

密码学

第十五讲 密码协议

张焕国

武汉大学计算机学院

空天信息安全与可信计算教育部重点实验室





内容简介

- 第一讲 信息安全概论
- 第二讲 密码学的基本概念
- 第三讲 数据加密标准 (DES)
- 第四讲 高级数据加密标准 (AES)
- 第五讲 中国商用密码 (SMS4)
- 第六讲 分组密码的应用技术
- 第七讲 序列密码
- 第八讲 复习
- 第九讲 公钥密码 (1)





内容简介

第十讲 公钥密码 (2)

第十一讲 数字签名 (1)

第十二讲 数字签名 (2)

第十三讲 HASH函数

第十四讲 认证

第十五讲 密码协议

第十六讲 密钥管理 (1)

第十七讲 密钥管理 (2)

第十八讲 复习

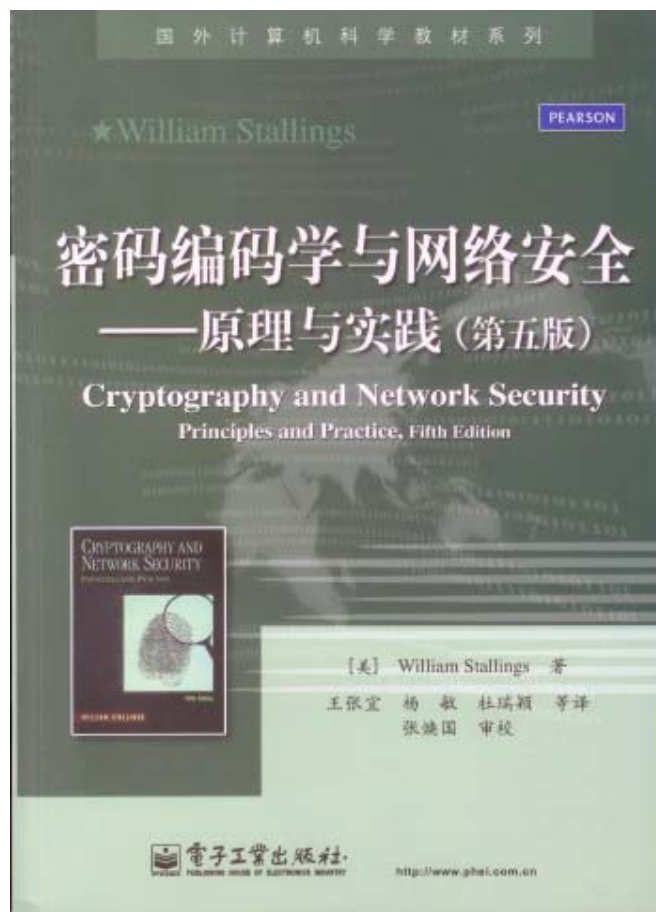


教材与主要参考书

教材



参考书



武汉大学



一、密码协议的概念

1. 协议的概念

- 所谓协议（Protocol），就是指两个或两个以上的参与者为了完成某一特定任务而采取的一系列执行步骤。

这里包含了三层含意：

- ① 协议是一个有序的执行过程。每一步骤都必须执行，且执行是依序进行的。随意增加和减少执行步骤或改变步骤的执行顺序，都是对协议的篡改或攻击。
- ② 协议至少要有两个参与者。虽然一个人可以通过执行系列的步骤来完成某种任务，但是它不构成协议。
- ③ 协议的执行必须能完成某种任务。





一、密码协议的概念

● 举例-1:

执行本协议，A把数据M安全地传送给B。

发方A:

- ① A首先查公钥数据库PKDB，查到B的公开的加密钥 K_{eB} 。
- ② A用 K_{eB} 加密M得到密文C: $C=E(M, K_{eB})$
- ③ A发C给B。

收方B:

- ① B接收C。
- ② B用自己的保密的解密密钥 K_{dB} 解密C，得到明文 $M=D(C, K_{dB})$ 。

- 我们已经知道: 该协议能确保数据秘密性，不能确保数据真实性。





一、密码协议的概念

2. 协议与算法的比较

- 算法是求解问题的一组有穷的运算规则，这些规则给出了求解特定类型问题的运算序列。算法具有以下特征：
 - ① 有穷性。一个算法总是在运算有穷步之后结束，而且每一步都可以在有穷时间内完成。
 - ② 确定性。算法的每一个步骤都必须有确定的含义，无二义性，并且在任何条件下算法都只有唯一的一条执行路径。





一、密码协议的概念

2. 协议与算法的比较

- ③ **输入**。算法可以有输入，也可以无输入。这些输入是在算法开始执行前提供给算法的。
- ④ **输出**。算法有一个或多个输出。这些输出是与输入有某种确定关系的量。
- ⑤ **能行性**。算法的执行所花费的时间和空间是在现实计算资源条件下可实现的。





一、密码协议的概念

2. 协议与算法的比较

- 协议和算法都是一组有穷的运算或处理步骤。它们都要求具有有穷性、确定性和能行性。
- 协议强调至少要有两个参与者，而且双方之间还要进行通信。而算法却不要求这一点。
- 例如，计算 N 以内的自然数的和的方法，对一个合数进行因子分解的方法，都是算法，却都不是协议。因为它们都不要求至少要有两个参与者，一个人就可以计算完成。
- 协议强调完成某一特定任务，而算法强调问题求解。换句话说，协议强调处理，而算法强调计算。





一、密码协议的概念

2. 协议与算法的比较

- 协议的执行步骤在粒度上比较粗、比较宏，例如协议的一个步骤可以是执行一个算法。而算法的执行步骤在粒度上比较细，其步骤常常是一些基本运算和操作。
- 由于算法强调计算，所以输入和输出都是一些量。与算法类似，协议也有自己的输入和输出，输入通常是协议执行的一些条件，而输出则是协议执行的结果，结果通常表现为一种状态。
- 总而言之，算法和协议是两种不同层次上的概念。算法是低层次上的概念，而协议是高层次上的概念，协议建立在算法的基础之上。





一、密码协议的概念

3. 安全协议

- 协议是网络通信的基础之一。网络通信的各方根据协议进行消息的交互、数据的传递和信息的共享。良好的网络通信协议应当高效和节省，并且能确保信息的安全性。
- 我们称具有安全功能的协议为安全协议。因为密码技术是确保信息安全的关键技术，所以安全协议都采用密码技术。因此，通常又称安全协议为密码协议。
- 在网络通信中，人们利用密码协议实现诸如密钥交换、身份认证、站点认证、报文认证等安全功能。在电子商务中，人们利用密码协议实现安全电子交易。





一、密码协议的概念

3. 安全协议

- 协议的安全性则根据具体的协议不同，而有不同的含义。通常可以包含以下的部分或全部属性：
 - 认证性
 - 秘密性
 - 完整性（真实性）
 - 不可否认性
 - 公平性（电子商务协议要求）





一、密码协议的概念

4. 协议分类

根据密码协议的功能可以将其划分为以下四类：

① 密钥建立协议

网络通信系统中的密钥建立协议，**用于在通信的各方之间建立会话密钥**。会话密钥是用于保护一次会话通信的密钥。协议中的密码算法可以采用对称密码，也可以采用公钥密码。

② 认证协议

网络通信系统中的认证协议主要包括身份认证协议，通信站点认证协议，报文认证协议等。





一、密码协议的概念

4. 协议分类

③ 身份认证和密钥建立协议

把身份认证和密钥建立结合起来，形成了认证和密钥建立协议。首先进行通信实体的身份认证，然后建立会话密钥，随后通信实体就可以进行保密通信了。这类协议是保密通信中最常用的一类协议。

④ 电子商务协议

在电子商务中通过协议进行电子交易和电子支付，电子商务除了关心秘密性、完整性外，还十分关心交易的公平性。





二、密码协议的设计与分析

1. 密码协议的安全性

● 密码协议的安全缺陷

■ 我们给大家介绍了公钥密码的三种基本工作方式。每种都是一个密码协议：

- ① 只加密不签名的协议可确保数据秘密性，不能确保数据真实性。
- ② 只签名不加密的协议可确保数据真实性，不能确保数据秘密性。
- ③ 先签名后加密的协议可同时确保数据秘密性和数据真实性。

