XML技术及安全基础

◆ 冯柳平　编著

中国工信出版集团

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

XML 技术及安全基础

冯柳平　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

图书在版编目（CIP）数据

XML 技术及安全基础 / 冯柳平编著. —北京：电子工业出版社，2017.1
ISBN 978-7-121-27153-3

Ⅰ. ①X… Ⅱ. ①冯… Ⅲ. ①可扩充语言—程序设计 Ⅳ. ①TP312

中国版本图书馆 CIP 数据核字（2015）第 216098 号

策划编辑：董亚峰
责任编辑：郝黎明
印　　刷：北京季蜂印刷有限公司
装　　订：北京季蜂印刷有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编　100036
开　　本：720×1 000　1/16　印张：18.75　字数：360 千字
版　　次：2017 年 1 月第 1 版
印　　次：2017 年 1 月第 1 次印刷
定　　价：48.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：（010）88254694。

前　言

XML 是一种可扩展标记语言，具有可描述性、结构化、易扩展等特点，并且可以跨平台使用，在网络数据存储和交换中发挥着越来越大的作用。例如数字出版中，数字内容要支持多业态发布，多平台阅读查看，需要一种能跨平台交互并便于网页显示的数据存储格式，XML 通过自定义标签来定义结构化数据内容，不需要依赖于软件和硬件即可完成数据传输，是理想的数据存储传输格式；XML 在电子商务的内容定义和信息交换中也起着重要作用。

但另一方面，在 XML 应用中诸多不安全因素又导致隐私信息和商业机密的泄漏，保证数据存储和传输的安全性已成为迫切的问题，基于 XML 的安全技术，得到了广泛关注和重视。W3C 和 IETF 推出了一系列 XML 安全规范，XML 安全技术的应用不断扩展，一些大公司如 Microsoft、IBM 等都在其产品中加入 XML 安全技术。

XML 安全技术将 XML 技术融合到数据加密、数字签名、权限管理、接入控制、认证鉴别等技术中，用以保护 XML 数据乃至网络中各种数据的安全。本书介绍 XML 及其安全技术，全书共分为 8 章。第 1 章密码学概述，主要介绍对称密码体制和公钥密码体制，消息认证和数字签名。第 2 章 XML 基础，介绍 XML 标准和规范，以及 XML 的基本语法。第 3 章 XML Schema 与有效性验证，介绍 XML 模式语言规范和 XML Schema 的基本语法。第 4

章 DOM 接口技术，介绍 DOM 的主要接口、XPath 和 DOM 实例。第 5 章 XML 加密，介绍 XML 加密规范和基本结构，XML 加密的 Java 实现。第 6 章 XML 数字签名，介绍 XML 数字签名规范的基本结构，XML 签名的 Java 实现。第 7 章 XML 密钥管理规范，主要介绍密钥信息服务规范和密钥注册服务规范。第 8 章安全断言标记语言 SAML，介绍 SAML 体系结构，以及 SAML 断言、协议、绑定和配置。

本书可作为高等学校计算机科学与技术、信号与信息处理相关专业高年级学生及硕士研究生信息安全技术课程的教材，也可用作为相关领域研究人员的参考书。本书约需 40～60 学时讲授。

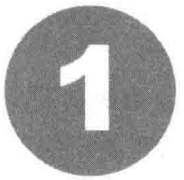
在本书的编写过程中，参考了国内外 XML 技术和 XML 安全相关的众多文献。本书得到了高端印刷装备信号与信息处理北京市重点实验室师生的大力支持，研究生曹晓鹤对本书的程序进行了验证，并在书稿编排、校对过程中做了大量工作。本书得到了国家自然科学基金项目（No. 61370140）、协同创新中心绿色印刷与出版技术项目（No.PXM2016_014223_000025）和北京印刷学院学科与研究生教育项目的资助。在此一并表示感谢。

由于编者水平有限，书中难免存在不妥乃至错误之处，敬请读者不吝指正。

编　者

2016 年 4 月

目　录



第1章

密码学基础

加密技术主要分为对称密码体制和公钥密码体制。1949年，C. E. Shannon发表了“Communication Theory of Secrecy System”，对他所创立的信息论的概念和方法做了进一步发挥，并精辟地阐明了关于密码系统的分析、评价和设计的科学思想，成为现代密码学的基础。1977年7月15日，美国国家标准局（National Bureau of Standards，NBS）正式颁布数据加密标准（Data Encryption Standard，DES）。随着DES的出现，人们对对称分组密码展开了深入的研究和讨论。现已有大量的分组密码，如DES的各种变形、IDEA算法、SAFER系列算法、RC系列算法、Skipjack算法、Rijndael算法等。

