电子商务安全

华东理工大学计算机系
翟洁

加密算法

数字签名

CA认证

支付协议

加密算法

加密算法：

J(x)	=	F(x)	+	10
密文		明文		密钥

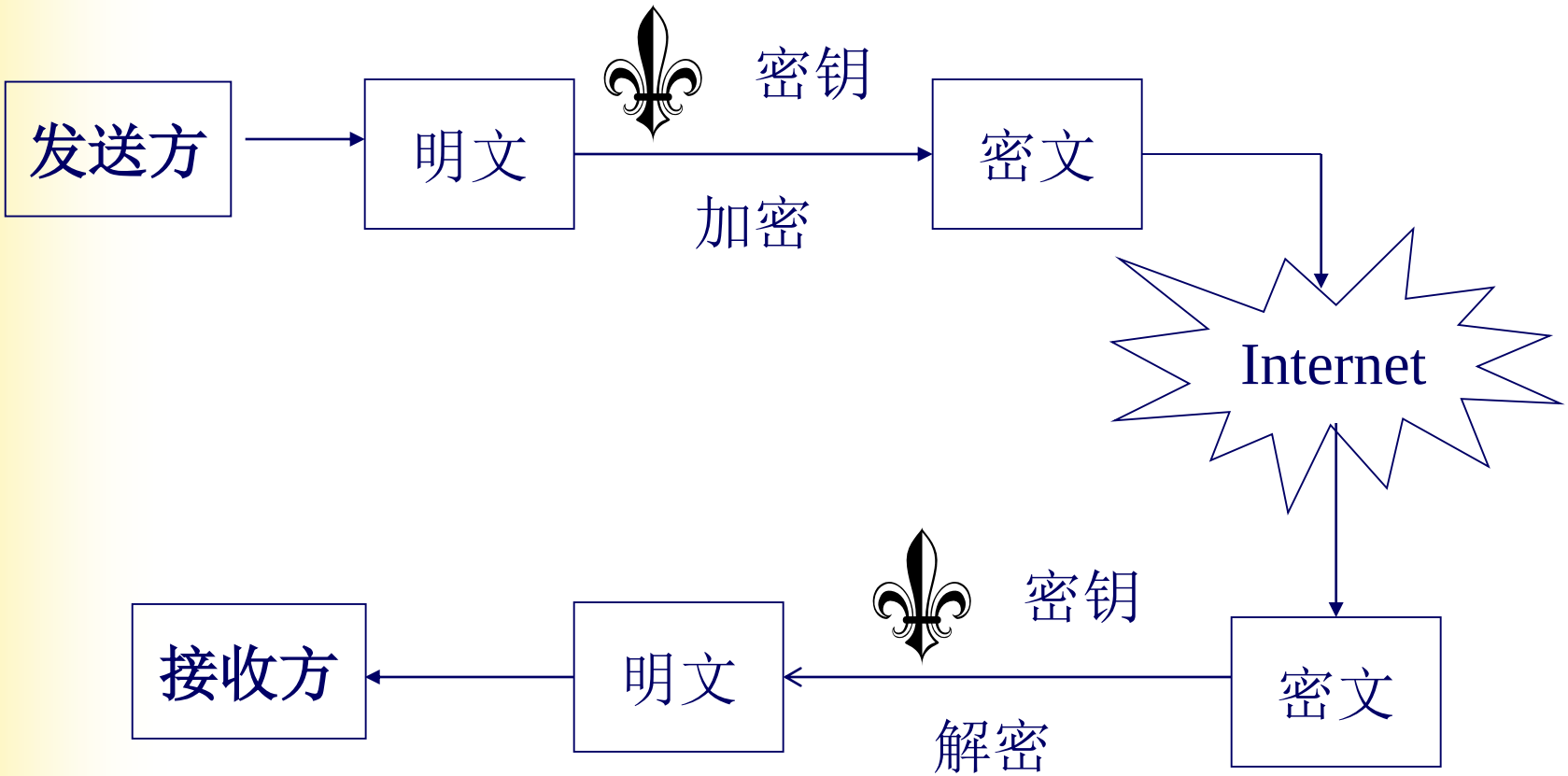
解密算法：

