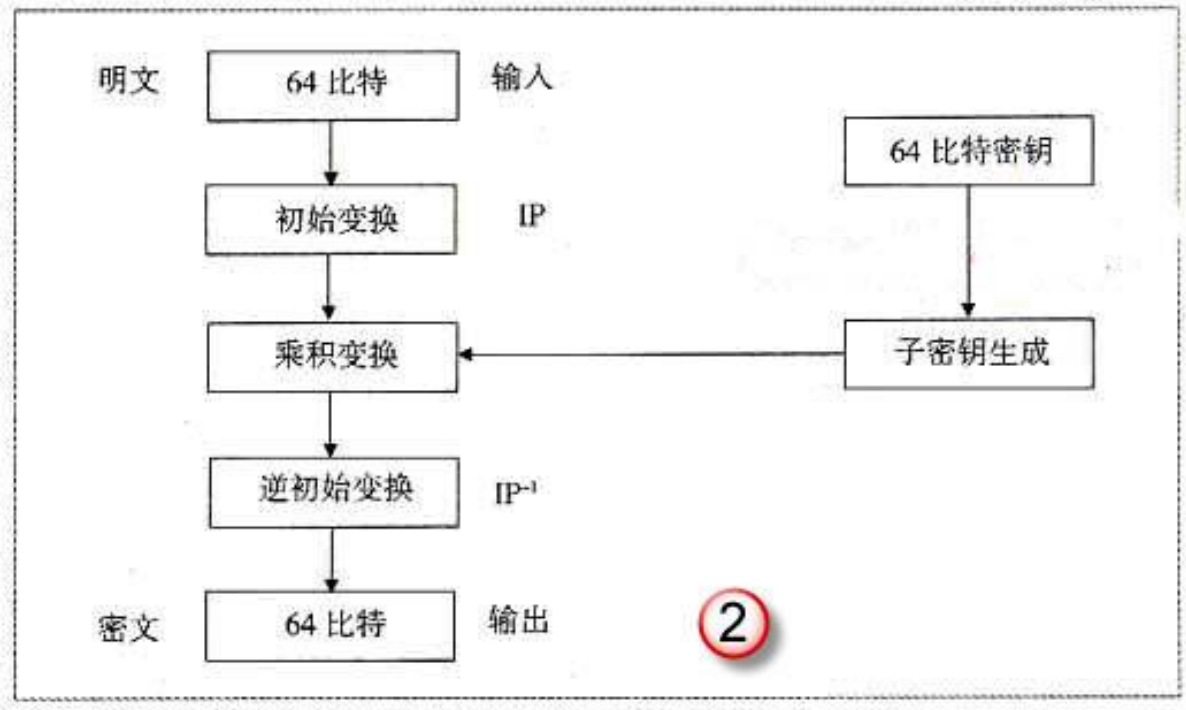


11. DES 算法

DES（Data Encryption Standard）是一种经典的对称算法。其数据分组长度为 64 位，使用的密钥为 64 位，有效密钥长度为 56 位（有 8 位用于奇偶校验）。它由 IBM 公司在 70 年代开发，经过政府的加密标准筛选后，于 1976 年 11 月被美国政府采用，随后被美国国家标准局和美国国家标准协会(American National Standard Institute， ANSI) 承认。

该技术算法公开，在各行业有着广泛的应用。DES 算法从公布到现在已有 20 多年的历史，随着计算机能力的飞速发展，DES 的 56 位密钥长度显得有些短了。现在，已经有可能通过穷举的方法来对其进行攻击。但是除此以外，还没有发现穷举以外的能有效破译 DES 的方法。

