第 4 章：公钥密码学

4.2 基本概念与 RSA 算法

赵俊舟

junzhou.zhao@xjtu.edu.cn

2025 年 3 月 22 日

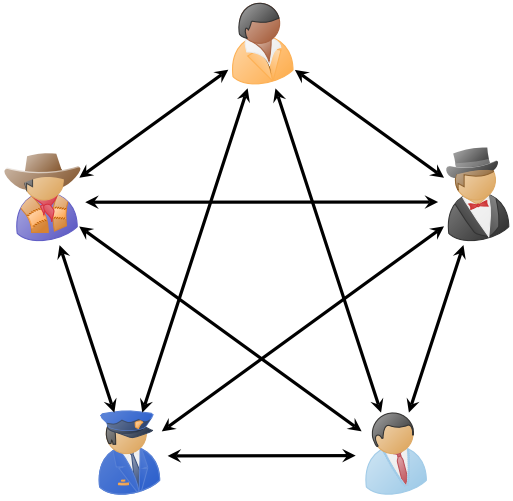
目录

目录

对称密码体制的问题

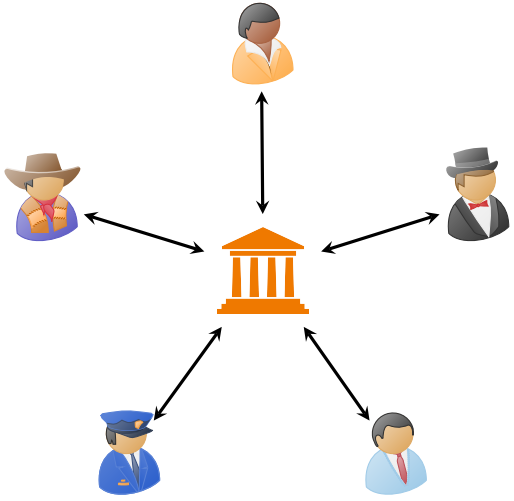
- 加密能力与解密能力捆绑在一起。
- 密钥分发困难：密钥更换、传递和交换需要可靠信道。
- 密钥管理困难：无法满足陌生人之间通信的保密要求。
- 身份认证问题：难以保障可信通信。

对称密码体制的问题



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

对称密码体制的问题



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

Whitefield Diffie 和 Martin Hellman

644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

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

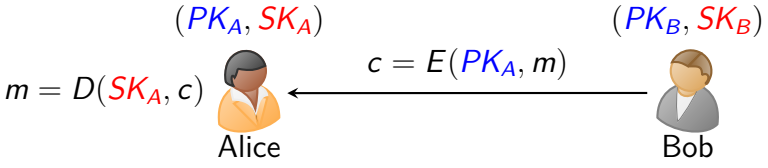
Stanford Report, March 1, 2016

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.