■ 现在我们指出，这些结论在不考虑协议攻击的情况下是正确的。如果考虑攻击，将会出现新情况。





二、密码协议的设计与分析

1. 密码协议的安全性

● 举例-2: 分析先签名后加密协议

$A \rightarrow B: E(D(M, K_{dA}), K_{eB})$

的安全缺陷。

- 第一种攻击: 假设B不诚实
- B收到报文后用自己的解密密钥 K_{eB} 解密, 可得到 $D(M, K_{dA})$ 。他再用C的公开的加密钥 K_{eC} 加密后发给C。即 $B \rightarrow C: E(D(M, K_{dA}), K_{eC})$ 。
- C收到后会以为是A直接与他通信, 而不知道是B重发A发给B的消息。
- 原因: 报文中没有报文源宿的标识, 没有进行认证。





二、密码协议的设计与分析

1. 密码协议的安全性

● 举例-2: 分析先签名后加密协议

$A \rightarrow B: E(D(M, K_{dA}), K_{eB})$

的安全缺陷。

- 第二种攻击: 假设T是攻击者
- 由于报文中没有时间信息, 也不进行报文时间合理性的认证, 所以T可以把截获到的以前的A发给B的报文重播发给B, 而B不能发现。
- 为了对抗重放攻击, 数据中必须有时间标志信息, 并进行时间认证。





二、密码协议的设计与分析

1. 密码协议的安全性

● 举例-3: 分析先加密后签名协议

$A \rightarrow B: D(E(M, K_{eB}), K_{dA})$

的安全缺陷。

■ 假设T是攻击者

■ T截获A发给B的报文。

■ T先用A的公开加密钥验证签名，可得到

$E(M, K_{eB})$ 。

■ T再用自己的保密的解密密钥 K_{dT} 签名后发给B。即

$T \rightarrow B: D(E(M, K_{eB}), K_{dT})$ 。





二、密码协议的设计与分析

1. 密码协议的安全性

● 举例-3: 分析先加密后签名协议

$A \rightarrow B: D(E(M, K_{eB}), K_{dA})$

的安全缺陷。

- B收到后会以为是T直接与他通信，不知道是T重发A发给B的消息。如果M表示某种承诺或凭证，现在的消息是由T签名的，A就会认为这种承诺或凭证关系是A和T之间的，其实应是A和B之间的。
- 此外，T还可以把截获到的以前的A发给B的报文，重发给B。
- 问题的原因：没有对发送方和收方进行认证，没有对文的时间进行认证。





二、密码协议的设计与分析

1. 密码协议的安全性

- 密码协议存在安全缺陷是比较普遍的。估计超过一半的公开协议存在安全缺陷。
- 攻击分类
 - ① 对协议中的密码算法进行攻击。
 - ② 对协议中的密码技术进行攻击。
 - ③ 对协议本身进行攻击。
- 防范对密码算法和密码技术的攻击，不属于协议安全研究内容。
- 在研究协议安全时，总是假设密码算法和密码技术是全的。





二、密码协议的设计与分析

1. 密码协议的安全性

- 对协议本身的攻击又可分为**被动攻击**和**主动攻击**
 - 被动攻击是指协议外部的实体对协议的全部或部分执行过程实施窃听，收集协议执行中所传送的消息，并分析消息，从中得到自己感兴趣的信息。
 - 攻击者的窃听不影响协议的执行，所以被动攻击难于检测。因此在设计协议时应当考虑的重点是确保协议能够抵抗被动攻击，而不是检测被动攻击。
 - **主动攻击是指攻击者试图篡改协议中传送的消息，插入新的消息，甚至改变协议的执行过程。**
 - 显然，主动攻击比被动攻击具有更大的危险性。常见的主动攻击有重放攻击，等。



二、密码协议的设计与分析

1. 密码协议的安全性

● 举例-4: 分析下面的协议

①A→B: $(ID_A, ID_B, E(M, K_{eB}))$, 其中 ID_A, ID_B 是A、B为标识符;

