第 7 章：密钥管理与密钥分发
Key Management and the Public-Key Revolution

赵俊舟

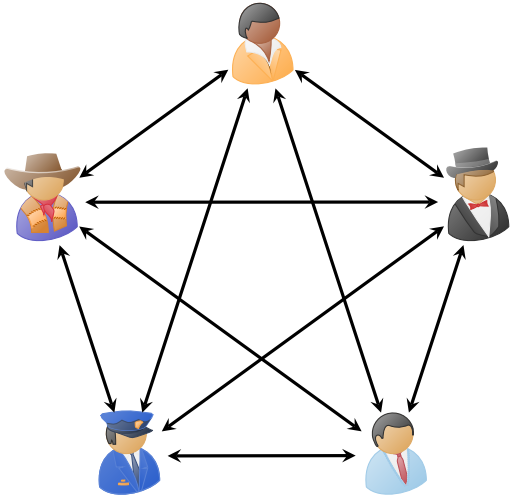
西安交通大学网安学院
junzhou.zhao@xjtu.edu.cn

2025 年 12 月 20 日

目录

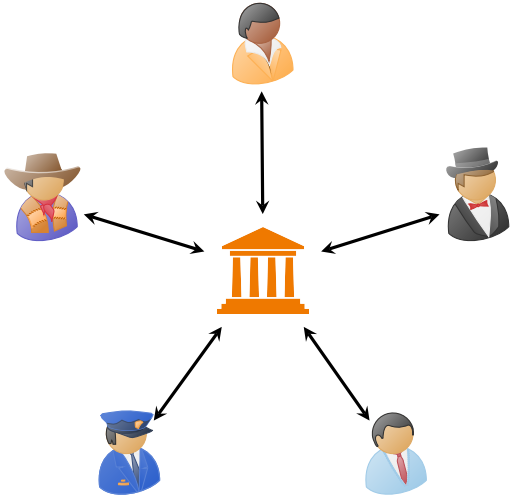
目录

私钥密码的问题



- **密钥分发困难**：如何在任意两个人之间分发只有他们自己知道的密钥？
- **密钥管理困难**：n 个人相互通信需要管理 $\binom{n}{2}$ 对密钥。

私钥密码的问题



- 使用第三方中央可信服务器可以减少密钥数量
- 通信/计算瓶颈、单点故障
- 是否真实存在可信第三方中央服务器？

Whitefield Diffie 和 Martin Hellman

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.**

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

Stanford | News

Home Find Stories For Journalists Contact

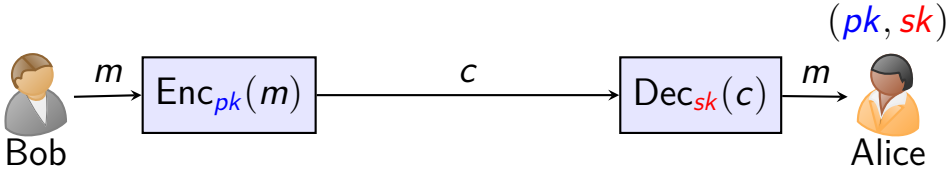
Stanford Report, March 1, 2016

Stanford cryptography pioneers Whitfield Diffie and Martin Hellman win ACM 2015 A.M. Turing Award

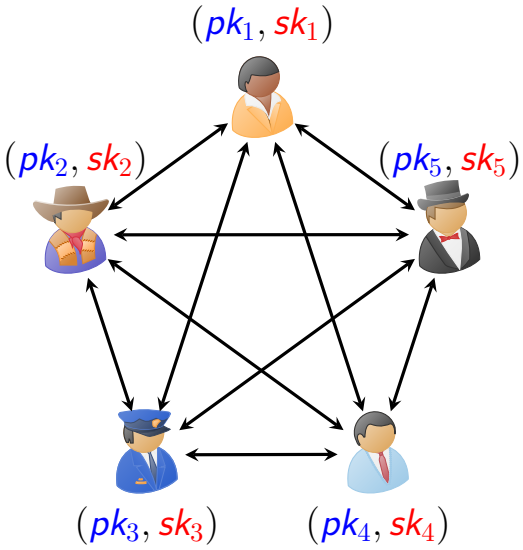
The groundbreaking algorithm from Whitfield Diffie and Martin Hellman enabled a secure Internet and sparked a clash with the NSA that foreshadowed current privacy battles between government agencies and Silicon Valley companies.

