PGP & GPG

Email for the practical paranoid

By Michael W.Lucas

序言

介绍

许多人一听到数据加密就觉着繁琐，甚至有些恐慌。（或者说高大上？？）。毕竟，加密技术一直是军方，商业的秘密。电影和小说使用加密作为他们的情节需求，完全忽视加密在现实中是如何运作的。而那些对密码学感兴趣的人，直接扎到那些繁琐的数学公式上面去，其中对于那些没有很深数学背景的人来说，那些繁琐数学公式足以让你打退堂鼓（- -！）。所有的这些都归咎于围绕着密码学的一股神秘气息（迷之微笑^ ^!）。

说实话，现代密码学背后的数学知识真的很难，很难，很难。但是（敲黑板），运用那些别人已经写好的工具去做那些密码相关的事情却是不难的，如果你知道一些基本的使用方法，什么场合使用什么密码技术（就像使用Word一样简单。哦耶！。。不过Word好像也很难哦。。。。）。这本书，PGP&GPG，将会一步一步的带着你走进密码和电子签名的世界（现在不理解也没关系，这不马上要学习嘛。）。还会教你如何使用工具（这就是我们跟猴子的区别！），这样，当你跟人分享信息的时候，你可以确信你的信息是安全的！

这本书不是要列出密码技术的方方面面。它不会教你如何手算出公钥，也不会涉猎所有的现代密码算法。但是，它将充分的介绍加密和数字签名背后的想法，使你能够明智地选择在不同特定情况下应使用哪些算法。我也会展示如何把加密算法，电子签名这些技术和邮件结合起来，这样你就可以很容易的和别人安全的交流。还有如何安装Pretty Good Privacy（PGP）（自己查查到底什么意思，有助于理解。），和Gnu Privay Guard（GPG），在你的电脑上，包括Windows，或者是Unix-like 操作系统。最后，如何使用这些工具保证你的个人信息的安全。（没错，我说的就是你硬盘里的种子。^ ^）。

NOTE：PGP 是OpenPGP标准的实现，GPG是一种免费的同样标准的再实现。如果你不知道上面那句话是啥意思，那就对了。。如果你知道上面那句话的含义，直接看第一章吧。

OpenPGP的故事还得从很多年前说起。（放心，不是历史课）。

PGP的故事：

加密是一门很老的科学，随着计算机越来越强大，研究加密的人也越来越多。政府官员越来越担心加密技术的普及。虽然加密技术对老百姓来说是有效的用途的，但它也是犯罪分子的强大工具。1991，第266条条例草案（说的当然是美国啦。），提到一条说，所有的加密工具都要有政府后门（简单来说，他们可以操控这些加密工具）。尽管这条法案当时还在商量中，Phil Zimmermann这个人结合好几种常用的算法，写入了一个软件，也就是Pretty Good privacy，即PGP。PGP背后的思想，在当时，那些计算机学家，数学家早就知道很多年了，所有它的概念没有什么创新性。但它这个最大的创新就是它这个软件可以被任何人在个人计算机就可以使用！！早期的PGP版本就可以拥有军用级别的加密技术！尽管266条草案一点点要成为法律条款，Phil Zimmermann的一个朋友尽很大的努力把PGP这个软件广泛传播出去，赶在这个条款合法化之前。这个PGP软件在互联网上大范围传播。他们的积极行动终于把“禁止加密“条款虐杀在摇篮中。

Phil Zimmermann，一个反核的倡导者，相信PGP对于那些持有不同政治意见的人，反政府武装的人，还有那些因为他们的信仰会给他们带来很大风险的人，将有很大的帮助。也就是说，对于全世界的人都有帮助。自从第二次世界大战，美国政府就把加密技术看成一种对国家安全的威胁。并且不允许它在美国传播（想了解更多的话，在[www.wikipedia.org](http://www.wikipedia.org)看“Export of Cryptography词条，反正我没看过）。有些国家是不容许这样加密软件进入他们国家的。这些条例也被称作ITAR（International Traffic in ArmsRegulations），并且把加密技术视为战争武器！！

Phil Zimmermann决定绕过这项规定，那要怎么做呢？用咬文嚼字的方法钻法律的空子。就是用代码和软件概念上的区别。

Phil Zimmermann起先用源代码的方式写的这个软件，就像我们每天写的文本一样。然后用电脑工具把这些源代码转换为机器代码。计算机领域都是这样的方式。源代码不是软件，就像汽车蓝图不是汽车一样。但是源代码和汽车蓝图对于最终产品都是必不可少的。然后呢，Phil Zimmermann把源代码直接以书的形式分享出去。（你他娘的真是个人才。。）

书籍可不是软件，即使书里面有源代码，机器可以用这些源代码生成软件。而且书籍可不是武器！（作者在这里写了条小note，说那些把计算机专业书砸到脚上的人可不这么想。哈哈，我解释一下：是因为计算机专业书一般都很厚，动不动就得1千多页。女生可以用来防身哦。哈哈）。不过尽管针对密码学的书是有出口限制的，Phil Zimmermann还是把他的书推出了海外。所以世界上的人就可以根据书上的代码搭建他们自己的PGP软件。他们很快的从这些说明中构建了软件，并且PGP迅速成为全球的数据加密标准。

正如你可能猜测的那样，美国政府认为这种行为仅仅是解决出口限制的一种手段。Zimmermann 还有他的支持者把书里写的言论视为自由言论（Free Speech），归为第一修正法案。然后美国政府就起诉了，在接下来的三年里，Zimmermann去了几次法庭。

这场官司把Zimmermann变成了计算机领域的英雄！很多人就下载PGP软件看看到底是啥玩意。然后有一部分人最后就用上它了。Zimmermann的法律辩护基金甚至进一步传播了PGP诉讼的消息。在国会听证会上，Zimmermann读了他从来自压迫政权和战乱地区的人民的邮件，说PGP拯救了生命，为公众做出了巨大贡献，使他意识到他的工作有多宝贵。还有，PGP软件在书出版之前就已经在互联网上可以下载了。那本书仅仅是一个合法的幌子，让它能够在海外的人也能用上。

OpenPGP：

即使没有美国政府在其中作祟，PGP还是有一些技术上的问题，是被一些专家提出来的。其中最明显的就是，PGP大量的用了受专利保护的RSA和IDEA算法。所以任何人想把PGP商业化使用，需要上缴专利费。许多科学家认为这样不行。因为他们想要一种可以公共使用还可以商用的加密系统，条件一定要免费！

Zimmermann在1998年提供了一个解决方案。他的公司，PGP Corporation，提交了一个改进PGP的设计，名字为OpenPGP。OpenPGP定义了标准，使不同的程序可以自由并且安全的交流，采用的是一种改良PGP协议的版本，还包括很多不同的加密算法。这样的结果可以让人们和公司写出自己的符合OpenPGP的程序，能让这些程序满足他们自己的需求。（私人定制啊！）

!!!!!!!!现在是23：46了，好累。已经坐在沙发上写了好几个小时。但才翻译到21页，还有200来页呢。。。我真的能翻译完吗？？明天我在努力吧。

OpenGPG有多安全：

OpenPGP标准被认为是军事级别，最尖端的安全系统。尽管你看到所有的安全产品都用这些词，，，OpenPGP确实很安全，它被多国政府，大型工业厂商，安全专家所信任。（总之就是很安全的意思）。

但上面那句话也不是说OpenPGP完全解决了计算机安全。错误的使用OpenPGP可以让你相信你是安全的，当事实上你不是的时候。就像你出去度假，忘了把大门锁上。不好的计算机管理就像把大门锁上，但把钥匙放在垫子下，给任何人找到的机会。

还有，拥有足够的计算能力，是有可能破解OpenPGP中的加密算法的。NSA（没错，斯诺登泄密的那个，什么？你不知道斯诺登？刚从山洞出来？？维基一下）据谣言说他们有特殊的计算机专门破解这些加密算法的。当然了，如果有人愿意花费几百万美元得到你的信息，还有其它更简单的方法，没必要破解加密的。所以，当正确配置好OpenPGP，OpenPGP足够强大，足以让人们选择另一种违反隐私的方法，而不是试图破解加密。

