基于 RSA 信息安全加密系统的研究与实现

◆郭晟南　蒋学勤

(贵州理工学院大数据学院　贵州　550003)

摘要：RSA 公钥加密算法是目前最常用的公钥加密算法之一，基于 RSA 算法的信息安全加密系统可以为网络数据通信安全保障。本文首先将对 RSA 信息安全加密技术进行简单介绍，包括 RSA 信息加密技术和信息系统安全技术等，在此基础上，探讨基于 RSA 算法的安全加密系统设计与实现，主要包括加密系统设计、加密算法选择、安全性分析和系统主要功能实现等。

关键词：RSA 算法；信息安全加密技术；系统设计及实现

0　引言

在信息技术的发展过程中，信息系统安全是信息技术应用的重要前提，只有确保信息数据的安全性，才能真正发挥信息技术的优势。特别是在军事等重要领域，信息系统的安全性必须得到保障。随着信息技术的快速发展，信息加密、解密技术也在不断更新和发展，传统的防火墙技术等只对数据包的报头部分进行检验，难以做到对病毒、间谍软件等全方位防范。基于 RSA 算法设计安全加密系统，可以解决这一问题，为信息数据的完整性和保密性提供保障。

1　RSA 信息安全加密技术

1.1RSA 信息加密技术概述

RSA 公钥加密算法最早是由罗纳德·李维斯特、阿迪·萨莫尔和伦纳德·阿德曼在 1977 年时共同提出的一种公钥加密技术，由三人姓氏的首字母命名，迄今为止仍然是应用最广泛、最有影响力的公钥加密算法。采用 RSA 公钥加密算法设计信息加密系统，可以成功抵御大多数密码攻击，是 ISO 推荐的公钥加密技术。通常情况下，只有 RSA 公钥长度较短时，才有可能被破解，没有任何能够可靠破解 RSA 公钥密码的方法。因为 RSA 算法是基于一个数论事实设计的加密算法，即两个大质数相乘的结果容易得到，但对其进行因式分解却很难，所以可以将其乘积公开作为加密秘钥。由于 RSA 算法容易被理解和操作，能够同时被用于数字签名和加密，因此得到了非常广泛的应用，先后经过多次改进，目前一般使用长度为 1024 位的 RSA 密钥。

1.2 信息系统安全

信息系统安全主要体现在四个方面：(1)信息数据的完整性，要求信息数据在传输过程中，能够保证内容的安全和可靠，非法改动其中任一要素，都会导致信息数据无法执行或出现较大损失；(2)身份可识别性，信息在传输过程中，要明确收发双方的信息，明确信息来源和目的地，否则信息传输过程无法完成。此外，身份可识别也抗抵赖的基本措施，信息发送者需要对信息内容负责，信息接收者同样需要对信息的接收和使用安全负责，这是落实信息数据管理责任的基础；(3)保密性要求，信息在传递过程中要确保信息内容不能被轻易破解，即使信息数据被窃听，窃听者也无法获取信息内容；(4)时效性要求，信息数据在网络系统中要保持较快的传输速度，不能因加密、解密过程造成过高的信息延迟，否则会影响因袭价值。综合考虑以上几方面要求，使用 RSA 算法设计信息安全加密系统，可以在最大程度上保障信息的安全性和可靠性。

2　基于 RSA 算法的安全加密系统设计及实现

2.1 加密系统设计

基于 RSA 算法的加密系统设计主要包含以下几方面内容

(1)数字签名的实现，数字签名是实现身份认证和抗抵赖的重要手段，要确定签名者的唯一信息标识，并能通过第三方验证，解决出现的争端，比如使用报文摘要的数字签名技术，信息发送方取报文摘要，使用己方私钥进行加密，将加密摘要和报文同时发送给信息接收方。

(2)RSA 算法在数字签名技术中的应用，算法输入为 RSA 私钥和消息，输出为数据分组和产生签名。采用这种经过改进的 RSA 算法，可以缩短数字签名时间，同时能够提升信息安全性。

(3)加密系统模型设计，随着针对成熟算法的密码破解方法不断增加，单一使用任何一种信息加密技术，都无法为信息的完整性、保密性提供保障。为保护网络信息安全，一方面要对 RSA 等成熟加密算法进行不断改进，另一方面要将对称加密和公钥加密结合起来，设计更加难以破解的加密模型。基于此类思想的信息安全机密系统主要包括三个模块，即登录模块、加密模块和解密模块。其中加密模块和解密模块分别对应 IDEA、RSA、Md5 等算法的加密和解密以及综合加密、解密功能。

(4)系统通信协议设计，在数据传输过程中，要约定好数据包格式、总长度、类型、经过加密的对称会话密码及加密报文等。规定好各个字段的顺序，接收方根据顺序进行解密，并对信息传输方的身份以及信息完整性进行验证。

3　加密算法选择

在上述安全加密系统中，总共用到四种信息加密技术，即私钥加密技术、公钥加密技术、报文摘要加密技术和随机数产生方法。通过四种加密技术的综合运用，提高系统的安全防护能力。在进行设计时，需要对每一种信息加密技术的算法进行选择，具体包括：

(1)私钥加密算法，常用的算法包括 DES 算法极其变形算法，比如 GDES、New DES 算法等，还可以选择 IDEA 算法或 RC5 算法等。

(2)公钥加密算法，由于概算法与私钥加密存在本质性的不同，基于数学函数实现，每种单向函数均可成为公钥密码算法，目前使用较多的包括 RSA 算法、椭圆曲线算法、背包密码算法等，其中 RSA 算法的特点是加密速度慢，但安全性高，通过对 RSA 改进算法的应用，可以解决效率问题，为信息安全提供保障。

(3)报文摘要加密算法的选择，其输入为任意长的报文字段，经加密运算后得到固定长度输出，难以通过反向运算破解。报文摘要加密技术可以分为三种类型，即基于单向函数的报文摘要算法、使用分组密码的报文摘要算法以及基于软件的报文摘要算法，具体可以使用 MD、MDS、SHA-1 算法等。

(4)随机数产生方法的选择，IDEA 秘钥是随机产生的，基

（下转第 38 页）

参考文献：

[1] Bengio Y, Simard P, Frasconi P. Learning long-term dependencies with gradient descent is difficult.[J]. IEEE Transactions on Neural Networks，1994.

