高等院校信息安全专业规划教材

密码协议形式化分析

- 论述了国内外最新的密码协议形式化分析方法与设计准则
- 建立了完整而系统的密码协议研究理论
- 介绍了当前最为流行的几个密码协议的实现方法

王亚弟　束妮娜　韩继红　王　娜　编著
沈昌祥　审

机械工业出版社
CHINA MACHINE PRESS

高等院校信息安全专业规划教材

密码协议形式化分析

王亚弟　束妮娜　韩继红　王　娜　编著
沈昌祥　审

机械工业出版社

本书对现在国内外最新的密码协议形式化分析方法与设计准则进行了比较详细的论述，建立了完整而系统的密码协议研究理论，并介绍了当前最为流行的几个密码协议的实现方法。

全书共8章，分别介绍了密码协议所涉及的密码学基础知识，密码协议的概念、缺陷与可能受到的攻击类型，现有的一些密码协议形式化分析方法，密码协议的设计准则，密码协议分析的主要形式化语言和分析工具，Kerberos协议、IPSec协议、SSL协议、X.509以及SET协议这五个密码协议的实现方法和工作原理。

本书适合作为高等院校信息安全专业本科生、研究生使用，也可供从事信息安全研究的科技人员参考。书的最后附有相关的参考文献，提供了与本书有关的资料，供有兴趣的读者参考。

图书在版编目（CIP）数据

密码协议形式化分析/王亚弟等编著. —北京：机械工业出版社，2006.9
（高等院校信息安全专业规划教材）
ISBN 7-111-19229-X

Ⅰ.密… Ⅱ.王… Ⅲ.密码－理论－高等学校－教材 Ⅳ.TN918.1

中国版本图书馆CIP数据核字(2006)第054622号

机械工业出版社(北京市百万庄大街22号 邮政编码 100037)
策 划：胡毓坚
责任编辑：陈振虹
责任印制：李 妍
北京诚信伟业印刷有限公司印刷
2006年7月第1版·第1次印刷
184mm×260mm·16.5印张·406千字
0001—2000册
定价：29.00元

高等院校信息安全专业规划教材

编委会成员名单

出版说明

信息技术的发展和推广，为人类开辟了一个新的生活空间，它正对世界范围内的经济、政治、科教及社会发展各方面产生重大的影响。如何建设安全的网络空间，已成为一个迫切需要人们研究、解决的问题。目前，与此相关的新技术、新方法不断涌现，社会也更加需要这类专门人才。为了适应对信息安全人才的需求，我国许多高等院校已相继开设了信息安全专业。为了配合相关的教材建设，机械工业出版社邀请了解放军信息工程大学、解放军理工大学通信工程学院、上海交通大学、西安电子科技大学、湖南大学、南京邮电学院等高校的专家和学者，成立了教材编委会，共同策划了这套面向高校信息安全专业的教材。

本套教材的特色：

1. 作者队伍强。本套教材的作者都是全国各院校从事一线教学的知名教师和学术带头人，具有很高的知名度和权威性，保证了本套教材的水平和质量。

2. 系列性强。整套教材根据信息安全专业的课程设置规划，内容尽量涉及该领域的方方面面。

3. 系统性强。能够满足专业教学需要，内容涵盖该课程的知识体系。

4. 注重理论性和实践性。按照教材的编写模式编写，在注重理论教学的同时注意理论与实践的结合，使学生能在更大范围内、更高层面上掌握技术，学以致用。

5. 内容新。能反映出信息安全领域的最新技术和发展方向。

本套教材可作为信息安全、计算机等专业的教学用书，同时也可以供从事信息安全工作的科技人员以及相关专业的研究生参考。

机械工业出版社

序

随着信息技术和网络技术的飞速发展，信息网络的广泛应用已成为社会进步和发展的重要标志之一，由此引发的网络安全问题越发显得重要。密码协议（也称安全协议）作为保证网络安全的基础和关键，对于保证网络安全起着十分重要的作用。20世纪70年代末以来，密码协议的安全性分析和研究已取得令人瞩目的成就，已经成为一个研究热点。但是，由于密码协议设计与分析的复杂性，使得该研究变得更加困难并具有挑战性，同时也是一项紧迫且意义重大的工作。

