志存高远 责任为先

密钥分配

地址：赣州市红旗大道86号 信息工程学院
网址：www.jxust.edu.cn
邮编：341000

目录/Contents

Key Notes

- **topics of cryptographic key management / key distribution are complex**
  - **cryptographic, protocol, & management issues**
- **symmetric schemes require both parties to share a common secret key**
- **public key schemes require parties to acquire valid public keys**

01
Part

对称加密的对称密钥分发

基于对称加密的密钥分配

- **对于对称加密，加密双方必须共享相同的密钥，并且必须保护该密钥不被其他人读取。**
- **为了避免攻击者获知密钥，通常需要经常频繁地进行密钥更改。**
- **密钥分配技术**
  - **向希望交换数据的双方提供密钥的方法，而不允许其他人查看密钥。**

密钥分配

对于双方A和B，有以下选项：

1. 可以通过A选择密钥并将其物理传送到B。
2. 第三方可以选择密钥并将其实际交付给A和B。
3. 如果A和B先前和最近使用过密钥，则一方可以使用旧密钥加密新密钥，将新密钥发送给另一方。
4. 如果A和B各自具有到第三方C的加密连接，则C可以在加密链路上向A和B传递密钥。

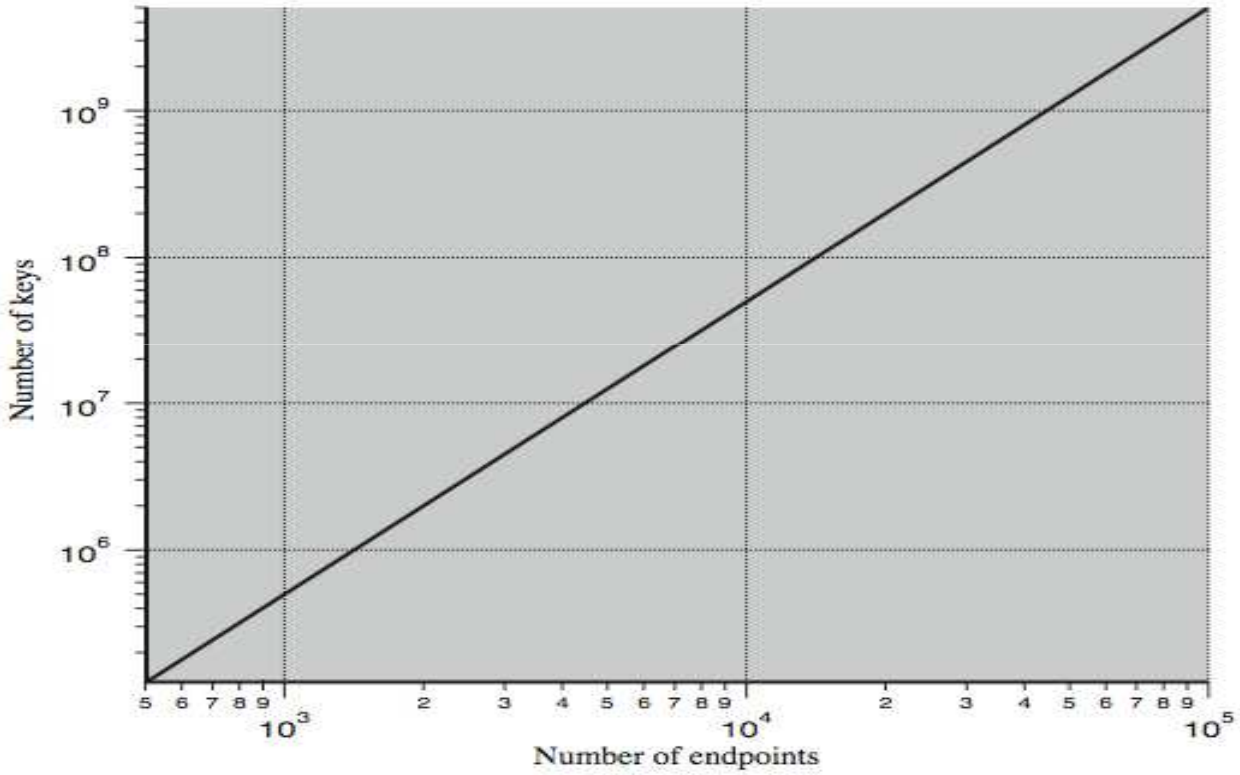
密钥分配

- 第1、2种选择要求手动传递密钥
  - 对于链路层加密是合理的，但对于端到端的加密，手动传递是笨拙的
- 第3种选择对于链路层加密和端到端的加密都是可能的
  - 第1个密钥如何传？
- 为端到端加密提供密钥，第4种选择更可取

