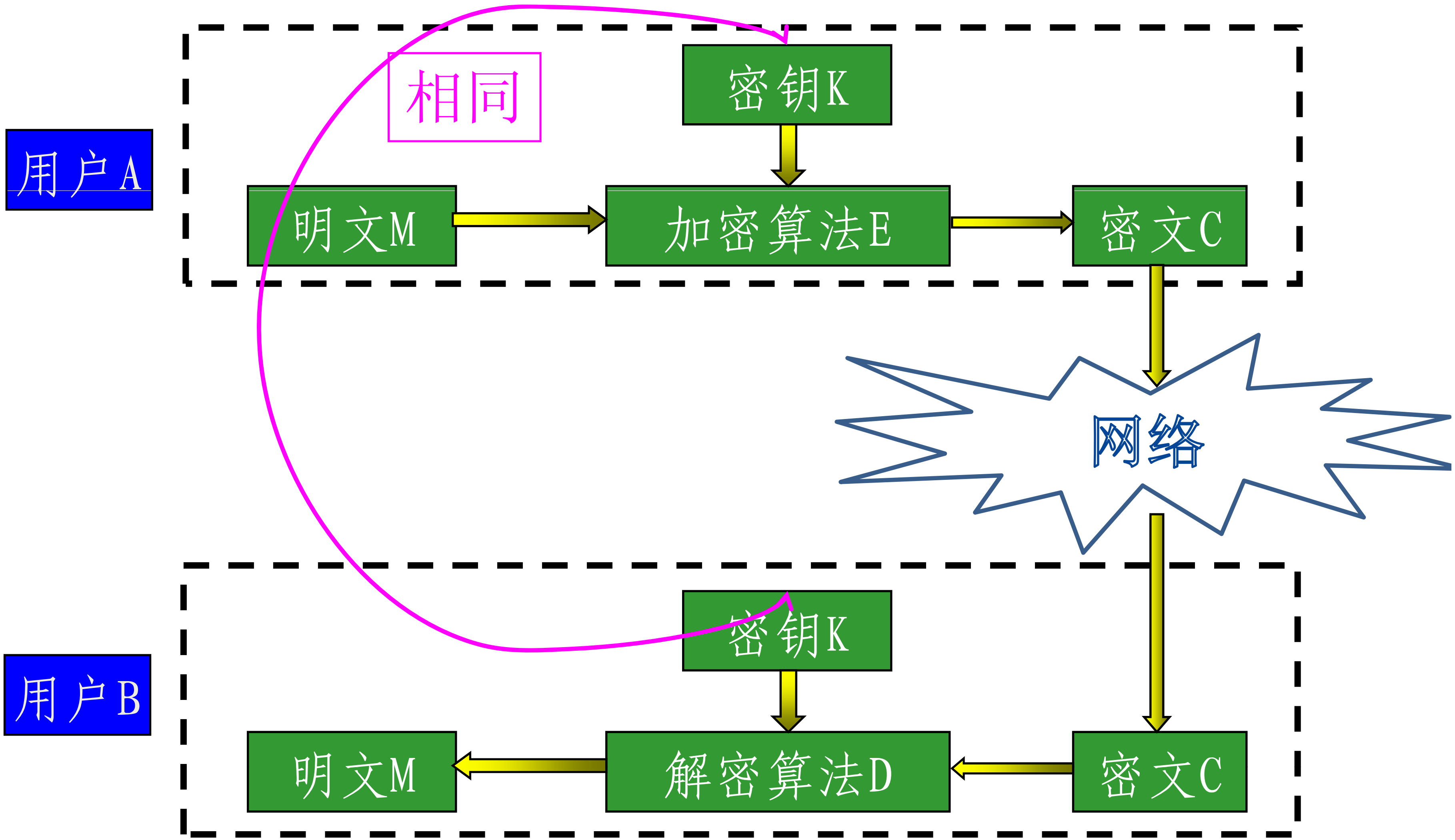
第五章　密钥管理与公钥革命

By 张鹏
深圳大学计算机与软件学院
zhangp@szu.edu.cn

目　　录

对称密码模型



1 对称密码的限制

- 已知密钥，可加密与解密。然而加密者与解密者处于不同的地理位置，密钥如何分发？
- 任何密码系统的强度都与密钥分发方法有关。
- 密钥分发方法是指将密钥发送给希望交换数据的双方而不让别人知道的方法。

