解读PGP协议

1 总览

SMTP是一个push协议，用于发送电子邮件。PGP是一种加密技术，用于保护电子邮件的安全性。PEM是一种安全标准，用于建立基于证书中心的安全机制。

SMTP（简单邮件传输协议）是一个用于在服务器之间发送电子邮件的协议。它是一个标准协议，定义了电子邮件如何在互联网上发送和接收。

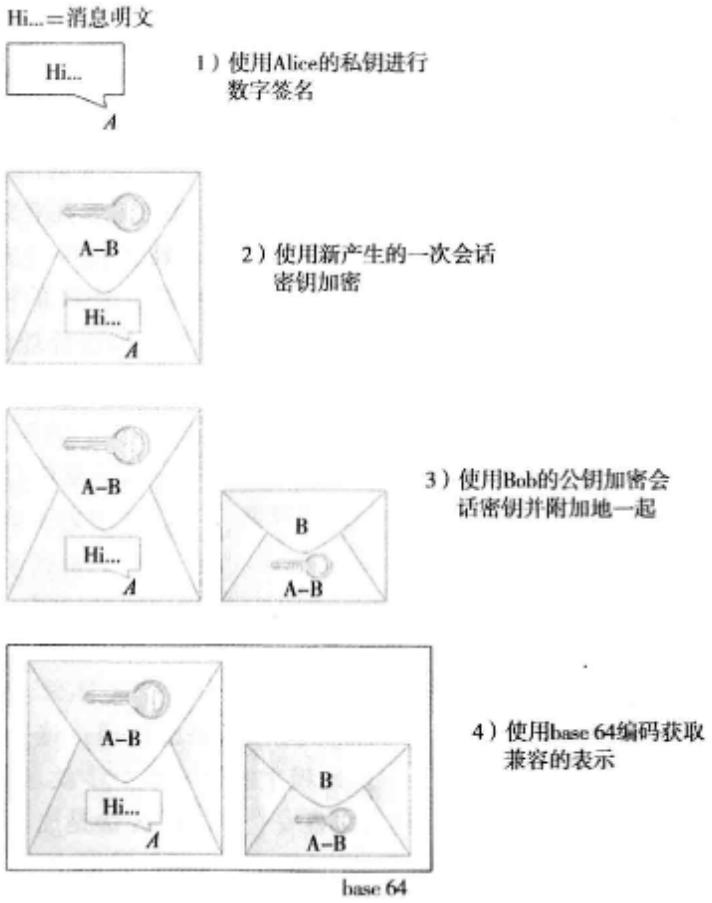
PGP（Pretty Good Privacy）是一个用于加密和解密电子邮件信息的安全协议。它提供端到端的加密，这意味着只有发件人和预定的收件人可以阅读电子邮件的内容。PGP使用一个公钥和一个私钥来加密和解密信息。

要在SMTP中使用PGP，必须将电子邮件客户端或服务器配置为使用这些协议。这通常涉及到生成一个密钥对（公钥和私钥）并导入收件人的公钥。当发送电子邮件时，客户端或服务器将使用收件人的公钥对邮件进行加密，而当收件人收到邮件时，他们可以使用自己的私钥对邮件进行解密。

PGP和PEM都提供了一种安全的方式来发送电子邮件，它们通常被需要保护敏感信息的企业、政府和个人所使用。然而，它们确实需要一些设置和配置，而且双方必须使用兼容的软件和协议才能使加密和解密过程正常进行。

PGP是一种广泛用于电子邮件安全的方法。它提供了认证、机密性、数据完整性、不可否认性。PGP最早由Phil Zimmerman发明的，并且已经成为IETE的标准，称为OpenPGP。PGP适用于用于使用“信任网络”模型来分发密钥而不是用树型的分层结构。
PGP的机密性和接收方认证依赖于电子邮件的接收方拥有一个发送者知道的公钥。为了提供发送方认证和不可否认性，发送方必须拥有一个接收者知道的公钥。这些公钥是通过证书和信任网络PKI进行预分发的。这些证书可以进一步指明支持哪些密码算法或者密钥拥有者推荐哪些密码算法。

