移动应用开发（七）

——密码学初步

张凯斌

福建农林大学
资源与环境学院

2025.4.7

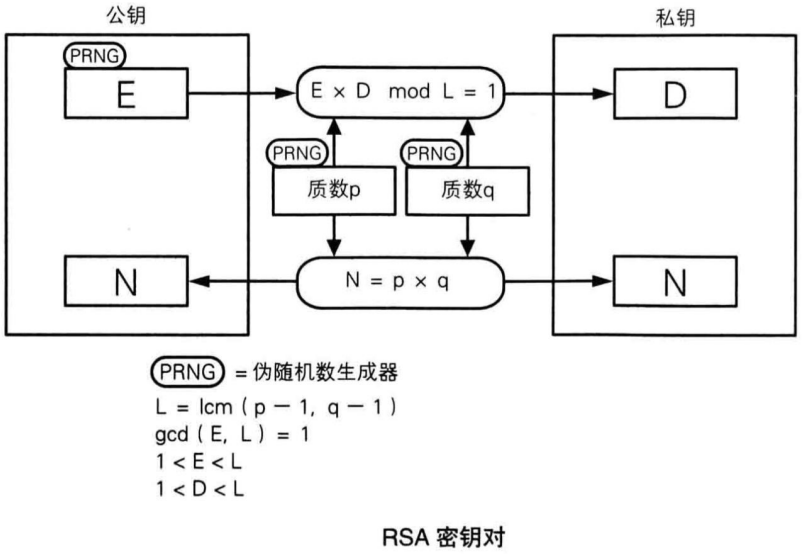
关于密码学

“It is naive to assume that people on computer networks are honest. It is naive to assume that the managers of computer networks are honest. It is even naive to assume that the designers of computer networks are honest.”

