RSA 算法及其安全性分析

□ 于晓燕

摘要：本文系统的对传统密钥的特点进行了分析，详细介绍了公开密钥密码体制和RSA公钥密码体制的工作原理，对RSA算法的安全性进行了深入的分析。

关键词：传统密钥；公共密钥；RSA算法；安全性

随着互联网的快速发展，传统的处理事务的方式也在改变，现在开发了许多能够在网络环境下进行的公共业务（例如银行缴费系统、网上购物系统以及电子政务系统等），给我们带来了极大的方便。我们可以足不出户的在家里缴纳话费，这样做非常方便快捷。因而越来越多的企事业单位都开始运用互联网思维进行办公或销售，人们也越来越习惯在网络上消费，与此同时，也降低了网络系统的安全性能。系统所面临的主要风险有：用户登录密码的安全性和用户身份的认证的可靠性。这就需要我们对所发送的信息进行加密。

一、公开密钥密码体制

在一般的数据加密体制中，在数据通信之前需要给它分配一个密钥，这个密钥是不公开的，只有数据通信的双方知道这个密钥，发送者把所要发送的数据都用分配的这个密钥进行加密，而接受者也是用分配的这个密钥对要接收到的加密信息进行解密。也就是说，加密与解密是对称的，解密过程是加密过程的逆过程。但是，这种数据加密体制就存在着一些弊端，存在的这些问题如下：(1) 发送方和接收方同用一个密钥，在有些情况下是不容易办到的。(2) 想要保守秘密，通常要时常更换密钥，因此频繁的更换密码使得管理密钥就比较麻烦。(3) 在网络通信的情况下，如果有 n 个用户，每两个用户都要进行加密通信，就需要有 n(n-1)/2 种不同的密钥，当 n 比较大时，密钥数量就会很大，在管理密钥上就存在一些困难。

这些就是一般密钥在现代通信的使用上存在着一定的局限性，也就是基于这些问题，提出了公开密钥密码体系。

基于数论的公钥密码体系，在后来我们称之为 RSA 密码体制，该密码体制已经被用到了电子邮件发送、电子商务交易、虚拟专用网络等很多商业系统中。互联网上很多系统的安全都依赖于 RSA 密码体制。

在一些电子商务系统的交易过程中经常会在网上传输一些重要信息、敏感信息等(比如我们在网站上购买东西，在线支付，都涉及到银行卡的转账问题），所以在传输数据之前必须先对这些数据进行经过加密后，再在网上进行传输。如果仅仅采用对称密钥加密技术进行加密，密钥分发问题不能得到很好的解决，而 RSA 公钥密码技术虽然能够很好的解决密钥分发这个问题，但是存在一些加密速度缓慢的问题。为了解决这个问题，可以结合对称加密技术和公开密钥技术的优点，它克服了对称密钥中密钥分发管理困难和公开密钥中加密速度慢的问题，同时使用两种不同的加密技术来获得公开密钥技术的灵活性和对称密钥加密技术的高效性。在实际应用在，信息发送方采用对称密钥来加密信息内容，然后将此对称密钥接收方的公开密钥加密之后，将它和加密后的信息一起发送给接收方，接收方先用相应的私有密钥打开数字信封，得到对称密钥，然后就使用对称密钥解开加密信息。

公开密钥密码体系的基本思想如下：

在数据通信时，通信双方有两把密钥，一把是不保密的，所有的人都能看到的，就像电话号码，咱们称这个密钥是公开密钥，另一把是不公开的，咱们称它为秘密密钥，这两把密钥是一对一的关系。建立一个公开密钥数据库，把所有用户的公开密钥都放在里面，这个公开密钥数据库就相当于电话号码簿。当一个用户 A 向别的用户 B 发出通信要求的时候，首先可以通过公开密钥库查找到 B 的公开密钥，然后用 B 的公开密钥对所要传出的数据进行加密，然后把用密钥加密后的数据传输出去；在收到加密数据的用户中，只有用户 B 的秘密密钥才能把收到的密文解密成原文。RSA 算法就是在公开密钥密码的算法提出之后出现的一种基于公开密钥体制的优秀加密算法，它是基于简单的数论事实：将两个大素数相乘，然后要对其乘积进行因式分解，这样做并不简单。因此可以设想将乘积公开作为加密密钥。RSA 算法是以推广的欧拉定理为基础而提出的。