Diffie 和 Hellman 提出的新设想

- 每个用户有一个加密密钥 pk，一个解密密钥 sk。
- 解密密钥 sk 需要保密，而加密密钥 pk 可以公开，要求 pk 的公开不影响 sk 的安全。
- 若发送方要向用户发送消息 m，可查询用户的公开密钥 pk，加密后得到密文 $c = \mathrm{Enc}_{pk}(m)$。
- 用户收到密文 c 后，用只有该用户拥有的解密密钥 sk 对 c 进行解密得到明文 $m = \mathrm{Dec}_{sk}(c)$。

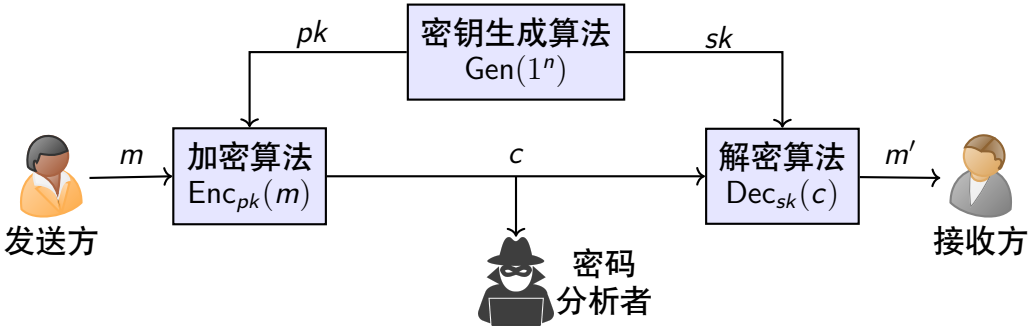


公钥密码的基本特点



- 加密与解密能力分开。
- 密钥分发简单，n 个用户只需要 $2n$ 个密钥。
- 可以满足陌生人之间的保密通信。
- 可以实现数字签名。

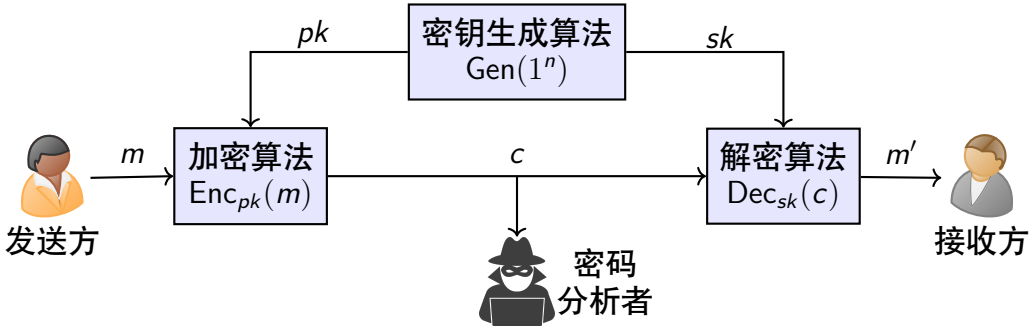
公钥密码（Public-Key Encryption）



由定义在空间 $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ 上的运算 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ 构成

- $\mathcal{K}$ 为密钥空间，$\mathcal{M}$ 为明文空间，$\mathcal{C}$ 为密文空间
- $\mathsf{Gen}: \{0,1\}^n \mapsto \mathcal{K} \times \mathcal{K}$ 为密钥生成函数
- $\mathsf{Enc}: \mathcal{K} \times \mathcal{M} \mapsto \mathcal{C}$ 为加密运算，并且 $c = \mathsf{Enc}_{pk}(m)$
- $\mathsf{Dec}: \mathcal{K} \times \mathcal{C} \mapsto \mathcal{M}$ 为解密运算，并且 $m = \mathsf{Dec}_{sk}(c)$

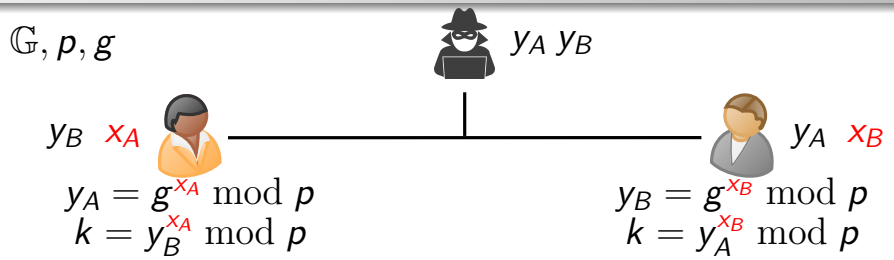
对公钥密码的要求



- **正确性**：$\mathrm{Dec}_{sk}(\mathrm{Enc}_{pk}(m)) = m$
- **计算效率**：加解密算法的计算效率应足够高，便于系统实现。
- Kerckhoffs **准则**：系统的安全性不依赖于对加解密算法的保密，而是私钥。