密码协议的安全性分析方法主要有两大类：一类是非形式化的分析方法（也称为攻击验证方法）；一类是形式化的分析方法。非形式化方法，是根据已知的各种攻击方法对协议进行攻击，以攻击是否有效来检验密码协议是否安全，这种分析方法的关键是在于攻击方法的选择。然而，非形式化方法只是停留于发现密码协议中是否存在已知的缺陷，不能全面客观地分析密码协议。形式化分析方法能够全面、深刻地检测到密码协议中细微的漏洞，不仅能发现已知的攻击，而且能够发现未知的攻击。形式化分析方法是采用各种形式化的语言或模型，为密码协议建立模型，并按照规定的假设、分析和验证方法，验证密码协议的安全性。目前有多种形式化分析方法，采用不同的技术和方法从不同的侧面对密码协议进行安全性分析。

《密码协议形式化分析》一书的作者们多年从事密码协议的安全性研究，对设计和分析实用密码协议的具体原则、方法和相关形式化理论与技术进行了系统的研究。本书在分析总结该领域众多研究成果的基础上，结合作者多年从事的理论研究和科研实践工作，对密码协议形式化分析验证方法的理论和技术作了系统的阐述，是一本比较全面论述密码协议形式化分析的书籍，对学习和了解密码协议形式化分析方法、指导密码协议的设计和分析具有较好的参考价值。

中国工程院院士　沈昌祥

前　言

随着计算机网络的普及与发展，人类对网络的依赖越来越大。计算机网络的最大特点是开放性，它给人们带来巨大便利的同时，也对网络上信息的安全保护提出了巨大的挑战。如果不能切实有效地解决计算机网络的安全问题，必将影响到它的应用及发展。采用密码技术的密码协议是构建安全网络环境的基石，密码协议的目标不仅仅是为了实现信息的加密传输，更重要的是为了解决网络中的安全问题，它的正确性对于网络安全极其关键。但是密码协议的设计是困难且易于出错的，直观的原因是密码协议是在攻击者存在情况下的异步通信，攻击者能够截获、分解，以及修改所交换的消息。因此，密码协议的执行具有高度不确定性，即便是对有限条件约束下的密码协议也要求分析潜在无限可能的攻击者行为。也就是说，有些密码协议往往不如它们的设计者所期望的那样安全。其实，密码协议中的很多缺陷和漏洞往往不是因为协议中使用的密码算法引起的，而是由协议自身的结构引起的。密码协议安全性的达成需从两方面着手：一是通过一些方法在协议设计过程中加以指导；二是在协议设计完成后进行安全性分析。目前，密码协议的设计与分析已成为一个研究热点，研究人员已提出多种形式化方法来解决这个问题。本书对现在国内外最新的密码协议形式化分析方法与设计准则进行了比较详细的论述，建立了完整而系统的密码协议研究理论，并介绍了当前最为流行的几个密码协议的实现方法。

全书共8章。第1章介绍了密码协议所涉及的密码学基础知识，包括密码体制、数字签名、Hash函数、密钥管理与分配以及公钥证书和基础设施。第2章主要介绍了密码协议的概念、缺陷与可能受到的攻击类型，以及密码协议形式化分析的研究现状与面临的挑战。第3、4、5章分别介绍了现有的一些密码协议形式化分析方法，包括形式逻辑方法、模型检测方法和定理证明方法。第6章介绍了密码协议的设计准则。第7章介绍了密码协议分析的主要形式化语言和分析工具。第8章介绍了5个密码协议的实现方法和工作原理，包括Kerberos协议、IPSec协议、SSL协议、X.509以及SET协议。