二、RSA 算法的实现

（一）算法描述

首先，定义下列一些参数为描述 RSA 算法所用：

（1）参数 m 和 n 为随机的、互不相等的较大素数，对 m 、n 严加管理，一定要保密，不让任何人知道。

（2）$r=m\times n$ r 是两个较大素数 m 和 n 的乘积。(r 是公开的）

（3）欧拉函数 $\Phi(r)=(m-1)(n-1)$ （秘密的）

（4）S_k ——解密密钥，是秘密的，满足 $P_k\cdot S_k = t\Phi(r)+1$

（5）P_k ——加密密钥，是公开的，满足（ P_k ，$\Phi(r)$ ）=1；

（6）X ——明文（秘密的）

（7）Y ——密文（公开的）

其中，P_k 满足 P_k 与 $\Phi(r)$ 互素，S_k 满足 $P_k\cdot S_k\equiv(\mathrm{mod}\,\Phi(r)$ 的条件。

若用 X 代替 $a^{\Phi(n)+1}\equiv a(\mathrm{mod}\,n)$ 式中的 a，即 $a=X$，并使 $t\Phi(r)+1 = P_k\cdot S_k$，则有、

$$X^{P_k\cdot S_k}\equiv X(\mathrm{mod}\,r) \tag{1}$$

即明文 X 自乘 $P_k\cdot S_k$ 后对 r 取模，仍是明文本身。数据加密的过程就是对明文 X 自乘 P_k 次幂后按 r 取模，由 (1) 式，可建立加密过程为：

$$E(X,P_k)=Y\equiv X^{P_k}(\mathrm{mod}\,r) \tag{2}$$

数据解密的过程则是对密文 Y 自乘 S_k 次幂后按 r 取模：

$$D(Y,S_k)=Y^{S_k}(\mathrm{mod}\,r)\equiv X^{P_k\cdot S_k}(\mathrm{mod}\,r)\equiv X(\mathrm{mod}\,r) \tag{3}$$

由 (2) 式和 (3) 式可知，RSA 算法的加密方程和解密方程如下：

密文 Y 等于明文 X 的 P_k 次方 mod r，这是加密的过程；

明文 X 等于密文 Y 的 S_k 次方 mod r 这是解密过程。

根据乘法运算的可交换性质，$S_k\cdot P_k = P_k\cdot S_k$ 可知，先进行加密运算再进行解密，与先进行解密算法再进行加密算法的计算结果是完全一致的。

对于任意整数 m，$X^{P_k}(\mathrm{mod}\,r)\equiv(M+m)^{P_k}(\mathrm{mod}\,r)$，每个明文 $X,X+r,X+2r;...,X+m$ 将产生同样的密文，为了避免每个明文加密后产生同样的密文，X 必须限制在 $0\le X\le r-1$ 范围内，这样，明文变换成密文才是一对一的。这就要求在对明文进行加密过程中，需要先将明文 X 分成一连串的数据块，每个数据块的值限定在 $\{0,1,2\cdots r-1\}$。

（二）RSA 算法的安全性

自从公钥体制问世以来，学者们就提出了分析它的安全性问题，它们的安全性都是基于复杂的数学难题的，RSA 密钥体制的安全性在于大整数素数因子分解的难题，而大整数因子分解问题是数学上的著名难题，至今没有有效的方法能够破解。下面我们分析一些 RSA 算法需要破解的流程：