密钥分配

- 第4种选择需要一个密钥分发中心（Key Distribution Center, KDC）
- KDC决定哪些系统之间允许相互通信
- 当两个系统被允许建立连接时，KDC就为这条连接提供一个一次性会话密钥

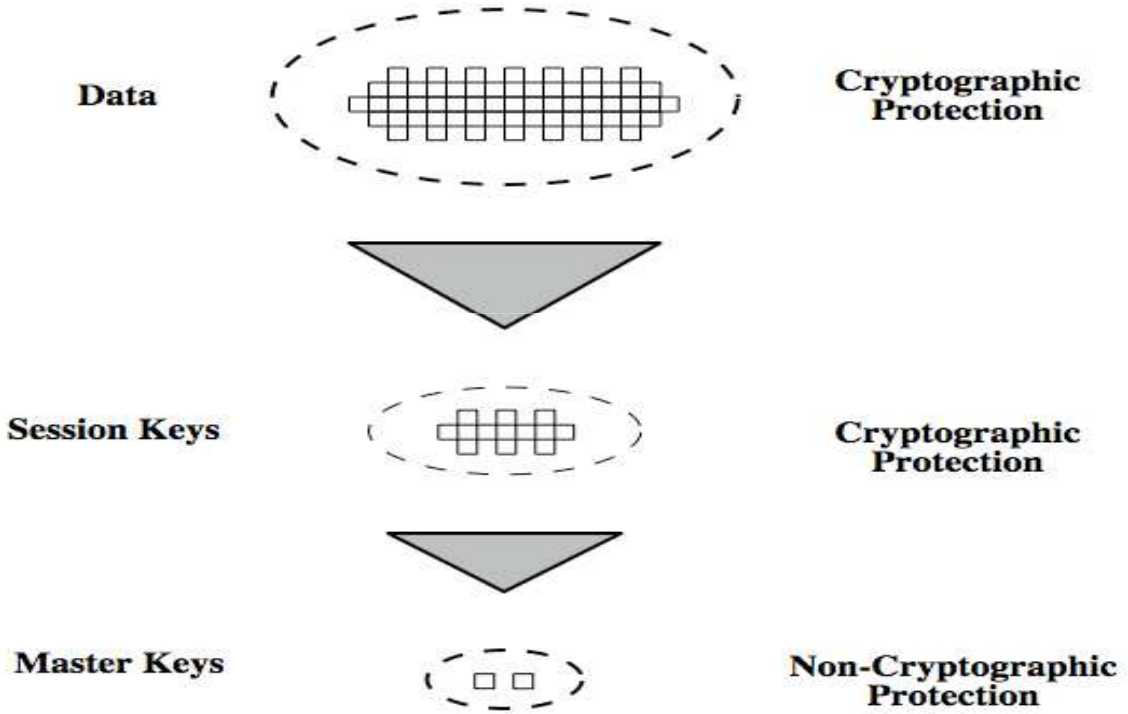
Key Distribution Task



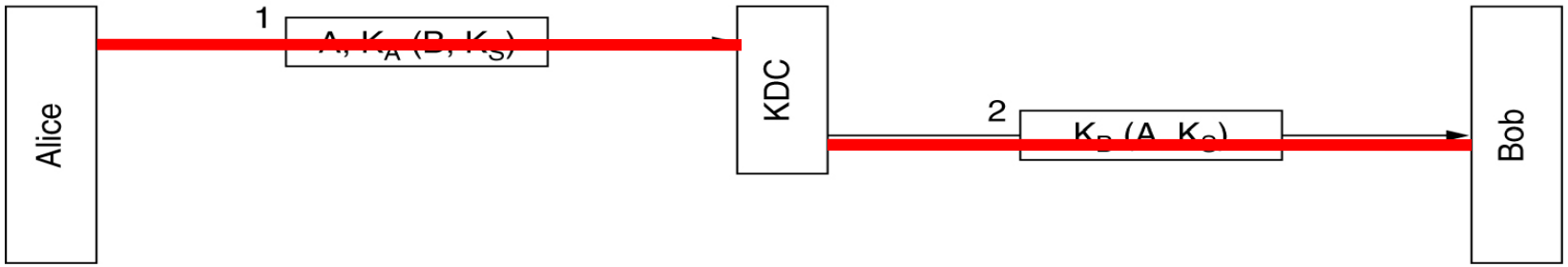
Key Hierarchy

- **第4种选择，需要用到两种类型的密钥：**
  - **会话密钥：当两个端系统（主机、终端等）希望通信，它们建立一条逻辑连接（如虚电路）。在逻辑连接持续中，所有用户数据都使用一个一次性的会话密钥加密。**
  - **永久密钥：用于在实体之间用于分发会话密钥。**