②B→A: $(ID_B, ID_A, E(M, K_{eA}))$, 以表示收到M。

■ 攻击这一协议:

①攻击者T截获A发送给B的消息 $(ID_A, ID_B, E(M, K_{eB}))$, 并篡改为 $(ID_T, ID_B, E(M, K_{eB}))$ 。

②攻击者T将 $(ID_T, ID_B, E(M, K_{eB}))$ 发送给B。

③B接收到 $(ID_T, ID_B, E(M, K_{eB}))$ 后根据协议规定, 给T返回 $(ID_B, ID_T, E(M, K_{eT}))$ 。

④T接收 $(ID_B, ID_T, E(M, K_{eT}))$, 解密获得消息M。





二、密码协议的设计与分析

1. 密码协议的安全性

● 举例-4

- 原因之一是，协议的设计不合理，B回送的表收到数据的报文中含有明文数据M。如果回送报文中没有M，则攻击者将不能得到M。
- 另一原因是，发方和收方标识符没有与数据M加密绑定，以致于可被篡改。
- 另外，上述协议的报文中也没有时间信息，也进行时间认证，所以也不能抵抗重播攻击。





二、密码协议的设计与分析

2. 密码协议的设计原则

- 如果在协议设计阶段就充分考虑到一些可能破坏协议安全性的问题，并加以避免，将是有益的。
- 协议的设计原则
 - ① 消息独立完整性原则
 - 协议中的每一消息都应准确地表达出它所想要表达的含义。消息含义的解释应完全由其内容来决定，而不用借助于上下文来推断。
 - 假设协议的一个步骤为 $A \rightarrow B: M$ ，想表达A把数据M发给B。因为M没有与A和B绑定，光从M看不出是由A发给B的，要借助于上下文来分析。这样攻击者就可以替换数据M或替换发方和收方。
 - 协议的描述可以用形式化语言来描述，也可以用自然语言来描述。但形式化语言描述更严格。





二、密码协议的设计与分析

2. 密码协议的设计原则

- 协议的设计原则

- ② 消息前提准确原则

- 与消息相关的先决条件应当明确给出，并且其确定性与合理性应能得到验证。
 - 不仅要考虑消息本身，还要考虑与每条消息相关的条件是否合理，每条消息所基于的假设是否够成立。





二、密码协议的设计与分析

2. 密码协议的设计原则

- 协议的设计原则

- ③ 主体身份标识原则

- 如果一个主体的标识对于某个消息的含义是重要的，就应当在消息中明确地附加上主体的名称。
- 主体的名称可以以明文形式出现。也可以采用加密或签名技术对主体名称进行保护。





二、密码协议的设计与分析

2. 密码协议的设计原则

- 协议的设计原则

- ④ 明确加密目的原则

- 明确采用加密的目的，否则将造成冗余。
- 采用密码算法并不是协议安全的代名词，密码算法的不正确应用可能导致协议出现错误。
- 应用密码算法时必须知道为什么要应用以及如何应用它。
- 加密可以实现多种安全目的，如秘密性、完整性和认证性等，但是在应用时必须确保它能够实现你所希望的某种安全目标。





二、密码协议的设计与分析

2. 密码协议的设计原则

● 协议的设计原则

⑤ 明确签名原则

- 签名可以确保数据的真实性和抗抵赖。
- 如果需要同时采用签名和加密，应当采用先签名后加密的方式。
- 应当对数据的**Hash**值进行签名，不直接对数据签名。





二、密码协议的设计与分析

2. 密码协议的设计原则

● 协议的设计原则

⑥ 随机数的使用原则

- 在协议中使用随机数可以认证消息的新鲜性。
- 在使用随机数时，应当明确其所起的作用和属性。
- 问题的关键是随机数最好是真正随机的，至少具有足够安全的伪随机性。