要想破译由 RSA 算法加密以后的密文 Y，首先需要知道 S_k，但 S_k 不是已知的；只有 P_k 是已知的，由 $P_k\cdot S_k = 1\mathrm{mod}\,\Phi(r)$ 可知，要想求出 S_k，又必须知道 $\Phi(r)$，但 $\Phi(r)$ 也是未知的，其中 r 是

已知的；由 r= $m \cdot n \cdot \Phi(r)=(m-1)(n-1)$，要想求出 $\Phi(r)$，只有先知道了 m，n，然而 m，n 也不是公开的，所以，只有对 n 因式分解才能得到 m，n。

当 r 比较小的时候，对 r 进行因式分解不难，然而，随着 r 的不断增大，用目前已有的算法来对 r 进行因式分解，会比较困难。所以，当 n 很大时，要破解密文就变成一件不是那么容易的事了。目前只有比较短的 RSA 钥匙才可能被解破。RSA 密码体制的研究中包含了因子分解、加密过程、密钥管理等问题，尽管 RSA 密钥体制相对很安全，但是在实际运用 RSA 密钥体制的过程中往往也存在一些问题，这些问题大多是由于误用密码体制、错误选择参数和实现有缺陷等方面原因造成的。

三、结论语

RSA 算法在保密方面运用的很好，所以它也被广泛的用在各种安全领域或认证领域，比如网络服务器和 IE 浏览器的安全方面，电子邮箱登录的安全和认证、对远程登录的用户的安全进行保证以及电子信用卡支付系统等领域。我们能够预测到，RSA 的应用将越来越广泛。到 2008 年为止，世界上还没有任何一种可靠的攻击 RSA 算法的算法。只要 RSA 密钥的长度足够长，用 RSA 加密的信息实际上是不能被解破的。但是在分布式计算和量子计算机理论日趋成熟的今天，RSA 加密的安全性受到了很大的挑战。

参考文献

[1] 冯克勤. 初等数论 [M]. 合肥，中国科学技术大学出版社，1995，58-61.

[2] 吴文森. 公开密钥密码体制 RSA 算法的实现和应用 [J]. 计算机工程，1993，17（2）：28-32.

[3] 周玉洁，冯登国. 公开密钥算法及其快速实现 [M]. 北京：国防工业出版社，2002，7-8.

[4] 冯登国，林东岱，吴文玲. 密码学导引 [M]. 北京，科学出版社，1999，23-55.

[5] 张焕国. 计算机安全保密技术 [M]. 北京，机械工业出版社，1994，28-32.

[6] 陈鲁生，沈世镒. 现代密码学 [M]. 北京，科学出版社，2002，57-72.

（作者单位：济南职业学院计算机学院）

作者简介：于晓燕（1982～），女，工学硕士，济南职业学院计算机学院教师，讲师。

（上接第 94 页）

来展示复杂的面板线路，示波器等仪器，讲解枯燥难懂，学生难以理解各种电路图的工作原理，只是按部就班的按照老师灌输的思路进行理解，而没有自己的想法，更别提创新思维和知识转化应用。改革实验方法，可以在实验教学中进行虚拟仪器设备实验，利用虚拟存储示波器采集实验数据，利用计算机网络技术分析和处理数据。结合电子设计自动化（EDA）技术和软件编程技术是学生有机会在实验中直接观摩到动态的实验过程。引入EWB仿真软件，引导学生进行模拟实验。模拟电路设计故障，要求学生仔细观察故障情况下的电路工作状态，引导学生自主分析和解决问题。在学生具备一定的基础之后，鼓励学生自己设计较为复杂的综合性题目并提交分析报告，由教师进行评价和反馈。