本书是在我国著名的信息安全专家沈昌祥院士的提议、指导和帮助下完成的，沈院士还在百忙中担任了本书的主审。在本书出版之际，我们向沈院士致以真挚的谢意。

作　者

目　录

第1章 引 论

1.1 密码体制

1.1.1 基本原理

密码体制是密码协议的基础。采用密码方法可以隐蔽和保护需要保密的消息，使未授权者不能提取信息。被隐蔽的消息称为明文。由明文变换成的另一种形式的信息，称为密文或密报。这种变换过程称为加密。其逆过程，即由密文恢复出原明文的过程称为解密。对明文进行加密时所采用的一组规则称为加密算法。传送消息的预定对象称为接收者，他对密文进行解密时所采用的一组规则称为解密算法。一般而言所使用的加解密算法是公开的。加密和解密算法的操作通常都是在一组密钥的控制下进行的，分别称为加密密钥和解密密钥。密钥是密码体制安全保密的关键，加解密操作的使用受限于对所涉及的密钥的访问的适当约束。加密与解密过程如图 1-1 所示。

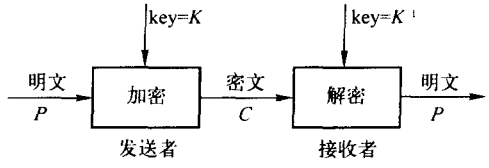

图 1-1 加密与解密

其中，P 表示明文，C 表示密文，K 表示加密密钥，K^{-1}表示解密密钥。

1.1.2 密码体制分类

密码体制从原理上可分为两大类，即单钥体制（又称为对称密码体制）和双钥体制（又称为公钥密码体制或非对称密码体制）。

1. 单钥体制

在单钥体制中，加密密钥和解密密钥相同，因此又称为对称密码体制。对数据进行加密的单钥系统如图 1-2 所示。系统的保密性主要取决于密钥的安全性。如何产生满足保密要求的密钥是这类体制设计和实现的主要课题。另一个重要问题是如何将密钥安全可靠地分配给通信双方，这在网络通信条件下就更为复杂，包括密钥产生、分配、存储、销毁等多方面的问题，统称为密钥管理。这是影响系统安全的关键因素，即使密码算法再好，若密钥管理问题处理不好，也很难保证系统的安全保密。有关密钥管理的内容将在第 1.4 节中讨论。

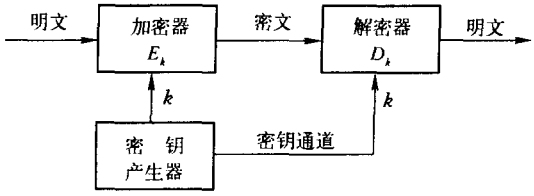

图 1-2 单钥保密体制

单钥体制的古典算法有简单代换、多表代换、同态代换、多码代换、乘积密码等多种。现代算法有 DES、IDEA、AES 等。

单钥体制不仅可以用于数据加密，也可用于消息的认证，如可以在口令认证系统中用来验证用户的身份。

2. 双钥体制

双钥体制的观点是由 Diffie 和 Hellman 在 1976 年首次提出的，它使密码学发生了一场变革。采用双钥体制的每个用户都有一对选定的密钥：一个是公开密钥，可以对任何其他用户公开，以 K 表示；另一个则是私有的秘密密钥，仅为自己拥有，以 K^{-1} 表示。公开的密钥 K 可以像电话号码一样注册公布，因此双钥体制又称为公钥体制或非对称密码体制。加密算法 E 和解密算法 D 都是公开的。虽然 K^{-1} 是由 K 决定的，但从已知的 K 推导出 K^{-1} 在“计算上是不可行的”。

双钥体制的主要特点是将加密和解密能力分开，因而可以实现多个用户加密的消息只能由一个用户解读，或只能由一个用户加密消息而使多个用户解读。前者可用于公共网络中实现保密通信，而后者可用于认证系统中对消息进行数字签名。

