信息安全数学基础

熊 虎
信息与软件工程学院
xionghu.uestc@gmail.com

任课教师

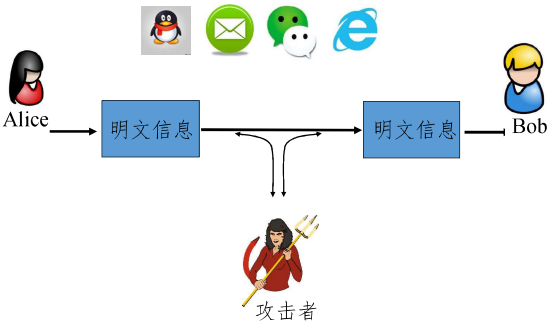
■在包括IEEE汇刊在内的高质量国际期刊及会议上发表学术论文80余篇，其中SCI收录50余篇，出版英文专著2部。主持国家自然科学基金在内的十多个国家及省部级课题。

熊虎
xionghu.uestc@gmail.com
博士，教授，博导
研究方向：
网络安全与密码学

■指导留学生、硕士生、博士生二十余名，承担《信息安全数学基础》、《近世代数》、《Network Security》等多门本科生及硕博士课程。

- 为什么要学习《信息安全数学基础》？
- 《信息安全数学基础》包含什么内容？
- 如何学习《信息安全数学基础》？

公开信道上的“安全”通信



传统的对称密码体制

- 对称密码体制(例如DES, AES) 允许两个用户利用提前共享的秘密来建立“安全信道”
- 通信双方共享秘密并不容易…

密钥管理

- 考虑一个具有N个用户的团体，如果用户两两之间都需要进行安全通信：
- 采用对称密码体制来保护用户之间的通信:
  - 每个用户需要与其余的N -1个用户共享私钥
  - 整个系统需要管理N(N -1)/2个密钥

密钥分发

- *用户之间如何在安全通信前共享秘密?*
  - 需要一个安全信道来共享密钥…
- 尽管密钥分发可以采用如下方式解决…
  - 例如, 物理接近, 可信“快递”
    - **(注意:这并不意味着对称密码体制没有意义)**

不支持“开放系统”

- 如果两个没有预先建立关系的用户需要建立安全通信,
  - 他们什么时候共享密钥呢?
- 这个场景并不遥远!
  - 顾客发送信用卡信息给商家
  - 用户发送电子邮件给单位中的所有同事

“传统的”对称密码体制无法解决上述问题!

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

***Abstract*—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.**

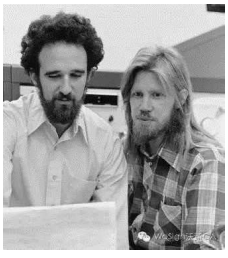
I. Introduction

We STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

Section III proposes two approaches to transmitting keying information over public (*i.e.*, insecure) channels without compromising the security of the system. In a *public key cryptosystem* enciphering and deciphering are governed by distinct keys, E and D, such that computing D from E is computationally infeasible (*e.g.*, requiring 10^{100} instructions). The enciphering key E can thus be publicly disclosed without compromising the deciphering key D. Each user of the network can, therefore, place his enciphering key in a public directory. This enables any user of the system to send a message to any other user enci-

Diffie和Hellman因为提出“公钥密码”这一概念获得 2015 年ACM图灵奖



第一个实用的公钥密码算法RSA获得2002年ACM图灵奖

- **2002年图灵奖获得者:**

Ronald L. Rivest

-- PhD, Stanford; MIT

Adi Shamir

-- PhD, Weizmann; Weizmann

Leonard M. Adleman

-- PhD, Berkeley; USC

- **获得ACM 图灵奖的主要工作**
  - **在公钥加密算法上所做的杰出贡献(RSA算法)**
  - **当前在互联网传输、银行以及信用卡产业中被广泛使用**

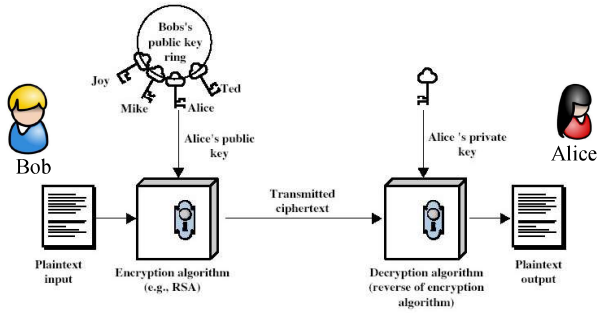
公钥密码体制

- 主要思想：
  - 一些问题呈现出“非对称性”- 从一个方向计算非常容易，而从另一个方向计算则很困难
  - 例如：计算任意给定整数的乘积很容易，而计算给定大整数的因子则非常困难

公钥密码体制

- 每个用户生成一个密钥对：一个公钥pk和一个对应的私钥 sk
  - 公钥将在系统内被公开
  - 私钥由用户本人安全保管
- 私钥由用户本人使用，而公钥则由系统中其他用户使用
- 公钥密码体制也被称为： 非对称密码体制

公钥密码体制的基本思想



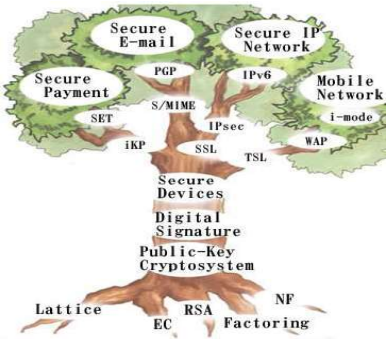
公钥密码体制的优势：

- 密钥分发：
  - 公钥能够采用公开（认证的）信道进行传输；
- 密钥管理：
  - 在用户N个用户的系统中，每个用户只需安全保管自己的私钥和N-1个其他用户的公钥。整个系统仅仅需要维护N个公钥；
- 开放系统：
  - 即使是没有预先建立关系的用户也能通过对方的公钥建立安全通信。

公钥密码体制的应用：

- Hyper Text Transfer Protocol over Secure Socket Layer (Https)
- Pretty Good Privacy (PGP): secure E-mail
- Military, Government…

公钥密码学数学基础



为什么要学习《信息安全数学基础》？

《信息安全数学基础》包含什么内容？

如何学习《信息安全数学基础》？

课程组成与特点

组成

初等数论

近世代数

驱动

RSA，El-Gamal，ECC

信息安全数学基础

课程简介

课程内容：初等数论，近世(抽象)代数（以PPT为准）

课程目的：培养抽象思维能力和严格的逻辑推理能力
为学习《密码学》、《安全协议》等专业课打好基础

上课时间：周四晚第9-11节

上课地点：第二教学楼408

教材及参考用书

- 教材
  《信息安全数学基础》，聂旭云，廖永建，熊虎，科学出版社，2019
- 参考书籍
  《公钥密码学的数学基础》，王小云，王明强，孟宪萌，科学出版社，2013
  《近世代数基础》，张禾瑞，高等教育出版社，1978
  《初等数论》，潘承洞,潘承彪著，北京大学出版社,2003

信息安全数学基础

成绩构成

平时表现（到课，作业）：20%

实验：10%

期中考试：10%

期末考试：60%

为什么要学习《信息安全数学基础》？

《信息安全数学基础》包含什么内容？

如何学习《信息安全数学基础》？

课程组成与特点

特点

抽象

概念、结论多

建议

应用驱动，反复研习

课程学习方法及脉络

课程学习方法及脉络

方法

初等数论->近世代数?

近世代数->初等数论?

脉络

同余->剩余类(群) ->剩余类环->剩余系->同余式

谢谢!