第六讲　公钥密码

郑燕飞

公钥密码体制基本概念

* 公钥密码(又称双钥密码和非对称密码)，是1976年由W. Diffie和 M. Hellman在其“密码学新方向”一文中提出的，见划时代的文献：

  W.Diffie and M.E.Hellman, New Directrions in Cryptography, IEEE Transaction on Information Theory, V.IT-22.No.6, Nov 1976, PP.644-654

公钥密码体制基本概念(Cont.)

* 公钥系统

用陷门函数f作为加密函数，将f公开，并公开加密密钥。此时加密密钥便称为公开密钥，记为Pk。 f函数的设计者将δ 保密，用作解密密钥，此时δ 称为秘密钥匙，记为Sk。由于加密函数是公开的，任何人都可以将信息x加密成y=f(x)，然后送给函数的设计者（当然可以通过不安全信道传送）；由于设计者拥有Sk，他自然可以解出$x=f^{-1}(y)$。

双钥体制（公钥体制）

系统中，加密密钥称公开密钥（public Key）可以公开发布（电话号码注册）；而解密密钥称私人密钥（private key,简称私钥）。

* 加密：

M=D(E(M,pub-key),private-key)

* 认证：

M=E(D(M,private-key),pub-key)

双钥体制（公钥体制）

- 同时实现加密和认证(A----->B)

C：A发给B的密文

c=E(D(m,private-key-A),pub-key-B)

m：B恢复出的明文

m=E(D(c,private-key-B),pub-key-A)

常规加密和公开密钥加密

运行条件	运行条件
加密和解密使用同一个密钥和同一个算法	使用同一个算法进行加解密 两个密钥，一个加密，一个解密
发送方和接收方共享密钥和算法	发送方和接收方各拥有一对密钥中的一个
安全条件	**安全条件**
密钥必须保密	私钥必须保密
解密报文不可能，至少不现实	解密报文不可能，至少不现实
通过算法和密文样本不足以确定密钥	通过算法、公钥和密文样本不足以确定私钥

公钥密码体制基本概念(Cont.)

- 单向函数

  是满足下列条件的函数f：

  (1)给定x，计算y=f(x)是容易的；

  (2)给定y， 计算x使y=f(x)是困难的。

  (所谓计算$x=f^{-1}(Y)$困难是指计算上相当复杂)

公钥密码体制基本概念(Cont.)

- 陷门单向函数

  满足以上（1），（2）和

  （3）存在δ，已知δ 时,对给定的任何y，若相应的x存在，则计算x使y=f(x)是容易的。

  δ 称为陷门信息。

公钥密码体制基本概念(Cont.)

- 用于公钥体制的陷门单向函数
  - 离散对数问题
  - 大数分解
  - 二次剩余问题
  - 多项式求根

公钥密码体制基本概念(Cont.)

- 公钥体制的应用
  - 加密解密
  - 数字签名
  - 密钥交换

某些算法适合所有的三种应用，而有些可能只适用于这些应用的一种或两种。

费马定理

- 费马定理

  如果 p 是素数，a 是不能被 p 整除的正整数，则

  $$a^{p-1} \equiv 1 \bmod p$$

- 一种等价形式

  如果 p 是素数，a 是任意正整数，则

  $$a^{p} \equiv a \bmod p$$

欧拉函数

- $\phi(n)$ ，欧拉函数

  表示小于n的且与n互素的正整数个数
- 对于素数p，有

  $$\phi(p) = p - 1$$
- 对于 $n = pq$ ，p 和 q 为不同的素数，有 $\phi(n) = \phi(pq) = \phi(p) \times \phi(q) = (p-1) \times (q-1)$

欧拉定理

- 欧拉定理

  对于任何互素的整数 a 和 n，有

  $$a^{\phi(n)} \equiv 1 \bmod n$$

- 推论

  给定两个素数 p 和 q，以及整数 $n = pq$，m，其中 $0 < m < n$，有

  $$m^{\phi(n)+1} = m^{(p-1)(q-1)+1} \equiv m \bmod n$$

ＲＳＡ公钥算法

* Diffie和Hellman开创性的论文为密码学带来新的方法和挑战。
* RSA公钥算法是由Rivest,Shamir和Adleman在1978年提出来的（见Communitions of the ACM. Vol.21.No.2. Feb. 1978, PP.120-126)该算法的数学基础是初等数论中的Euler（欧拉)定理，并建立在大整数因子的困难性之上。RSA是最早的公钥体制的挑战响应者，也是最受广泛接受和实现的公钥体制。