双钥体制用于保密通信如图 1-3 所示。图中假定用户 A 要向用户 B 发送机密消息 m。若用户 A 在公钥本上查到用户 B 的公开密钥 K_B，就可用它对消息 m 进行加密得到密文 $c=E_{K_B}(m)$，而后送给用户 B。用户 B 收到后以自己的秘密密钥 K_B^{-1} 对 c 进行解密得到原来的消息

$$m=D_{K_B^{-1}}(c)=D_{K_B^{-1}}\left(E_{K_B}(m)\right)$$

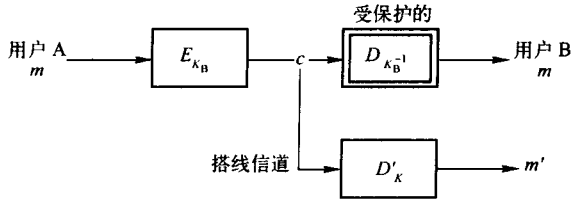

图 1-3　双钥保密体制

系统的安全保障在于从公开密钥 K_B 和密文 c 推出明文 m 或解密密钥 K_B^{-1} 在计算上是不可行的。由于任一用户都可用用户 B 的公开密钥 K_B 向他发送机密消息，因而密文 c 不具有认证性。

为了使用户 A 发给用户 B 的消息具有认证性，可以将双钥体制的公开密钥和秘密密钥反过来用，如图 1-4 所示。用户 A 以自己的秘密密钥 K_A^{-1} 对消息 m 进行 A 的专用变换 $D_{K_A^{-1}}$，得到密文 $c=D_{K_A^{-1}}(m)$ 送给用户 B，B 收到 c 后可用 A 的公开密钥 K_A 对 c 进行公开变换就可得到恢复的消息

$$m=E_{K_A}(c)=E_{K_A}\left(D_{K_A^{-1}}(m)\right)$$

由于 K_A^{-1} 是秘密的，其他人都不可能伪造密文 c，在用 A 的公开密钥解密时得到有意义的消息 m。因此，可以验证 m 来自 A 而不是其他人，从而实现了对 A 所发消息的认证。

为了同时实现保密性和认证性，可以采用双重加、解密，如图 1-5 所示。在明文消息空间和密文消息空间等价，且加密、解密运算次序可换，即 $E_K(D_K^{-1}(m))=D_K^{-1}(E_K(m))=m$ 的条件下就不难用双钥体制实现。例如，用户 A 要向用户 B 传送具有认证性的机密消息 m，

可将 B 的一对密钥作为保密之用，而将 A 的一对密钥作为认证之用。可按图 1-5 的顺序进行变换。A 发送给 B 的密文为

$$c = E_{K_B}\left(D_{K_A}^{-1}(m)\right)$$

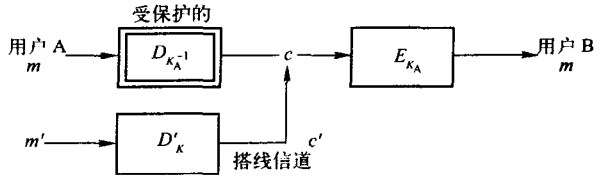

图 1-4　双钥认证体制

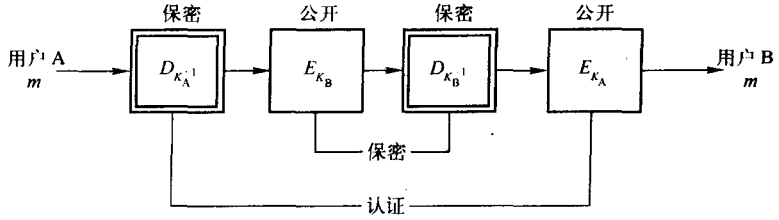

图 1-5　双钥保密和认证体制

B 恢复明文的运算过程为

$$\begin{aligned} m &= E_{K_A}\left(D_{K_B}^{-1}(c)\right) \\ &= E_{K_A}\left(D_{K_B}^{-1}\left(E_{K_B}\left(D_{K_A}^{-1}(m)\right)\right)\right) \\ &= E_{K_A}\left(D_{K_A}^{-1}(m)\right) \end{aligned}$$

1977 年由 Rivest，Shamir 和 Adleman 提出了第一个比较完善的公钥密码算法，这就是著名的 RSA 算法。从那时起，人们基于不同的计算问题，给出了大量的公钥密码算法，如背包、Rabin、EIGamal、椭圆曲线等。目前关于数字签名的研究主要集中在基于公钥密码体制的数字签名研究上。