**术语用法**

PGP，GPG还有OpenPGP？晕头转向了？没事，现在就解释一下。

* PGP只是指PGP公司（还记得吗，之前那个创立的公司）的产品。如果你看到PGP这个词，它只是指那个产品，不是GPG，或者其它OpenPGP标准的产品。如果你把其他产品称作PGP，PGP的朋友们会不高兴的。- - ！
* GPG是Gnu privacy guard tool（自由软件基金会写的一个工具）。如果你把他们的产品叫为PGP，他们会不高兴的。
* OpenPGP这个词对PGP，GPG，还有其它PGP的产品都是适用的。对，还有其它符合OpenPGP标准的产品。许多厂商把OpenPGP的功能集成到他们的产品里面。但是PGP，GPG是最出名的。如果你把他们的产品称为OpenPGP，没有人会不高兴的。^ ^

现在的PGP公司：

今天，PGP公司是密码学和信息安全领域的主要参与者，为许多不同的平台提供PGP软件，从PC到手持设备甚至黑莓手机。PGP公司的软件保证了从电子邮件到即时消息到病历的安全。

PGP公司提供了OpenPGP标准的产品，并且可以运行在很多流行的操作系统上。它提供的PGP系统可以流畅的与邮箱结合。

PGP是一个商用软件，PGP公司提供全方位的相关支持服务。我们将会讲PGP桌面版。因为PGP是一个商业产品，所以你要花钱哦。（什么，你要免费的？早说啊，要不我就不翻译这段了。那看下面）。

GPG是什么东东？：

GPG就是一个免费的OpenPGP标准的产品。Windows，unix-like，包括苹果的系统都是可以使用的。

因为GPG是符合OpenPGP标准的，它可以和其它使用符合OpenPGP标准产品的人交流。免费就是说你可以免费得到它，并且你是可以查看它的源代码，当然了，对于大多数人来说是没用的。但是，对于那些想要对源码修改的人来说是很重要的。（free 不好翻。懒得揣摩了。原谅我直接简单翻译了。。）。

PGP 和 GPG：

GPG免费，PGP得花钱。那为什么不一直用GPG呢？里面有几条原因。考虑的方面包括：操作简单，支持，透明度，支持的算法。下面就逐个介绍一下，然后选好你到底要用哪个。

简单使用：（ease of use）

要想用GPG，对于命令行你得不发怵。尽管各种GPG插件提供了友好的用户界面，但它们并未与主要产品紧密集成。当GPG更新的时候，那些插件可能不更新。我反正是不可能让我的爷爷用GPG，除非我真的很想一星期跟他聊5天。

PGP公司花费了很多努力让他们的产品对用户友好，就像其他桌面应用一样。如果我需要给销售部，市场部，会记部门安装加密软件，就用户友好这一条，我就会直接选择PGP。

支持：

PGP公司拥有很大的支持机构。你可以直接打电话咨询他们，还有一整个咨询团队来解决你的问题。当你买了PGP软件，你可以有30天的免费安装，还有安装支持，对于大多数人，足以可以基本使用PGP软件。后续支持就得花钱了。

GPG支持机构，就是典型的自由软件。用户得自己去读手册，访问他们的网站，然后再邮件询求帮助（就是不能做伸手党，有问题，自己试着解决）。没有电话寻求帮助。如果你是那种遇到问题，就给他们打电话，开撕，直到他们解决你的问题。那GPG不适合你。

一般来说，阅读本书将为您提供在日常沟通中使用任何一款软件所需的一切。尽管你可以会找到一个极端问题，那个有可能就是程序错了。如果你碰到这样问题，其他用户很有可能也遇到过，你可以上网查一查。我觉得网上的答案比电话询问要快的多。

透明度：

透明度是指这个软件有多少是可见的。对于大多数人来说，这不是重要的。----他们只是想这个软件正常工作就可以了，不会让系统崩溃，或伤害到他们的数据。你很可能就是这个类别的。但是，在安全领域，透明度是非常重要的。

那些在乎安全的人，（--比如数十亿美元或许多人的生命依赖于在这个信息保持隐秘），专门花钱雇专家来审查他们的软件。审查代码，和算法的流程也叫做审计。

加密是一门古老的科学。它其中一个规则就是，知道加密算法是如何运作的，并不能帮助你破解它。那些可以供公众审计的加密方案是那些密码专家唯一重视的。OpenPGP背后的密码学已经被不断审计10多年了。如果能找到OpenPGP中的问题，你在密码学界肯定就会出名了。就像你造了一辆高性能汽车，并且一加仑汽油可以跑100英里，在汽车领域的轰动。这两者看着都不太可能，但很多人都去尝试。

