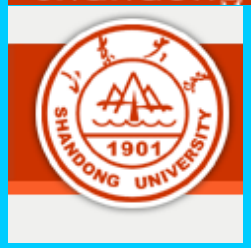

Computer Science&Technology School of Shandong University

Security Protocols & Standards

--- PKI Principles and technology sd03031340

(Chapter 5 PKCS# & IEEE P1363)

Instructor: Hou Mengbo 侯孟波
Email: houmb AT sdu.edu.cn
Office: Information Security Research Office.
Rm: Office Building 421

背景

- 由于公钥密码被广泛接受已成为事实，如果要将其发展成为广泛应用的技术，就必须有支持**互操作的标准**。
- 即便是所有的用户都认同公钥密码技术，使各种不同的实现版本相兼容也是必需的。
- 互操作性要求严格按照一个获得认可的标准格式来传输数据，这里所描述的标准就为互操作性提供了基础。

Part One PKCS

Public-Key Cryptography Standards

PKCS

- PKCS标准是Public-Key Cryptography Standards的简称。公钥密码标准 PKCS 是由 **RSA 实验室**与其它安全系统开发商为促进公钥密码的发展而制订的一系列标准，是最早的公钥密码标准，也是公钥密码发展过程中最重要的标准之一,涉及消息语法和算法。
- 自 1991 年作为一份会议结果，由早期的公钥密码使用者公布以来，PKCS 文档已经被广泛引用和实现。许多正式和非正式工业标准部分内容的制订都参照了PKCS，如 ANSI X9, PKIX, SET, S/MIME和 SSL 等。
- **RSA Lab**在标准制订过程中起了很重要的作用：发布了认真撰写的标准描述文档；保持了标准制订过程的决策权威；负责收集其它开发者所提出的修改和扩充意见；适时发布标准的修订版；提供了实现该标准的参考资料和指导。
- 服务于公钥密码体制的兼容性、互操作性。
- 已经成为事实上的国际标准。

PKCS标准列表

PKCS #1: RSA Cryptography Standard RSA 密码 (#2/#4: add to #1)
PKCS #3: Diffie-Hellman Key Agreement Standard DH 密钥交换
PKCS #5: Password-Based Cryptography Standard 基于口令的密码
PKCS #6: Extended-Certificate Syntax Standard 扩展证书语法
PKCS #7: Cryptographic Message Syntax Standard 密码消息语法
PKCS #8: Private-Key Information Syntax Standard 私钥信息语法
PKCS #9: Selected Attribute Types 可选择的属性类型
PKCS #10: Certification Request Syntax Standard 认证请求语法
PKCS #11: Cryptographic Token Interface Standard 密码令牌接口
PKCS #12: Personal Information Exchange Syntax Standard 个人信息交换语法
PKCS #13: Elliptic Curve Cryptography Standard 椭圆曲线密码
PKCS #14: Random Number Generation Standards 随机数生成
PKCS #15: Cryptographic Token Information Format Standard 密码令牌信息格式

标准范围(1) -Digital Signature

- The "signer" signs a "message" such that anyone can "verify" that the message was signed only by the "signer" and thus not modified by anyone else. This can be implemented using a message digest algorithm and a public key algorithm to encrypt the message digest.

What is standardized? (Digital Signatuers)	
Specific message digest algorithms.	PKCS# 1
Specific public key algorithms.	PKCS# 1, 3, 13
Algorithm independent syntax for the digitally signed message.	PKCS# 7
Syntax for private keys.	PKCS# 1, 8
Syntax for encrypted private keys.	PKCS# 8
Method for deriving secret keys from passwords.	PKCS# 5

标准范围(2) - Digital Envelopes

- Digital Envelopes: The "sender" seals the "message" such that only the "receiver" can open the sealed message. The message is encrypted with a secret key and the secret key is encrypted using the receiver's public key.

What is standardized? (digital Envelop)	
Algorithm independent syntax for the digitally enveloped message.	PKCS# 7
Syntax for private keys.	PKCS# 1, 8
Syntax for encrypted private keys.	PKCS# 8
Method for deriving secret keys from passwords.	PKCS# 5

标准范围(3) - Digital Certificates

- Digital Certificates: A "Certification Authority" signs a "special message" which contains the name of a user and the user's public key in such a way that "anyone" can verify that the "special message" was signed only by the "Certification Authority" and as a result trust the user's public key. This "special message" is termed as a certificate request and it is digitally signed using a "signature algorithm".