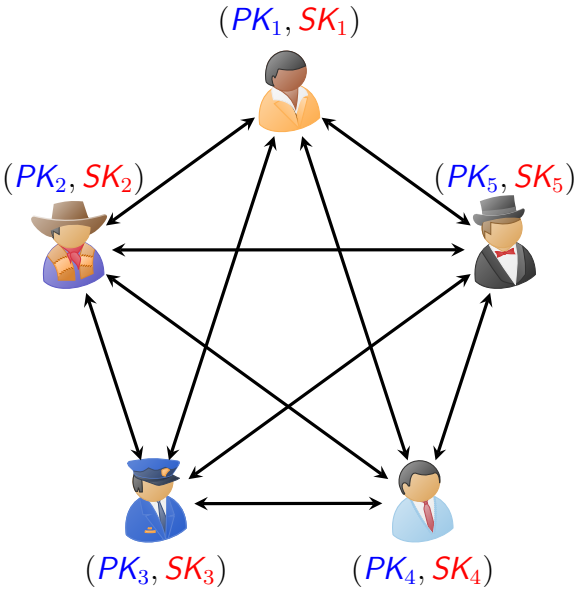
W. Diffie 和 M. Hellman 提出的新设想

- 每个用户 A 有一个加密密钥 PK_A，一个解密密钥 SK_A。
- 解密密钥 SK_A 需要保密，而加密密钥 PK_A 可以公开，要求 PK_A 的公开不影响 SK_A 的安全。
- 若用户 B 要向用户 A 秘密发送明文 m，可查询 A 的公开密钥 PK_A，加密后得到密文 $c = E(PK_A, m)$。
- 用户 A 收到密文 c 后，用只有用户 A 才拥有的解密密钥 SK_A 对 c 进行解密得到明文 $m = D(SK_A, c)$。



非对称密码体制的基本特点

- 加密能力与解密能力分开。
- 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。



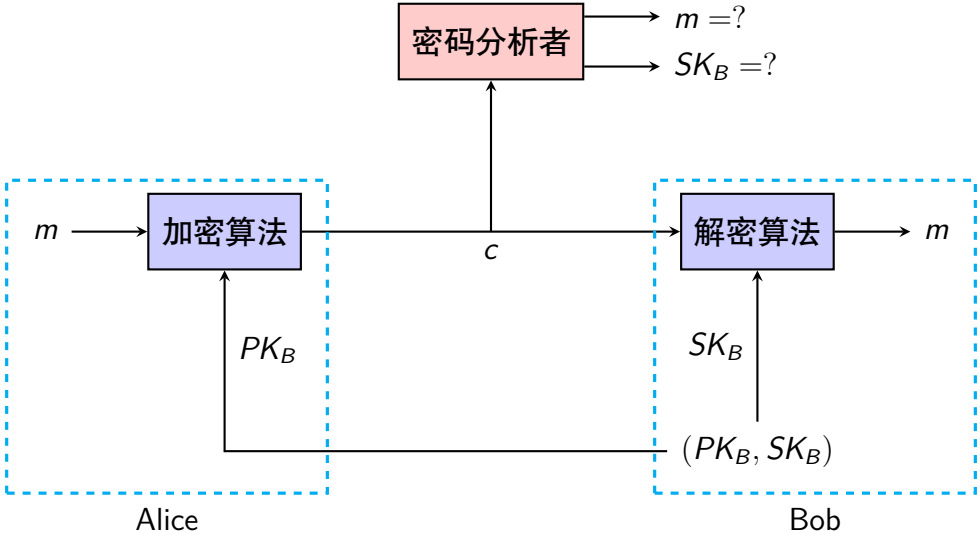
公钥密码体制

公钥密码体制的组成

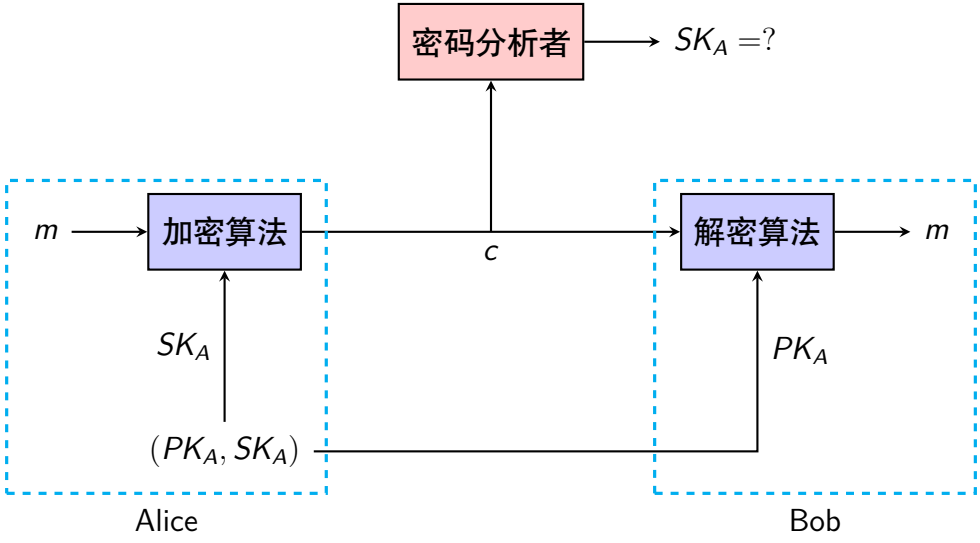
- 明文：算法的输入，可读信息或数据。
- 加密算法：对明文进行转换。
- 公钥和私钥：算法的输入，分别用于加密和解密。
- 密文：算法的输出，依赖于明文和密钥。
- 解密算法：根据密文和密钥，还原明文。