ＲＳＡ公钥算法

- ＲＳＡ密码体制描述如下：
  - 首先，明文空间P＝密文空间$C=Z_n$.(分组是小于或等于$\log_2 n$的整数).
  - 密钥的生成

    选择p,q，p,q为互素数，计算n=p*q，φ(n)=(p-1)(q-1)

    选择整数e 使(φ(n),e)=1,1<e<φ(n)),

    计算d,使$d=e^{-1} \bmod \varphi(n)$,

    公钥Pk={e,n};私钥Sk={d,n}。

ＲＳＡ公钥算法

- ＲＳＡ密码体制描述如下：
  - 加密（用e,n）
    明文：$M<n$　　密文：$C=M^e \pmod n$.
  - 解密（用d,n）
    密文：C　　明文：$M=C^d \pmod n$

ＲＳＡ公钥算法

- ＲＳＡ成立的理由

因选择d，e使得d=e^{-1} mod φ (n)，

有：　ed = 1 mod φ (n)，

根据Euler定理的推论：给定满足n=pq的两个素数p和q，以及满足0<M<n的整数M，

有：$m^{k\phi(n)+1} = m^{k(p-1)(q-1)+1} \equiv m \bmod n$

M^{ed}= M mod n。

现在：

$C = M^e \bmod n$

$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

$= M \bmod n$

ＲＳＡ公钥算法

* 例子

1． 选素数p=47和q＝71，得n=3337，

  $\varphi(n)=46\times70=3220$；

2． 选择e=79，求得私钥$d=e^{-1}\equiv1019 \pmod{3220}$。

3． 公开n=3337和e=79.

4． 现要发送明文688，计算：

$$688^{79} \pmod{3337}=1570$$

5． 收到密文1570后，用私钥d＝1019进行解密：

$$1570^{1019} \pmod{3337}=688$$

ＲＳＡ公钥算法

- ＲＳＡ的安全性
  - 强力攻击
  - 数学攻击（两个素数乘机的因子分解）
  - 定时攻击
    - 利用测定RSA解密进行的时间来估计解密指数d，然后再精确出d的值

RSA公钥算法

- 密码体制的参数选择
  - n的确定（p,q必须是强素数）
  - 建议选择p和q大约是100位的十进制素数。 模n的长度要求至少是512比特。EDI攻击标准使用的RSA算法中规定n的长度为512至1024比特位之间，但必须是128的倍数。国际数字签名标准ISO/IEC 9796中规定n的长度位512比特位。

ＲＳＡ公钥算法

- 密码体制的参数选择
  - e的选择（EDI国际标准中规定 $e=2^{16}+1$，ISO/IEC9796中甚至允许取e＝3，e为小整数时运算快，但存在问题。）
  - d的选择（d要大于$n^{1/4}$）

RSA公钥算法

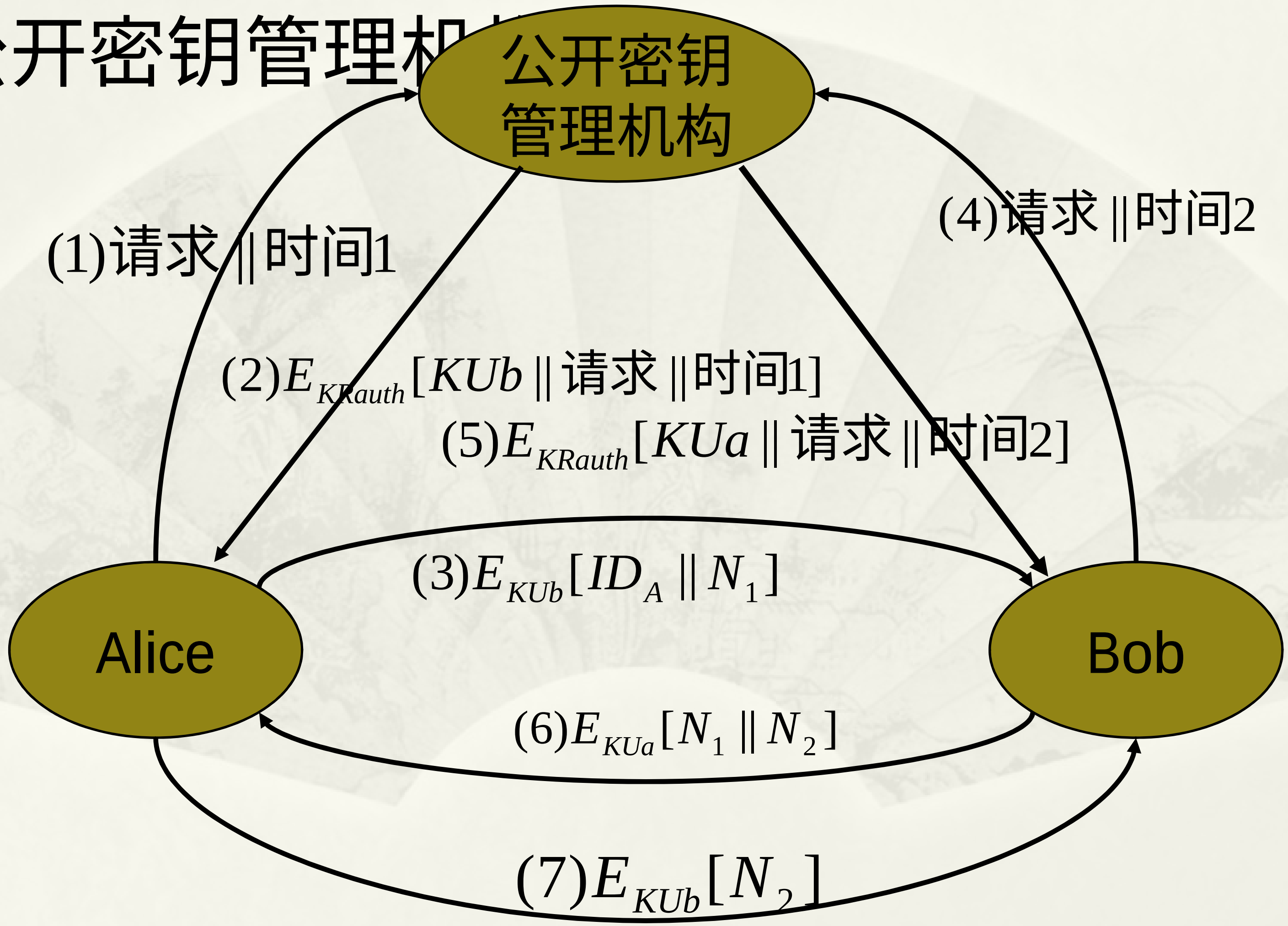
- 加密和解密
  - 计算x的n次幂
- 密钥的产生
  - 确定两个大素数p&q
    - 几乎所有的测试方法都是概率性的
  - 计算d或e的乘法逆元