What is standardized?	
Algorithm independent syntax for certification requests.	PKCS# 10
Syntax for public keys.	PKCS# 1
Specific signature algorithms.	PKCS# 1

标准范围(4) - Key Agreement

- Key Agreement: Two "communicating parties" agree upon a secret key by exchanging messages without any prior agreements. Typically this consists of a two-phase key agreement algorithm. One party initiates the key agreement and this triggers the "first phase" of the key agreement after which both parties exchange the results of the first phase. After this, both parties initiate the "second phase" of the key agreement and as a result both parties arrive at the same secret key.

What is standardized?	
Algorithm independent syntax for key agreement messages.	PKCS# 3
Specific key agreement algorithms.	PKCS# 3

PKCS#1： RSA 密码标准

- 1.0 – 1.3 版是为参加 RSA 公司 1991 . 2 – 3 的公开密钥密码标准会议而发布的。
- 1.4 版是 1991 .6 首次公开发布的 PKCS 的一部分。1.4 版作为NIST/OSI 实现工作组的 SEC-SIG-91-18 标准文档发布。
- 1.5 版合并了几个版本的变化，包括参考文献的更新和增加修订历史。1.5 版是作为 IETF RFC 2313 发布的。
- 2.0 版编入了在文档结构方面的主要变化，而且引入了 RSAES-OAEP 加密方案。尽管由于这几年 来的密码发展不再允许使用 MD4，但这个版本继续支持 1.5 版中的加密和签名操作。2.0 版是作为 IETF RFC 2437 发布的。
- 2.1 版引入了多素数 RSA 和 RSASSA-PSS 带附属 的签名方案。这个版本同时支持 2.0 版中的方案。

PKCS#1： RSA加密标准

- 该文档介绍基于 RSA 公钥密码系统的实现方法，包括：密码原语、加密方案、带 附属的签名方案、密钥和方案的 ASN.1 描述。是为计算机和通信系统的一般应用和具 有灵活性的系统的一般应用而编写的。
- 第一部分是介绍。
- 第二部分是对文档中使用到的符号的定义。
- 第三部分详细说明了 RSA 公钥和私钥的类型。
- 第四、五部分详细 说明了几个原语，或基本数学操作（数据转换原语、密码系统原语（加密—解密、签名—验证））。
- 第六、七和八部分涉及加密和签名方案。第六部分概述PKCS #1 V1.5 中介绍的方法，第七部分定义了基于 OAEP 的加密方案，第八部分定义了基于 PSS 的带附属的签名方案。
- 第九部分详细说明了在 第八部分中定义的签名方案的编码方法。

PKCS#3： Diffie-Hellman密钥协商标准

- 1.0–1.2 版是为参加 1991 年 2 月和 3 月在 RSA 数据安全公司的公钥密码标准会议 而发布的标准。
- 1.3 版是 1991 年 6 月发布的 PKCS 标准的一部分。1.3 版同时被 NIST/OSI 实现工作组作为 SEC-SIG-91-19 标准文档。
- 1.4 版合并了一些修改，更新了参 考文献，加入了版本更新历史。该标准描述了实现 Diffie-Hellman 密钥交换的一种方式，双方不经过事先勾通，就 能够产生一个只有他们才知道的密钥(尤其是窃听者无法得知该密钥)。这个密钥可被双 方用于以后的秘密通信。
- 该标准的主要应用是建立秘密通信的协议，如 OSI 模型的传 输层和网络层通信协议的建议[ISO90a][ISO90b]。

PKCS#5：基于口令的加密标准

- 本文对基于口令的密码技术的实现提出了相关建议，涵盖了以下几个方面：
  - 密钥生成函数、加密方案、消息鉴别方案、用 ASN.1 语法对技术进行标识。这些有着一定伸缩性的建议是针对计算机和通信系统中的普通应用软件提出的，特别针对了敏感信息的保护，例如：对 PKCS#8 中私钥的保护。
- 本文不涉及其它的基于口令的密码技术，例如：基于口令的密钥实体鉴别和密钥制定协议；并且也不涉及口令的选择。本文代替了 PKCS#5 1.5版,但包含了相应的兼容技术。