PGP准备由A通过电子邮件发送到B的消息的步骤：



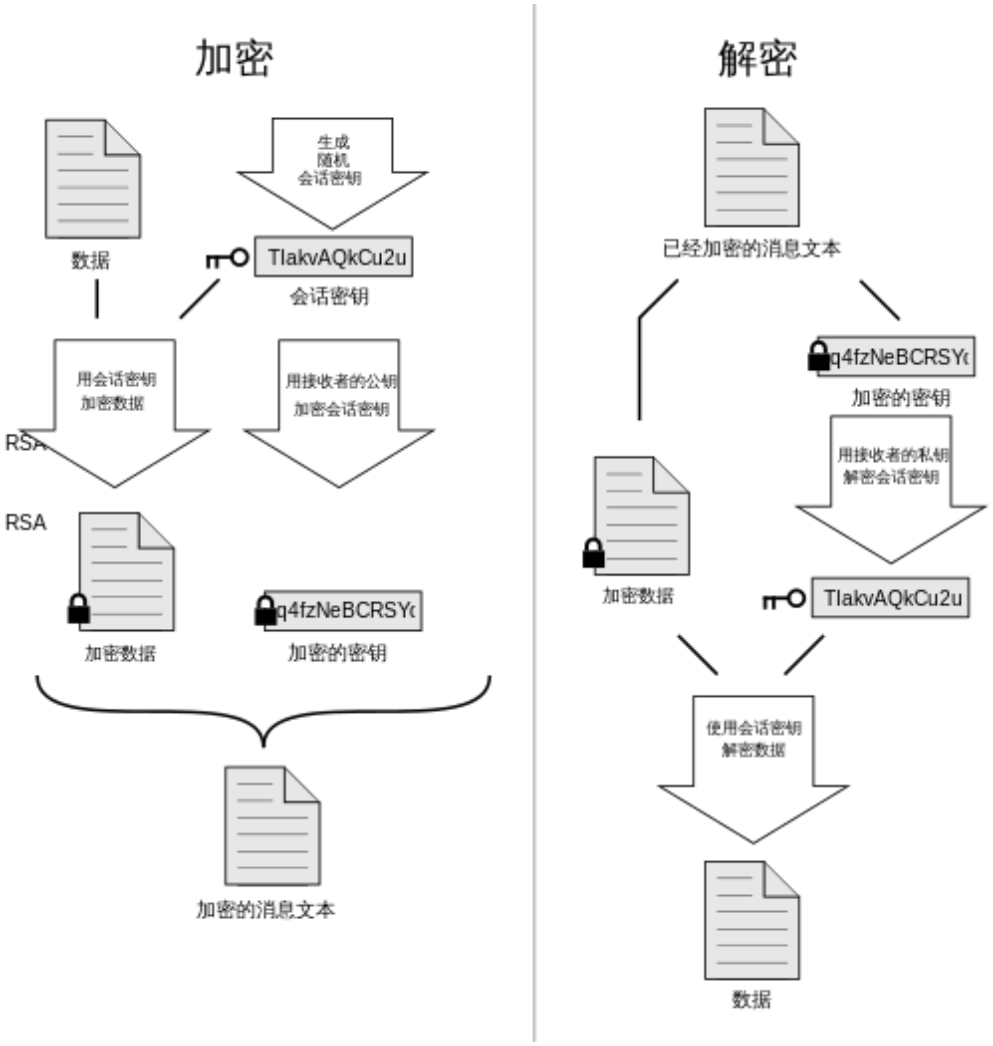
假设 A有一条消息通过电子邮件传递给B。A的PGP应用程序执行如图所示的步骤。首先，A对消息进行数字签名，MD5、SHA-1和SHA-2协议族都是可以用于数字签名的散列函数。然后，A的PGP应用程序为仅有的这条消息产生一个新的会话密钥，所支持的对称密钥密码包括AES和3DES。数字签名后的消息通过该会话密钥被加密，会话密钥本身被B的公钥加密后追加到消息后。A的PGP应用程序会提示A以前赋给B的公钥的信任程度，这是根据A所拥有的B的证书的数量以及对每个证书的签名者的信任度来确定的。最后，对消息进行base64编码，转换成一种ASCII兼容的表示形式。这不是为了安全，而是因为电子邮件消息必须以 ASCII形式发送。通过电子邮件接收到PGP消息后，B的PGP应用程序按逆序执行上述过程来得到原始的明文消息，并确认A的数字签名——同时提示B对 A的公钥的信任程度。

电子邮件有一个不同寻常的特性，它允许PGP在这个单条消息数据传输协议中嵌入适当的认证协议，从而避免提前进行任何消息交换。A 的数字签名足以认证它自己。虽然无法证明消息是及时的，但传统的电子邮件也不是及时的。另外，也无法证明消息是原始的，但B作为一个电子邮件用户，通常能够从电子部件副本中恢复信息（这在正常操作情况下也不是不可能的）。A可以确定只有B 能够读取消息，因为会话密钥是用B的公钥加密的。虽然该协议没有向 A证明B 确实存在并收到了电子邮件，但从B回送给 A的经过认证的电子邮件能够提供证明。

2 PGP协议及其相关文献

2.1 概述

PGP加密由一系列散列、数据压缩、对称密钥加密，以及公钥加密的算法组合而成。每个步骤均支持几种算法，用户可以选择一个使用。每个公钥均绑定一个用户名和/或者E-mail地址。



PGP工作原理示意图

wiki：https://zh.wikipedia.org/wiki/PGP

2.2 文献

[1]Pretty Good Privacy：PGP简述

[2]PGP Message Exchange Formats-Philip Zimmermann

PGP消息交换格式,PGP作者所作。

[3]Why I Wrote PGP-Philip Zimmermann

我为什么写PGP？ PGP作者所作

[4]Efficient Deniably Authenticated Encryption and Its Application to E-mail

高效的可否认认证加密及其在电子邮件中的应用,作者提出了PGP的两个弱点：(1) 数字签名提供了发件人的不可否认的证据，这在一些电子邮件应用中是不需要的(2) 效率低，因为这些方法使用两种公钥加密原件：公钥加密和数字签名。为了克服上述两个缺点，作者引入了一个新的概念，称为可否认的认证加密。

[5]文远. PGP安全电子邮件系统研究与实现[D].北京邮电大学,2007.

本文介绍了当前非常流行的安全电子邮件加密标准PGP，并通过对PGP的介绍，详细分析了PGP可能存在的一些安全问题。

[6]钟泽秀.电子邮件安全协议—PGP[J].硅谷,2014,7(08):140-141.

本文介绍电子邮件的传输过程，引出安全电子邮件的重要性，然后介绍电子邮件安全协议 PGP，涉及到的 IDEA、RSA、MD5 加密算法以及其安全性分析

[7]宋玉璞,周爱霞,肖汉.E-mail安全协议PGP[J].计算机科学,2008(03):46-48.

本文从单钥密码IDEA算法、双钥密码RSA算法、单向杂凑算法MD5算法等分析了安全电子邮件协议PGP的实现原理和实现流程;描述了PGP所提供的安全业务;并从RSA、IDEA、MD5、随机数等安全性方面分别研究了PGP的安全性能