但是，PGP和GPG不仅仅是加密算法。其中有很多都是其它代码。那些坏人可以利用那些其他代码，找到代码的漏洞，然后攻破软件所提供的安全。那些源码需要技术人员去审计，以确保他们的安全。GPG的源码谁都可以审计，全世界不同技术水平的人都可以。PGP的源码只能被它的消费者审计。但许多消费者都会雇专家来帮他们审计。

算法支持：

早期的PGP用的是那些被申请专利的算法。现在其中有些算法已经属于公共了，但其中一个（IDEA）在欧洲还是被专利保护的。OpenPGP没有用那些算法。你不用了解IDEA是什么，但你得能分辨出来，如果你之后碰到的话。

GPG不支持IDEA，因为IDEA不是完全免费的。（！！后面那段话没啥用，我就不翻了。好吧，我还是很懒的。）。

OpenPGP和相关法律：

OpenPGP使用了一些很强大的公开密钥加密算法。而且是真的强大。那些执法人员也不能攻破那些由GnuPG妥善保护的文件。有些政府不希望他们的公民拥有如此强大的保护。有些国家允许他们的公民使用强大的加密算法，但是必须是可以攻破的。有些国家要求必须把密钥上缴国家，所以如果你以后变成罪犯，他们可以用你的密钥来解密你的数据。

咨询当地法律把。（我也不知道咱国家是啥态度。不过好像中国人不怎么在意隐私。）

本书内容：

尽管这本书不会全面介绍密码学，但确实包含了一大部分OpenPGP，PGP，GPG的相关内容。

1. “密码学入门启蒙“（就相当于上幼儿园一样。哈哈）包含了加密的基本思想。我将会讨论OpenPGP使用的简单加密种类。把加密系统和代码区分开的是什么。还有你应该什么场合使用什种类的加密技术。
2. “了解OpenPGP“将会教你OpenPGP的基本思想。我会谈到Web of Trust（一个相互信任的圈子，要不然我怎么知道你就是你？）keys，subkeys，keyrings和keyservers（我觉着还是了解英文比较好，不能瞎造词）。我也会讲如何安全的管理你的密钥。如何让你的密钥得到签署或撤销，以及如何让你的密钥公开可用。
3. “安装PGP“将会引导你安装PGP桌面版
4. “安装GPG“将会引导如何安装GPG在你的电脑上，包括Windows操作系统，和Unix-like系统
5. “The Web of Trust“将会讨论OpenPGP密钥是如何联系到一起的，身份验证和签名密钥。这可能是OpenPGP使用最重要的一部分。真正的安全不是来自软件，而是来自人。不幸的是人也是安全系统里面最薄弱的环节。。就像一条锁链最强的能力是来自于最脆弱的一环。- -）。在那里我将会讨论好的方式和坏的方式去处理签名密钥。
6. “PGP密钥管理“让你通过PGP软件管理Web of Trust。
7. “GPG密钥管理“向你展示通过GPG管理Web of Trust。
8. “OpenPGP和邮件“讨论如何把OpenPGP整合到你的邮箱中（其实这么说不对，我也不知道怎么翻比较好，但是你get the idea）。还有一些邮件配合PGP的使用问题。比如加密信息的备份等。
9. “PGP和邮件“讨论如何使用PGP软件来收发邮件
10. “GPG和邮件“包含整合GPG到不同邮箱中。
11. “其它OpenPGP注意事项“向你展示如何解决一些OpenPGP的使用问题。如何在圈子中使用OpenPGP。还有利用一些GPG和PGP其它的重要功能。

别浪费我宝贵的时间了，我到底需要读哪些章节？

这本书包涵了两个不一样实现的同一加密系统。你只需读你感兴趣的那部分就可以。但是哪部分是哪部分？？

仔细阅读关于PGP和GPG的讨论，前面已经提到过了。然后你做决定。

如果你想用PGP，看那些关于OpenPGP，和PGP的章节。章节：1-3，5-6，8-9，11。

如果你想用GPG，看那些关于OpenPGP，和GPG的章节。

章节：1-2, 4-5, 7-8, 11。GPG的章节会比PGP更多。因为用GPG的朋友必须学的更多。

当然，如果你想都了解，把整本书看完。也不是很长嘛。200来页。也许某一天你会很高兴你今天的决定的。

第一章

使用OpenPGP，你不需要完全了解现代密码学。但你需要了解其中基本知识。你也必须要知道OpenPGP提供哪些保护和哪些没有提供。这章将会提供密码学背后基本思想的简单介绍。