PKCS#5：基于口令的加密标准

- 在很多公钥密码应用软件中, 用户的安全最终依赖于一个或多个秘密文本或口令。 虽然在一个常规的密码系统中并不直接把口令用作密钥，但在用口令进行密码操作时仍 需对口令进行处理。此外, 由于口令通常从一个相对较小的空间中选取, 在对其进行处 理时要特别注意抵抗搜索攻击。

口令产生密钥的方法-salt

- 基于口令的密码术的一种通常的方法是**将口令与 salt 相结合以生成密钥**，用口令可生成一个巨大的密钥集，可以把 salt 看作是对这个密钥集的一个索引， 不需要对 salt 进行保密。虽然一个攻击者可能会构 建一个包含所有可能口令的表（一种所谓的“字典攻击”），但构建一个包含所有可能 密钥的表是十分困难的，因为对每一个口令都存在非常多的可能密钥。因而，攻击者只 能对每个 salt 来搜索所有的口令。

口令产生密钥的方法-迭代

- 基于口令的密码术的另一种方法是**建立一种代价相对较高的密钥生成技术**，从而增 加穷举搜索代价。这种方法的一种途径就是，在密钥生成技术中引入一个**迭代次数**，用来表示对某个生成密钥的基础函数的迭代次数。它对于 合法者来说并不形成一种负担，但对攻击者却是一种严重的负担。
- 在 PKCS #5 v1.5 中， Salt 和迭代次数构成了基于口令密码术的基础， 并且也被用 在本文中的多种密码操作中。因而，本文定义的基于口令的密钥生成技术是一个关于**口 令、salt 和迭代次数**的函数，其中后两个量不需保密。从一个基于口令的密钥生成函数能很容易的得到基于口令的加密和消息鉴别方案。

其他应用

- 基于口令的密钥生成函数得到其它的应用。
  - 例如，我们可以仅用一个密钥生成函数来**生成一个密钥集**，而不必逐个的 生成密钥。密钥集中的密钥可以就是密钥生成函数的输出串的各个子串。这种方法可以用在一个面向会话的协议中，作为构建密钥系统的一部分。
  - 另一种应用是**口令检查**，其中：密钥生成函数的输出和 salt 以及迭代次数都被保存起来，以用于对口令的验证。在本文中，认为口令是一个任意长度的字节串，并不特别要求它被解释为一个文本 串。但为了提高的互用性，仍然希望应用软件能遵循通用的文本编码规则.

PKCS＃6：扩展证书语法标准

- 一个扩展证书由 X.509 公钥证书和一系列被证书发行者签名的属性组成。于是属性和内附的 X.509 公钥证书能够被单独的一个公钥密码操作验证，当需要时还能提取出普通的 X.509 公钥证书。包含一系列属性的目的是使认证操作得到扩充，能够通过公钥操作验证给定实体其它信息，如电子邮件地址。PKCS #9 中给出比较详细的属性列表。
- 本标准最初应用在 PKCS #7 的密码报文中，其它的应用正在开发之中。

PKCS#7：密码消息语法标准

- 1.0–1.3 版是 1991 的 2 月和 3 月在 RSA 数据安全公司的公钥密码标准化会议上发布的最早版本。
- 1.4 版是 1991 年 6 月发布的 PKCS 初始版本的一部分。1.4 版同时被 NIST/OSI 的实现工作组作为 SEC-SIG-91-22 标准发。
- 1.5 版合并了几处编辑上的 改动，包括对参考文献的更新和修订历史的添加。
- 本标准描述了**用于加密数据的一般语法**，如数字签名和数字信封等。该语法允许循 环，一个信封可以嵌套在另一个中，一方也可以对打入数字信封的数据作数字签名。该标准也允许使用任意属性，如签名时间可发消息内容一同被认证，也可以提供与 签名相关的附属签名。该语法还能提供一种证书和证书撤销列表传输方式。该标准也适用于 Privacy-Enhanced Mail (PEM)中的签名数据和签名加密数据内容，构造了一个 PEM 适用模式，不进行任何加密操作就可以转换为 PEM 消息。PEM 消息也可以被转换为签名数据和签名加密数据内容类型。