---- “Applied Cryptography”, second edition, Bruce Schneier

你喜欢M豆吗（1/5）

- 世界上有两种“密码”
  - 一种是为了防止其他小朋友拿走你的M豆采取的措施
  - 一种是那一套不知道在干些什么的数学公式和逻辑流程



RSA 密钥对

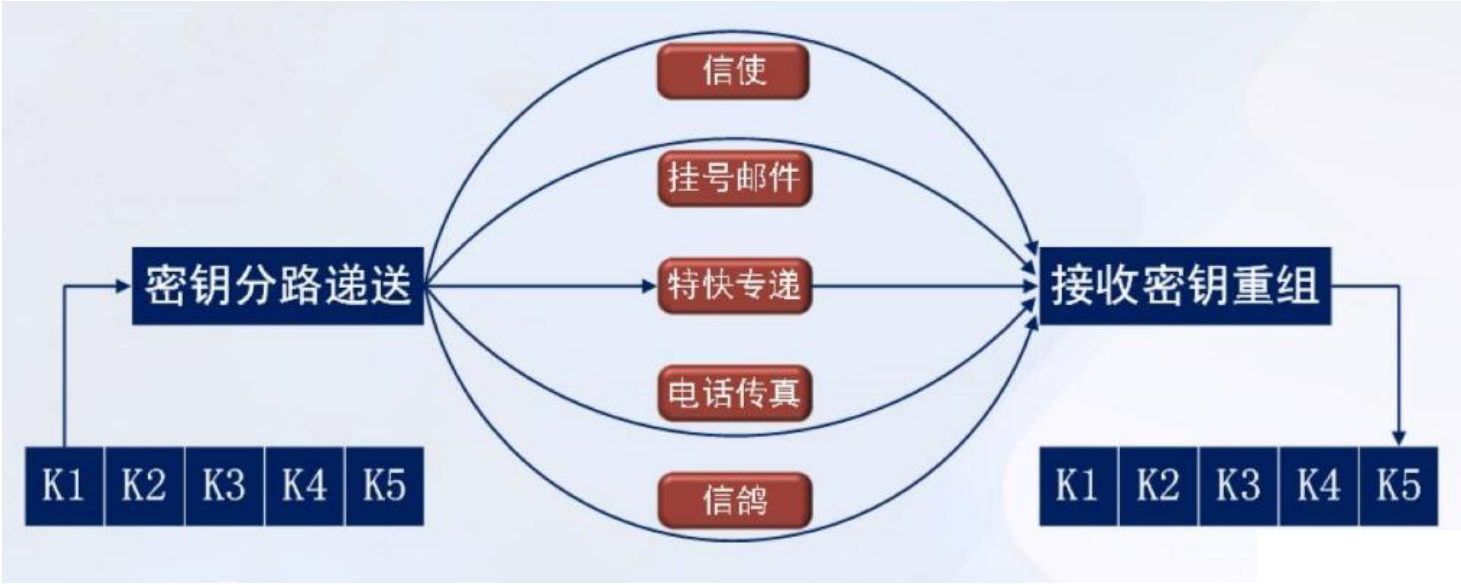
- 这两种其实没本质区别

你喜欢M豆吗（2/5）

- 课程要结束了，送你一袋M豆吧
  - 一些假设
    - 我们相隔万里
    - 很多人极其喜欢M豆，他们但凡有机会就想拿走
  - 一些问题
    - 我可以直接把M豆快递给你吗?
    - 可以用一个上锁的罐子装着M豆快递给你吗?

你喜欢M豆吗（3/5）

- 一个难题：钥匙如何给你呢？
  - 我坐飞机上门给你送个钥匙
  - 我委托一个可信第三方上门给你送个钥匙
  - 或者……



你喜欢M豆吗（4/5）

- 如果我们可以用不同的钥匙完成安全送递呢
  - 你用你的钥匙
  - 我用我的钥匙

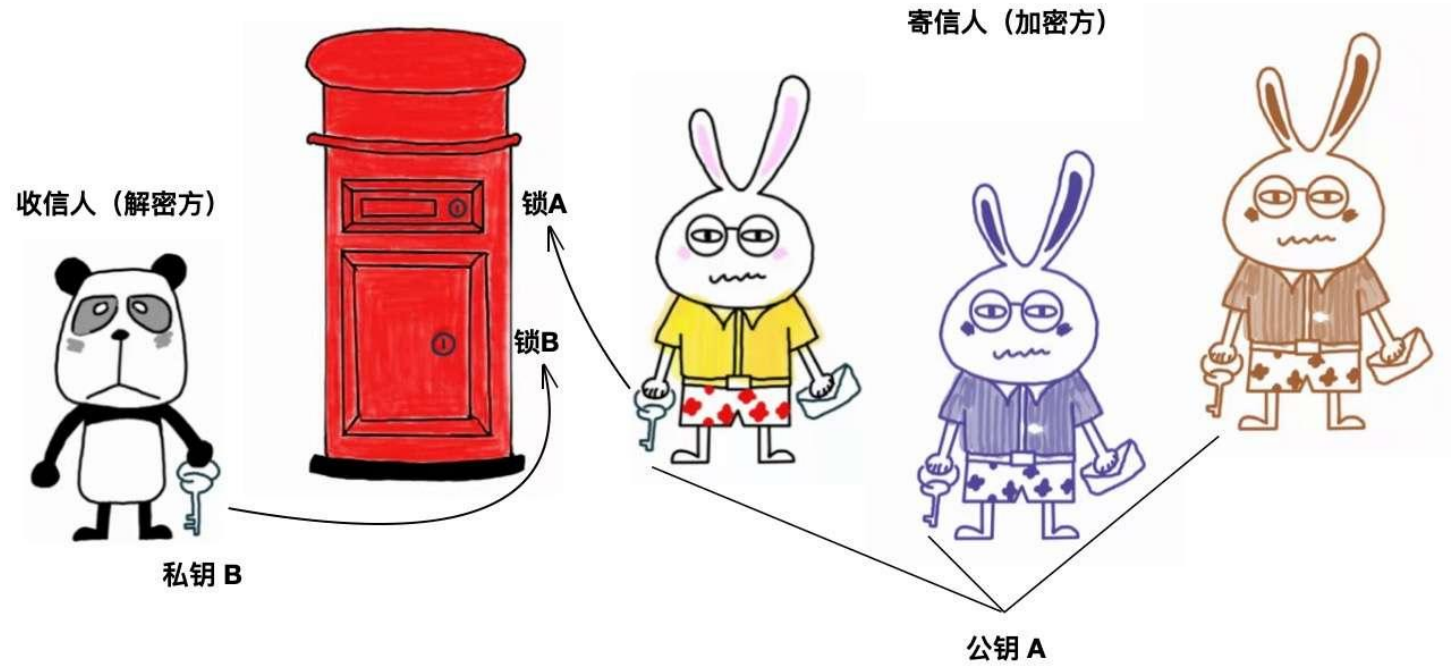
?