Key Hierarchy



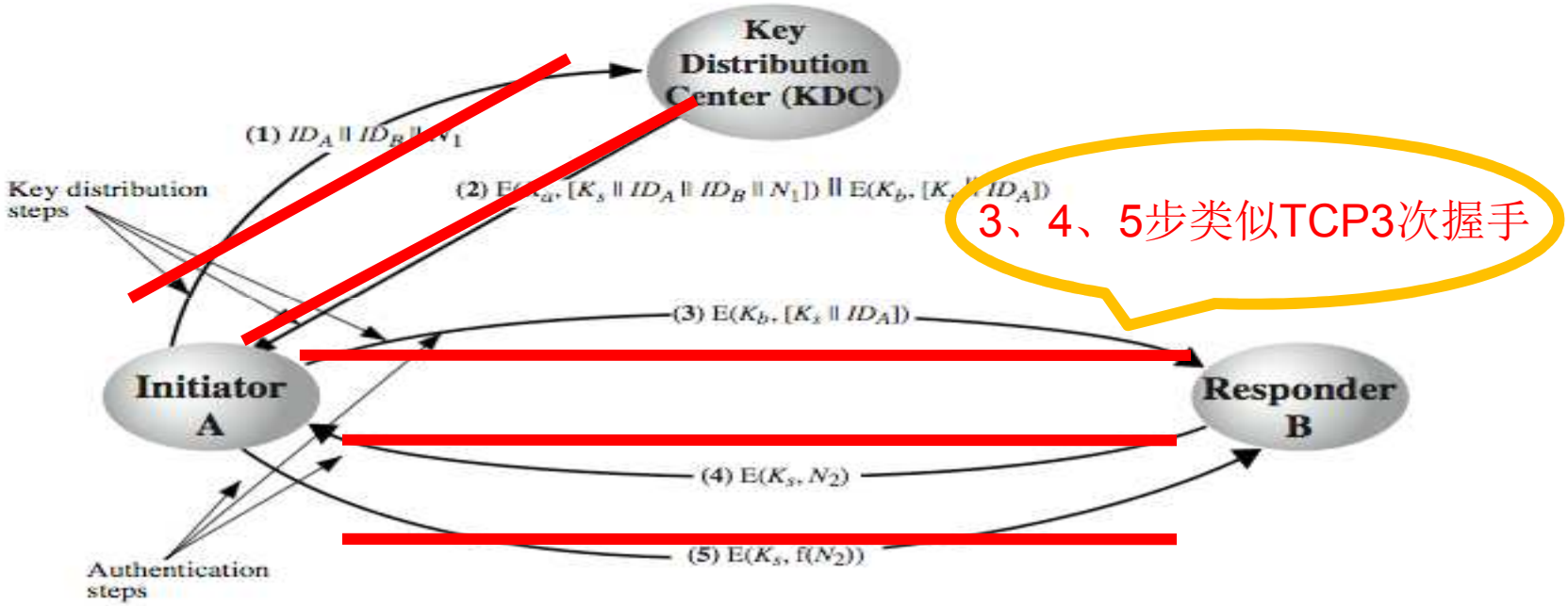
基于对称加密的密钥分配



重放攻击

解决方案：时间戳　临时值　时间戳+临时值

基于对称加密的密钥分配



Key Distribution Issues

- **hierarchies of KDC’ s required for large networks, but must trust each other**
- **session key lifetimes should be limited for greater security**
- **use of automatic key distribution on behalf of users, but must trust system**
- **use of decentralized key distribution**
- **controlling key usage**

02
Part

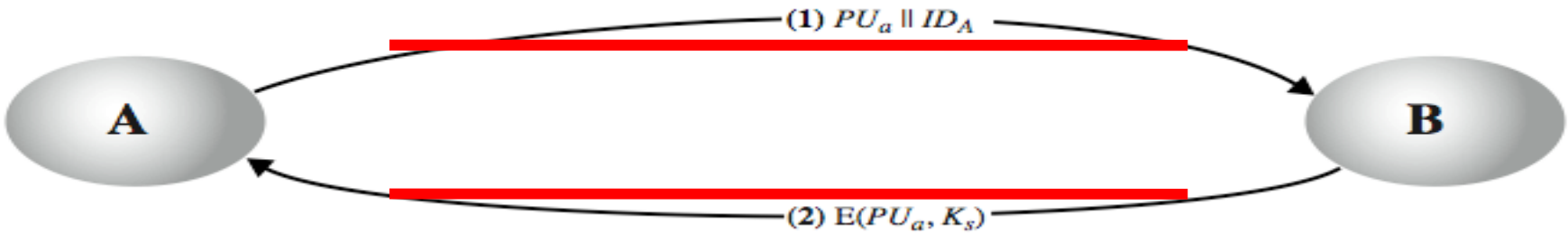
非对称加密的对称密钥分发

Symmetric Key Distribution Using Public Keys

- **public key crypto systems are inefficient**
  - **so almost never use for direct data encryption**
  - **rather use to encrypt secret keys for distribution**
- **使用传统加密时，双方能够安全通信的基本要求是它们能共享密钥**
- **可以使用Diffie-Hellman进行密钥分发，但不能为两个通信者提供认证**