PKCS#8：私钥信息语法标准

- 1.0 版是 1991 年 2 月和 3 月 RSA 公司的公开密钥加密标准会议上发布的版本。1.1 版是 1991 年 6 月 PKCS 标准最初公开发行的一部分，也作为 NIST/OSI 实现工作组作为 SEC-SIG-91-23 标准发布。1.2 版合并了几处编辑上的改动，包括对参考文献的更新和修订历史的添加。
- 本标准描述**一种私钥信息的语法**。私钥信息包含一个对应于某个公钥算法的私钥和一个属性集。
- 还描述**一种加密密钥的语法**。基于口令的加密算法（例如在 PKCS#5 中描述的某一种算法）可以用来加密私钥信息。包含属性集的目的是通过属性信息为用户提 供一个快捷的方式确立信任，如辨识名(DN)或顶级证书权威机构(CA)的公钥等信息。 尽管这样的信任可通过数字签名确立，但使用只有用户知道的密钥加密过程同样高效并易于实现。

PKCS＃9： 可选属性类型标准

- 1.0 版是 1991 年 6 月发布的 PKCS 标准的一部分。1.0 版同时作为 NIST/OSI 开 发工作组的 SEC-SIG-91-24 标准发布。1.1 版合并了部分修改，包括更新了参考文献加入了版本修订历史。
- 在第 6 部分加入了 challengePassword、unstructuredAddress、 和 extendedCertificateAttributes 几个属性类型，第7部分加入了challengePassword、unstructuredAddress 和 extendedCertificateAttributes 几个对象标识。2.0 版 也合并 了几处修改，并作了一些实质性改动。

- 本文档描述了两个辅助对象类：pkcsEntity 和 naturalPerson，一些新的属性类型 和匹配规则。所有的 ASN.1 的目标类、属性、匹配规则都能够导出用在其它的环境中。 定义在本文档中的属性类主要用于与 PKCS 相关数据集及包括 PKCS#12 PFX PDUS、 PKCS#15 令牌和加密私钥的 pkcsEntity 类的连接。定义在本文档中的属性类用于与 PKCS#10 证书请求及包括电子邮件地址、介质、非结构化名称、非结构化地址的 naturalPerson 目标类。定义在本文档中的属性类用于包括内容类型、消息摘要、签名 时间、序列号、随机场合和附属签名的 PKCS#7 数字签名消息。属性将用于 SignerInfo 和 AuthenticatedData 值的 authenticatedAttributes 及 unauthenticatedAttributes 域特 别适用于 PKCS#10 的属性类型是盘查口令和扩展请求属性。这些属性被用在 CertificationRequestInfo 值的 attributes 域。

PKCS#10：认证请求语法标准

- 1.0 版是该文档的早期版本(也作为 version 1.5 发布)，1.7 版合并了几处改动，更新了参考文献，修改了 ASN.1 类型的定义。
- 本文档描述了**认证请求的语法**。一个认证请求包括一个 DN名称、一个公钥、一 个属性集，由要求认证的实体整体签名。认证请求被发送到一个认证权威(certification authority)并转换为 X.509 公钥证书。
- 包含属性集有两重目的：
  - 提供给定实体 的其它相关信息；
  - 提供 X.509 证书的内部信息。
- PKCS #9 给出了一个比较详细的属性列 表。 认证机构(Certification authorities)也可以要求一个非电子形式的请求并返回非电子 形式的回执。

PKCS#11：密码令牌接口标准

- 本文档为那些保存密码信息、执行密码函数的设备确定一种应用设计接口（API），该接口称做 Cryptoki，是 cryptographic token interface（密码令牌接口）的缩写，它遵循 一种基于对象的简单方法，提出技术独立性（各种各样的设备）和资源共享（多个应用 程序访问多个设备）的目标，把设备的一种通用逻辑视图，即密码令牌，提供给应用程 序。
- 本文档通过使用 ANSI C 语言确定需要密码服务的应用程序数据类型和函数。这些数据类型和函数将由 Cryptoki 库的供应者通过 C 字头文档提供。
- Cryptoki 把应用需求从密码设备的中分离出来，应用程序不必转换成另一种不同的设备接口或在不同环境下运行。本版本支持许多密码机制。新机制能在不改变通用界面的情况下添加 进来。