密钥管理

* 公开密钥的分配
  * 公开宣布
  * 公开可以得到的目录
  * 公开密钥管理机构
  * 公开密钥证书

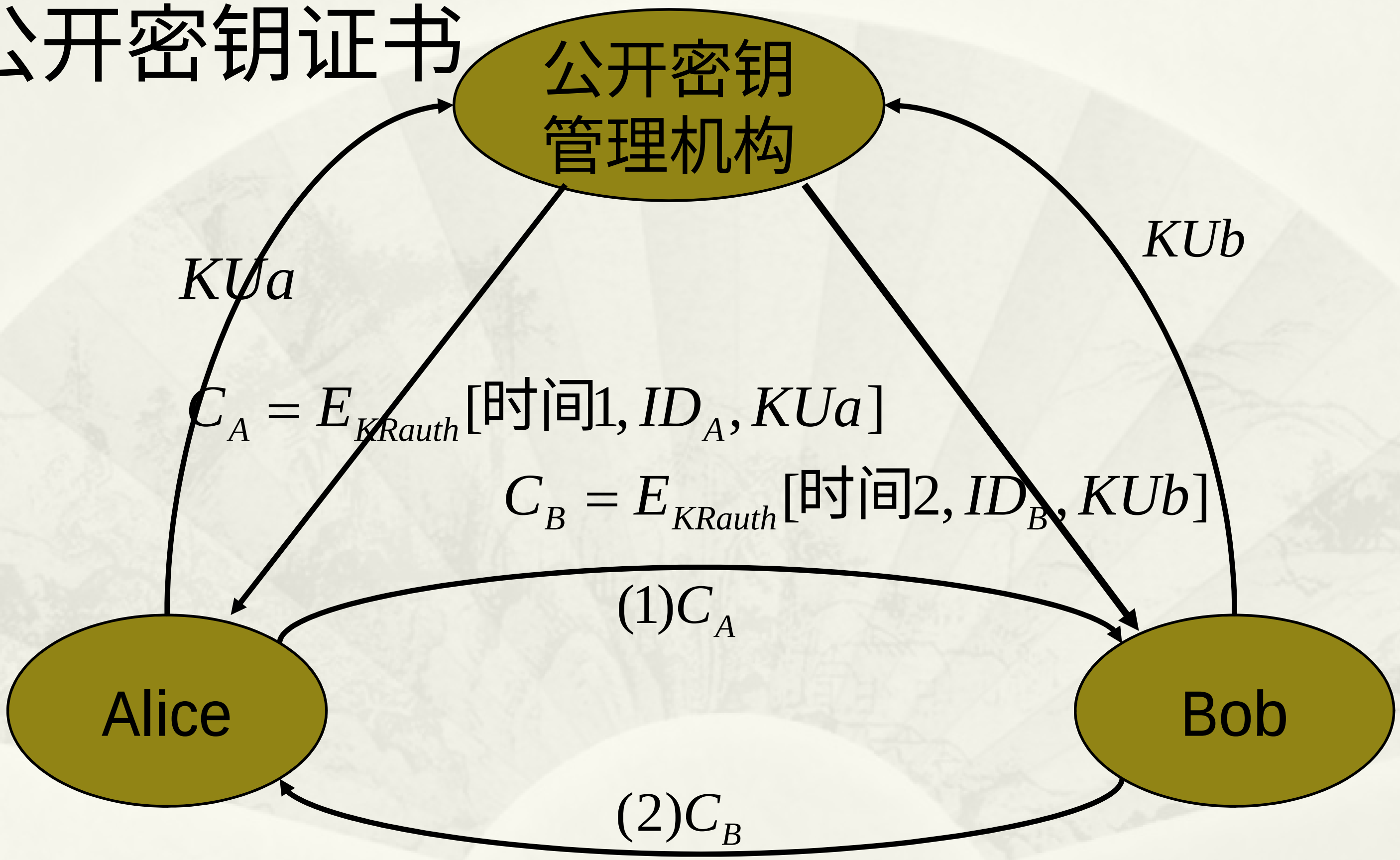
密钥管理

- 公开密钥管理机



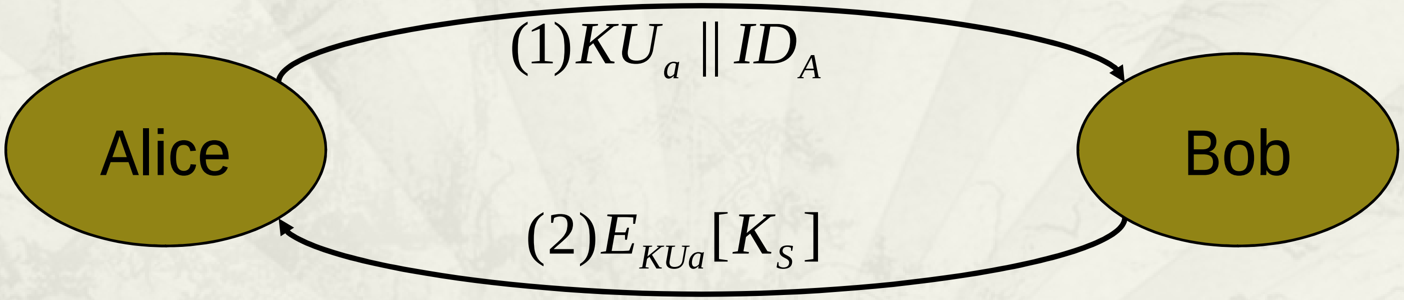
密钥管理

