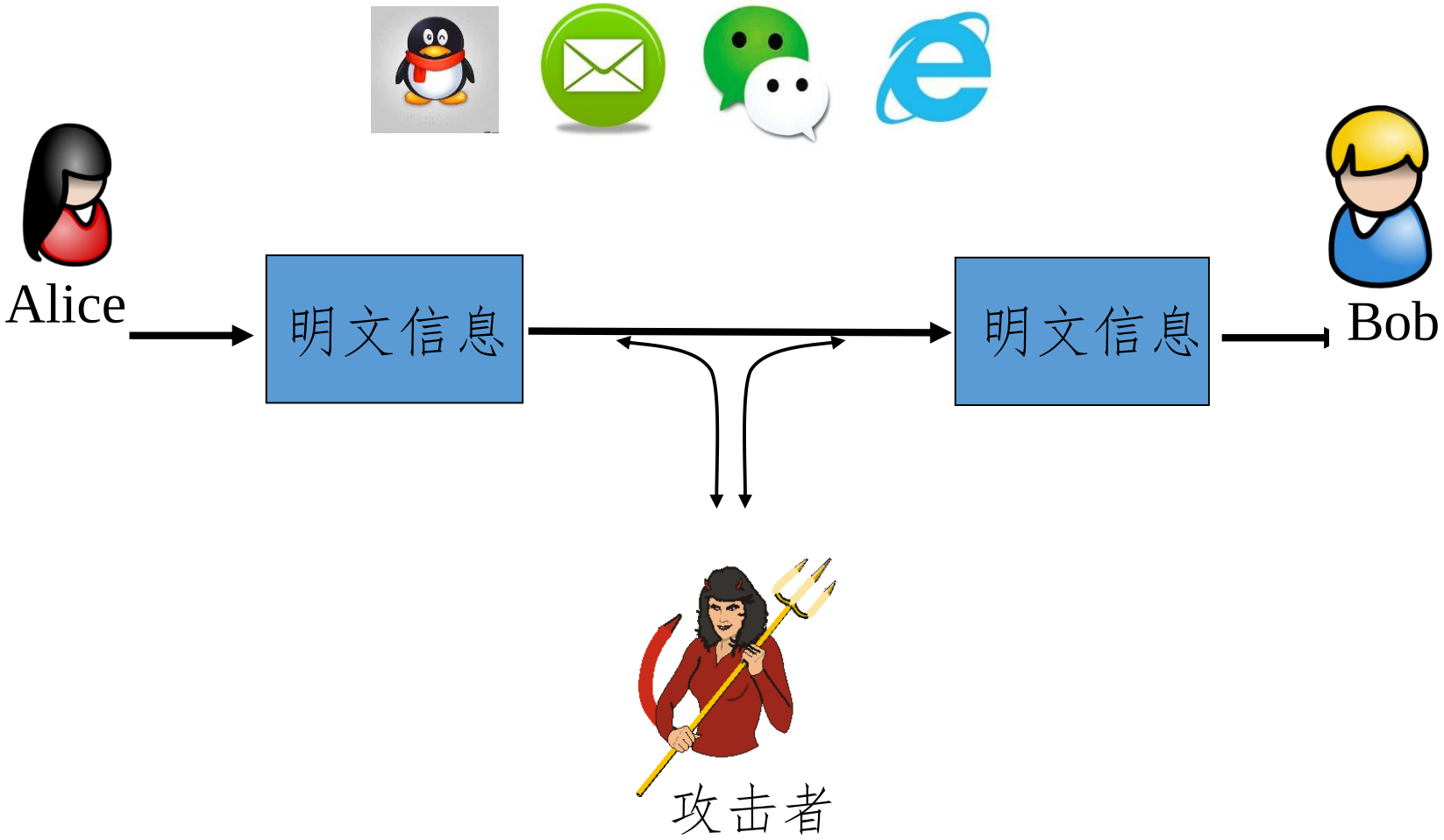
现代密码学

第三十一讲 公钥密码的基本概念和困难问题

信息与软件工程学院

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.**

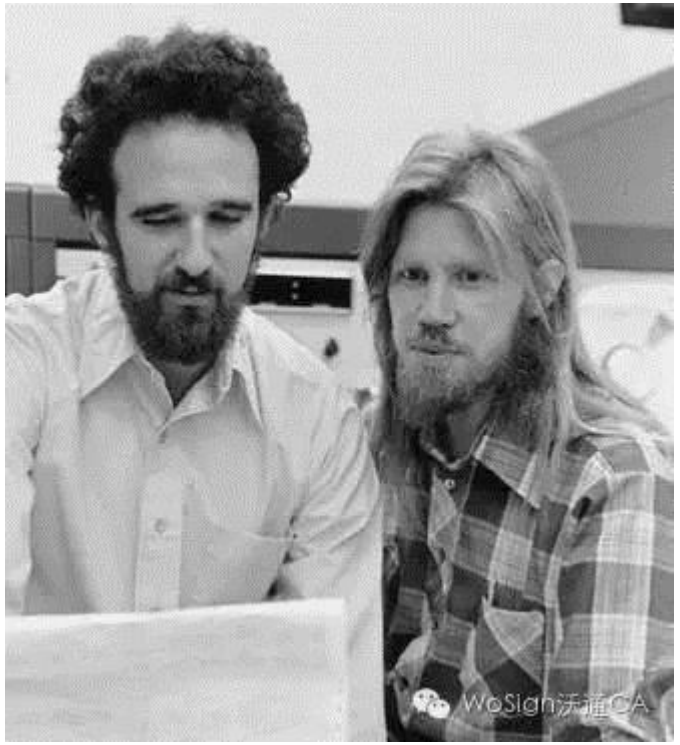
I. Introduction