- 公钥算法依赖于一个加密密钥和一个与之相关的不同的解密密钥。算法有如下特点：
  - 仅由密码算法和加密密钥来确定解密密钥在计算上不可行
  - 两个密钥的任何一个都可用来加密，另一个用来解密

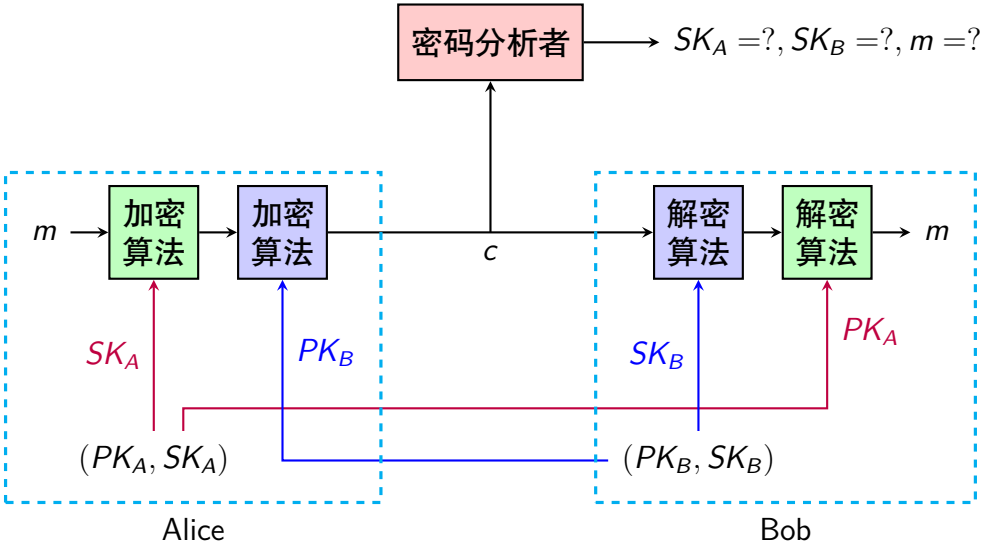
公钥密码：实现保密



公钥密码：实现认证



公钥密码：同时实现保密与认证



公钥密码体制的应用

- **加密/解密**：发送方用接收方的公钥对消息加密
- **数字签名**：发送方用其私钥对消息签名，可以对整体消息签名或对消息的摘要签名
- **密钥交换**：通信双方交换会话密钥

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie–Hellman	No	No	Yes
DSS	No	Yes	No

公钥密码体制的要求

- 容易产生一对密钥（公钥 PK 和私钥 SK）。
- 不难计算 $c = E(\mathrm{PK}, m)$ 和 $m = D(\mathrm{SK}, c)$。
- 知道 PK, 计算 SK 不可行。
- 不知道 SK，即使知道 PK, E, D 及 c，计算 m 不可行。
- 对明文 $m, E(\mathrm{PK}, m)$ 有定义，且 $D(\mathrm{SK}, E(\mathrm{PK}, m)) = m$。
- 对密文 $c, D(\mathrm{SK}, c)$ 有定义，且 $E(\mathrm{PK}, D(\mathrm{SK}, c)) = c$。
- 两个密钥可以交换顺序，即