OpenPGP能做什么：

这个章节的其余部分将会介绍OpenPGP是怎么做好它的工作的。通过结合Hash（哈希），公钥加密，数字签名，OpenPGP允许你实现一定的机密性，完整性，不可否认性和真实性。这些术语都有特定的意思，我们会在后面讨论的。作为终端用户，你应该了解OpenPGP是如何工作的，这样你就知道它的局限性。

OpenPGP只能做六件事情，而这六件事恰恰是现代email架构所缺失的，但在特定场合却是至关重要的。你使用OpenPGP做什么取决于你想完成的六项任务中的哪一项。下表1-1.

表1-1 密钥的用法

|  |  |
| --- | --- |
| 期望效果 | 要做的 |
| 我想要任何阅读这条消息的人都知道这是我发的。我没法否认它。 | 用你的私钥对这条信息进行数字签名。 |
| 我想要验证发送数字签名过的消息的人的身份是否就是他口中的他。（就像我怎么确认你就是你口中说的你） | 用发件人的公钥验证签名。 |
| 我想要给收件人发消息，并且只有他能读。 | 用对方的公钥给信息加密。 |
| 我想要解密我收到的消息。 | 用你的私钥给消息解密。 |
| 我想要给收件人发消息，只有他能读，而且我还想让收件人知道，这条消息肯定是我发的。 | 用对方的公钥给信息加密，用你的私钥给这条信息进行数字签名。 |
| 我想要解密，验证这个有数字签名的信息 | 用你的私钥给信息解密，用对方的公钥验证数字签名 |

当你不知道怎么做的时候，看看这个表格。虽然密码学可以以多种方式使用，但这个表格涵盖了几乎所有常见的OpenPGP用法。

让我们看看OpenPGP是如何做到这些的。

Note：原文是这么写的。When in doubt, consult this table当我看到前半句，我想起了另一句话。顺便给广大男同胞一个建议。When in doubt，kiss the girl。Don’t let go。我终于失去了你（挺好听的，李宗盛的更沧桑，赵传的，也不错）。^ ^.

术语：

术语比如code（暗号），cipher（加密的算法），cryptosystem(密码系统)，encryption system（加密系统）。Encryption（加密），encoding（编码）。许多人认为他们是一样的。大多数人都错了。你不需要精通密码学的语言。但，在我们开始之前，我们需要就我们要用的词汇达成一致。

明文和密文：

密码学对信息特供保护。这条信息可以是email，你公司的财务报表，你家狗的照片，或其它任何东西。在没有加密的状态下，这条信息也被称为明文，大家可以不借助任何特殊的软件就可以看的。（当然了，照片的话，你当然需要合适的软件去浏览，但是它一般都是可以看的）

在明文被加密后，大家看得就是密文。举个例子，如果你用专门看照片的软件看加密过的照片，你看到的只是一堆乱码。

举个例子，下面是一个明文信息，某些人几十年前会非常乐意拦截：

|  |
| --- |
| Attack pearl Harbor December 7 |

如果你用OpenPGP对这条信息进行加密成为密文，它就会变成下面这样：

|  |
| --- |
| -----BEGIN ①PGP MESSAGE-----  Version: ②GnuPG v1.4.0 (③FreeBSD)  hQEOA2HvKhYFm1VREAP/QlSUVjc89OHbalb6+MNceJdJjaVb2FGZGFSowg1IkCYr  b+wjMY4z0HoPty1hzW1wqPsWSiMLxZl24HQWWOPan8K2+LesErqeig4HEbMP23u4  QdUv4iOq9T1hoNvVb0IypXluMIquze2r8r+X3hllwqAOn9ahz5VnVKj/OVnQi80E  ... |