PKCS#12：个人信息交换语法标准

- 本标准描述了**个人身份标识信息传递语法**，包括私钥、证书、各种形式的秘密数据及其扩展。支持本标准的计算机、应用程序、浏览器、因特网服务等将允许用户导入、导出，并使用一套统一的个人身份标识信息。
- 本标准支持用户信息以机密、完整的方式**直接传递**。大部分能够保证机密性和完整性的安全手段，需要源平台和目标平台都拥有用于数字签名和加密的密钥对，本标准同时支持基于口令的机密性和和完整性保护方法，可以用于不能提供可信密钥对的环境。软硬件实现都应受本标准约束。
- 本标准可以看作是在构建在 PKCS #8 的基础之上的，包含了其他的基本内容，但是增加了补充的标识信息、私钥，并且通过非对称密钥方式的机密性和完整性保护方提供了更高层次的安全。

PKCS#13：椭圆曲线加密标准

- 定义了在椭圆曲线加密体制下，数据加密和数据签名的标准。该标准还在制订中，是 RSA 实验室的 PKCS 系列中一个新标准，涵盖了基于椭圆曲线的公钥密码技术的内容。

PKCS#13：椭圆曲线加密标准

- 椭圆曲线密码体制由于需要较小的密钥规模就能达到很高的安全强度。
- 椭圆曲线密码标准化的工作正在展开。X9.F.1 是 ANSI 为金融服务开发的 标准，正在发展两个标准：用于数字签名的 ANSI X9.62 和用于密钥交换与传输的 ANSI X9.63。IEEE P1363 正在为将不同的椭圆曲线为公钥密码形成一个通用的标准。
- PKCS #13 将提供一个将椭圆曲线和其它 PKCS 应用相融合的规范(尚未推出)。将包括椭圆曲线密码体制的以下方面：参数的生成和有效性检验；密钥 生成和有效性检验；数字签名；公钥加密；密钥交换；参数、密钥和加密方案的 ASN.1 语法；安全性分析。

PKCS#14：随机数产生标准

- 定义了伪随机数产生方面的标准。

PKCS#15 ： 密码令牌信息格式标准

- 版本 1.0 发布于 1999 年 4 月。版本 1.1 加入了对其他 认证方式的支持（例如生物认证，外部认证等）；加入了对更详细的访问控制信息的支持；加入了对软令牌的支持（“虚拟智能卡”）；加入了对卡可验证的证书的支持。
- 密码令牌，如集成电路卡（或 IC 卡），本身就是安全的计算平台，非常适合于为应 用提供增强的安全性和私密性的功能。它们可以处理认证信息，如数字证书，授 权和加密密钥等。此外，它们能够为敏感信息提供安全的存储和计算工具，这些敏感信 息可能有：私钥和密钥片断；计数和保存的值；口令和共享的秘密；授权和许可。

Part Two IEEE P1363

Standard Specifications for Public-Key Cryptography

IEEE P1363 标准

- IEEE P1363 项目来始于1994年,目的是开发密码学标准,包括公钥密码学的标准规范. 项目开始时只是规定了RSA和Diffie-Hellman算法的数学原语和密码技术,后来扩展了研究领域,如加入了椭圆曲线密码体制.
- 这些技术标准涉及密钥协商、公钥加密、数字签名和身份认证，还涉及到需要考虑的其他密码相关问题，如密钥管理和安全随机数生成等。

NIST新工作 – 后量子密码系统

- 2012 年：NIST 启动后量子时代密码(PQC) 项目，成立了包括 12 个密码专家的项目成员组；
- 2015年4月：NIST举行第一次PQC专题研讨会；
- 2015 年8 月：美国国家安全局(NSA) 就PQC发表声明；
- 2016 年2 月：NIST 发布PQC 工作报告(NISTIR8105)；
- 2016 年2 月：NIST 就PQC 的标准化提出初步设想；
- 2016 年8 月：NIST 制定出对PQC 新算法的要求和评估标准的初稿，并公开征求意见；
- 2016 年9 月：初稿征求意见期结束；
- 2016 年12 月：NIST 正式确定对新算法的要求和评估标准，面向全世界征求PQC 新算法；
- 2017 年11 月30 日：是提交PQC 新算法的截止日期。

后量子时代密码系统的现状

- 截止到2017年11月30日前，NIST共收到各种后量子时代公钥密码方案82项，其中59项有关秘钥分发/加密解密，另23项有关身份认证/电子签名。这些方案来自六大洲的25个国家。中国也提交了一个方案，但与量子密码通信技术完全无关。
- 在提交的82项方案中，有些方案受到较多的关注，它们都是达到抗量子攻击所必需的安全级别为128位的公钥密码。