[2]Surhone L M, Tennoe M T, Henssonow S F. Long Short Term Memory[J]. Betascript Publishing，2010.

[3]Pascanu R, Mikolov T, Bengio Y. On the difficulty of training recurrent neural networks[C]// International Conference on International Conference on Machine Learning. JMLR.org，2013.

[4] Chung J, Gulcehre C, Cho K H, et al. Empirical Evaluation of Gated Recurrent Neural Networks on Sequence Modeling[J]. EprintArxiv，2014.

[5]Bengio Y, Schwenk H, Sen é cal J S, et al. Neural Probabilistic Language Models[J]. Journal of Machine Learning Research，2003.

[6] Mikolov T, Karafi á t M, Burget L, et al. Recurrent neural network based language model[C]// INTERSPEECH 2010, Conference of the International Speech Communication Association, Makuhari, Chiba, Japan, September. DBLP，2010.

[7] Botha J A, Blunsom P. Compositional Morphology for Word Representations and Language Modelling[J]. Computer Science，2014.

[8]Luong T, Socher R, Manning C D. Better Word Representations with Recursive Neural Networks for Morphology[C]// Conference，2013.

[9] Santos C N D, Guimarães V. Boosting Named Entity Recognition with Neural Character Embeddings[J]. Computer Science，2015.

[10] Bengio Y, Simard P, Frasconi P. Learning long-term dependencies with gradient descent is difficult.[J]. IEEE Transactions on Neural Networks，1994.

[11] Srivastava R K, Greff K, Schmidhuber J. Training very deep networks[J]. Computer Science，2015.

[12]Marcus M P, Marcinkiewicz M A, Santorini B. Building a large annotated corpus of English: the penntreebank[M]. MIT Press，1993.

[13] Hinton G E, Srivastava N, Krizhevsky A, et al. Improving neural networks by preventing co-adaptation of feature detectors[J]. Computer Science，2012.

[14]Zaremba W, Sutskever I, Vinyals O. Recurrent Neural Network Regularization[J]. EprintArxiv，2014.

[15]骆小所.语言的接缘性及其分支学科[J].云南师范大学学报(哲学社会科学版)，1998.

[16]雷铁安，吴作伟，杨周妮.Elman 递归神经网络在结构分析中的应用[J].电力机车与城轨车辆，2004.

（上接第 35 页）

于随机数产生方法实现，因此要确保随机数产生的随机性，由计算机产生的伪随机数实际是根据一定计算方法实现的，如果随机性不够，就会被穷举攻击破解。

4 安全性分析

信息安全加密系统是网络信息安全系统的子系统，与网络信息安全的其他子系统密切相关。对其自身的安全性而言，则受选用的加密技术以及各组件安全的影响。从上述设计方案来看，系统安全性具体表现为：（1）IDEA 算法的安全性，目前还未发表能够破解 IDEA 算法的密码学攻击方法，采用明文攻击方法破解 IDEA 加密报文的时间比宇宙年龄还要长。但实际上 IDEA 算法存在随机数产生方法的漏洞，如果随机数随机性不够高，会使其密钥穷举空间被极大压缩，进而有可能被破解；（2）RSA 算法的安全性，RSA 算法安全性是建立在一个合数进行因数分解的难度基础之上，随着数论的发展可能会找到更加高效的分解算法，导致 RSA 算法的安全性被降低。虽然可以通过加长密码长度提高其安全性，但也会导致加密、解密效率被增加。这些都是在信息安全系统设计过程中需要注意的问题。

5 系统主要功能实现

选定加密算法，可以对信息安全加密系统的主要功能进行设计与实现。系统主要功能包括：（1）操作人员身份识别功能，每个操作人员使用专用口令，系统可以对其操作记录进行查询。具体功能包括口令输入、验证以及提示信息显示等；（2）信息加密功能，对需要加密的信息数据进行综合加密处理，生成加密文档，该模块的输出是加密后的乱码信息；（3）信息解密功能，对受到的加密文档进行综合解密处理，使用解密算法将乱码信息还原成原数据信息，并生成解密文档。

6 结束语

综上所述，RSA 算法是一种难以被破解的公钥加密算法，在信息加密系统设计中的应用可以有效提升信息安全防护能力。基于 RSA 算法对信息加密系统进行设计，综合使用多种加密技术，构建综合加密、解密功能模块，可以显著提高破解加密数据的难度，进而为数据传输安全提供保障。此外，通过改进 RSA 算法的应用，还可以解决 RSA 算法加密、解密效率低的问题。

参考文献：

[1]刘波，严俊，姚茂华.地理信息安全加密系统的实现与应用[J].测绘通报，2017.

[2]代赞美.基于 Ecc 的 OPENVPN 安全通信设计与实现研究[D].昆明理工大学，2015.

[3]袁宗伟.基于 RSA 和 AES 加密系统的网络信息传输的安全技术研究[D].西安电子科技大学，2011.

贵州省科技厅技术基金项目：黔科合 J 字[2014]2082 号。