DES 算法的数据流程图如下图所示：

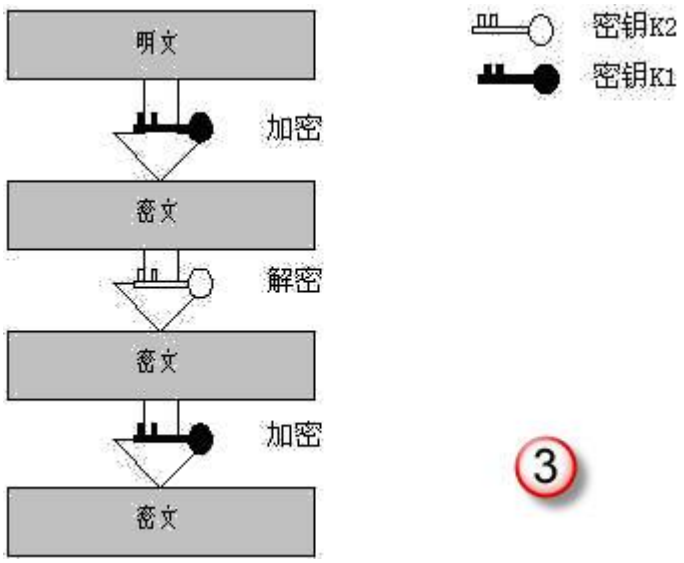


12. 三重 DES

DES 算法现在已经不能提供足够的安全性，因为其有效密钥只有 56 位。因此，后来又提出了

三重 DES（或称 3DES），该方法的强度大约和 112 比特的密钥强度相当。

这种方法用两个密钥对明文进行三次运算。设两个密钥是 K1 和 K2，其算法的步骤如图所示：



1．用密钥 K1 进行 DES 加密。

2．用 K2 对步骤 1 的结果进行 DES 解密。

3．用步骤 2 的结果使用密钥 K1 进行 DES 加密。

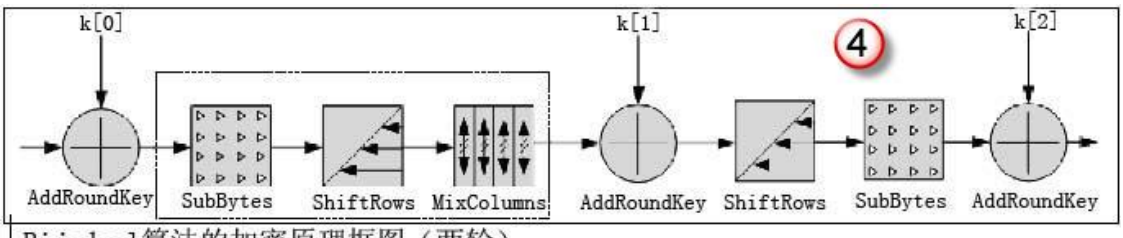
13. AES 算法

1997 年 1 月美国国家标准和技术研究所（NIST）宣布征集新的加密算法。2000 年 10 月 2 日，由比利时设计者 Joan Daemen 和 Vincent Rijmen 设计的 Rijndael 算法以其优秀的性能和抗攻击能力，最终赢得了胜利，成为新一代的加密标准 AES(Advanced Encryption Standard)。

Rijndael 加密：

Rijndael 是一个密钥迭代分组密码，包含了轮变换对状态的重复作用。轮数 Nr 的值取决于分组和密钥的长度。对于 AES，当密钥长度为 128 比特时，Nr =10；当密钥长度为 192 比特时，Nr =12；当密钥长度为 256 比特时，Nr =14。

Rijndael 算法的加密过程如图 1 所示。它包括一个初始密钥加法，记作 AddRoundKey，接着进行 Nr-1 次轮变换(Round)，最后再使用一个轮变换(FinalRound)。



Rijndael算法的加密原理框图（两轮）

轮变换由 4 个步骤组成：SubBytes，ShiftRows，MixColumns 和 AddRoundKey。最后一轮与前 Nr -1 次轮变换稍有不同，省掉了其中的 MixColumns 步骤。

步骤 SubBytes 是 Rijndael 算法中唯一的非线性变换。

步骤 ShiftRows 是一个字节换位，它将状态中的行按照不同的偏移量进行循环移位。使第 i 行

第 j 位的字节移动到位置（j -Ci）mod Nb，移动偏移量 Ci 的值依赖于 Nb 的取值。其中 Nb =分组长度/32，对于 AES，Nb 取固定长度 4。

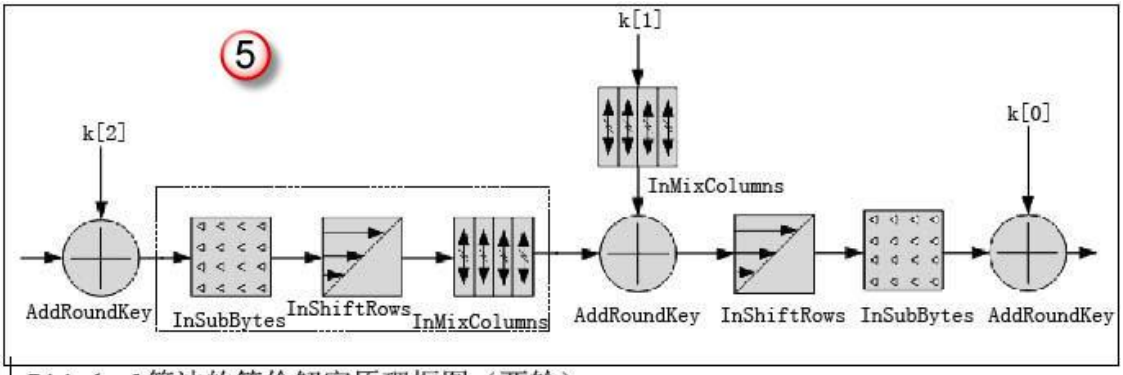
步骤 MixColumns 是作用在状态各列的置换算法。

密钥加法 AddRoundKey 将状态与一个轮密钥进行异或。轮密钥是由密码密钥通过密钥编排方案[1]导出。轮密钥的长度等于分组的长度。

Rijndael 解密:

Rijndael 解密算法有 2 种形式。一种是直接解密算法，即直接利用步骤 InsubBytes，InvShiftRows，InvMixColumns 和 AddRoundKey 的逆并倒置其次序对数据进行解密。

另一种是等价解密算法，其实现原理如图 2 所示。等价解密算法有利于有效实现良好的运算次序。



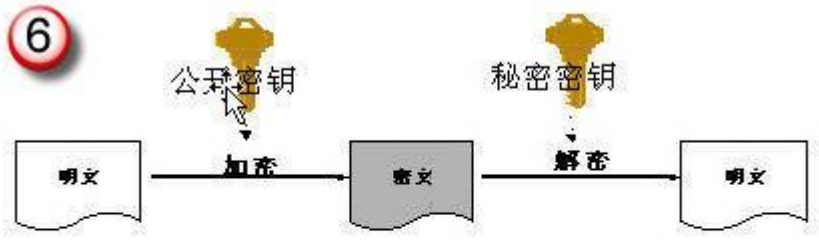
Rijndael算法的等价解密原理框图（两轮）

14. 非对称算法的概念

所谓非对称算法就是指加密和解密用的不是同一个密钥。

非对称算法的密钥分为二部分，通常称为“公钥”和“私钥”（或者称为“公开密钥”和“秘密密钥”）。公钥和私钥存在数学上的关系，使得用公钥加密的数据只能用对应的私钥解密，用私钥加密的数据只能用对应的公钥解密。但是从公钥中推导出私钥是很难的（理论上是可以推导出来的，但是实际上找不到这么强的计算能力）。

RSA,DSA 等算法属于非对称算法。



15. RSA 算法

RSA 算法是第一个能同时用于加密和数字签名的算法，也易于理解和操作。RSA 是被研究得最

广泛的公钥算法，从 1978 年提出到现在已近三十年，经历了各种攻击的考验，逐渐为人们接受，普遍认为是目前最优秀的公钥方案之一。通常认为破译 RSA 的难度与大数分解难度等价。算法以三个发明者的名字命名：Ron Rivest, Adi Shamir 和 Leonard Adleman。

RSA 算法的原理：

1、密钥对的产生：

选择两个大素数，p 和 q 。计算： n = p * q

然后随机选择加密密钥 e，要求 e 和 (p - 1) * (q - 1) 互质。最后，利用 Euclid 算法计算解密密钥 d，使其满足

e * d = 1 (mod (p - 1) * (q - 1))

其中 n 和 d 要互质。数 e 和 n 是公钥，d 是私钥。两个素数 p 和 q 不再需要，应该丢弃，不要让任何人知道。

2、加密

加密信息 m（二进制表示）时，首先把 m 分成等长数据块 m1 ,m2,..., mi ，块长 s，其中 2^s <= n, s 尽可能的大。加密的公式是：

ci = mi^e (mod n)

3、解密

解密时作如下计算：

mi = ci^d (mod n)

16. 散列算法

散列算法，也称为单向散列函数、杂凑函数、哈希算法、HASH 算法或消息摘要算法。它通过把一个单向数学函数应用于数据，将任意长度的一块数据转换为一个定长的、不可逆转的数据。这段数据通常叫做消息摘要（比如，对一个几兆字节的文件应用散列算法，得到一个 128 位的消息摘要）。消息摘要代表了原始数据的特征，当原始数据发生改变时，重新生成的消息摘要也会随之变化，即使原始数据的变化非常小，也可以引起消息摘要的很大变化。因此，消息摘要算法可以敏感地检测到数据是否被篡改。消息摘要算法再结合其它的算法就可以用来保护数据的完整性。

好的单向散列函数必须具有以下特性：

1) 计算的单向性：给定 M 和 H，求 h＝H(M)容易，但反过来给定 h 和 H，求 M＝H-1(h)在计算上是不可行的。

2) 弱碰撞自由：给定 M，要寻找另一信息 M′，满足 H(M′)＝H(M)在计算上不可行。

3) 强碰撞自由:，要寻找不同的信息 M 和 M′，满足 H(M′)＝H(M)在计算上不可行。

单向散列函数的使用方法为：用散列函数对数据生成散列值并保存，以后每次使用时都对数据使用相同的散列函数进行散列，如果得到的值与保存的散列值相等，则认为数据未被修改(数据完整性验证)或两次所散列的原始数据相同(口令验证)。

典型的散列函数有：MD5，SHA-1，HMAC，GOST 等。单向散列函数主要用在一些只需加密不需解密的场合：如验证数据的完整性、口令表的加密、数字签名、身份认证等。

17. 关于 MD5 和 SHA-1 等

2004 年，山东大学王小云教授攻破了 MD5 算法，引起密码学界的轩然大波。

MD5 的全称是 Message-Digest Algorithm 5（信息-摘要算法），在 90 年代初由 MIT Laboratory for Computer Science 和 RSA Data Security Inc 的 Ronald L. Rivest 开发出来，经 MD2、MD3 和 MD4 发展而来。