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



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

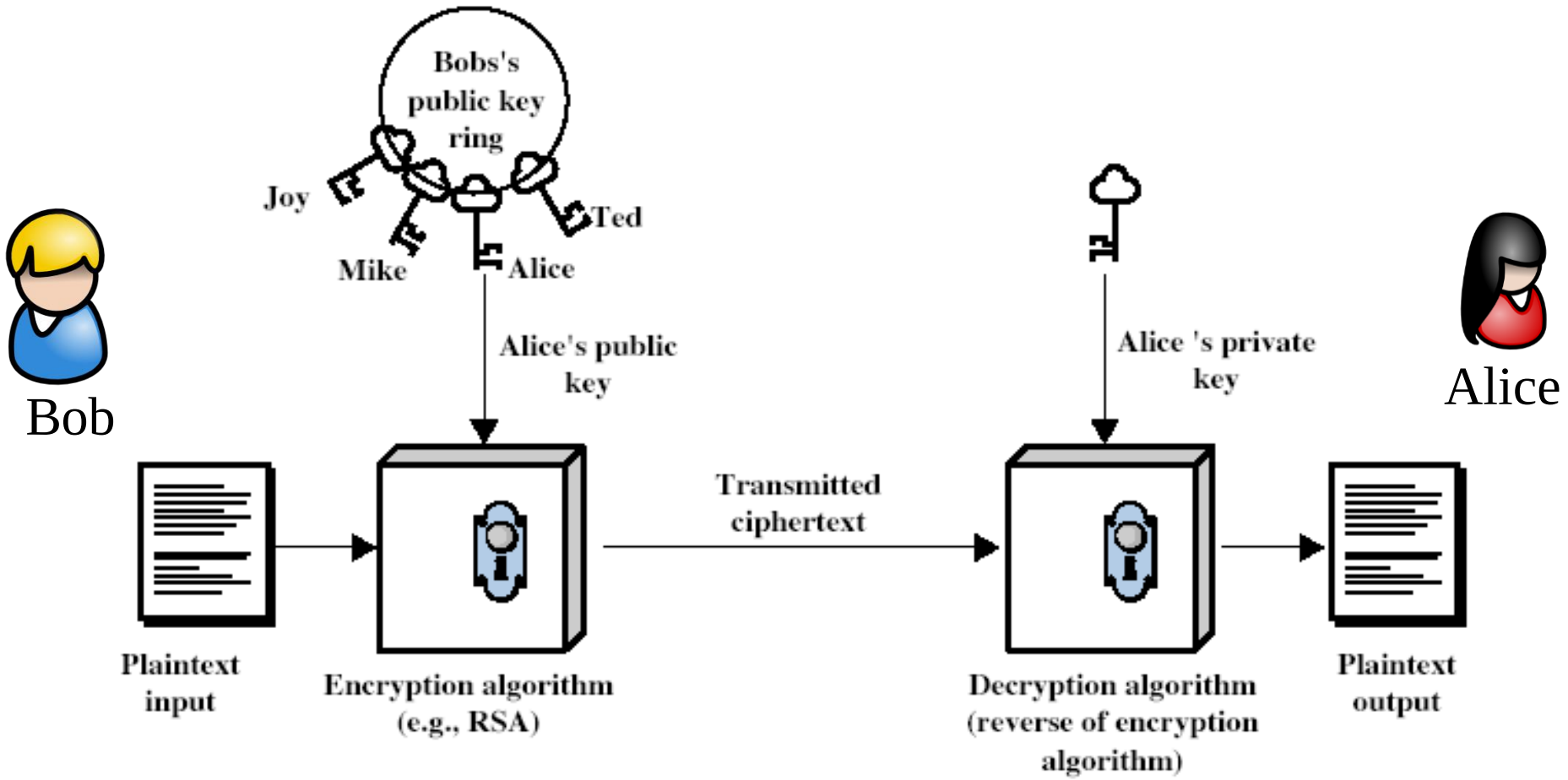
公钥密码体制

- 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…

感 谢 聆 听!

xionghu.uestc@gmail.com