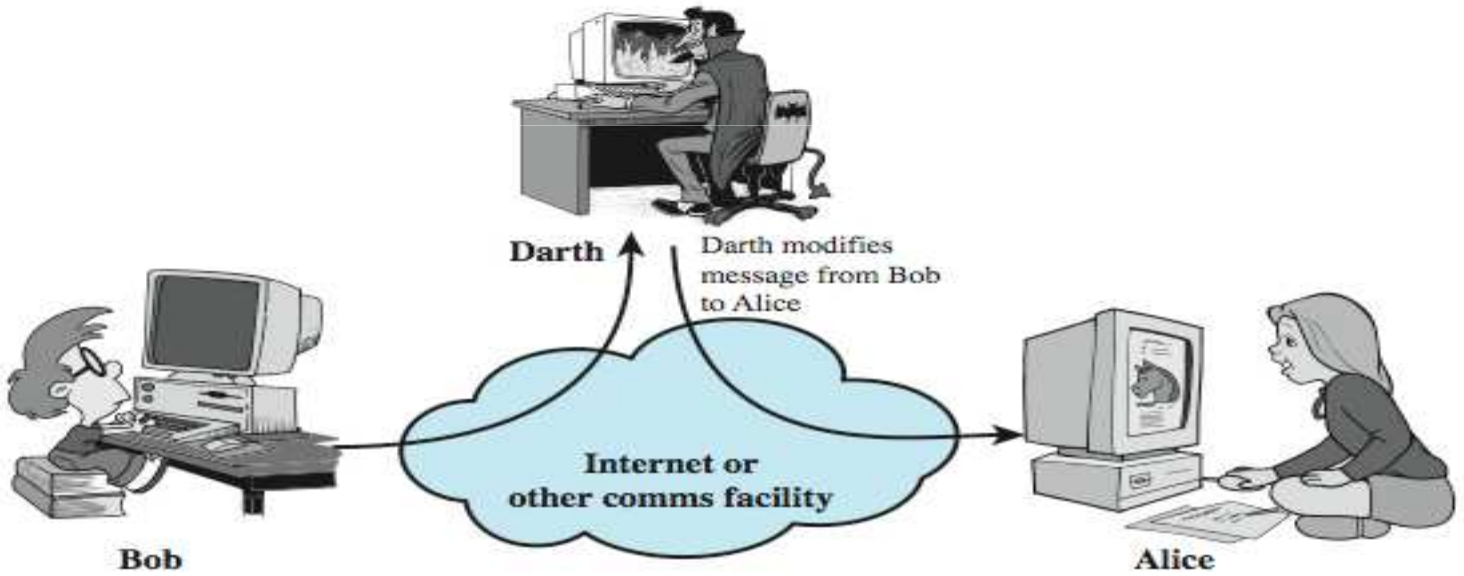
Simple Secret Key Distribution

- **Merkle proposed this very simple scheme**
  - **allows secure communications**