1 对称密码的限制

- 1）A选择密钥，并亲自交给B。
- 2）第三方选择密钥，并亲自交给A和B。

Solutions that are based on private-key cryptography are not sufficient to deal with the problem of secure communication in open systems where parties cannot physically meet and/or have transient interactions.

1 对称密码的限制

3）A和B有秘密渠道。

- 密钥分发问题：网络中有N个人，则每人需存储N-1个密钥。
- 密钥管理问题：密钥越多，存储空间越大，泄露的可能性越大。

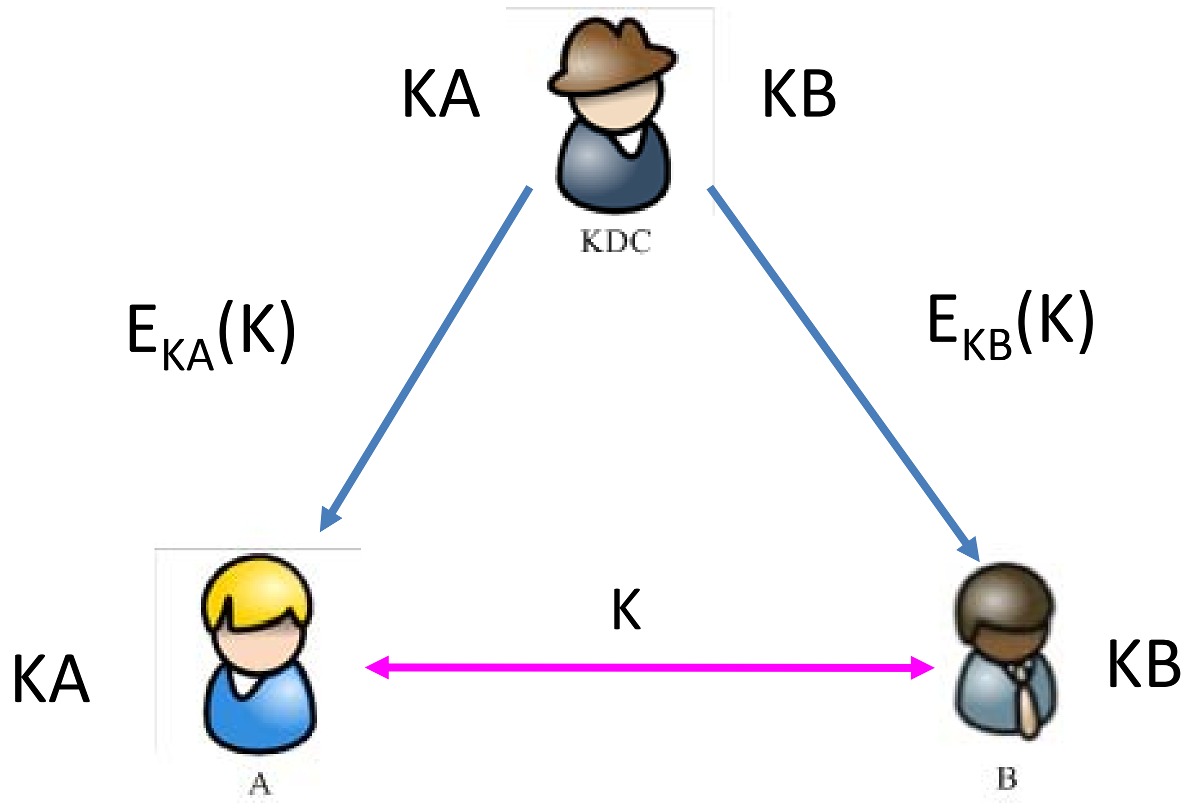
(You can hide a needle in a haystack but it’s hard to hide thousands of needles in a haystack.)

- 不适用于开放环境

1 对称密码的限制

4）A和B与第三方有秘密渠道。

- 密钥分发中心(key distribution center， KDC)
- 所有用户与KDC共享密钥



1 对称密码的限制

由此解决了密钥分发难题，密钥管理难题。

缺点：

- KDC要可信
- KDC易成为攻击点
- 系统单点失效

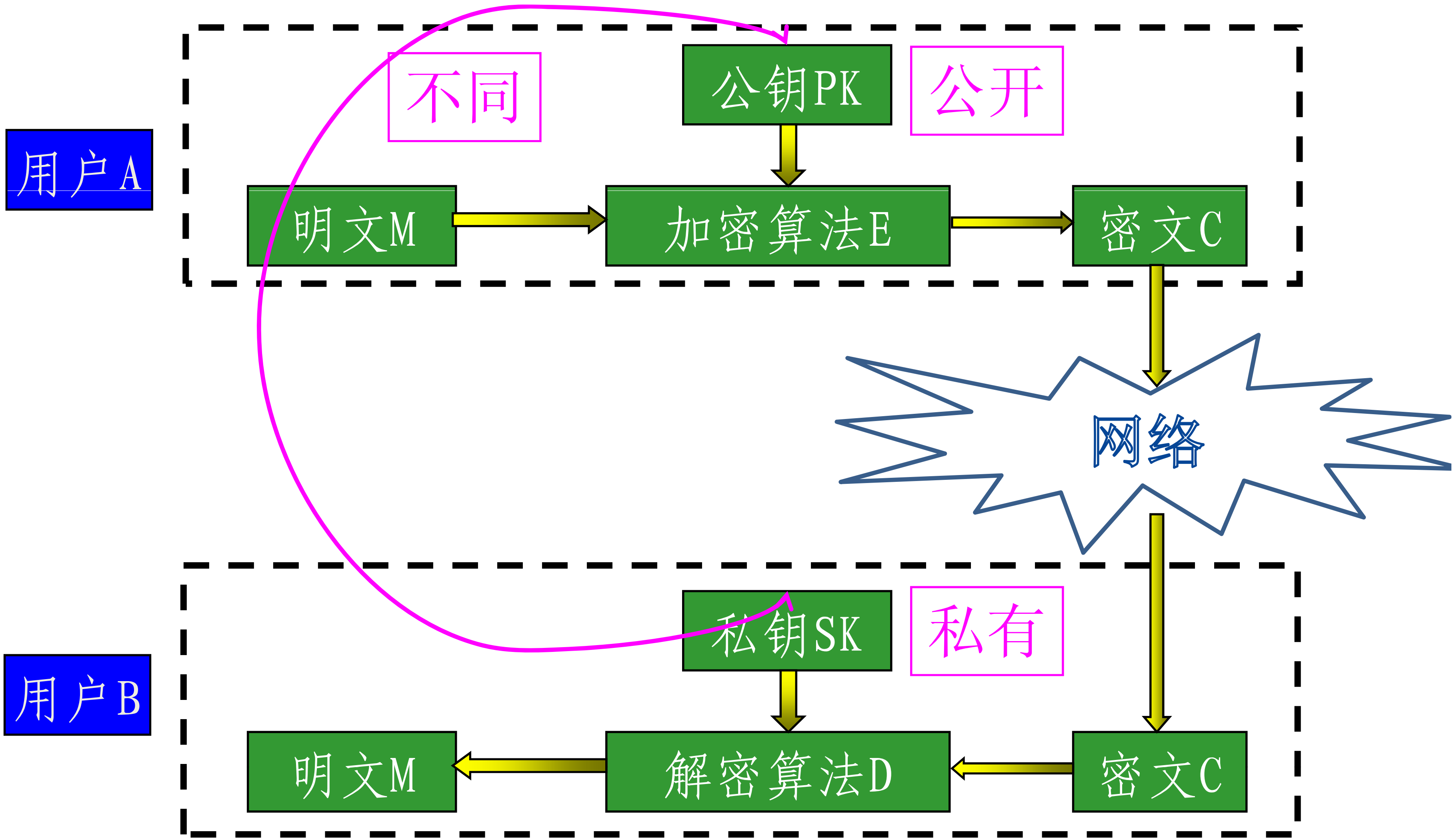
2 公钥革命

- 1976年， Whitefield Diffie与Martin Hellman发表了论文”New Directions in Cryptography”。
- 论文影响巨大，采用一种完全不同的方法研究密码学，是对称密码体制向公钥密码体制迈进的第一步。
- 现实世界存在许多不对称：

花瓶打碎了难以复原。

乘以两个素数容易，分解两个素数困难。

公钥密码模型



2 公钥革命

- 加密密钥公开，任何人可采用它加密。
- 即使加密密钥公开，方案依然是安全的。
- 这样的方案被称为公钥密码方案，其中加密密钥为公钥，解密密钥为私钥。
- 优点：将密码由政府、军事应用延伸至商业、个人应用。

密钥分发：公钥可公开发布，如微博等。

密钥管理：每个用户仅需存储自身的私钥。

2 公钥革命

- Diffie-Hellman介绍了3个不同的公钥密码原语：
- 1）公钥加密
- 2）数字签名
- 3）密钥交换

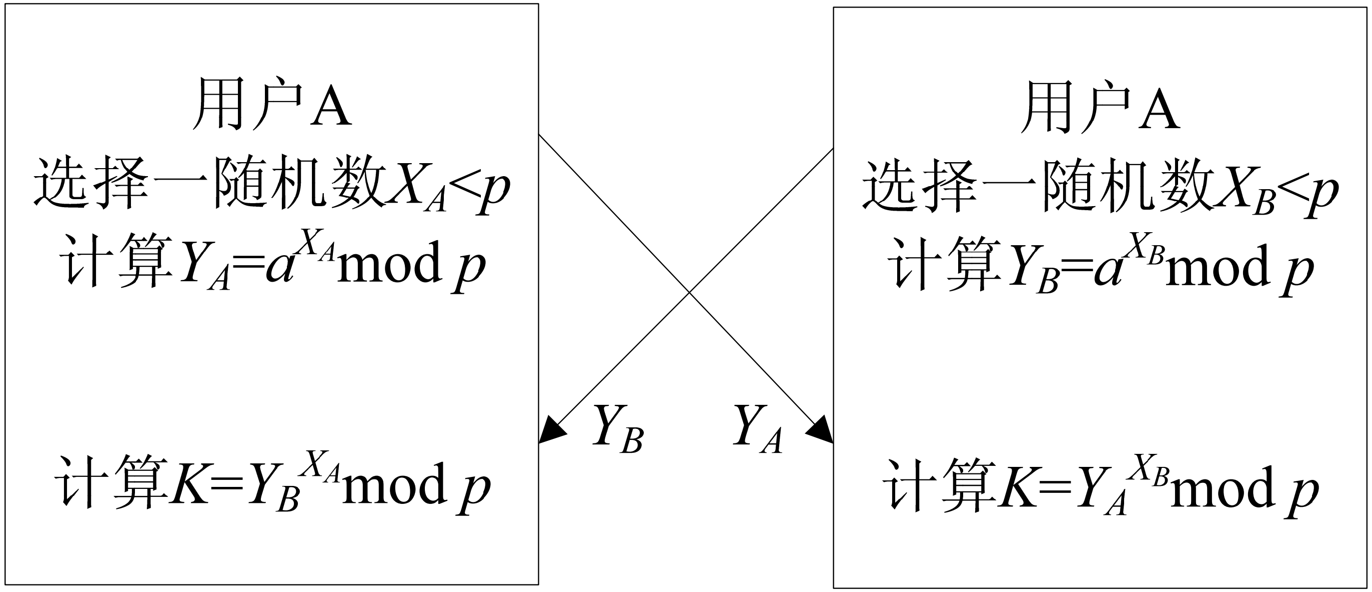
3 Diffie-Hellman密钥交换

- Diffie - Hellman密钥交换是W. Diffie和M. Hellman于1976年提出的第一个公钥密码算法，已在很多商业产品中得以应用。

- 算法的唯一目的是使得两个用户能够安全地交换密钥，得到一个共享地会话密钥，算法本身不能用于加解密。

3 Diffie-Hellman密钥交换

p是大素数，a是p的本原根，p和a为公开参数。



- 算法的安全性基于求离散对数的困难性。

3 Diffie-Hellman密钥交换

- 正确性： $Y_B^{XA} \bmod p=(a^{XB} \bmod p)^{XA} \bmod p$

  $=(a^{XB})^{XA} \bmod p$

  $=a^{XBXA} \bmod p$

  $=Y_A^{XB} \bmod p$

- 因$\mathrm{X_A}$，$\mathrm{X_B}$是保密的，敌手只能得到p，a，$\mathrm{Y_A}$，$\mathrm{Y_B}$，要想得到K，则必须得到$\mathrm{X_A}$，$\mathrm{X_B}$中的一个，这意味着需求离散对数。因此敌手求K是不可行的。

- 简单的DH协议(未进行认证)容易受到中间人攻击。

3 Diffie-Hellman密钥交换

例如：p＝97，a＝5。

① A秘密地选X_A＝36，并计算$Y_A=5^{36}mod97$＝50，发送Y_A至B。

② B秘密地选$X_B=58$，并计算$Y_B=5^{58}mod97$＝44，发送换Y_B至A。

③ A 接收Y_B后计算$K=Y_B^{XA}$ mod97＝44^{36}mod97＝75