F(x)	=	J(x)	-	10
明文		密文		密钥

加密算法

对称加密体制

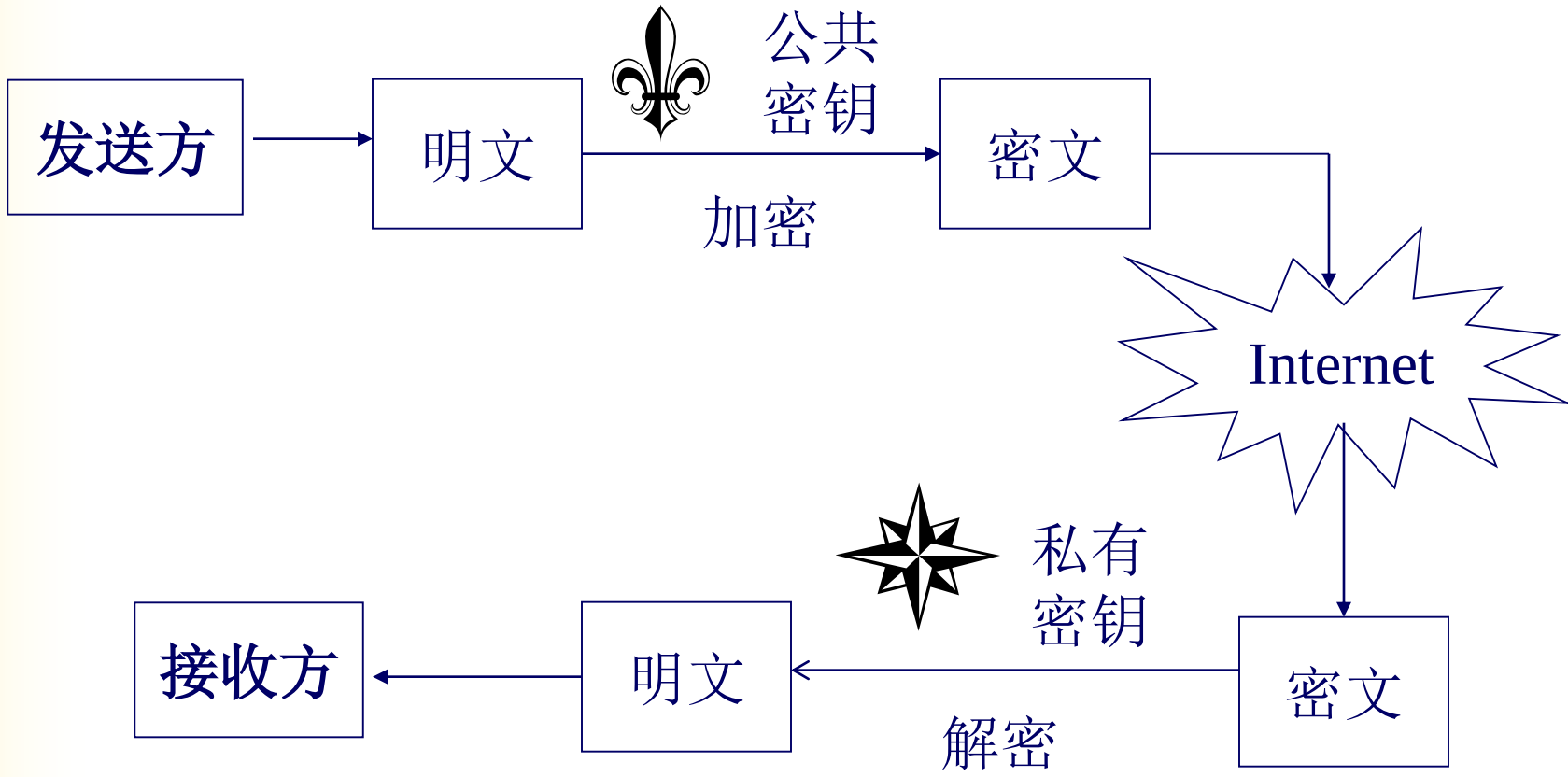
——加密和解密使用同一把密钥



加密算法

不对称加密体制

——加密和解密使用不同的密钥