1976年W. Diffie和M. E. Hellman在“New Directions in Cryptography”中第一次提出了公钥密码学概念，开创了密码学的新领域。从公钥密码的思想提出以来，国际上已经提出了许多公钥密码体制，1977年麻省理工学院（Massachusetts Institute of Technology，MIT）三位年轻的科学家R. L. Rivest、A. Shamirh和L. M. Adleman设计的基于大整数因子分解问题的RSA算法，是目前最有影响力的公钥密码体制。T. Elgamal于1985年提出了基于有限域上离散对数问题的ElGamal算法，它至今仍然是一个安全性能良好的公钥密码体制。1985年华盛顿大学的N. Koblitz和IBM的V. Miller提出椭圆曲线密码ECC（Elliptic Curve Cryptography）算法，它是基于椭圆曲线离散对数

问题的公钥密码体制。由于椭圆曲线密码具有安全性能高、处理速度快、带宽要求低和存储空间小等特点，正在为越来越多的人所关注。

数字签名技术通常用来进行数据完整性、不可否认性和身份的认证，它利用散列函数保证了数据的完整性，同时结合了公钥密码与对称密码的优点，保证信息的机密性与不可否认，在商业、金融业等领域起着极其重要的作用。数字签名技术发展到今天，其理论研究和应用开发工作都得到了长足的发展。1994 年 5 月 19 日美国国家标准技术研究所（National Institute of Standards and Technology，NIST）公布了数字签名标准（Digital Signature Standard，DSS），其中的数字签名算法（Digital Signature Algorithm，DSA）是 ElGamal 算法和 Schnorr 算法的变形。

1.1 密码学概述

1.1.1 密码体制与密码系统的基本模型

一个密码体制通常由五部分组成。

① 明文空间 M：全体明文的集合。

② 密文空间 C：全体密文的集合。

③ 密钥空间 K：全体密钥的集合。通常每个密钥 $k \in K$ 都由加密密钥和解密密钥组成，即 $k=(k_e, k_d)$，k_e 与 k_d 可能相同，也可能不同。

④ 加密算法集合 E：由加密密钥 k_e 控制的加密变换的集合。

⑤ 解密算法集合 D：由解密密钥 k_d 控制的解密变换的集合。

设 $m \in M$ 是一个明文，$k=(k_e, k_d) \in K$ 是一个密钥，则有

加密过程：$c=E_{k_e}(m) \in C$；

解密过程：$m=D_{k_d}(c) \in M$。

其中，E_{k_e} 是由加密密钥 k_e 确定的加密变换，E_{k_d} 是由解密密钥 k_d 确定的解密变换。在一个密码体制中，为了使人们能够正常地进行加解密变换，必须要求解密变换是加密变换的逆变换，即 $\forall m \in M$，均有 $D_{k_d}(E_{k_e}(m))=m$。

一个密码系统的基本模型如图 1-1 所示。

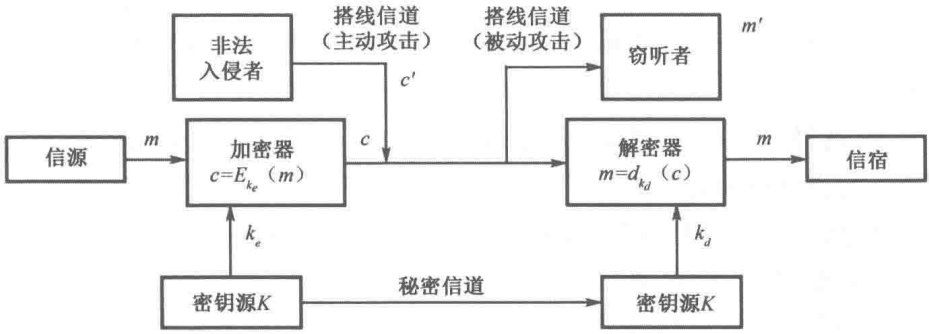


图 1-1　密码系统的基本模型

1.1.2　Kerckhoff 假设和密码系统的安全性

C. E. Shannon 提出了无条件安全性（又称完善保密性）的概念：如果对于所有明文 P 和密文 C，都有 $P_r(P)=P_r(P|C)$成立，则称该分组密码关于当前密钥具有无条件安全性，其中 $P_r(P)$表示明文 P 在消息空间上的分布概率，$P_r(P|C)$表示条件概率。在无条件安全性的模型下，假定攻击者具有无限计算资源（如时间、空间、设备和资金等）。要达到无条件安全性，一个最基本的要求是：密钥长度至少要和待加密的消息的总长度相等，一个密钥比特只使用一次，这在绝大多数情况下是不切实际的。实际中，一个固定的密钥可以用来加密大量的明文块。