2004 年 8 月 17 日的美国加州圣巴巴拉召开的国际密码学会议（Crypto'2004）安排了三场关于杂凑函数的特别报告。在国际著名密码学家 Eli Biham 和 Antoine Joux 相继做了对 SHA-1 的分析与给出 SHA-0 的一个碰撞之后，来自山东大学的王小云教授做了破译 MD5、HAVAL-128、 MD4 和 RIPEMD 算法的报告。王小云教授的报告轰动了全场，得到了与会专家的赞叹。

不久，密码学家 Lenstra 利用王小云提供的 MD5 碰撞，伪造了符合 X.509 标准的数字证书，这就说明了 MD5 的破译已经不仅仅是理论破译结果，而是可以导致实际的攻击，MD5 的撤出迫在眉睫。

安全散列算法 1(SHA-1）是由 NSA 设计的，并由 NIST 将其收录到 FIPS 中，作为散列数据的标准。它可产生一个 160 位的散列值。SHA-1 是流行的用于创建数字签名的单向散列算法。

在 MD5 被王小云为代表的中国专家破译之后，世界密码学界仍然认为 SHA－1 是安全的。2005 年 2 月 7 日，美国国家标准技术研究院发表申明，SHA－1 没有被攻破，并且没有足够的理由怀疑它会很快被攻破。而仅仅在一周之后，王小云就发布了消息，说明了 SHA-1 算法寻找一对碰撞的复杂度是 2^69，而不是密码学家以前认为的 2^80。

如何理解这个结果呢？在很多报道中，包括山东大学的网站上，都说 SHA1 被攻破了，被破解了，云云。作者对这类说法持保留态度。引用王小云教授论文中的说法：

“对于 SHA0，这种攻击很有效，我们能够在不超过 2^39 次 Hash 操作中找到实际的碰撞。我们也对弱化到 58 步的 SHA1 进行了攻击，并在不超过 2^33 次 Hash 操作中找到了实际的碰撞。”

“SHA0 和 58 步的 SHA1 是作为 80 步完整 SHA1 的简化版，用来验证我们的新方法的效率的。此外，我们的分析表明，减弱到 70 步的 SHA1 的碰撞复杂度是 2^50 次 Hash 操作。基于这个估计，我们期望在现在的超级计算机上能找到 70 步 SHA1 的真实碰撞。”

所以，严格说来应该这样理解：这个结果把攻破 SHA1 的计算量降低了 2000 倍。在某些情况下，SHA1 似乎走到了不安全的边缘。

MD5 被攻破了，SHA1 也不那么安全了，怎么办呢？现在看来，还有 SHA-256 和 SHA-512 等算法可用。密码学家也在研究新的散列算法。

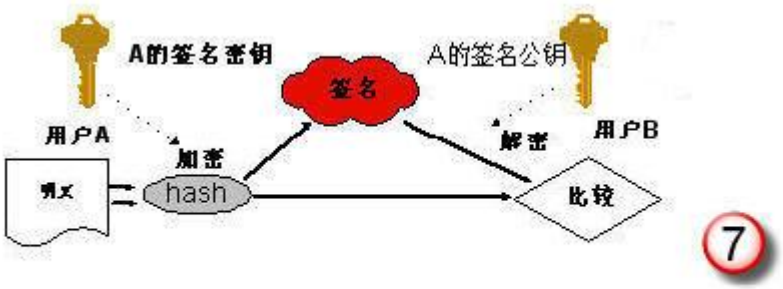
18. 数字鉴名

密码技术除了提供信息的加密解密外，还提供对信息来源的鉴别、保证信息的完整和不可否认等功能，而这三种功能都是结合数字签名技术来实现的。

简单地说，数字签名的原理可以这样理解：用非对称算法的私钥加密的内容只能用对应的公钥来解密。而私钥是不公开的。因此，如果一段信息能用某个人的公钥解密，那么它一定是用此人的私钥加密的。它和物理的签名一样，是很难伪造的。

在实际应用中，数字签名的过程通常是这样实现：

将要传送的明文通过一种函数运算(Hash)转换成报文摘要(不同的明文对应不同的报文摘要)，报文摘要用私钥加密后与明文一起传送给接受方，接受方用发送方的公钥来解密报文摘要，再将接受的明文产生新的报文摘要与发送方的报文摘要比较，比较结果一致表示明文确实来自期望的发送方，并且未被改动。如果不一致表示明文已被篡改或不是来自期望的发送方。



19. 数字证书

为了保证互联网上电子交易及支付的安全性，防范交易及支付过程中的欺诈行为，必须在网上建立一种信任机制。这就要求参加电子商务的买方和卖方都必须拥有合法的身份，并且在网上能够有效无误的被进行验证。数字证书是一种权威性的电子文档。它提供了一种在 Internet 上验证您身份的方式，其作用类似于司机的驾驶执照或日常生活中的身份证。它是由一个由权威机构----CA 证书授权(Certificate Authority)中心发行的，人们可以在互联网交往中用它来识别对方的身份。当然在数字证书认证的过程中，证书认证中心（CA）作为权威的、公正的、可信赖的第三方，其作用是至关重要的。

数字证书颁发过程一般为：用户首先产生自己的密钥对，并将公共密钥及部分个人身份信息传送给认证中心。认证中心在核实身份后，将执行一些必要的步骤，以确信请求确实由用户发送而来，然后，认证中心将发给用户一个数字证书，该证书内包含用户的个人信息和他的公钥信息，同时还附有认证中心的签名信息。用户就可以使用自己的数字证书进行相关的各种活动。数字证书由独立的证书发行机构发布。数字证书各不相同，每种证书可提供不同级别的可信度。可以从证书发行机构获得您自己的数字证书。

随着 Internet 的普及、各种电子商务活动和电子政务活动的飞速发展，数字证书开始广泛地应用到各个领域之中，目前主要包括：发送安全电子邮件、访问安全站点、网上招标投标、网上签约、网上订购、安全网上公文传送、网上缴费、网上缴税、网上炒股、网上购物和网上报关等。

20. CA

CA 是 Certification Authority 的缩写。CA 中心，又称为数字证书认证中心。CA 中心作为电子交易中受信任的第三方，负责为电子商务环境中各个实体颁发数字证书，以证明各实体身份的真实性，并负责在交易中检验和管理证书；数字证书的用户拥有自己的公钥/私钥对。证书中包含有证书主体的身份信息、其公钥数据、发证机构名称等，发证机构验证证书主体为合法注册实体后，就对上述信息进行数字签名，形成证书。 在公钥证书体系中，如果某公钥用户需要任何其它已向 CA 注册的用户的公钥，可直接向该用户索取证书，而后用 CA 的公钥解密解密即可得到认证的公钥；由于证书中已有 CA 的签名来实现认证，攻击者不具有 CA 的签名密钥，很难伪造出合法的证书，从而实现了公钥的认证性。 数字证书认证中心是整个网上电子交易安全的关键环节,是电子交易中信赖的基础。他必须是所有合法注册用户所信赖的具有权威性、信赖性及公正性的第三方机构。
CA 的核心功能就是发放和管理数字证书。概括地说，CA 认证中心的功能主要有：证书发放、证书更新、证书撤销和证书验证。具体描述如下：

（1）接收验证用户数字证书的申请。
（2）确定是否接受用户数字证书的申请，即证书的审批。
（3）向申请者颁发（或拒绝颁发）数字证书。
（4）接收、处理用户的数字证书更新请求。
（5）接收用户数字证书的查询、撤销。
（6）产生和发布证书的有效期。
（7）数字证书的归档。
（8）密钥归档。
（9）历史数据归档。

21. PGP

PGP 是 Pretty Good Privacy 的缩写。PGP 最初是 Phil Zimmermann 在 1991 年写的一套程序的名字。这套程序后来由 MIT, ViaCrypt, PGP Inc.维护和发布。现在的 PGP 由 Network Associates Inc. (NAI)作为商业软件进行销售。同时，PGP 也是一个网络标准的名字(RFC 2440: Open PGP Message Format)。在这里，我们主要讨论作为 RFC 标准的 PGP。

PGP 是一种以 RSA 等密码算法为基础，用来保护电子邮件等信息的安全性的系统。可以用它对你的邮件保密以防止非授权者阅读，它还能对你的邮件加上数字签名从而使收信人可以确信邮件是你发来的。它让你可以安全地和你从未见过的人们通讯，事先并不需要任何保密的渠道用来传递密匙。

它的加密方法用的是我们前面讨论过的算法。它与其它系统不同的地方在于它的密钥管理。

一个成熟的加密体系必然要有一个成熟的密钥管理机制配套。公钥体制的提出就是为了解决传统加密体系的密钥分配过程保密的缺点。比如网络黑客们常用的手段之一就是"监听"，如果密钥是通过网络传送就太危险了。对 PGP 来说公钥本来就要公开，就没有防监听的问题。但公钥的发布中仍然存在安全性问题，例如公钥被篡改（public key tampering），这可能是公钥密码体系中最大漏洞 。用户必须确信用户的公钥属于需要收信的那个人。