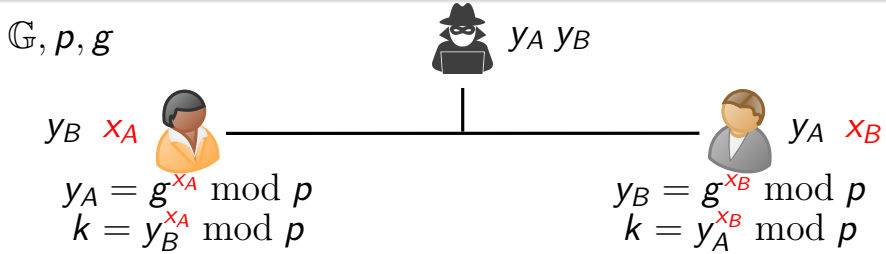
目录

Diffie-Hellman 密钥交换协议



- Alice 和 Bob 选择大素数 p，群 $\mathbb{G}$ 和它的一个生成元 g；
- Alice 选择一个随机数 x_A 作为自己的私钥，并计算公钥 $y_A = g^{x_A} \bmod p$，并将 y_A 发送给 Bob；
- Bob 选择一个随机数 x_B 作为自己的私钥，并计算公钥 $y_B = g^{x_B} \bmod p$，并将 y_B 发送给 Alice；
- Alice 计算 $k = y_B^{x_A} \bmod p$ 作为会话密钥；
- Bob 计算 $k = y_A^{x_B} \bmod p$ 作为会话密钥。

Diffie-Hellman 密钥交换协议



Alice 计算 k

$$k \equiv y_B^{x_A} \equiv g^{x_B x_A} \pmod{p}$$

Bob 计算 k

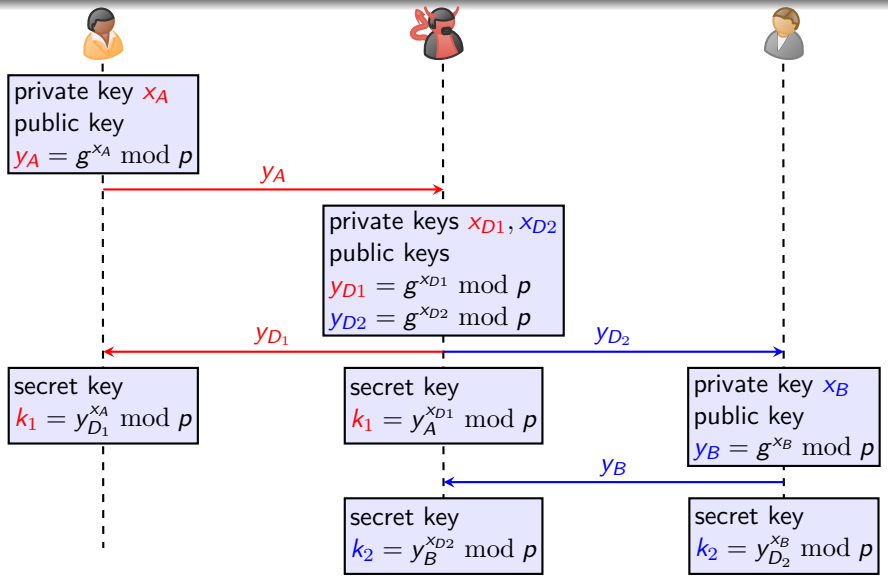
$$k \equiv y_A^{x_B} \equiv g^{x_A x_B} \pmod{p}$$

- Eve 虽然知道 y_A, y_B，但无法获得 x_A 或 x_B，所以无法得到 k。
- Eve 由 $y_A = g^{x_A} \bmod p$ 计算 x_A 是一个离散对数问题。
- Eve 由 $y_B = g^{x_B} \bmod p$ 计算 x_B 也是一个离散对数问题。

Diffie-Hellman 密钥交换举例

- Users Alice & Bob who wish to swap keys;
- Agree on prime $p = 353$ and $g = 3$;
- Select random secret keys:
  - A chooses $x_A = 97$,
  - B chooses $x_B = 233$.
- Compute public keys:
  - $y_A = 3^{97} \bmod 353 = 40$ (Alice)
  - $y_B = 3^{233} \bmod 353 = 248$ (Bob)
- Compute shared session key as:
  - $k = y_B^{x_A} \bmod 353 = 248^{97} \bmod 353 = 160$ (Alice)
  - $k = y_A^{x_B} \bmod 353 = 40^{233} \bmod 353 = 160$ (Bob)

中间人攻击 Man-in-the-middle Attack



原因：未对通信参与方进行身份认证，需借助数字签名。

小结

1. 公钥密码学
2. Diffie-Hellman 密钥交换协议