你喜欢M豆吗（5/5）

- 确实安全送到了，但好像还是有点麻烦
  - 我要是提前有你的锁就好了
  - 一开始就可挂着你的锁快递过去
- 一个无法被逆向工程的锁
  - 物理上可以上用工程手段
  - 信息上可以用数学手段 —— 非对称加密
    - 非对称加密的通信双方各自准备一对公钥和私钥
    - 公钥是公开的，由信息接受方提供给信息发送方，用来对信息加密
    - 私钥由信息接受方保留，用来解密
    - 非对称加密也称为公钥密码，但非对称加密这种叫法更可以体现出加密和解密使用不同的密钥的这一最大特点

小测试

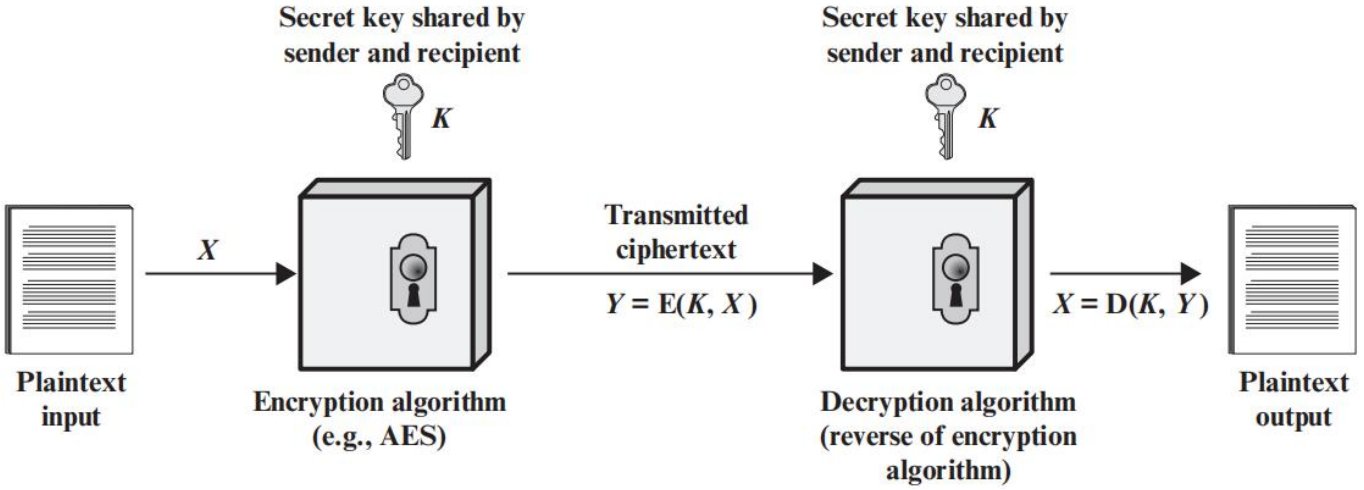
- 下面是什么加密算法



A: 对称加密　　B: 非对称加密　　C: 啥也不是

加解密的那些事（1/4）

- 最基本的对称加密结构
  - 原文（Plaintext）：我们想表达的原始信息
  - 加密算法（Encryption Algorithm）：对原文进行的一些操作
  - 解密算法（Decryption Algorithm）：本质上与加密算法相反
  - 密钥（Secret Key）：与原文和算法都无关的独立变量
  - 密文（Ciphertext）：经过带密钥的加密算法转换之后的信息



加解密的那些事（2/4）

- 对抽象加密结构的一些具体体会
  - 最基本的加密算法：替换（Substitution）
    - 一个古老又经典例子：凯撒密码（Caesar Cipher）
      - 通过把字母移动一定的位数来实现加解密
    - 字母序表

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

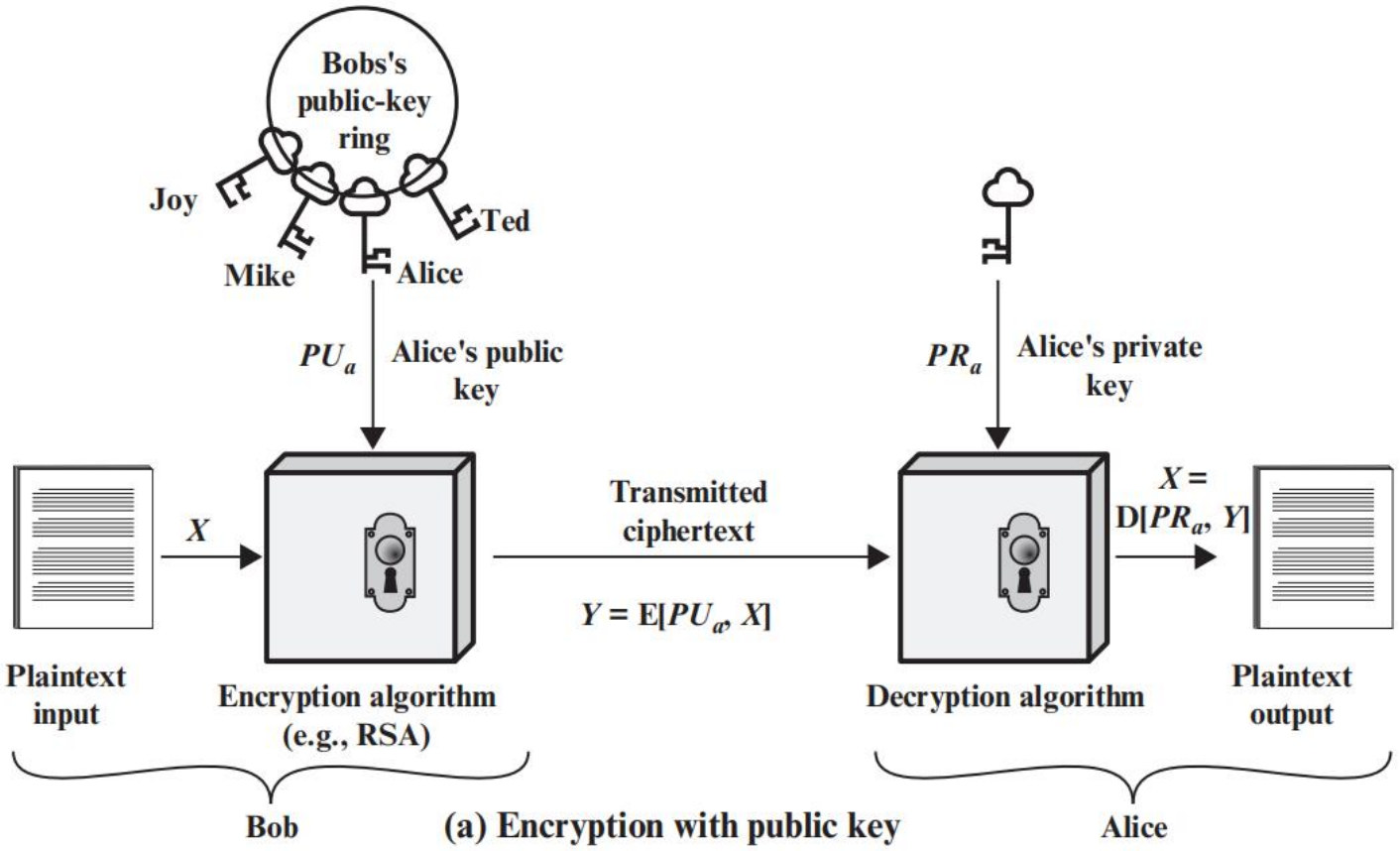
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

