深圳大学考试答题纸

(以论文、报告等形式考核专用)

二○ 21 ～二○ 22 学年度第 2 学期

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 课程编号 | 1500210001R | | 课序号 | | 1 | | 课程名称 | | 离散数学(荣誉) | | 主讲教师 | 闫巧 | | 评分 |  |
| 学 号 | 2020151002 | | | 姓名 | | 郑杨 | | 专业年级 | | 2020级软件工程腾班 | | | | | |
|  | | | | | | | | | | | | | | | |
| 教师评语： | | | | | | | | | | | | | | | |
| 题目： | | Application of Number Theory in Public Key Cryptography | | | | | | | | | | |  | | |

Application of Number Theory in Public Key Cryptography

Abstract

本文回顾了密码学的历史发展，对现代密码学的一个分支——公钥密码学的基本思想进行阐述。对公钥密码学的经典算法进行回顾，详细叙述了RSA算法与ElGamal算法并使用数论的知识证明了他们的正确性与安全性。

Introduction

密码学早在公元前400多年就已经诞生，其发展大概可以分为3个阶段：1949年前的古典密码学阶段；1949年至1975年为近代密码学阶段，密码学逐渐成为科学的分支；1976年之后，进入现代密码学阶段，对称密钥密码学得到进一步发展，产生了密码学新方向——公钥密码学[1]。公钥密码学的基本思想由R. Merkle最早在1974年提出[2]，之后Diffie与Hellman以单向陷门函数为基础，首次提出了“公钥密码”的概念[3]。此类密码中加密和解密使用不同的密钥，其中，用于加密的叫做公钥，用于解密的叫做私钥。

在第一个公钥加密算法提出之前，所有的密码系统都为对称加密系统，如图1所示，但这个系统存在许多问题，其中的一个问题是：由于加密和解密的密钥只有一个，发送方和接收方都必须知道密钥。也就是说，密文和密钥需要同时由发送方发送给接收方，这同时也引出了一个问题，密钥应该如何发送才能保证安全性呢？这个问题本质上和加密信息是一致的，答案就是把密钥再进行加密，但是这样做并无法从根源上解决问题，因为密钥加密之后还会产生新的密钥，所以正如你所看到的，这个问题是加密和密钥的无限循环。Diffie与Hellman在[3]中提出的密钥协商算法已经解决了密钥传递过程的泄密问题。然后，对称加密系统还存在密钥管理与单方泄密问题。

Diffie与Hellman在[3]中提出的新系统解决密钥管理与泄密问题，他们的密码属于非对称密码，有两个不同的密钥：公钥和私钥。私钥是解密密钥，公钥是加密密钥。如果一个人Bob想要向另一个人Alice发送一段加密信息，他需要做的只是用Alice发布的公钥进行加密，那么全世界唯一可以解开这段密文的就只有Alice，因为只有她拥有私钥。这样的加密规则建立在单向陷门函数上，也就是通过公钥计算私钥是几乎不可能的，这也保证了安全性。但是，Diffie与Hellman只是提供了基本的概念，并没有找出满足他们要求的单向陷门函数。

Rivest、Shamir和Adleman这个团队，基于Diffie与Hellman的想法，历程一年终于找到了符合要求的函数，并提出了对应的加密解密算法[5]。除了加密与解密功能，这个算法同时具有电子签名功能。可以使用私人持有的解密密钥对信息进行“签名”，任何人都可以使用对用的公钥来验证此签名。签名无法被伪造，且签名者无法否认该签名的有效性。他们所提出的算法被称为RSA算法。

在RSA算法提出之后，ElGamal、椭圆曲线等公钥加密算法被相继提出，密码学进入了一个全新的发展时期。一般来说，公钥密码的安全性由相应的数学问题在计算机上的难解性来保证，利用了数论的一些相关知识可以对其安全性进行说明。

Public-Key Cryptosystems

在公钥加密系统中，加密算法一般都是公开的，把一个加密算法公之于众经受时间和广大使用者检验的做法是值得推荐的。因此，在加密算法公开的前提下，保证加密的安全依赖于密钥的安全性。

公钥加密系统把加密与解密过程视为两种程序，分别用E和D表示，明文消息与密文消息分别用M和C表示，那么公钥加密系统有以下四种特性：

1. 对于加密后的密文C=E(M)，对应的解密程序能够处理得到明文：D(C)=D(E(M))=M
2. 加密过程E和解密过程D是容易计算的
3. 由公开的加密程序E无法轻易计算得到解密程序D
4. 对明文消息先进行解密处理再进行加密处理仍然可以得到明文，也即：E(D(M))=M

其中，特征(a)(b)在传统的对称加密系统中也是成立的，保证了加密的原始目的。特征(c)保证了密钥的安全性，即使用公钥无法轻易计算出私钥。特征(d)使得签名功能得以实现。

公钥系统中的每个用户，都会生成属于自己的公钥与私钥，公钥公开存放于公共文件中方便其他用户查看，私钥自己保管。

RAS

1. Key Generation

每一个用户生成自己的公钥与私钥的流程如下：

1. 随机选取两个大素数p和q
2. 计算p和q的乘积n=p×q
3. 随机选取一个与f(n)=(p-1)(q-1)互质的数e,也即使得gcd(e, (p-1)(q-1))=1的数e
4. 计算e关于模f(n)的乘法逆元d，也即计算满足ed=1(mod (p-1)(q-1))的数d
5. 将(e,n)公开作为公钥，将(d,n)保存作为私钥

由上述密钥生成流程可知，会产生以下信息：

p,q,n,f(n),d,e

其中除了e与n公开之外，其他信息都需要严格的保密，原因在xxx节会说到。下一节将介绍RAS算法加密与解密的方法。

1. Encryption and Decryption Methods

假设Alice和Bob是公钥加密系统中的两个用户，此时Alice想要向Bob发送一段加密信息C，且Alice已经获得了Bob的公钥(e,n)，加密与解密过程如下：

1. Alice将明文分解为若干块，使得每个块可以表示为一个[1,n-1]的整数，由于块与块之间是相互独立的，这里只考虑某一块，假设某一块的信息表示为整数M.
2. Alice使用Bob的公钥进行如下运算得到加密信息C，并将C发送给Bob



1. Bob接收到C之后，使用自己保留的私钥(d,n)进行以下运算进行解密，得到M



接下来的问题是，证明(1)(2)两个公式的正确性，将在下一节进行阐述。

1. Mathematical Principles
2. Details
3. Example
4. Security

Reference

[1] R. Merkle, “Secure communication over an insecure channel,” Communications of the ACM.

[2] Diffie W. and Hellman M., New directions in cryptography. IEEE Trans. Inform. Theory IT-22, 1976.

[3] Michael Calderbank, “The RSA Cryptosystem: History, Algorithm, Primes,”2007.

[4] R.L.Rivest, A.Shamir, L.Adleman, “A method for obtaining digital signatures and public-key cryptosystems,*”* Communications of the ACM, 1978.

[5] A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms