第八讲：电子商务安全性引论

一、电子商务

二、安全电子支付系统

三、电子投票

四、电子拍卖

五、公平交换

一、电子商务

电子商务的概念

Internet 的迅速发展不仅给人们带来了无穷无尽的信息，而且改变了人们的生活方式。在商业领域，基于 Internet 的电子商务向传统的商务模式提出了尖锐的挑战，成为学术界和产业界的热点话题之一，引起了人们的极大兴趣。在21世纪，电子商务将成为人类信息世界的核心与网络经济发展的驱动力，将对人们生活的方方面面，包括经济、政治、文化等领域产生巨大的影响。

利用电子数据交换 (EDI)、电子邮件 (E-mail)、电子资金转账 (EFT) 及 Internet 等主要技术在个人间、企业间和国家间进行的无纸化业务和服务信息（包括商品信息及其订购信息、资金信息及其支付信息、安全及其认证信息等）的交换。

一、电子商务

目前，商务的电子化也发展到一个新的阶段，基于因特网的电子商务（ Electronic Commerce ）阶段。**它是信息社会发展到新阶段的重要标志。**

新的基于 Internet 的商务将可利用世界范围连通的、无中心管理机构、可交互、低成本的 Internet 发展业务。为大、中、小企业，尤其是中、小企业创造了几乎是相同的、平等的机会。网上交易的费用仅是传统商业方式的八分之一。这为电子商务提供了新的发展机遇。

一、电子商务

根据Forrester Research预测：

- 1999年商家之间 (business-to-business) 的交易额将为1998年的两倍多，可达到 1090 亿美元，为商家和消费者之间 (business-to-consumer) 的交易额的6倍；
- 2003年预计可达10 000亿美元。

因特网作为处理商务的主要渠道之一正在全球范围内成为不可避免的趋势。

一、电子商务

电子商务的安全隐患

- 信息安全隐患：交易双方隐私信息的泄漏、丢失、篡改。攻击者通过非法入侵或线路窃听等手段获取交易方的隐私信息，盗用商业机密和资源；线路发生故障，安全措施不当等造成信息丢失；攻击者使用非法手段删除、修改某些重要信息，破坏消息的完整性。
- 信用风险隐患：就消费者来说，在网上购物时可能存在恶意透支消费，重复花费，拖欠货款等行为；就卖方来说，存在出售伪劣产品、短斤少两、拖延发货时间、不公平竞争、重复存储、陷害买方等行为；买卖双方抵赖交易行为。

一、电子商务

- 管理安全隐患：交易中心管理松懈和混乱所造成的安全因患。工作人员职业道德低下、安全意识不高、盗用他人账户、恶意追踪用户、陷害勾结他人。管理混乱为攻击者入侵创造了条件，穷竭系统资源，合法用户得不到正常的服务。
- 法律规范隐患：法制不健全，规范不统一。没有形成一个大家所认可的电子商务运行标准，使得交易混乱，犯罪行为不断，发生纠纷无法仲裁和袒护某方。

二、安全电子支付系统

一般，用户与电子商务的商家或零售商通过一个 HTTP 客户机或 WWW 浏览器软件相互作用。所以，此软件的图形用户接口(GUI) 应当逼真地模仿一个实际商店环境。当用户决定要**在线逛商店**时，一般要访问一个熟悉商店的主页，并选择商品，从一个零售商店购货或寻求服务、商店连接到所选的商家，商家向用户提供主页。主页中可能包括有关商品或服务的信息，可从特定站点购买。用户选择所需的物品，与商家相互作用，并进行必要的支付。相应地，商家要访问客户的银行，对其支付进行适当的认证。若支付合法，商家就通知客户接受其支付，交易即完成。稍后，商家银行从客户银行得到支付，并通知客户有关的转账已完成。

二、安全电子支付系统

经由 Internet 的电子商务一般都特别依赖于已开发并得到广泛使用的**电子支付系统**。这类系统可能涉及几个参与者和支付方法，下面介绍一些支持电子商务的电子支付方法，特别着重介绍**电子货币**、**电子支**票、**信用卡支付**和**微支付**。此外，还有一些其它支付方式，如**现金订货**、**银行支票**、**借贷 (debit) 卡支付**、**购买订货** (Purchase Order) 以及**旅行支票**等。有一些完全不采用密码的电子支付系统，最有名的就是First Virtual Holdings 公司的系统。在此系统中，用户向**First Virtual**提供其身份和信用卡信息进行注册。First Virtual 则签署用户的First Virtual 的惟一身份号给相应的商家。商家则请 First Virtual 交易所证实这个身份号，First Virtual 认可客户的支付。一旦收到认可信息，就采用离线转账。