$$D(\mathrm{PK}, E(\mathrm{SK}, m)) = D(\mathrm{SK}, E(\mathrm{PK}, m))$$

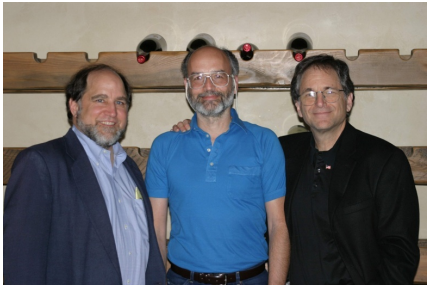
公钥密码体制的分析

- 穷举攻击：公钥密码易受穷举攻击，解决方法是使用长密钥。同时为了便于实现加密和解密，又希望密钥足够短。目前公钥密码仅限于密钥管理和签名。
- 从给定的公钥计算出私钥：尚未在数学上证明对一特定公钥算法这种攻击是不可行的。因此包括 RSA 在内的任何算法都是值得怀疑的。
- 穷举消息攻击：攻击者用公钥对所有可能的消息加密，并与传送的密文匹配，从而解密任何消息。抵抗的方法是在要发送的消息后附加随机数。

目录

RSA 非对称加密算法

- 1977 年，Ron Rivest、Adi Shamir、Len Adleman 提出了非对称加密算法 RSA，基于大合数的素因子分解难题。
- 1994 年 4 月一个小组通过 Internet 合作，8 个月时间成功分解 129 位的数，大约 428 比特；1999 年分解 155 位合数，最新的记录是 2005 年 5 月分解 200 位十进制数。
- RSA 专利于 2000 年 9 月 20 日到期。



Adi Shamir

- 1952 年出生于以色列，现任以色列魏兹曼科学研究院计算机科学与应用数学系教授。
- Adi Shamir 是信息加密和解密领域的顶尖专家。他是 RSA 加密算法的开发者之一，该方法改变了世界计算机通信的面貌，是电子商务和信息安全的基本支柱。

RSA 密码体制算法流程

Alice 按照以下步骤生成自己的公私钥

1. 随机选择两个秘密大素数 p 和 q，$p \neq q$;
2. 计算公开模数 $n = pq$ 及秘密欧拉函数 $\phi(n) = (p-1)(q-1)$;
3. 选择一个小于 $\phi(n)$ 且与 $\phi(n)$ 互素的数作为公钥 e;
4. 计算私钥 $d = e^{-1} \bmod \phi(n)$;
5. 公开 n, e。

3、4 步中的 e 和 d 可以交换

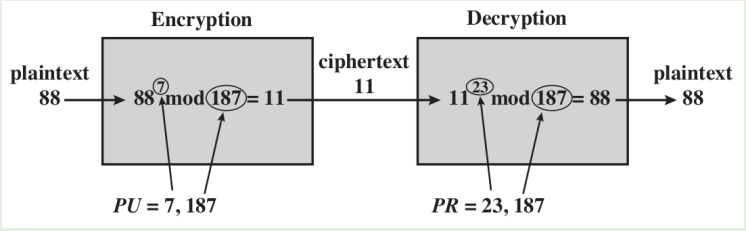
加密及解密

- Bob 用公开的 n 和 e 对消息 $m \in \mathbb{Z}_n$ 加密：$c = m^e \bmod n$
- Alice 利用自己的私钥 d 对密文 $c \in \mathbb{Z}_n$ 解密：$m = c^d \bmod n$

RSA 解密正确性的推导

- 如果按照规定的方式加密，则
$$m = c^d \bmod n = m^{ed} \bmod n$$
要能正确解密须说明 $m^{ed} \equiv m \pmod{n}$。
- 由于 $n = pq$，利用 CRT 的推论：
$$\text{如果} \begin{cases} m^{ed} \equiv m \pmod{p} \\ m^{ed} \equiv m \pmod{q} \end{cases}, \text{则有} \ m^{ed} \equiv m \pmod{n}$$
- 由于 $ed \equiv 1 \pmod{\phi(n)}$，则
$$\begin{aligned} m^{ed} &\equiv m^{k\phi(n)+1} \equiv m^{k'(p-1)+1} \equiv m^{k'p-k'+1} \\ &\equiv m^{k'p} m^{-k'+1} \equiv m^{k'} m^{-k'+1} \equiv m \pmod{p} \end{aligned}$$
同理可证 $m^{ed} \equiv m \pmod{q}$。

RSA 算法举例



- 选择 $p = 17, q = 11$，则 $n = pq = 187$，$\phi(n) = 160$；
- 选择 $e = 7$ 满足 $\gcd(7, 160) = 1$，$d = 23$；
- 公钥 $PK = 7$，私钥 $SK = 23$；
- 明文 $m = 88$；
- 加密计算 $c = 88^7 \bmod 187 = 11$；
- 解密计算 $m = 11^{23} \bmod 187 = 88$。

目录

能否由公钥计算私钥？

- 第三方密码分析者如果想要解密密文 c，需要知道 Alice 的私钥 d。
- RSA 算法中模数 n 和公钥 e 公开，第三方密码分析者能否由公开信息计算出 Alice 的私钥 d？
- 计算私钥 d 需要计算 $d = e^{-1} \bmod \phi(n)$，但是 $\phi(n)$ 未公开。
- 计算 $\phi(n)$ 的难度等同于对模数 n 进行因数分解，但是因数分解问题（FAC）属于单向函数，当 n 足够大时，目前没有高效求解算法。
- 因此 RSA 算法的安全性依赖于单向函数 FAC 难题的求解。

数学攻击

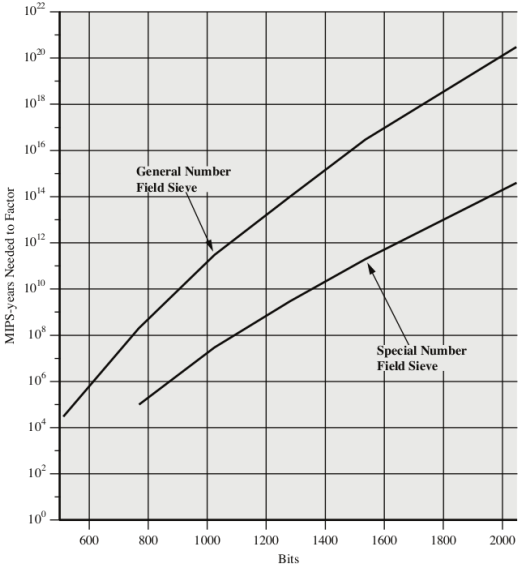
- 1977 年，RSA 的三位发明者在《科学美国人》杂志上发布一段密文让读者解密，解得明文者可获得 100 美元，他们预言需要 4×10^{16} 年才能解得明文。
- 这里 n 为 129 位十进制位，或 428 位二进制位。
- 但是，一个在互联网上工作的小团体只用了 8 个月的时间，于 1994 年 4 月正确解密。
- RSA 实验室也发布了使用不同 n 长度加密的密文，让公众解密。

数学攻击

Table 9.5 Progress in RSA Factorization

Number of Decimal Digits	Number of Bits	Date Achieved
100	332	April 1991
110	365	April 1992
120	398	June 1993
129	428	April 1994
130	431	April 1996
140	465	February 1999
155	512	August 1999
160	530	April 2003
174	576	December 2003
200	663	May 2005
193	640	November 2005
232	768	December 2009

MIPS-years Needed to Factor



- MIPS: million instructions per second
- MIPS-year: the number of instructions executed during one year of computing at one MIPS.
- GNFS 和 SNFS 是两种大数分解算法

数学攻击

- n 的位数应取 1024 到 2048 位；
- p 和 q 的长度应仅相差几位，p 和 q 都应约在 10^{75} 到 10^{100} 之间；
- $(p-1)$ 和 $(q-1)$ 都应有一个大的素因子；
- $\gcd(p-1, q-1)$ 应该较小。

小结

1. 公钥密码学的基本原理
2. RSA 非对称加密算法
3. RSA 的安全性分析