④ B接收Y_A后计算$K=Y_A^{XB}$ mod97＝50^{58}mod97＝75

4 离散对数难题

欧拉函数：设 n 是一正整数，小于 n 且与 n 互素的正整数的个数称为 n 的欧拉函数，记为 $\phi(n)$。例：$\phi(6)=2$，$\phi(7)=6$，$\phi(8)=4$。若 n 是素数，则显然有 $\phi(n)=n-1$

定理 1：若 n 是两个素数 p 和 q 的乘积，则 $\phi(n)=(p-1)(q-1)$。

定理 2（欧拉定理）：若 a 与 n 互素，则 $a^{\phi(n)}=1 \bmod n$。

4 离散对数难题

定义 3：满足方程 $a^m = 1 \bmod n$ 的最小正整数 m 为模 n 下 a 的阶。

定理 4：若模 n 下 a 的阶为 $\phi(n)$，即 $a^{\phi(n)} = 1 \bmod n$，则称 a 为 n 的本原根。则：

$$a, a^2, \cdots, a^{\phi(n)}$$ 在模 n 下互不相同且都与 n 互素

4 离散对数难题

例：$n=9$，$\varphi(n)=6$，考虑到：

$$2 \bmod 9 = 2, 2^2 \bmod 9 = 4, 2^3 \bmod 9 = 8$$

$$2^4 \bmod 9 = 7, 2^5 \bmod 9 = 5, 2^6 \bmod 9 = 1$$

所以 2 为 9 的本原根。

4 离散对数难题

设 p 是素数， a 是 p 的本原根。则：

$a^{\phi(p)} = 1 \bmod p \Rightarrow a^{p-1} = 1 \bmod p$ 。

$a, a^2, \cdots, a^{p-1}$ 在模 p 下互不相同且都与 p 互素，即：

$a, a^2, \cdots, a^{p-1}$ 在模 p 下产生 1 到 $p-1$ 的所有值。

4 离散对数难题

对 $\forall b \in \{1,\ldots,p-1\}$，有唯一的 $i \in \{1,\ldots,p-1\}$，使得 $b = a^i \bmod p$。

离散对数难题：已知 a, p, i 求 b 容易，已知 a, p, b 求 i 困难。

举例：计算 $2^5 \bmod 9 = 5$ 容易，从 $2^i \bmod 9 = 5$ 求 i 困难。i 不唯一，可以是 5,11,17,23. . .

4　离散对数难题

习题：求25的所有本原根。

Q&A