现代密码学中，通常是在计算安全性的模型下研究密码的安全性。一个密码系统是计算上安全的，指的是破译该系统所需的努力超越了攻击者的破译能力，或破译该系统的难度等价于求解数学上的某个已知难题。在计算安全性的模型下，假定攻击者拥有的计算资源是有限的。

Kerckhoff 假设：除了密钥之外，假定攻击者知道所有有关明文的统计特性、加密和解密的详细过程、密钥空间及其统计特性。Kerckhoff 假设意味着密码系统的安全性完全依赖于密钥的安全性。

在 Kerckhoff 假设下，根据攻击者所掌握的信息，密码分析者的攻击模型可分为以下几种。

① 唯密文攻击（Ciphertext-only Attack）：密码分析者仅知道一些密文。

② 已知明文攻击（Known-plaintext Attack）：密码分析者知道一些明文和相应的密文。

③ 选择明文攻击（Chosen-plaintext Attack）：密码分析者可以选择一些明文，并得到相应的密文。

④ 选择密文攻击（Chosen-ciphertext Attack）：密码分析者可以选择一些密文，并得到相应的明文。

其中唯密文攻击的攻击强度最弱，其他情况下的攻击强度依次增加。

1.2 对称密码体制

在对称密码体制中，加密密钥 k_e 与解密密钥 k_d 相等。按照加密方式的不同又可分为两大类——分组密码和流密码，我们主要讨论分组密码。基于 Shannon 理论的 Feistel 密码结构，是当前大多数重要对称分组密码的基本结构。DES 算法是第一个也是最重要的现代对称加密算法。

1.2.1 分组密码的设计思想与 Feistel 密码结构

设计一个分组长度为 n 的分组密码，其本质就是构造 GF(2^n) 上的一个受密钥 k 控制的置换。给定一个密钥 k，就得到一个具体的 GF(2^n) 上的置换，不同的密钥应该对应不同的置换。

1949 年，Shannon 在“Communication Theory of Secrecy System”一文中提出了代换-置换网络（Substitution-Permutation Networks，S-P 网络）的思想，S-P 网络是基于代换和置换这两个基本操作的。而且 Shannon 认为，为了抵抗对手对密码体制的统计分析，必须对明文做混淆（Confusion）和扩散（Diffusion）处理，有效地隐藏明文的统计特性。混淆和扩散是现代分组密码的设计基础。

所谓混淆，就是将密文与密钥、密文与明文之间的统计关系变得尽可能复杂，使得窃密者即使获取了关于密文的一些统计特性，也无法推测出密钥

或明文。使用复杂的非线性变换可以达到比较好的混淆效果。

所谓扩散，就是让明文中的每一个比特影响密文中的许多比特，或者说让密文中的每一比特受到明文中许多比特的影响，使明文统计结构扩散消失到大批密文统计特性中。

对于分组密码，在早期的研究中，基本上是基于 Feistel 结构进行的。Feistel 建议使用乘积密码的概念来逼近简单代换密码。乘积密码是指依次使用两个或两个以上基本密码，所得结果的密码强度将强于所有单个密码强度。特别地，Feistel 建议交替地使用代换和置换。实际上，这是 Shannon 提出的交替使用混淆和扩散乘积密码的实际应用。图 1-2 描述了 Feistel 提出的密码结构。

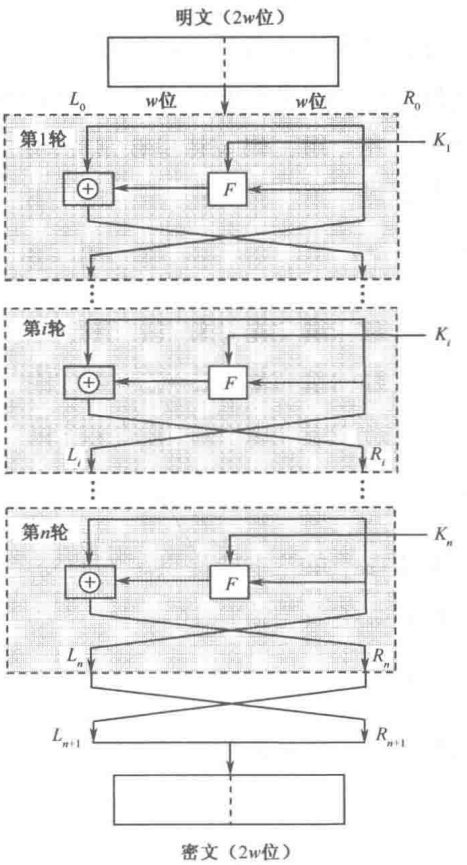


图 1-2　Feistel 密码结构