下面举个例子来说明这个问题：以用户 A 和用户 B 通信为例，现假设用户 A 想给用户 B 发信，首先用户 A 就必需获取用户 B 的公钥，用户 A 从 BBS 上下载或其它途径得到了 B 的公钥，并用它加密了信件发给了 B。不幸的是，用户 A 和 B 都不知道，另一个用户 C 潜入 BBS 或网络中，侦听或截取到用户 B 的公钥，然后在自己的 PGP 系统中用用户 B 的名字生成密钥对中的公钥替换了用户 B 的公钥，并放在 BBS 上或直接以用户 B 的身份把更换后的用户 B 的"公钥"发给用户 A。那用户 A 用来发信的公钥是已经是更改过的，实际上是用户 C 伪装用户 B 生成的另一个公钥。这样谁都不会起疑心，但这样一来用户 B 收到用户 A 的来信后就不能用自己的私钥解密了，更可恶的是，用户 C 还可伪造用户 B 的签名给用户 A 或其他人发信，因为用户 A 手中的公钥是伪造 ，用户 A 会以为真是用户 B 的来信。

防止这种情况出现的最好办法是避免让任何其他人有机会篡改公钥，但能做到这一点的是非常困难的，一种方法是直接从用户 B 手中得到他的公钥，然而当他在远在他乡或在时间上根本不可达到时，这是不可办到的。

但 PGP 提出了一种公钥介绍机制来解决这个问题，其思路是这样的：如果用户 A 和用户 B 有一个共同的朋友 D，而 D 知道他手中的 B 的公钥是正确的。这样 D 就成为用户 A 和 B 之间的公证人，用户 B 为了防止别人篡改自己的公钥，就把经过 D 签名的自己的公钥上载到 BBS 上让用户去拿，用户 A 想要取得用户 B 的公钥就必需先获取 D 的公钥来解密 BBS 或网上经过 D 签名的 B 的公钥，这样就等于加了双重保险，一般没有可能去篡改它而不被用户发现，即使是 BBS 的管理员。这就是从公共渠道传递公钥的安全手段。

说到这里也许有人会想到，只通过一个签名公证力度是不是小了点。 PGP 当然考虑到了这一点，它的办法就是把由不同的人签名的自己的公钥收集在一起，发送到公共场合，这样可以希望大部分人至少认识其中一个，从而间接认证了用户的公钥。同样用户签了朋友的公钥后应该寄回给他，这样就可以让他通过该用户被该用户的其他朋友所认证。有点意思吧，和现实社会中人们的交往一样。PGP 会自动根据用户拿到的公钥中有哪些是朋友介绍来的，把它们分为不同的信任级别，供用户参考决定对它们的信任程度。也可指定某人有几层转介公钥的能力，这种能力是随着认证的传递而递减的。

如何安全地得到 D 或其他签名朋友的公钥呢？确实有可能用户 A 拿到的 D 或其他签名的朋友的公钥也假的，但这就求这个用户 C 必须对你们三人甚至很多人都很熟悉，这样的可能性不大，而且必需经过长时间的策划。当然，如果一定要追究这一点的话，那就是由一个大家普遍信任的机构担当这个角色，他被称为认证权威机构，每个由他签过字的公钥都被认为真的，这样大家只要有他的公钥就行了，认证这个人的公钥是方便的，因他广泛提供这个服务，假冒他的公钥是极困难的，因为他的公钥流传广泛。这样的"权威机构"适合由非个人控制组织或政府机构充当----这就是我们前面讨论过的 CA。

22. 数字信封

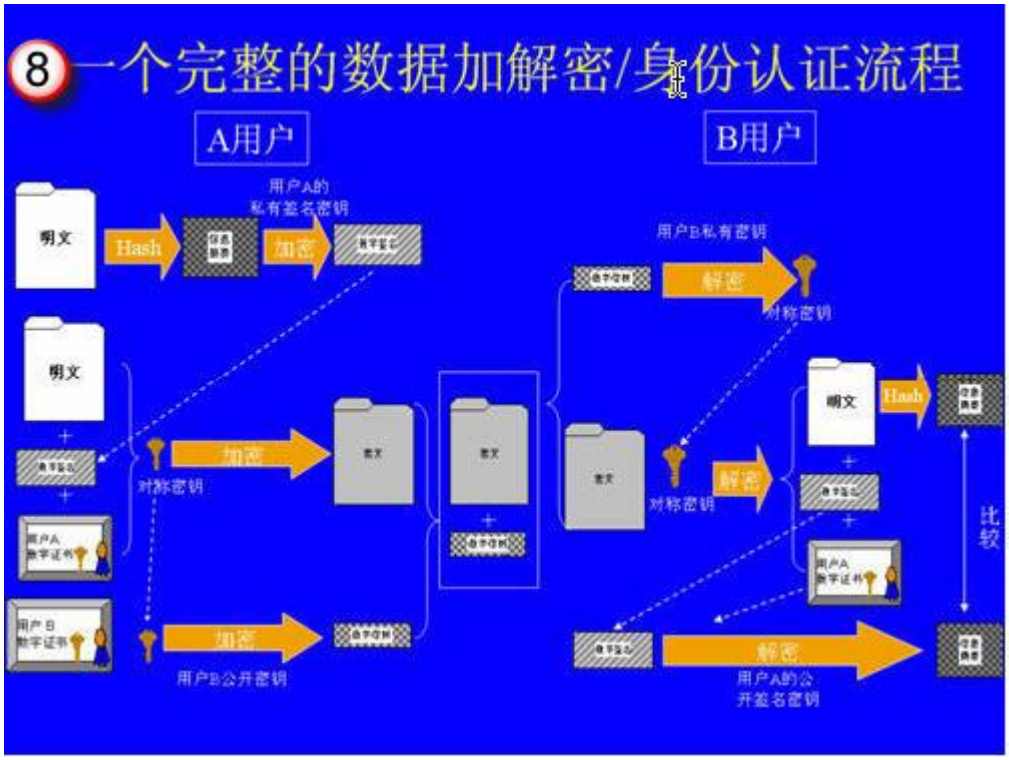
数字信封是一种综合运用对称算法、非对称算法、消息摘要算法和数字签名的消息加密机制。为什么要引入这种机制呢？这是因为：