特点：安全性好，但速度较慢

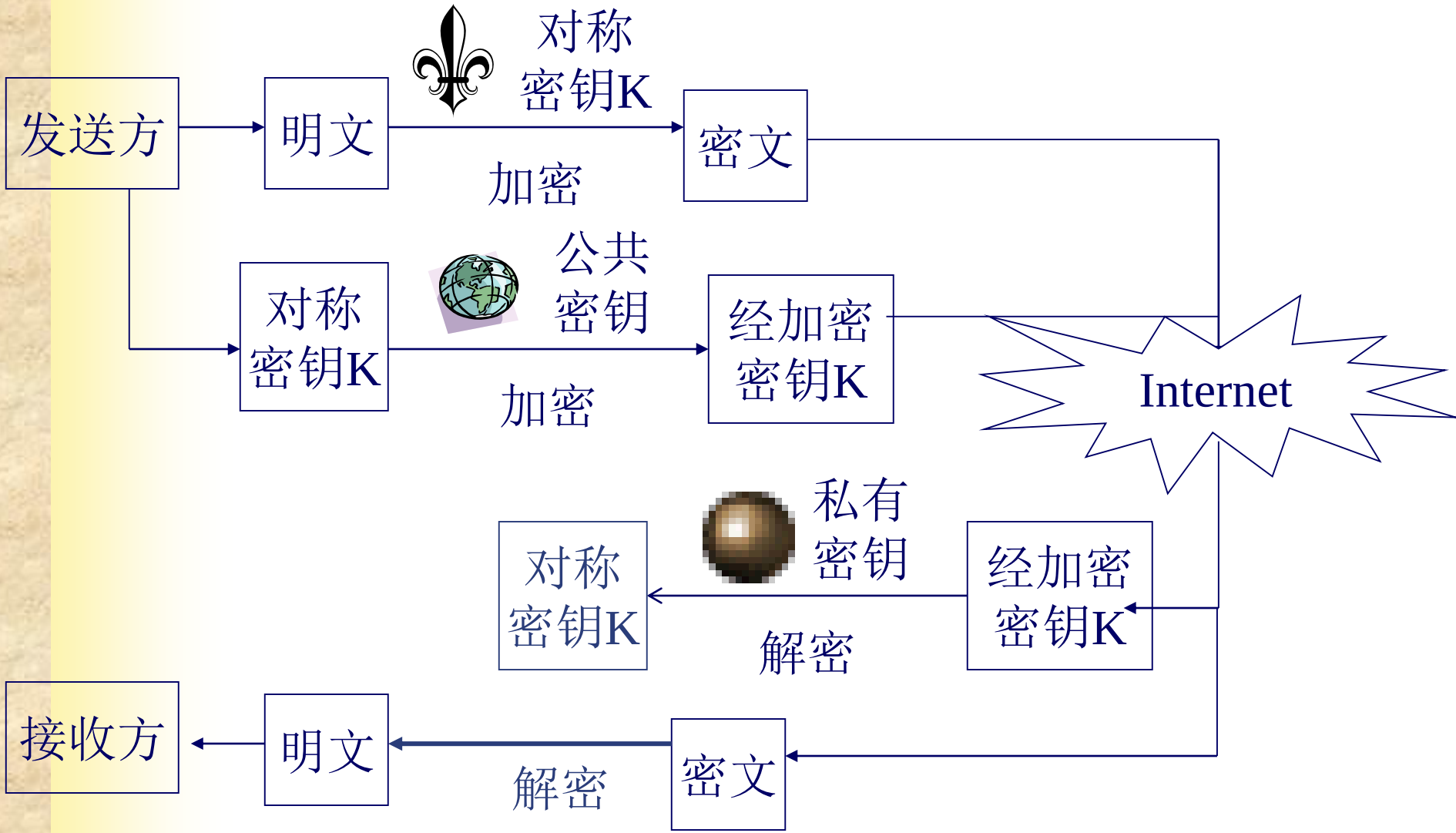
不对称密钥

- 02是原文；128是密文
- $C1 = m1^{e} = 02^{97} = 128 \ (\mathrm{mod}\ 209)$
- （209，97）是公钥

- $M1 = C1^{d} = 128^{13} = 02 \ (\mathrm{mod}\ 209)$
- （209，13）是私钥

加密方法

数字信封：对称加密和不对称加密相结合



每次交换信息都生成一把对称密钥

加密算法

数字签名

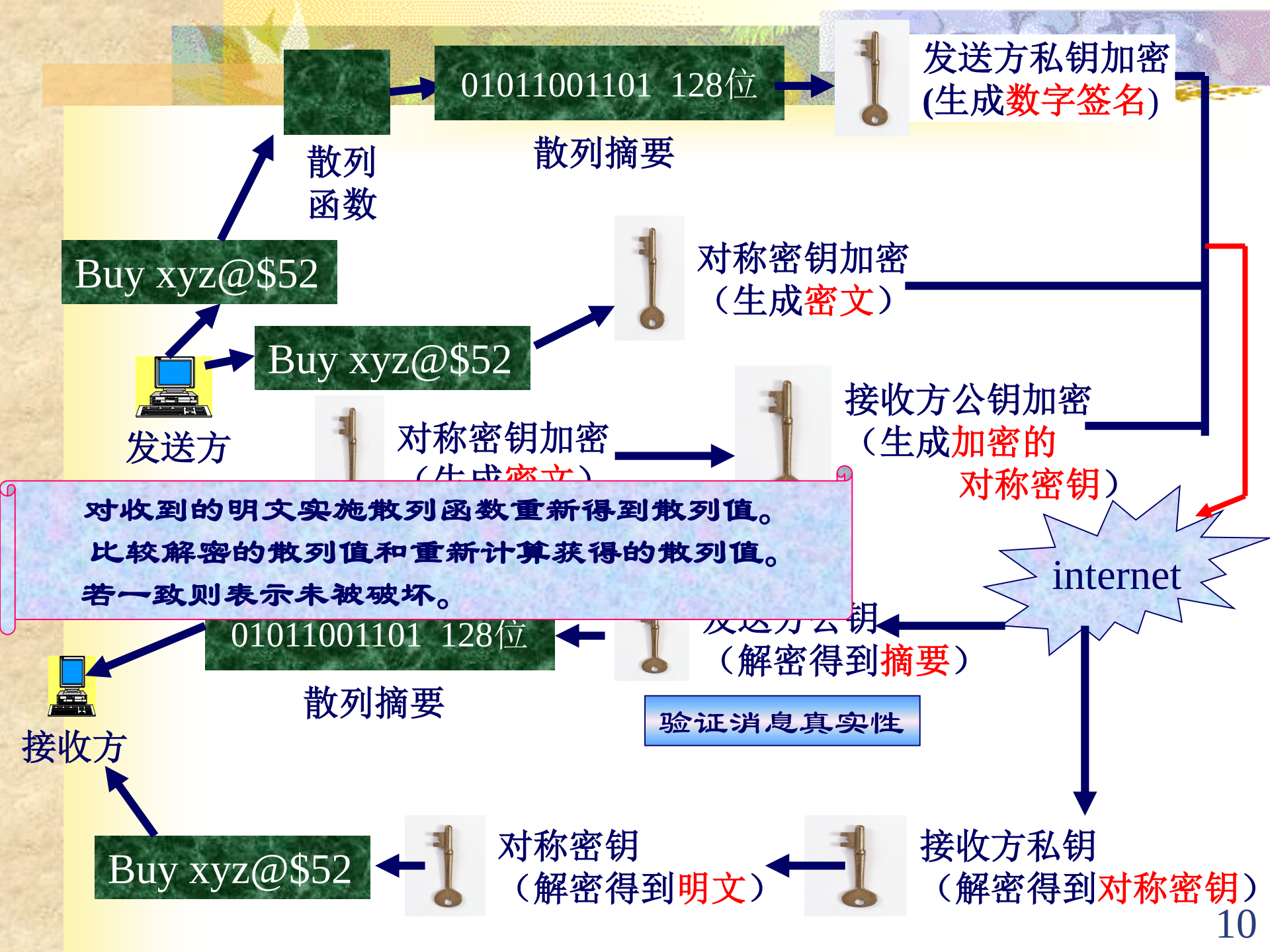
CA认证

支付协议

数字签名

散列函数

——一种可以产生一个称为消息摘要的固定长度数字的算法。


01011001101 128位
发送方私钥加密
(生成数字签名)
散列
函数
散列摘要
Buy xyz@$52
对称密钥加密
（生成密文）
Buy xyz@$52
发送方
对称密钥加密
接收方公钥加密
（生成加密的
对称密钥）
对收到的明文实施散列函数重新得到散列值。
比较解密的散列值和重新计算获得的散列值。
若一致则表示未被破坏。
internet
01011001101 128位
（解密得到摘要）
散列摘要
验证消息真实性
接收方
Buy xyz@$52
对称密钥
（解密得到明文）
接收方私钥
（解密得到对称密钥）