后量子密码算法举例

- NTRUEncrypt：基于阻格数学原理，最受关注。优点主要是内存占用低和运行速度快。缺点是涉及专利。
- McEliece与Goppa：McEliece加密系统是目前密码界的一颗新星，它是第一个在加密过程中使用随机化的算法。它的优点是比RSA更快捷，主要缺点是密钥位数过长。典型的RSA密钥的键长是2048位，而McEliece键长达512千位，是RSA的256倍。
- Ring Learning with Errors（RLWE，带错的环学习）：另一个很有希望的后量子密钥分发方法。它与场/集合理论中的问题有关，可以用于同态加密，这是密码界的另一个热点。RLWE使用7000位的密钥，比McEliece密钥短得多，与现在常用的RSA密钥长度在同一数量级。
- CECPQ1：一匹黑马。谷歌在RLWE基础上研发并做了实际测试。是椭圆曲线算法(Curve 25519)和RLWE变体的一种组合算法。浏览器测试除了发现增加了1毫秒的延迟外，并没有发现任何其他障碍。

后量子时代密码系统的展望

- 2017年12月：NIST公布所有提交的新算法；
- 2018年4月：召开第一届PQC算法标准化全会，由算法提交方作陈述，并听取专家意见；
- 对第一轮候选PQC算法进行16~18个月的评估和分析；
- 2019年9月：召开第二届PQC算法标准化全会；
- 对第二轮候选算法做出进一步评估和分析；
- 估计在2022年或稍后，PQC算法的标准草案会正式公布并开始征求意见。

要求和评估标准

- **1. 安全性。**先决条件和首要标准。对公钥密码新算法的安全性评估不仅要考虑量子计算机的攻击。
- **2. 运行性能。**高效率低成本是选择后量子时代新公钥密码系统的重要考量。
- **3. 兼容性。**必须与今日互联网的物理设备和各种通信协议兼容，必须与TLS无缝衔接。
- **4. 还要解决互联网安全的一些老问题和新矛盾，**诸如解密出错、PFS和侧道攻击等等。

观点：量子通信技术无法替代公钥密码系统

引自：2018年第3期 CCCF专栏：徐令予（UCLA）| 互联网安全的忠诚卫士

如何应对公钥密码未来的安全隐患，存在两条截然不同的路线：主流路线是美国国家标准与技术研究院的规划，用10年时间制定出后量子时代密码系统的新标准；另一方案是中国于2017年建成的京沪量子密码通信干线。这两种方案形成鲜明的对比，美国走的是保守改革的路线，中国采取了激进革命的路线。

- 论文《后量子时代的RSA》(eprint.iacr.org/2017/351.pdf)结论是现今使用的公钥密码RSA不会因为量子计算机的出现而消亡. 其观点是假设量子计算机已经建成，再假设量子计算机的量子位(Qbit)可以无限扩展，进一步假设该量子计算机的运行成本与现在通用电子计算机的成本相当，用这样一台想象出来的超级量子计算机来破解长度为Terabyte³的RSA公钥密码需要量子计算机进行2^100次的量子位操作。只要现行的RSA公钥增加字长和改善算法，就能迫使量子计算机的恶意攻击付出难以承受的代价，公钥密码在后量子时代具有足够长的生命力。
- 基于BB84协议的京沪量子通信干线只有公钥密码的第一项密钥分发功能；
- 而且量子通信在工程上还面临成本和可行性的严峻挑战；
- 目前的量子密码通信技术却完全无法进入互联网。不能与现存的密码系统兼容，不能成为TLS协议的组成部分。
- 信息安全问题是个很长的链条，密码技术只是其中的一个环节，密钥分发又是这一环节中的一个细节。保证这一个细节的安全当然是应该的，但某些媒体无限拔高它的重要性是不对的，声称要不惜一切代价提高它的安全性更是错误的。这可能会扭曲正常的资源配置，而且会误导公众。
- 量子密码通信的绝对安全仅仅停留在理论上，而在工程实施过程中由于存在噪声和检测设备缺陷等各种不可克服的因素，要做到绝对安全根本不可能。
- 严重的问题就在于“可信任中继站”。