公钥密码算法往往基于解决某些问题的计算困难性上，RSA 算法的安全性是基于分解大整数的困难性，这也引发了人们对因子分解这一古老的数论问题的兴趣并取得了一些可喜的进展。目前，最有实用价值的因子分解算法有二次筛法、数域筛法、椭圆曲线算法等。

单钥体制的缺点是在进行保密通信之前，双方必须通过安全信道传送所用的密钥，这对于相距较远的用户可能要付出太大的代价，甚至难以实现。另外在有众多用户的网络通信下，为了使 n 个用户之间相互进行保密通信，将需要 $\binom{n}{2} = n(n-1)/2$ 个密钥；当 n 大时，代价也是很大的。双钥体制则完全克服了上述缺点，特别适用于多用户通信网，它大大减少了多用户之间通信所需的密钥量，便于密钥管理。这一体制的出现是密码学研究中的一项重大突破。

1.2　数字签名

数字签名(Digital Signature)在信息安全，包括身份认证、数据完整性、不可否认性以及匿

名性等方面具有重要应用，特别是在大型网络安全通信中的密钥分配、认证以及电子商务系统中具有重要作用。数字签名类似于手写签名，具有不可仿造性和不可否认性。随着计算机网络技术的发展，数字签名技术也在不断发展，并得到广泛应用。

1.2.1 数字签名技术

数字签名与手写签名一样，是认证的主要工具，其主要目的是防抵赖、防否认、防冒充和防篡改。通过数字签名，可以对签名者身份、签名日期进行验证，对被签的消息内容进行认证，而且，在出现争执时，签名应能由第三方进行仲裁。因此，数字签名应满足以下主要条件：

1）数字签名必须是与被签消息相关的信息。

2）为了防止伪造和否认，签名必须使用签名者独有的信息。

3）接收者能验证签名，而任何其他人都不能伪造签名。

4）伪造数字签名在计算上是不可行的。

基于公钥密码体制和私钥密码体制都可以获得数字签名，目前主要是基于公钥密码体制的数字签名，常用的数字签名体制有 RSA、Rabin、EIGamal、Schnorr、DSS、GOST、离散对数等。图 1-6 和 1-7 分别为 RSA 和 DSS 签名方法的签名与验证过程。