你猜猜这是啥，祝你好运。尽管读者可以很容易看出这个①是OpenPGP加密过的，用的是②加密软件，运行在③操作系统上。但这些信息对于偷窥者而言都是没用的。当然，从坏蛋的角度来看，他确实可以知道关于你电脑的一些信息，进而利用这些信息攻击你的计算机，但那确是另一套技能。（感兴趣的可以看看Hacking Exposed 7th中文版也叫黑客大曝光）

（这里跳了一小段，我觉着没啥大用，就不翻译了。感兴趣的，原书P15，Codes）

Ciphers（看下面解释吧）：

Cipher就是把信息的内容按某种方式打乱各个字符的顺序。大多数孩子玩的Cipher就是把字母表中的字母与数字匹配。（A=1，B=2，C=3.。。。。）然后把整个信息写成一串数字而不是字母。

当然了，这种是一种非常糟糕的加密方式。它不仅广为人知，即便是那些不知道这个加密方式的密码学家，只需通过计算加密文本中各种数字的出现频率以及知道平均明文字母出现的频率来解密中等密文。

Hashes（哈希）：

哈希就是一种专门的对信息的数学计算。哈希是OpenPGP非常重要的工具。如果原来的信息发生改变（哪怕是少了个空格），这条信息的哈希值就会完全不同。比如说，“Attack Pearl Harbor December7”有以下哈希值（用的是SHA1算法）：

|  |
| --- |
| e8e0ee9cdc6cd03c880b5870983bb02d48fceaea |

很难看对吧？假设有人把这条信息改为“Attack Pearl Harbor December 6”, 就这一个数字的改变，将会有不同的哈希值：

|  |
| --- |
| 07937cc5fd92504006f5f192d95cf8d341a26d18 |

尽管你不会注意到这一变化，但是哈希值的比较将会让你注意到这一变化。

你不能从哈希值中复原明文。给定一个哈希值，没有捷径来生成一个匹配该哈希值的文件。

你可能也会看到checksums（校验）这个词，它是一个校验的算法，跟哈希相似。Checksums比哈希值生成要简单，只是做一些基本的检查。

Cryptanalysis（密码分析）：

尝试着在没有密钥的情况下，解密密文也被叫做密码分析。更复杂的密码以特定的方式重新排列字母或彻底改变明文，以便它能够抵抗诸如字符计数之类的方法的分析。

一般来说，通常，加密方式将明文与密钥组合以生成密文。而密钥的种类取决于将密钥和明文生成密文的算法。同样的，你可以用密文与密钥结合生成明文。

PGP密码学的目标：

OpenPGP的加密系统有三个基本特征：confidentiality（机密性），integrity（完整性），和nonrepudiation（不可否认性）（下面都会提到）。这些特征结合起来提供authenticity（真实性）。

Confidentiality（机密性）：

机密性是指信息内容是私密的。没有必要的密钥，算法，和工具是不能读到其中的明文的。在很多情况下，你不能防止别人读到你的密文，因为数据会从互联网上传输，信息可以被很多人看到。就像你放在信封里的信会被那些好奇的坏蛋打开看。但是，密文在没有密钥的人看，就是一堆乱码。当人们提到加密的时候，第一个想到的就是机密性。

Integrity（完整性）：

完整性是指保持信息原有的样子。通过使用OpenPGP你可以确认信息在传输的过程中没有被修改过。

在很多电脑系统，比如说常见的办公室环境，那些系统管理员不仅有查看文档的能力，还可以直接修改他们。当然了，大多数系统管理员都是不会那么做的。幸运的是，OpenPGP所提供的完整性会提示收件人，这条信息是否被修改过了。

Nonrepudiation（不可否认性）：

不可否认性指的是，一个人不能否认对这条信息进行了数字签名，这个能力在收发email中很重要。

比如有一天你的老板收到了一条看似来自你的email，里面包含你的辞职信，还有如果他不给你一堆补贴，你就要把他的一些特殊照片发到网上去。你可能会说，这邮件不是我发的，是假的。换句话说，你想否认你发的这条邮件。如果这条邮件没有用你的OpenPGP进行过数字签名，他很难证明是你发的这条邮件。但如果上面有你的数字签名，你是没办法否认的。