二、密码协议的设计与分析

2. 密码协议的设计原则

● 协议的设计原则

⑦ 时间戳的使用原则

■ 时间戳可用来确保消息的时效性

■ 当使用时间戳时，必须考虑各个计算机的时钟与标准时钟的误差，这种误差不应当影响协议执行的有效性。

■ 时间戳依赖于系统中时钟的同步，但是做到这一点是很不容易的。





二、密码协议的设计与分析

2. 密码协议的设计原则

● 协议的设计原则

⑧ 编码原则

- 协议中消息的编码格式与协议安全密切相关，应当明确协议中消息的具体数据格式，而且还要验证这种格式对安全的贡献。

⑨ 最少安全假设原则

- 在进行协议设计时，常常要对系统环境进行风险分析，做出适当的初始安全假设。如认为所采用的密码算法是安全的，认证服务器是可信的，等等。

- 但是注意，初始的安全假设越多，则协议的安全性就越差。这是因为，一旦初始的安全假设的安全性受到威胁，将直接威胁到协议的安全。因此，在协议设计时应当采用最少安全假设原则。





二、密码协议的设计与分析

3. 密码协议的分析

- 协议安全分析的目的就是要揭示协议是否存在安全漏洞和缺陷。
- 分析的方法有攻击检测方法和形式化分析方法。
- 攻击检测又称为穿透性检测，是一种非形式化的分析方法。它根据已知的各种攻击方法来对协议进行攻击，以攻击是否有效来检测协议是否安全。这种方法的缺点是只能发现已知的安全漏洞和缺陷，不能发现未知的安全漏洞和缺陷。
- 早期主要采用攻击检测。





二、密码协议的设计与分析

3. 密码协议的分析

● 形式化分析方法

① 形式逻辑方法

- 形式逻辑分析方法是一种基于知识和信仰的分析方法。
- 形式化逻辑以BAN逻辑为代表，还包括许多对BAN逻辑进行扩充和改进的其他逻辑。
- 这种方法定义了协议的目标，并确定了协议初始时刻各参与者的知识和信仰，通过协议中的发送和接收步骤产生新的知识，运用推理规则得到最终的知识 and 信仰。如果最终的知识 and 信仰的语句集合里不包含所要得到的目标知识和信仰的语句时，就说明协议存在安全缺陷。
- BAN逻辑简单、直观，使用方便，而且可以成功地发现协议中存在的安全缺陷。但是，由于BAN逻辑本身缺少精确定义的语义基础，所以它不能检测对协议的攻击。





二、密码协议的设计与分析

3. 密码协议的分析

② 模型检测方法

- 把密码协议看成一个分布式系统，每个主体执协议的过程构成局部状态，所有局部状态构成系统的全局状态。
- 每个主体的收发动作都会引起局部状态的改从而也就引起全局状态的改变。
- 在系统可达的每一个全局状态检查协议的安全性是否得到满足，如果不满足则检测到协议的全缺陷。





二、密码协议的设计与分析

3. 密码协议的分析

② 模型检测方法

- 模型检测方法已被证明是一种非常有效的方
它具有自动化程度高，检测过程不需要用户参与，如果协议存在安全缺陷就能够自动产生反等优点。
- 但是，因为这一方法是通过穷尽搜索存在攻击情况下所有可能的执行路径，来发现协议可能存在的安全缺陷，所以它的缺点是容易产生状态间爆炸问题，因而不适合复杂协议的检测。





二、密码协议的设计与分析

3. 密码协议的分析

③ 定理证明方法

- 定理证明方法试图证明协议满足安全属性，而是寻找对协议的攻击。因此，定理证明方法属正面证明方法。
- 比较有代表性的定理证明方法有Spi演算方法、归纳方法、串空间方法等。
- 定理证明方法是一种比较新的协议分析方法，有很大的发展空间。它的缺点是难于完全自动化。





二、密码协议的设计与分析

3. 密码协议的分析

- 协议的形式化分析将协议的描述形式化，借助于人工和计算机分析推理，来判断协议是否安全。
- 形式化分析方法与非形式化分析方法相比，能够全面、深刻地检测协议的细微的安全漏洞和缺陷。
- 它不仅能够发现已知的安全漏洞和缺陷，还能发现未知的安全漏洞和缺陷。
- 目前协议的形式化分析离实际应用还有距离，还需要大力研究。





作业题

1、p236第12题。





谢 谢！



武汉大学