1、对称算法速度比较快，与同等安全强度的非对称算法相比，一般要快三个数量级左右。但是对称算法需要通过一个安全的通道交换密钥（或协商密钥，或事先约定密钥）之后才能进行通信。

2、非对称算法较慢，但是它的优点是通信双方不必事先约定密钥就可以进行安全通信。

3、单纯的加密算法只能保证消息的机密性，但无法保证消息不被篡改。结合消息摘要和数字签名算法就可以保证数据的完整性，并能确认对方的身份。

具体操作如图所示。利用对称加密算法(比如 3DES)对比较长的消息进行加密，再利用接收者的证书对密钥进行加密，加密消息和加密密钥一起发送给消息接收者。后者利用自己的私钥对加密密钥解密得到密钥，接着用密钥对加密消息进行解密得到消息原文。与数字签名一样，消息的发送者不会涉及任何保密内容，只要知道接收者证书的人都可以向他发送数据信封封装消息。



23. 椭圆曲线算法

当今使用的非对称算法根据其基于的数学难题可大致分为三类：

1）整数分解（IF）体制，其安全性基于整数分解问题的难解性，典型例子是 RSA 体制和 Rabin 体制。

2）离散对数（DL）体制，其安全性基于（一般）离散对数问题的难解性，典型例子是 DSA 体制、ElGamal 体制和 Schnorr 体制。

3）椭圆曲线（EC）体制，其安全性基于椭圆曲线离散对数问题的难解性，典型例子是 ECDSA 体制。

椭圆曲线密码是在 1985 年由 Neal Koblitz 和 Victor Miller 独立提出来的。近年来，椭圆曲线体制由于其具有的很多技术优势，而受到越来越多密码学者的关注，逐渐形成了一个研究热点。它已被诸如 ANSI（American Natio nal Standards Institute）、IEEE（Institute of Electrical and Electroni cs Engineers）、ISO（International Standards Organization）和 NIST（National Institute of Standards and Technology）等标准化组织纳入为标准。它的技术优点包括：

1）安全性能更高：椭圆曲线离散对数问题的计算复杂度目前是完全指数级的，而 RSA 是亚指数级的。

2）计算量小和处理速度快：在相同的计算资源条件下，椭圆曲线体制比 RSA 和 DSA 有更快的处理速度。

3）存储空间占用小：椭圆曲线体制的密钥尺寸和系统参数与 RSA 及 DSA 相比要小得多。160 比特 EC 与 1024 比特 RSA、DSA 具有相同的安全强度，210 比特 EC 则与 2048 比特 RSA、DSA 具有相同的安全强度，这意味着它所占的存储空间要小得多。

4）带宽要求低。

椭圆曲线体制中最著名的是 ECDSA，它是数字签名算法（DSA）移植到椭圆曲线上得到的。在所基于的群是一般群和所用的 Hash 函数是抗冲突的假设下，它已被证明是安全的。它的系统参数中

选择的椭圆曲线的阶是近乎素数的，且它的签名长度至少为 320 比特。

24. 未来发展方向：量子力学与信息安全

物理学从经典物理学发展到相对论，又发展到量子物理学，每一步都使我们对世界有更深刻的理解，并带来新的技术进步。在信息安全方面，量子物理学以意想不到的方式带来了全新的思路和技术。

量子物理技术在密码学上的应用分为两类：一是利用量子计算机对传统密码体制的分析；二是利用单光子的测不准原理实现通讯过程中的信息保密，即量子密码学。

下面对这种新的方向作一个简要的介绍。

25. 量子计算机

1996 年，美国《科学》周刊科技新闻中报道，量子计算机引起了计算机理论领域的革命。同年，量子计算机的先驱之一，Bennett 在英国《自然》杂志新闻与评论栏声称，量子计算机将进入工程时代。目前，有关量子计算机的理论和实验正迅猛发展。