（三）培养学生创新能力

在应试教育背景下，学校教学以理论知识为主，而忽视了对学生动手能力的培养。学校学生缺乏解决实际工程问题的工作经验。如何在计划内的实践教学中培养和提高学生的工程和实践能力成为各个高校面临的最大挑战。在这个问题上，采取课内外结合的教学方式，实施开放式实验室教学是一个有效的解决方法。建立开放式实验室，鼓励学生在课余时间到实验室进行实验。在上课时，教师可以利用多媒体技术向学生介绍当今最先进的电子器件，电路设计和电子技术，开阔学生视野，带领他们领略科技的魅力。在电路制作课程中，鼓励学生自行设计不同的实验方案，锻炼学生逻辑思维能力和创新能力。在开放型实验室的基础上开展第二课堂，建立技能培训基地。创设情境，有计划，有组织的进行任务驱动式教学和探究协作式教学，提高学生的沟通能力，探究能力和团队意识。

（四）加强实验室的建设和管理

加强实验室的建设和管理是普通高等院校进行实践教学的重要环节，加大资金投入是保障。学校要在教学要求和招生规划的基础上建设高标准实验室，完善实验室建设和管理制度，对采购设备的质量、规格、价格等登记造册，以免出现“拿回扣”现象，损害学校利益。采取专人保管、维修制度，专人专责。完善实验室奖惩制度，提高实验室管理人员的工作积极性。

三、结束语

综上所述，高校进行电工电子技术实践教学要紧跟时代的发展，优化课程体系和内容，引入现代先进软件技术，推动学生创新能力的提高，培养高素质的综合性技术人才。加强实验室的建设和管理。为学生进行实训提供良好的平台。

参考文献

[1] 吴博琦，周路，赵阳，王超，王欢．电工电子技术教学环节浅析 [J]．才智，2019(02)：93.

[2] 邵娟．电工与电子技术课程多模式多层次的实践教学改革 [J]．科技视界，2018(32)：164-165.

[3] 魏光侠．信息化资源与中职电工电子课程教学深度融合的探究 [J]．职业，2018(28)：76-77.

[4] 王波，袁玲，刘伟均．关于电工技术课程的实践教学综合改革 [J]．课程教育研究，2018(17)：25-26.

（作者单位：景德镇学院）

作者简介：孙小霞（1980～），女，硕士研究生，讲师，研究方向为电子通信。石长华（1965～），男，硕士研究生，研究方向为自动控制、智能仪表。

（上接第 93 页）

施严格监督，要采取针对性措施实施设备降温，并且也要避免火花飞溅的问题。同时，要对变压器等其他设备实施接地处理，防止变压器受到雷电等灾害的破坏。第二，排氮残留危险点的预防措施。一般情况下都会在变压器内部通有氮气来对变压器进行保护，避免设备受到氧化。在变压器使用之前需要将内部氮气有效排出，一旦氮气排除不彻底存在残留就容易引发氮气中毒问题。因此在氮气没有完全排除之前严禁施工人员接近甚至进入到箱体内部，在对氮气进行检查时要确保良好的通风和照明条件。需要注意的是，要对照明系统电压进行有效控制，确保其安全性，防止发生触电等问题。

四、结束语

本文主要分析了配电线路变压器安装危险点的情况，在此基础上提出了相应的预防措施。通过本文的介绍能够对配电线路变压器安装提供一定参考和帮助。

参考文献

[1] 娄锋．配电线路变压器安装危险点及预控方案探讨 [J]．科技风，2018(11)：15-17.

[2] 潘建敏；葛少泽．配电线路变压器安装危险点及预控对策分析 [J]．才智，2013(05)：18-19.

[3] 赵淼．配电线路变压器安装危险点及预控对策研究 [J]．中国石油和化工标准与质量，2017(06)：88-91.

[4] 杨家强．配电线路变压器安装危险点及预控对策分析实践思考 [J]．中国高新区，2018(01)：18-19.

（作者单位：陕西省地方电力（集团）有限公司西乡县供电分公司）

作者简介：刘晓明（1976～），男，本科，助理工程师，研究方向为配电线路安全管理工作。