单凭这不可否认性就使其值得使用OpenPGP了。如果别人知道一般你发的email都是有数字签名的，他们就会知道，没有数字签名的email基本上就是假的，尤其是写的不符合你风格的内容。（当然，别人是有可能偷你的私钥，我们会在第二章讨论如何避免）

Note：在你情绪波动大的时候，不要给你的邮件数字签名。或者说别发。（这就是为什么酒壮怂人胆？表白就靠这个啊。：P）

Authenticity（真实性）：

想想以上那些效果全部同时发生。当你收到一个用OpenPGP加密过，并数字签名过的邮件，你就知道邮件的内容是任何窃听者都不能看到的。你还知道邮件内容是不没有被改变的。你还知道，该邮件来自有权以发件人的名义发送此类邮件的人。这条邮件肯定是真实的。坏蛋是没法做手脚的。（互联网上充斥着坏蛋，小心哦）

加密算法：

加密算法就是一种把密文转化为明文，在转回去的一种方法。算法的范围从简单到可怕的复杂。。。那些更能抵制密码分析破解的算法也被称作更好，更强的算法。不同的算法也有不同的密钥。（就像钥匙一样）

计算机代码最具有代表性的单元就是bit（比特）。当然这个词经常会被那些不知道自己在干什么的人说来说去。比如：“这个网站用了128-bits的加密算法，它肯定是安全的。” “我用的仅仅是40-bits的加密算法，我肯定是不安全的”。 Bits的数量仅仅是密钥中0，1的长度。一个有40个0和1组成的密钥也被称作40-bits密钥。去猜测一个密钥，你必须尝试每一个0和1的每个组合。由于40位密钥有数十亿个可能的值，因此猜测所有可能的密钥需要很长时间。一个128位密钥拥有大约300万亿的可能值，使得猜测密钥更加困难。随着计算机越来越快，破解的时间也在下降，但是还是超过了人类的生命时间。

大多数密码分析专家都不会去尝试暴力破解密钥。然而，他们直接分析破解算法。如果你有一个128位的密钥，但是你的算法不能很好地利用这个密钥，那么是有可能在没有密钥的情况下解密密文，或者猜测加密文本中的大部分密钥。如果你的密钥是40位的，但是因为算法中有一些漏洞，你可以自己猜出30位，那么剩下的猜出10位就变得很简单了。10位的组合，只有1024种组合，计算机可以很快的算出所有组合。事实上，安全性更依赖于所使用的算法而不是使用的位数。有些80位密钥的算法比一些160位密钥的算法更安全，可靠。

算法有很多不同的特点，其中大多数对于用户来说都是不相关的。但是你需要了解两种基本类型的算法：对称加密，非对称加密。

对称加密算法：

对称算法使用单个密钥进行加密和解密。上面提到的小孩用的替换加密算法就是一个非常简单的对称加密算法：把每一个字母替换为一个数字。一旦你有了这个密钥，你就可以加密，解密消息。当然你可以很容易改变密钥：你和收件人可以用 “A=9，B=&。。。“，然后加密同样的消息，生成不一样的密文。尽管坏蛋可以破解你之前的密文，得到旧的密钥。但他们还得重新来过，如果你改变密钥。大多人说的加密，一般都是对称加密算法。

用对称加密算法一个难点就是，你需要一个安全的方式把密钥让对方收到。但是，如果你有一个安全的方式发送密钥，那你就根本不需要加密，直接传输信息就可以了！！！如果你在使用互联网，那你根本就没有安全的路径发送密钥。互联网一直被监视的（我现在工作的地方，就是让我做一些协议解析的工作，抓到的数据包，分析然后还原文件。。所以你以后发送一些你不想让别人看到的信息，还是加密吧。那怎么做？继续往下看^ ^）

非对称加密：

非对称加密算法比对称加密算法要不容易破解。非对称加密采用不同的密钥进行加密，解密。你可能在以前电视剧上看到过，人们把一整块玉，分成二半，所以二个没有见过的人，都可以从拼合的玉，知道他们就是互相要找的人。你加密信息用一个密钥，解密的时候得用另一个密钥。你用哪个密钥加密还是解密都是可以的。如果你用密钥A去加密信息，收件人必须用密钥B去解密信息。但如果有人用密钥B去加密信息，要想解密信息必须用密钥A。

