浅谈两类通信安全问题

秦子茗[1]、杨锃涛[2]、刘迅[3]

摘要：通信安全的含义相当广泛：有基础到物理实现层面的，比如电磁安全所要考虑的电磁波泄露问题；有在传输层面的，比如对中间人攻击的对抗；还有在数据层面的，比如非对称或对称加密算法。从性质上总结，通信的安全性可以归结为保密性、完整性、真实性和不可抵赖性。本文将结合通信安全的性质，针对给定的两个具体通信安全问题开展讨论。

引言：伴随着互联网的高速发展，以网络为载体的通信在人类社会中占据着越来越重要的地位。现在人们的日常生活中，有很大一部分的通信依赖于互联网及其衍生产品，例如用微信和家人语音聊天、用邮件和导师联系，或者是在腾讯文档上分享一个文档来布置网络空间安全导论的作业。而正是因为对基于网络的通信手段的高度依赖，我们尤其应该考虑其中的安全性。毕竟这样一种通信不仅仅是作为交流的手段，其中所储存的信息和内蕴的生活方式，都正在成为我们日常生活的一部分。

1 云上数据保密问题

随着计算机网络的发展，越来越多的重要信息被存储在电脑中。而随着时间的发展，个人乃至组织对于文件编辑的时效性和便捷性的要求不断提高，于是云空间应运而生。而随之而来的就是上传至云空间的文件安全问题，对于这一问题，我有以下一些思考。

通过邹老师上课的提问：如何确保不被别人偷看我上传到云空间文件的内容。我对其进行了一些思考，并在查阅了有关文献后提出几点我的观点及考虑。下面我将从这几个方面进行报告。

首先想到的，就是在将文件上传到云端前就对其进行加密。在我脑海中最先想到的是对文件进行算法加密，或者将重要文件内容进行存储层面的拆分后分别进行加密。

前者，在查阅了相关资料后，发现现在主流的加密算法为 DES、3DES、AES 和 SM4 算法。而其中最主要使用的是 AES 和 SM4 算法。

AES 算法在实际应用中主要会涉及到有限域、状态矩阵和密钥矩阵、扩展密钥等概念。在实际应用 AES 算法的过程中，在有限域的条件范围之内，将需要被加密的数据以及密钥数据划分成 维数为 4×4、4×6 或 4×8 的矩阵，被加密

[1] 负责第二部分
[2] 负责第一部分
[3] 负责摘要、引言及结语部分

数据组成的矩阵是状态矩阵，而由密钥数据组成的矩阵则是密钥矩阵[3]。在形成矩阵之后，应用不同的密钥对数据进行多轮次的加密，这些用于加密的所有密钥集合被称为扩展密钥。

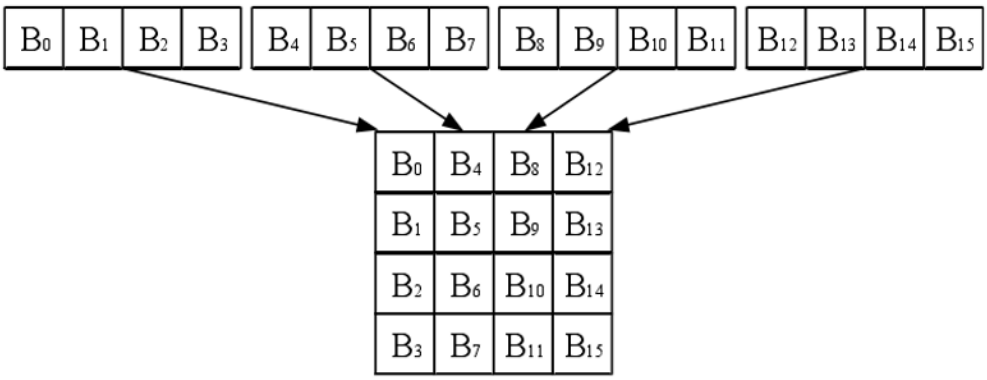

图 1：AES 算法：明文初始状态矩阵

SM 算法是我国以椭圆曲线密码体制（Ellipse Curve Cryptography, ECC)为基础，进行自主研发设计的一种密码算法，使用更加安全的机制，提升了计算量和复杂性;在数字签名和验证、随机数的生成等方面，使用了 SM3 算法和随机数生成器。SM3 算法比消息摘要算法第五版(Message Digest Algorithm, MD5)(128 位）更加安全;并且 SM3 算法的压缩函数结构与安全哈希算法 SHA-256 相似，但运算更为繁复。