原来的订单

Buy xyz@$52

散列摘要

解密后的订单

Buy xzy@$52

散列摘要

不一致，所以信息的完整性被破坏

加密算法

数字签名

CA认证

支付协议

CA认证

CA中心就是负责验证公钥主体的真实身份以及它与公钥的匹配关系的机构，在完成验证后，为网络用户发放数字证书。

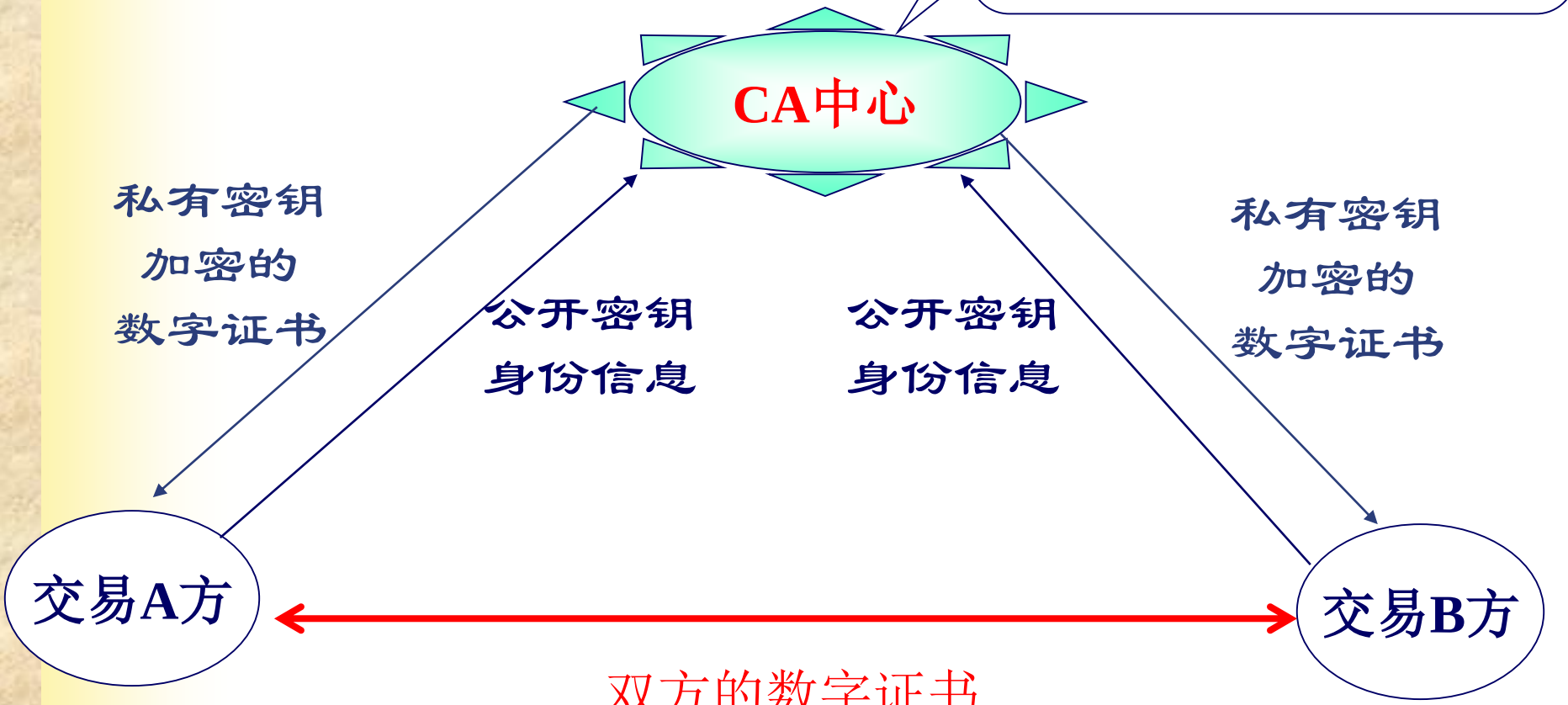
数字证书的内容：

- 证书持有人的身份信息
- 发放证书机构的数字签名和身份信息
- 证书持有人的公开密钥
- 数字证书的有效期
- 数字证书的号码
- ……

CA认证

CA认证的过程

用户私有密钥泄密或证书有效期已到，则作废原有证书

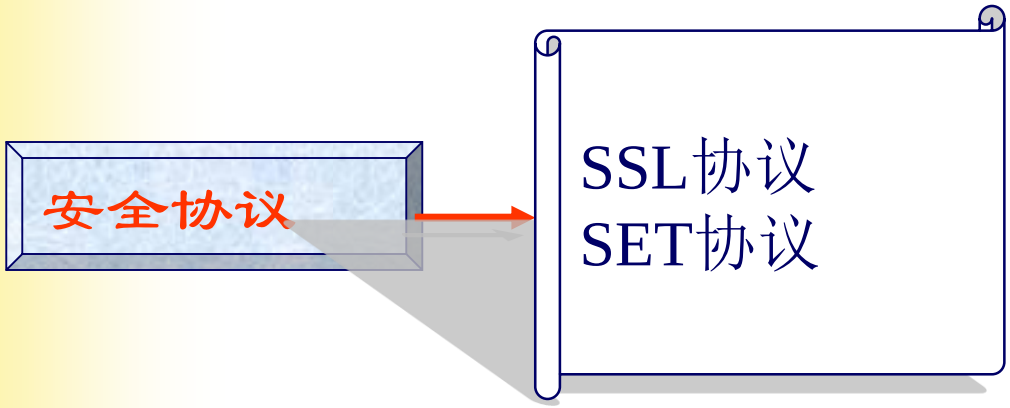


加密算法

数字签名

CA认证

支付协议


安全协议
SSL协议
SET协议

SSL（Secure Sockets Layer）协议

客户
浏览器

商家
服务器

双方的数字证书

安全交易过程

打印交易数据
留作凭证

客户

银行

开始
付货

采购
订单
付款
信息

确认或
付款成功

付款
信息

商家

SSL（Secure Sockets Layer）协议

客户浏览器

服务器

双方的数字证书

对称密钥K

- 无法提供不可否认性保护
- 商家通常将信息以不加密的格式存储

密钥K

加密

密钥K

Internet

私有密钥

对称密钥K

解密

经加密密钥K

服务器

明文

解密

密文

支付协议

SET（Secure Electronic Transaction）协议

双向签名

- 订购指令→商户
- 付款指令→支付网关

缺点：

在银行网络、商家服务器、顾客的PC上安装相应的软件，所以价格昂贵。

通知商家发货

商家

商家的软件转发
加密信息

清算所

商家银行

相互验证身份
SET加密得到的
订单和支付信息发送

清算所向发卡行
审核帐户和余额

发卡行将
款项划拨到
商家银行

消费者

消费者发卡行

选定SET支付

数字钱包、证书

小结

- 加密技术
- 数字签名
- CA认证
- 支付协议

谢谢大家！

华东理工大学计算机系
翟洁