但用非对称加密算法的时候，二个人可以用配对的密钥进行秘密沟通。OpenPGP就是基于非对称加密。

有一对这样特性的密钥A和密钥B会产生一个非常有趣的机会：如果你把密钥A公开发布出去，会有什么事情发生？公开密钥A，把它发到你的网页上，聚会上发给别人。把密钥A反向的写在你的脑门上，这样大家就可以看见你的密钥A，让任何人都可以看到。

公钥加密算法：

密钥A的唯一用途就是加密信息，并且只有你手中的配对的密钥B可以解密这条信息。这样，大家就可以加密信息，发送给你，而且只有你可以解密。你也可以发送只有他们可以解密的加密信息。这就是公钥加密算法的基石。公开的密钥被叫做公钥，你手中拿着那个叫做私钥。这两个合在一起，公钥（A）,私钥（B），叫做keypair。（一对密钥？？，我都是叫keypair，不知道中文是不是这么翻译）

每一个OpenPGP用户都有一个个人的keypair，其中公钥被广泛传播，私钥则被私藏起来（从名字中，应该也能看出来。。。。unless you‘re a - -!）OpenPGP提供了如果向世界公开公钥，因为你把公钥纹在脑门上也不是很有效。。。。

尽管OpenPGP使用密码口令（下面会提到）来保护你的私钥，总比坏蛋直接偷了你的私钥文件就可以伪装你，困难的多。任何拥有你私钥的人，都可以伪装成你。所以两个都要保护好（你电脑里的私钥文件，和密码口令）。后面，我会提到如何让公钥更公开，私钥更私密。

数字签名：

当你给一个没有加密的信息进行数字签名的时候，这条信息可以被任何人看里面的内容。数字签名只是告诉收件人，给他发邮件的是有与他用的公钥验证的配对私钥的。（也就是说，当你用公钥A验证信息成功的时候，你就知道发件人有私钥A‘ 的）。数字签名用了哈希（hash）和公钥加密二种方法。他们可以提供不可否认性和完整性，但是没有机密性。如果你想让全世界的人都知道，这是你发的信息，那么数字签名就是你所需要的。

在前面，你已经看到了，当别人修改了信息的时候，这条信息的哈希值（hash）也会完全改变，这也就能验证信息的完整性。如果你把信息的哈希值（hash）直接放在邮件里，那么就会出现问题：任何可以修改邮件的人，也可以修改哈希值（hash）来匹配他修改完的信息.。（我是不是应该用她？我看现在一些教材已经用she，而不用he了，女权胜利了？？）。

我们需要一个方法来防止哈希值（hash）被修改。我们的办法就是用公钥加密的方法来对信息进行数值签名。下面就是当你用OpenPGP软件执行数字签名的步骤：

1. 对你的信息生成哈希值（hash）
2. 对哈希值（hash）用你的私钥进行加密
3. 把加密过的哈希值（hash）作为附件到邮件
4. 把整个邮件，外加附件发出去

收件人会收到你的邮件信息还有附件（里面有你加密过的哈希值（hash））。收件人不需要OpenPGP来读这条信息（毕竟你没对信息进行加密）。但是他可以用OpenPGP软件来对附件哈希值进行解密，当然是用你的公钥啦。因为只有你才有你的私钥，所以这个哈希值（hash）也只能由你来生成。然后收件人可以自己对信息进行生成哈希值（hash）。然后查看两个哈希值是否一样。如果一样，收件人可以肯定的是，这条信息就是你发的。！love letter。。。。

如果有人修改了你原来的信息，那么任何去验证哈希值的人都会收到错误信息。如果你的公钥没法解密这个附件哈希值，那么这就说明这个附件哈希值是别人的私钥生成的。或者，你的公钥可以解开附件哈希值，但是匹配哈希值的时候，不一样，那么就说明，信息已经被篡改过了。（谁这么无聊？？？）

数字签名和非对称加密：

我们讨论过了哈希，可以告诉我们信息是否被修改。我们也讲了公钥加密：非对称加密的一种，加密过的信息只能被特定的人看，或加密过的信息只能来这特定的人。数字签名把二者结合起来。但是OpenPGP又更进一步。把发件人的私钥和收件人的公钥一起用，那么OpenPGP的信息被特定的人读，并且只能来自特定的发件人。下面图1表达了这个思想。