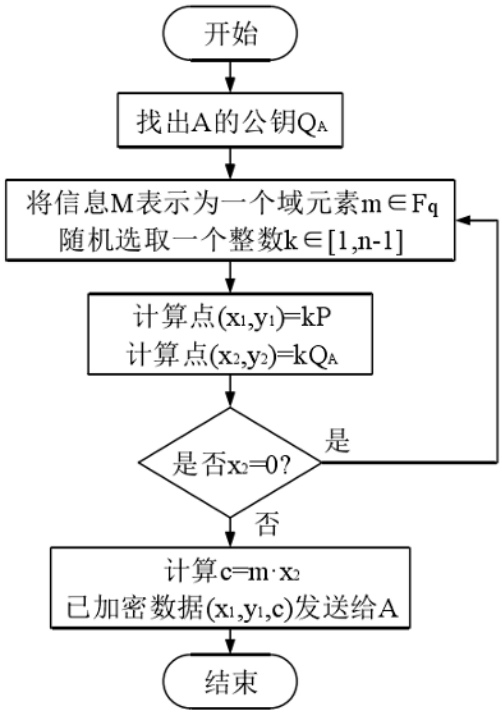

图 2：SM 算法：椭圆曲线加密流程

2 邮件收发的保密问题

进入大学后，我们使用各种邮箱工具进行沟通交流的频率大幅度增加，比如中科院的邮箱系统，163 邮箱，outlook，QQ 邮箱等。而在邮箱的日常使用过程中，安全问题似乎总是被我们遗忘：如何保证收到的邮件一定是对话用户所发？如何保证邮件通信的保密性而不被第三人窃取信息？而前段时间中科大“钓鱼邮件”事件更是引发了人们对于邮件安全的关注。下面我们就将浅析邮件收发中的保密问题。

首先介绍邮件收发原理。传输一封电子邮件需要三个主要步骤。第一，邮件从发送者的邮件用户代理（Mail User Agent，MUA） 中发出，通过 STMP 或 HTTP/HTTPS 传输到发送方服务提供商的邮件提交代理 （Mail Transfer Agent，MTA）。MTA 通过 SMTP 协议将消息发送给收件人的邮箱提供商。通过 IMAP（Internet Message Access Protocol）、POP（Post Office Protocol）或 HTTP/HTTPS，邮件传递代理（Mail De-livery Agent，MDA）将消息传递给接收用户。

以从 QQ 邮箱发邮件到 163 邮箱为例：

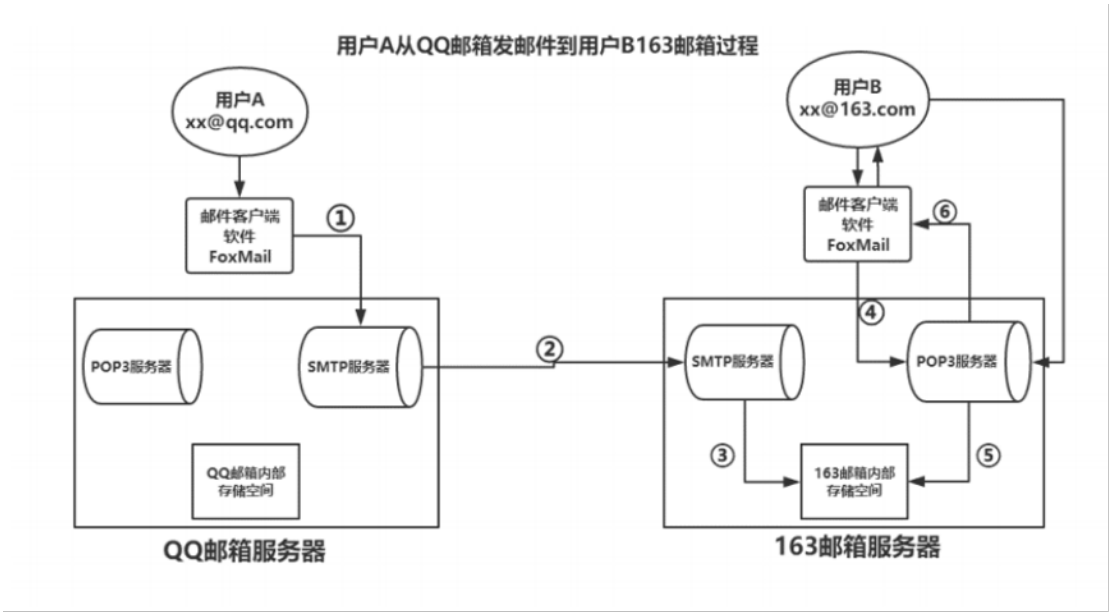

图 3：从 QQ 邮箱发邮件到 163 邮箱

这里需要介绍一下文中出现的两个协议：SMTP 和 POP3. 。SMTP 全称为 Simple Mail Transfer Protocol，即简单邮件传 输协议。SMTP 是电子邮件传输的互联网标准协议。SMTP 协议属于 TCP/IP 协议族，它帮助每台计算机在发送或中转信件时找到下一个目的地。通过 SMTP 协议所指定的服务器，我们就可以把 E—mail 寄到收信人的服务器。

POP 协议:(Post Office Protocol) 即邮局协议，用于电子邮件的接收，即邮局协议，用于电子邮件的接收，它是因特网电子邮件的第一个离线协议标准，POP3 允许用户从服务器上把邮件存储到本地主机同时删除保存在邮件服务器上的邮件，而 POP3 服务器则是遵循 POP3 协议的接收邮件服务器，用来接收