与经典计算机相比，量子计算机最重要的优越性体现在量子并行计算上。因为量子并行处理，一些利用经典计算机只存在指数时间算法的问题，利用量子计算机却存在多项式时间算法。这方面最著名的一个例子当推 Shor 在 1994 年给出的关于大数因子分解的量子多项式算法。

大数的因子分解是数学中的一个传统难题，现在人们普遍相信，对于经典计算机，大数因子分解不存在有效的多项式时间算法。这一结果在密码学中有重要应用，著名的 RSA 算法的安全性就基于大数因子分解。但 Shor 却证明，利用量子计算机，可以在多项式时间内将大数分解，这一结果向 RSA 公钥系统的安全性提出了严重挑战。

不过，量子计算机的实验方案还很初步。现在的实验只制备出单个的量子逻辑门，远未达到实现计算所需要的逻辑门网络。但是，总体来讲，实现量子计算，已经不存在原则性的困难。按照现在的发展速度，可以比较肯定地预计，在不远的将来，量子计算机一定会成为现实，虽然这中间还会有一段艰难而曲折的道路。

26. 量子密码

量子计算机对传统密码技术带来严重挑战的同时，也带来了全新的量子密码技术。

上世纪下半叶以来，科学家在“海森堡测不准原理”和“单量子不可复制定理”上，逐渐建立了量子密码术的概念。“海森堡测不准原理”是量子力学的基本原理，指在同一时刻以相同精度测定量子的位置与动量是不可能的，只能精确测定两者之一。“单量子不可复制定理”是“海森堡测不准原理”的推论，指在不知道量子状态的情况下复制单个量子是不可能的，因为要复制单个量子就只能先作测量，而测量必然改变量子的状态。

量子密码术突破了传统加密方法的束缚，以量子状态作为密钥,它具有不可复制性。任何截获或测试量子密钥的操作，都会改变量子状态。这样截获者得到的只是无意义的信息，而信息的合法接收者也可以从量子态的改变，知道密钥曾被截取过。与公开密钥算法不同，当量子计算机出现，量子密码术仍是安全的。这与以数学为基础的传统密码学不同，传统密码学的安全是一种相对的安全。而量子密码术是建立在物理定律基础上的，以人类现在所掌握的知识看来，似乎可以说是“绝对安全”了。

具体通信过程如下：

在发送者和接收者之间传送量子密钥的一种方式是，激光发射以两种模式中的一种极化的单光子。在第一种模式中，光子垂直或水平摆放（直线模式）；在第二种模式中，光子与垂直线呈 45 度角摆放（斜线模式）。

发送者（密码学家通常称之为艾丽斯）发送一串比特序列（量子振动的方向，即它们的偏振态，代表 0 或 1，形成一连串的量子位，或称量子比特）。随机选择光子直线或斜线的传送模式。接收者（在密码学语言中称为鲍勃）同样随机决定对接收比特的测量模式。海森伯的测不准原理表明，鲍勃只能用一种模式测量光子，而不能同时使用两种模式。只有鲍勃测量的模式和艾丽斯发送的模式相同，才能保证光子方向准确，从而保留准确数值。

传送完成后，鲍勃告诉艾丽斯，他使用哪种模式接收每一个光子，这一过程无须保密。然而，他不会透露每个光子代表的 0 或 1 的数值。然后，艾丽斯告诉鲍勃哪些模式是正确的。双方都将接收模式不正确的光子视为无效。正确的测量模式组成一个密钥，作为用来加密或解密一条信息的算法的输入值。

如果有人试图拦截光子流（称她为伊芙），海森伯的原理使她无法用两种模式同时测量。如果她用错误的模式对某一光子进行测量，必然会发生误差。通过对所选光子的比较和对误差的检查，艾丽斯和鲍勃就能够发现窃听者的存在。

27. 作者原创软件“我的地盘”，请大家支持！

您有没有遇到过这样的情况：电脑中保存的客户资料、财务数据、私人日记、聊天记录、图片电影……等重要文件被人偷看，给您带来巨大的损失？

从今天开始您不用再担心，“我的地盘”为您排忧解难！

“我的地盘”是一款安全强度高并且又简单易用的磁盘加密软件。它会给你的电脑增加一个加密盘，存放在这个加密盘中的所有内容会自动加密。每次加密盘使用完毕以后，您可以让它从计算机中消失，只有拥有正确密码才能让它重新出现。

“我的地盘”不同于那些采用隐藏方法进行加密的软件。它由安全行业专业人士开发，采用 AES、SHA256 等高强度密码算法，达到了金融行业的安全强度。

有了“我的地盘”，您的电脑中就有了一个牢固的保险箱，就有了一片真正属于您自己的空间，任何人都无法再窥探您的隐私。

“我的地盘”让您高枕无忧！

作者 Email：JimmyFan@FlagWare.net Banner@FlagWare.net
作者网站： http://www.FlagWare.net