    - 密文表达式

$$C = \mathrm{E}(k, p) = (p + k) \bmod 26$$

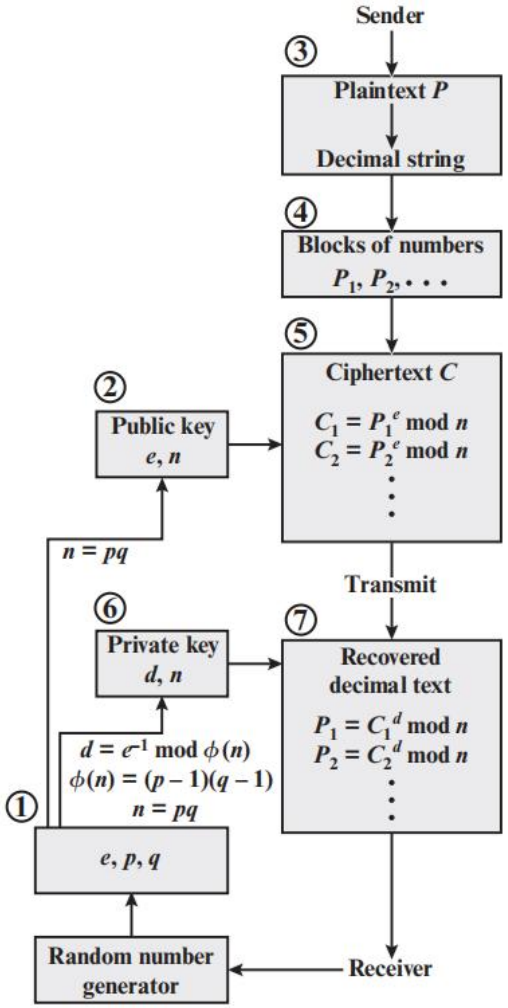
加解密的那些事（3/4）

- 感受一下非对称加密结构的味道
  - 特意保留一些原味，让大家知道我们真的是在学习加密算法

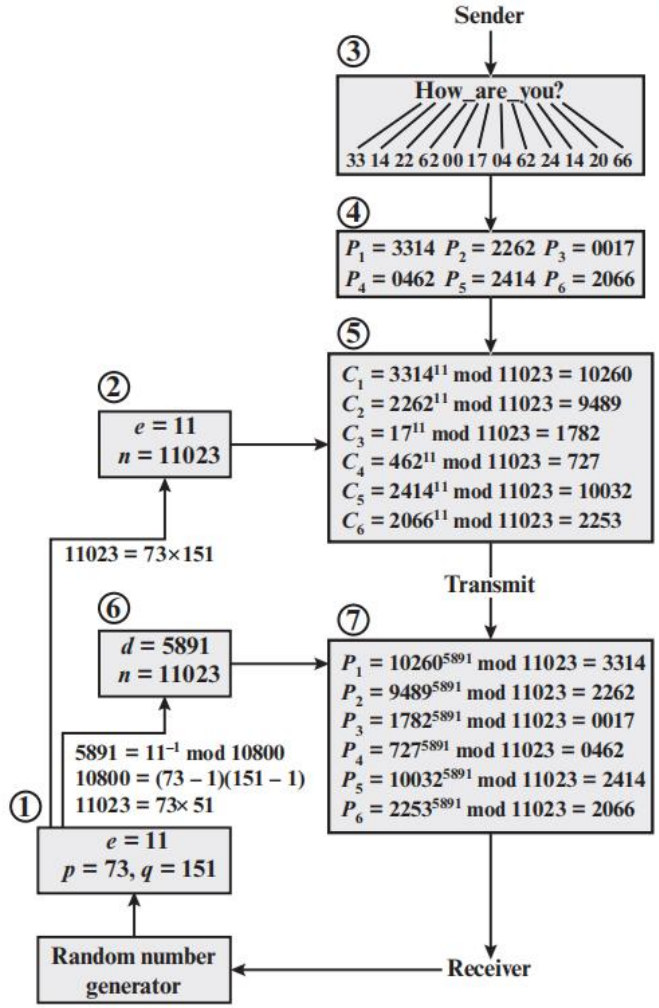


加解密的那些事（4/4）

- （contd.）
  - p和q都是质数且不相等
  - e和Φ(n)互质



(a) General approach



(b) Example

小测试

- 前面我们已经知道凯撒密码的密文表达式

$$C = \mathrm{E}(k, p) = (p + k) \bmod 26$$

- 那么凯撒密码的原文表达式是什么呢

$$p = \mathrm{D}(k, C) = (C - k) \bmod 26$$

Q&A

Good Luck!