电子邮件的。

安全电子邮件必须是运用各种安全机制来保障邮件在网络传送过程中的安全性，它应实现以下功能：机密性、完整性、身份认证、不可否认性。为了实现这一目标，人们提出了一系列安全电子邮件协议。如 PGP，S/MIME，PEM 等。在此，我们介绍目前电子邮件系统中应用最为广泛的一种加密技术：PGP。PGP 加密系统是采用公开密钥加密与传统密钥加密相结合的一种加密技术，也即对称加密与非对称加密结合的方式。公开密钥采用 RSA 加密算法，传统加密部分所使用的密钥称为“会话密钥”。每次使用时，PGP 都会随机产生一个 128 位的 IDEA 会话密钥，用来加密报文。公开密钥加密技术中的公钥和私钥则用来加密会话密钥，并通过它间接地保护报文内容。

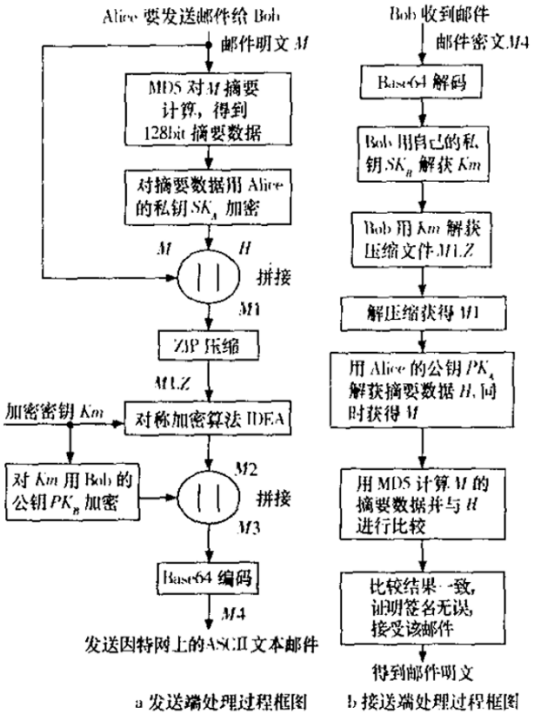

图 4：PGP 加密系统加密与解密流程

PGP 的具体加解密过程可分为以下四步（假定通信双方为 Ailce 和 Bob，双方都持有各自的由公钥算法所界定的秘密密钥 Ska,SKb，同时相互持有对方的公钥 PKa,PKb。）：

1. 发送方 Alice 对需要传输的文件用 MD5 摘要算法获得 128bit 的信息摘要，用自己的 RSA 私钥 SKa 进行加密得到 H；
2. Alice 生成一个自己的私有密钥 Km 用于 IDEA 算法对明文与 H 的拼接体加密，并用接收方的公开密钥对 Km 进行加密，将二者合并然后通过网络传输到接收方；
3. 接收方用自己的私有密钥 SKb 进行解密后得到发送方的私有密钥 Km，并用 Km 恢复出明文和 H 的拼接体，接着分开二者，并用 Alice 的公钥 PKa 解密 H 得到信息摘要；

4. Bob 对明文进行信息摘要运算，结果与 H 的解密结果进行比较，如果相同，则证明邮件是 Alice 发来的。因为只有接收方才拥有自己的私有密钥，所以即使其他人得到了经过加密的发送方的私有密钥，也因为无法进行解密而保证了私有密钥的安全性，从而也保证了传输文件的安全性。同时 RSA 私钥 Ska 仅属于 Alice，故数字签名 H 保证了邮件确从 Alice 处发来，同时解决了保密与认证问题。

PGP 还可以只签名而不加密，这适用于公开发表声明时，声明人为了证实自己的身份，可以用自己的私钥签名。这样就可以让收件人能确认发信人的身份，也可以防止发信人抵赖自己的声明。这一点在商业领域有很大的应用前途，它可以防止发信人抵赖和信件被中途篡改。

结语：本文对给定的云上数据保密问题、邮件收发保密问题这两个具体通信安全问题进行了探讨。以上的讨论结合了小组成员自己的思考，并且参考了真实世界中对具体安全问题的处理措施，例如 AES、EM 和 PGP 等加密技术。不过还有更多深层次的问题有待探讨，例如如何权衡安全问题中安全强度与处理效率两者的关系？这两者之间的关系是否有更多定量的评价手段？以上讨论的加密系统，只介绍了大致的操作流程，其数学上的安全性如何保证？这些问题，将留待小组成员在学习更多后解答。

参考文献：

1. 李博. 云存储数据的嵌入式加密算法设计与实现[D]. 黑龙江大学. 2021.000933.

2. 王亚涛. AES 加解密算法及其安全性分析[J]. 网络安全技术与应用,2022(09):33-35.

3. PGP 安全电子邮件的加密原理[J]. 崔健双,李铁克. 计算机工程与科学(2003)06—0025—03.

4. 电子邮件 SMTP/POP3 收发协议的研究与实现[J]. 付祝财,杨莘元,王阳. 信息技术,2004(08):57-59.

5. 基于 PGP 混合加密技术的安全电子邮件系统研究与实现[A]. 吴培飞. 计算机时代 (2016)03-39-04.