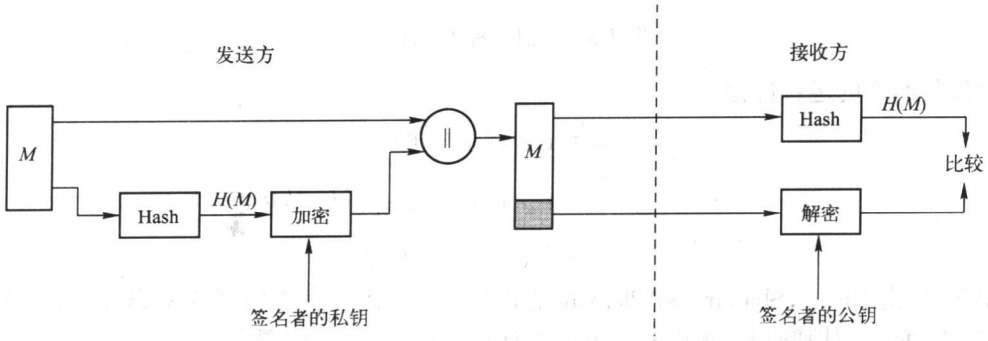

图 1-6　RSA 签名方法

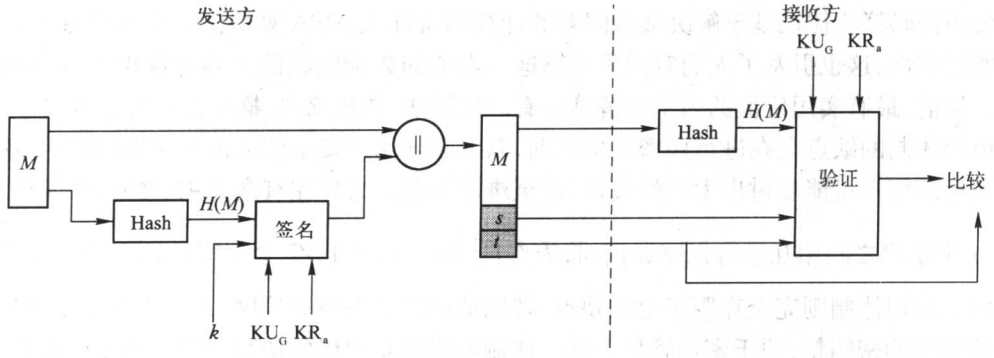

图 1-7　DSS 签名方法

在 RSA 方法中，数字签名和验证步骤如下：

1）发送方用一个 Hash 函数（如采用 SHA-1 或 MD5 算法）对消息进行处理，形成一个固

定长度的信息摘要。

2）发送方用自己的私钥对信息摘要进行加密，产生数字签名。

3）将数字签名和消息一起发送出去。

4）接收方用同样的 Hash 函数对消息进行计算，产生消息摘要 1。

5）接收方用发送方的公开密钥对数字签名解密，产生消息摘要 2。若消息摘要 1 和消息摘要 2 相等，则认为数字签名是有效的；否则，数字签名验证失败。因为只有发送方拥有私钥，因此只有发送方能够产生有效的签名。具体的 RSA 签名算法在 PKCS＃1[118]中进行了描述。

DSS 方法也使用 Hash 函数，签名函数的输入是 Hash 产生的消息摘要和为此次签名而产生的随机数 k，签名过程依赖于发送方的私钥 KRa 和一组通信伙伴所共有的全局公钥 KU_G，生成的签名由 s 和 t 两部分组成。接收方对接收到的消息进行 Hash 运算，并将生成的消息摘要和数字签名一起输入验证函数，验证过程依赖于发送方的公钥 KUa 和一组通信伙伴所共有的全局公钥 KU_G，若验证函数的输出等于签名中的 t，则签名有效。DSS 中使用的数字签名算法 DSA 在 FIPS186 中有详细完整的描述。

以上数字签名方法都属于直接数字签名，其有效性取决于发送方私钥的安全性。与之对应的还有一种仲裁数字签名方法，其基本原理是发送方将每条已签名的消息都先发送给仲裁者，仲裁者对消息及其签名进行检查以验证消息源及其内容，然后给消息加上日期并发送给签名接收者，同时指明该消息已通过仲裁者的检验。通过仲裁者的加入，可以防止签名者对发送消息的否认。

1.2.2 数字签名技术与加密技术的结合

在实际应用中，如果信息是可以公开的，但却必须保证信息不被伪造，则可利用数字签名技术来保证信息的完整性及不可伪造性。如果信息是保密的，则不仅要保证其完整性，而且要保证其保密性，此时需要信息加密技术与数字签名技术同时使用，其工作过程如下：

1）发送端 A 对发送信息 P 进行哈希运算，形成信息摘要 M。

2）A 用自己的私钥对摘要加密，得到 A 是数字签名 C_m。

3）A 随机产生一个对称加密密钥 k，并用该密钥加密信息 P 和 C_m，形成密文 P_m。

4）A 用接收方的公开密钥加密对称密钥，形成 C_k。

5）将 P_m 和 C_k 一起发送给接收方 B。

6）B 收到信息后用自己的私钥对 C_k 解密，获得对称加密密钥 k。

7）B 用 k 解密其余信息，得到明文 P 及数字签名 C_m。

8）B 利用同样的哈希函数对解密得到的明文 P 形成摘要 M'，并用 A 的公开密钥解密加密过的摘要 C_m，得到 M，如果 $M' = M$，则说明信息是正确的。

1.2.3 几种新型的数字签名方案

数字签名是互联网上不可缺少的安全处理技术，目前已有很多人在研究新的算法以适应特殊领域内数字签名的需求，主要包括以下几个方面。

1. 高效可验证的安全数字签名方案

这种数字签名方案能够防止通过猜测 RSA 算法的某些变量来选择信息进行攻击。它的