  - **no keys before/after exist**

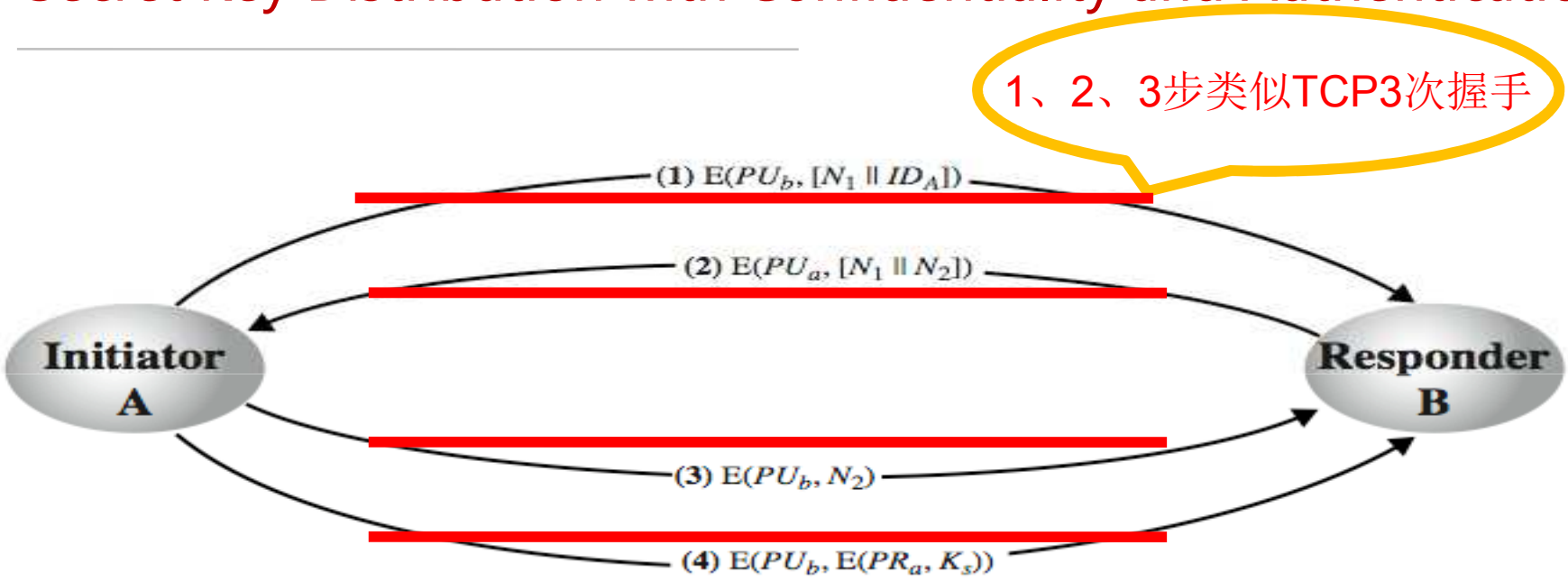


Man-in-the-Middle Attack

- **this very simple scheme is vulnerable to an active man-in-the-middle attack**