- 公开密钥证书

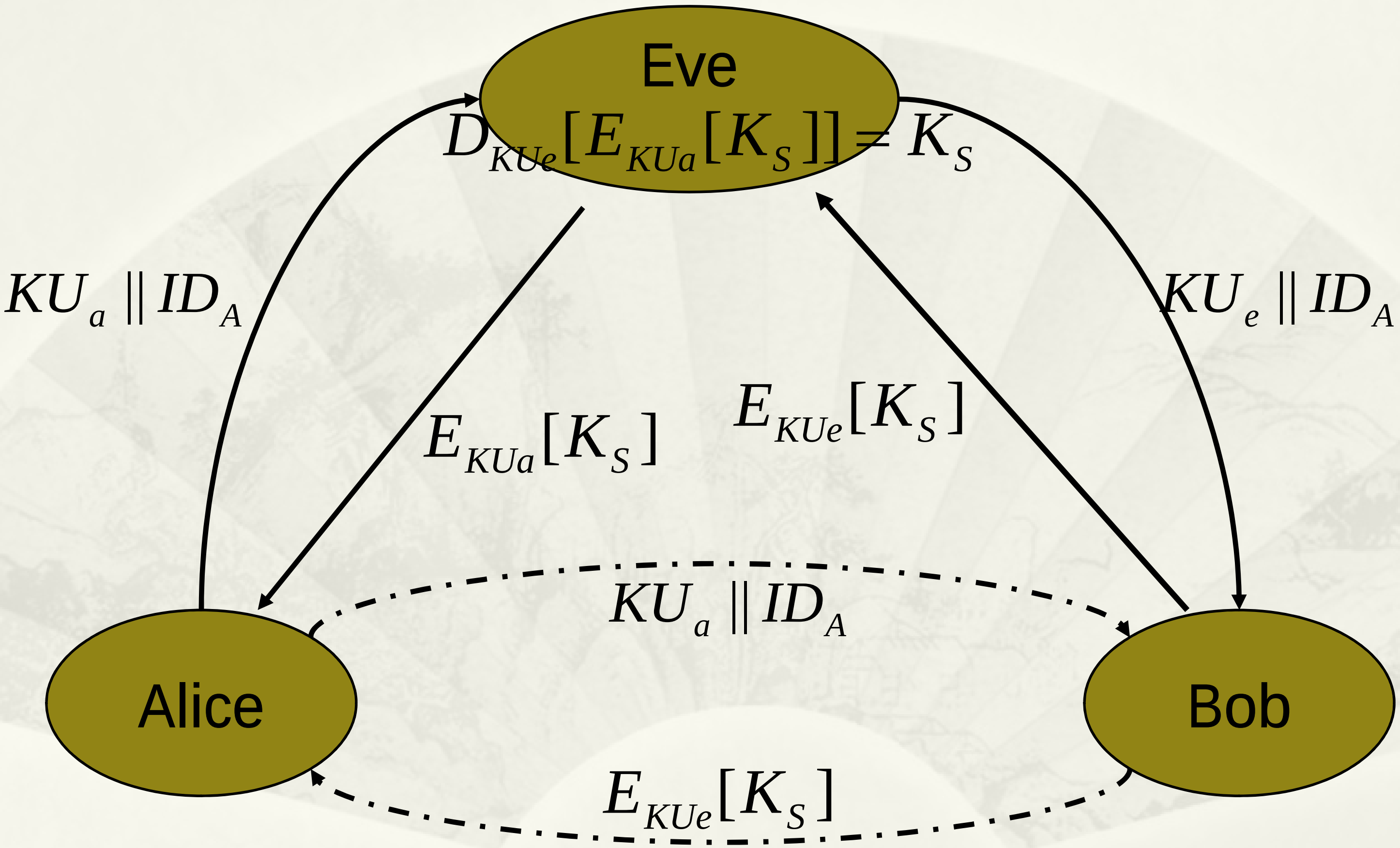

公开密钥管理机构
KUa
KUb
$C_A = E_{KRauth}[时间1, ID_A, KUa]$
$C_B = E_{KRauth}[时间2, ID_B, KUb]$
$(1)C_A$
Alice
Bob
$(2)C_B$

密钥管理

- 用公开密钥加密进行秘密密钥分配
  - 简单的秘密密钥分配

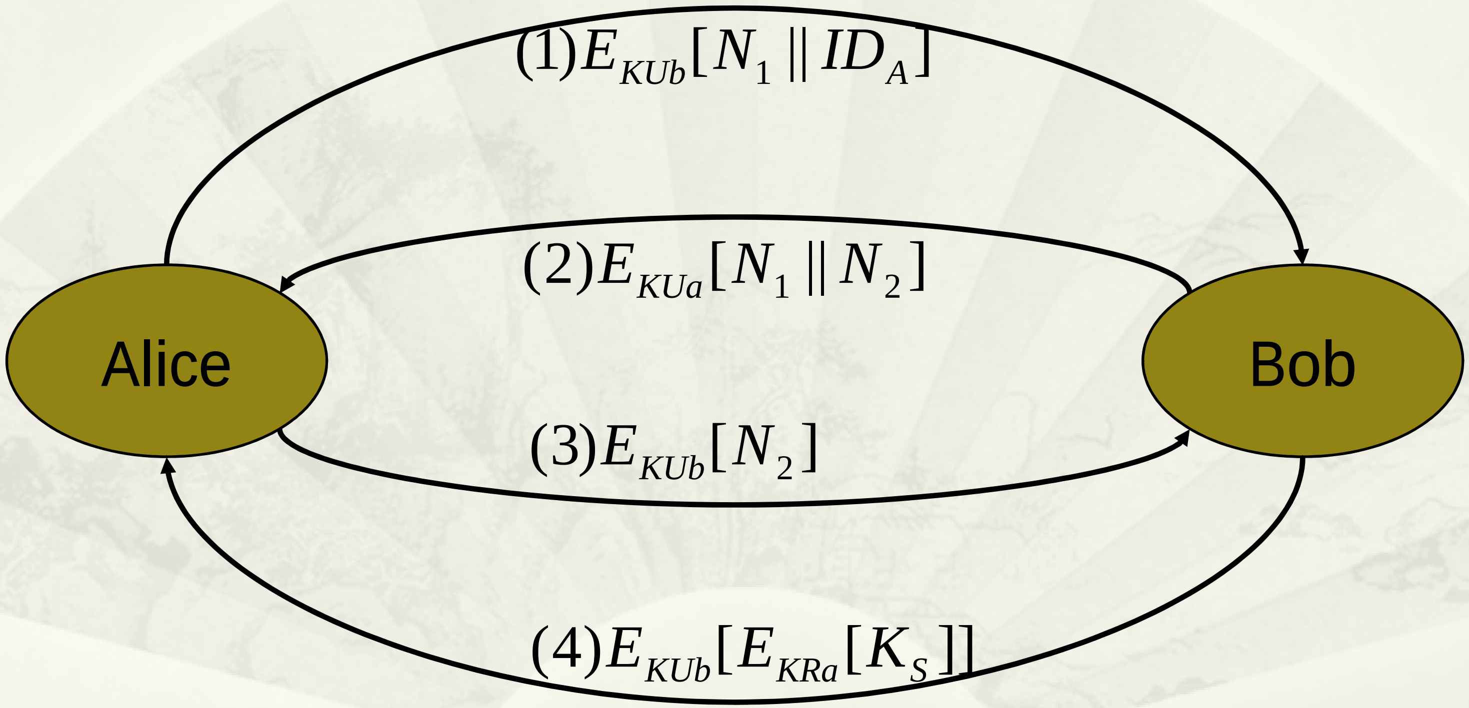


密钥管理


Eve
$D_{KUe}[E_{KUa}[K_S]] = K_S$
$KU_a \| ID_A$
$KU_e \| ID_A$
$E_{KUa}[K_S]$
$E_{KUe}[K_S]$
$KU_a \| ID_A$
Alice
Bob
$E_{KUe}[K_S]$

密钥管理

* 具有保密和鉴别能力的秘密密钥分配



密钥管理

- Diffie-Hellman密钥交换

用户A

产生：

随机的X_A <q;

计算：

$Y_A = \alpha^{X_A} \bmod q$

计算：

$K = Y_B^{X_A} \bmod q$

用户B

产生：

随机的X_B <q;

计算：

$Y_B = \alpha^{X_B} \bmod q$

计算：

$K = Y_A^{X_B} \bmod q$

用户A $\xrightarrow{Y_A}$ 用户B

用户B $\xrightarrow{Y_B}$ 用户A

END