Secret Key Distribution with Confidentiality and Authentication



基于公钥密码的秘密密钥的分发

- 当Bob想要与Alice通信时，按以下操作：

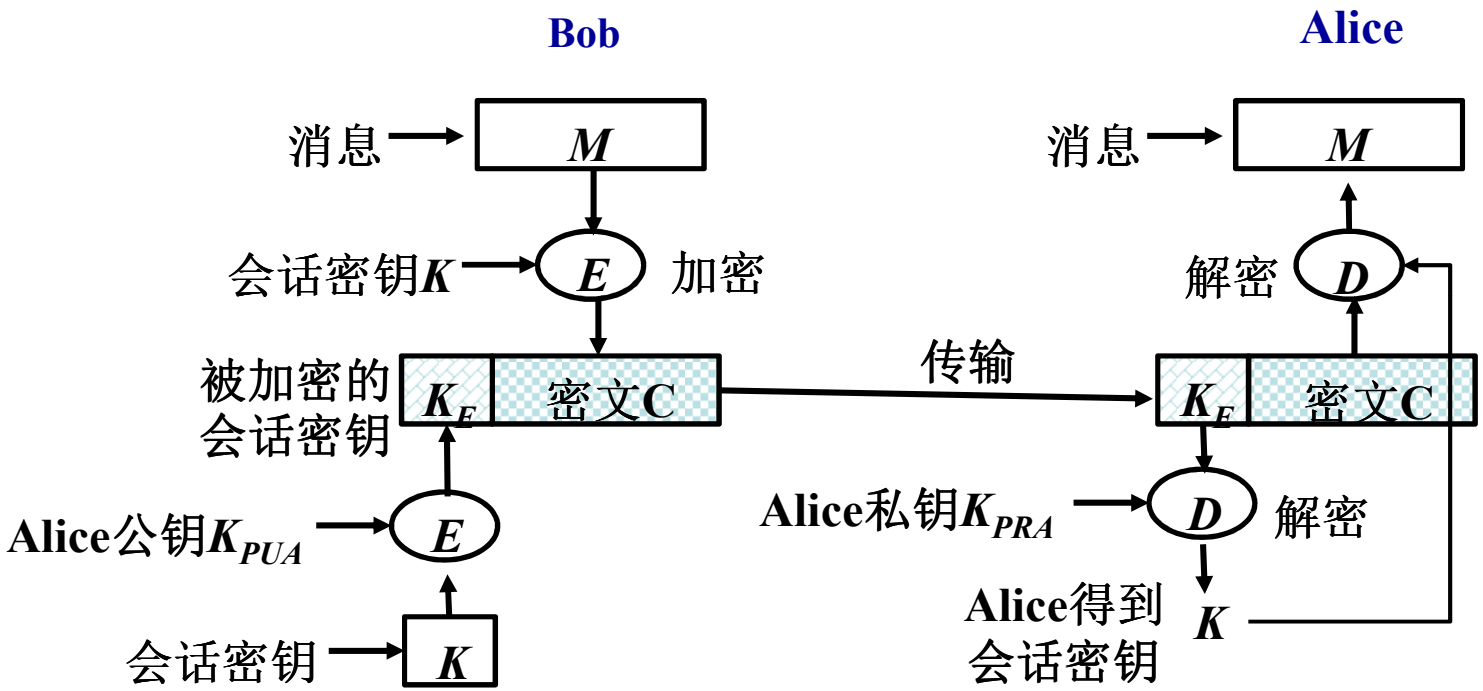
  （1）准备消息；

  （2）利用一次性传统会话密钥加密消息；

  （3）利用Alice的公钥加密会话密钥；

  （4）把加密的会话密钥附在消息上，并且把它发送给Alice。

基于公钥密码的秘密密钥的分发



Hybrid Key Distribution

- retain use of private-key KDC
- shares secret master key with each user
- distributes session key using master key
- public-key used to distribute master keys
  - especially useful with widely distributed users
- rationale
  - performance
  - backward compatibility

03
Part

公钥分发

Distribution of Public Keys

- **can be considered as using one of:**
  - **public announcement**
  - **publicly available directory**
  - **public-key authority**
  - **public-key certificates**

Public Announcement

- **users distribute public keys to recipients or broadcast to community at large**
  - **eg. append PGP keys to email messages or post to news groups or email list**
- **major weakness is forgery**
  - **anyone can create a key claiming to be someone else and broadcast it**
  - **until forgery is discovered can masquerade as claimed user**

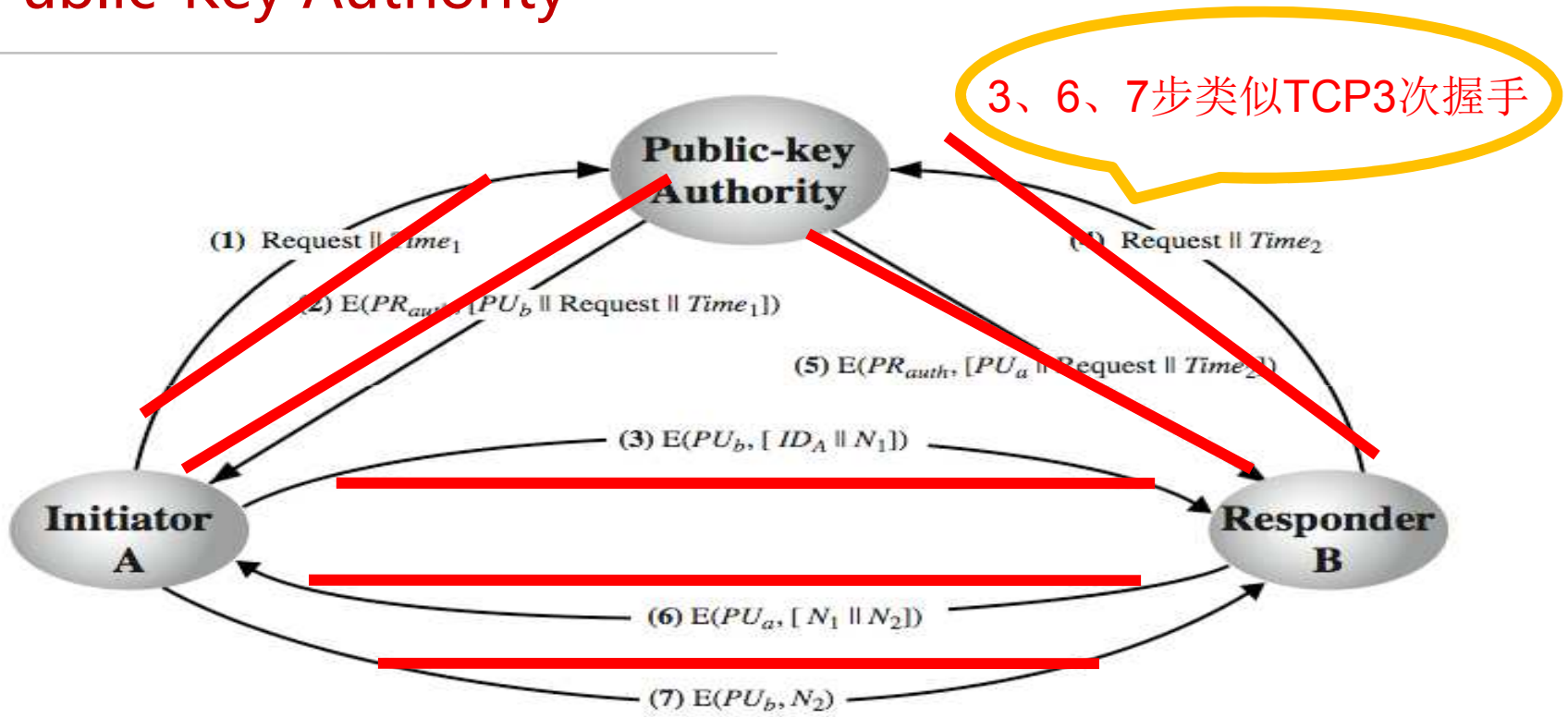
Publicly Available Directory

- can obtain greater security by registering keys with a public directory
- directory must be trusted with properties:
  - contains {name,public-key} entries
  - participants register securely with directory
  - participants can replace key at any time
  - directory is periodically published
  - directory can be accessed electronically
- still vulnerable to tampering or forgery

Public-Key Authority

- improve security by tightening control over distribution of keys from directory
- has properties of directory
- requires users to know public key for the directory
- users interact with directory to obtain any desired public key securely
  - does require real-time access to directory when keys are needed
  - may be vulnerable to tampering

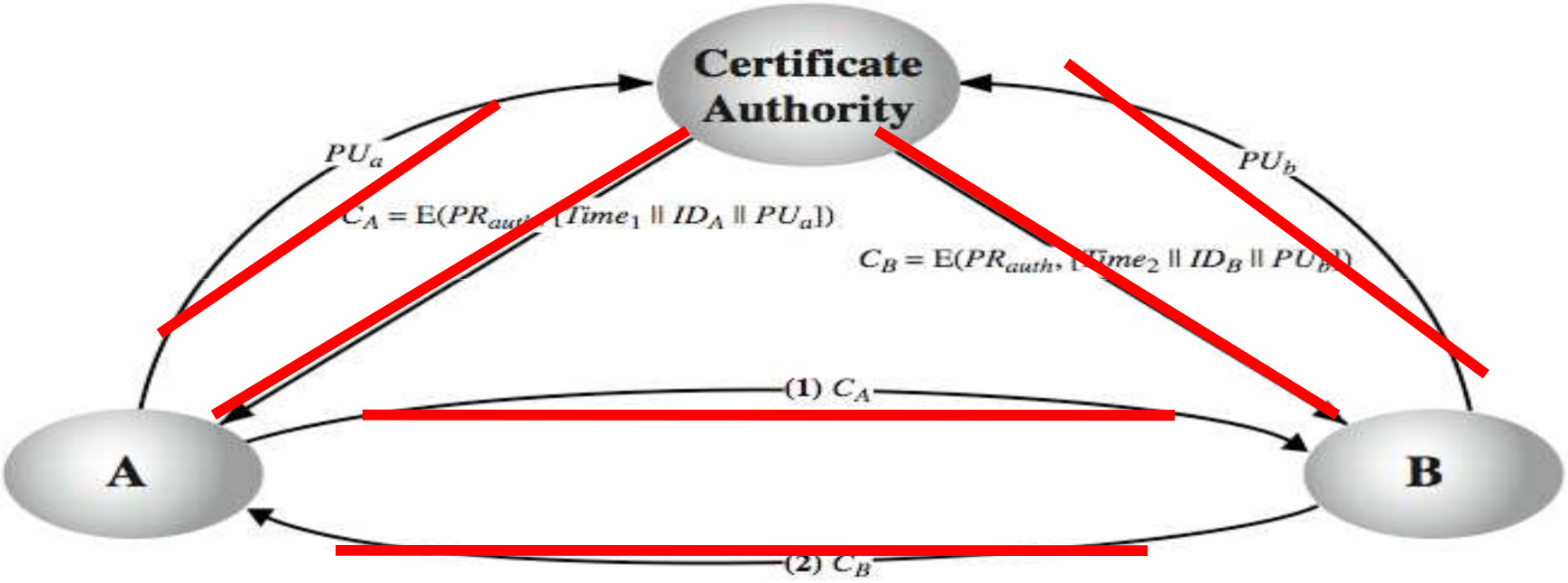
Public-Key Authority



Public-Key Certificates

- **certificates allow key exchange without real-time access to public-key authority**
- **a certificate binds identity to public key**
  - **usually with other info such as period of validity, rights of use etc**
- **with all contents signed by a trusted Public-Key or Certificate Authority (CA)**
- **can be verified by anyone who knows the public-key authorities public-key**

Public-Key Certificates



小结

- **对称加密的对称密钥分发**
- **非对称加密的对称密钥分发**
- **公钥分发**

志存高远 责任为先

感谢聆听

网址：www.jxust. edu.cn
邮编：341000