二、安全电子支付系统

电子支付系统的**核心**是一个 (或几个) **支付协议**。支付协议具有一般性，与所采用的传输媒质无关。事实上，支付协议可以采用 HTTP、使用 SMTP 的 e-mail 代理或使用特定应用协议的其它程序在 WWW 浏览器中实现。无论何种情况，它必须确保在电子支付协议执行中数据的安全。在不安全传输媒质遭到攻击时，攻击者只能得到无用的数据流。

未来可能有多种电子支付系统共存。因而，在相应系统的顶层应必须有一个**协商层**。1995年12月， WWW 财团 (W3C) 和 Commerce Net 财团联合资助 **JEPI** (**联合电子支付发起组织**—Joint Electronic Payment Initiative) 与关键工业界人士一起来保证**多支付、多协议和传输机构**能够在 Internet 上一起工作和**交互作用**。

二、安全电子支付系统

1. 电子货币 (E-money)。 数字 (Digital) 或电子货币提供实际货币的电子等价物。数字货币通过信息网络系统和公共信息平台实现流通、存取、支付。银行发行电子货币，客户可用电子货币从商家购物或服务，这是一种电子支付形式。在电子货币支付中有三方参与：

- 发行电子货币的银行。
- 客户。
- 商家。

客户和商家还可能在其它银行有账号。在这种情况下，这些银行都分别看作是客户的银行或商家的银行。

二、安全电子支付系统

电子货币的优点：数字现金优于纸币之处在于它安全(在生成、递送、存储、认证、交易等过程)、超距、迅速、低成本、匿名性、精确性，这大大强化了现金的可移动性。

- 现钞易被抢劫，必须小心放置和防盗，现钞越多，风险越大，其安全性投资也越大。
- 现钞转运成本高，美国转运现钞费用每年高达 $600亿。
- 高质量彩色复制和伪造技术使政府现钞越来越不安全，制造伪钞已成为经济战中的一个有力武器，可以破坏国家的经济和政府的稳定。信用卡和数字货币(卡)之区别在于后者具有匿名性

二、安全电子支付系统

电子货币支付有三个独立的不同阶段：

- 第一阶段。**客户得到电子货币**。他向银行发出指令，要求从他的账号中转一笔钱到电子货币发行银行。转账后，发行银行将相应数量的电子货币送给客户，客户将其存入他的硬盘或智能卡中。
  第二阶段。**用户用电子货币购物**。他从网上选好商品或服务，并将所需的电子货币传送给商家。商家向客户提供商品或服务。
  第三阶段，**商家将所得到电子货物兑换成实物货币**。将电子货币传送给发行银行。另一种方法是将电子货币传送给他的银行，商家再将其传送给发行银行兑换成实际货币。发行银行则将钱转到商家的银行，并将其转入商家的账号

二、安全电子支付系统

电子货币应满足：

- **通用性**，电子货币应当独立于特定系统的平台或地点。可作为**价值量度**、**流通手段**、**储蓄手段**、**支付手段**和**世界货币**。
- **匿名性** (anonymity)，现金交易不提供可以用于追踪以前持币人的信息。电子货币也应当提供这种匿名性，买主付给卖主，第二者可能不介入具体细节，甚至买主可采用化名签名 (pseudonym system)，卖主也不一定知道他的真实身份，此外对于交易地点亦可保密，中间人可能不知晓，银行也不能分析。因此，电子货币应当可以从一个人转到另一个人，而且不会留下任何有关谁在过去曾拥有这些电子货币的痕迹。但是在这种情况下它还必须保证每个电子货币的拥有者**仅能花一次**，一旦重复使用就能被检测出来。

二、安全电子支付系统

电子货币应满足：

- **找零**，电子货币应象实际货币那样有几种不同的币值且可用某种方法找钱。
- **安全地存储**，如在硬盘和智能卡中。
- **流动性** (liquidity)，数字现金能否被所有代理人接受作为一种支付方式与此关系极大，而数字现金易于在全球网上实现。
- **精确性** (Accuracy)，这对于数字现金不难实现。

二、安全电子支付系统

并非过去已提出的所有电子货币系统都满足这些性质。例如，目前对匿名性仍然有很大争议，因为它可能为非法洗钱或隐蔽的地下匿名电子货币系统提供可能性，这是人们所不希望的事。这就引向开发**公平匿名电子货币系统**，其中客户的匿名可以在一定条件下披露。

匿名电子货币的机制。1982年 David Chaum 开发了一种建立 RSA 签字和发行匿名电子货币的机制。

体制参数：令 d 是电子货币银行的 RSA 的秘密钥，(n, e)是公钥(用于对特定数字硬币如一美元进行签字)。此时，n是模，e 和 d 分别为互逆运算的指数，对所有 x，成立。

二、安全电子支付系统

- **数字硬币生成：**客户先对数字硬币生成一串数m、随机数r，r作为盲因子。而后计算$x = mr^e (\mathrm{mod}\, n)$ 并将y回送给客户。同时，银行从客户的账上减掉相应的钱数(我们讨论的情况下为1美元)。显然，如果客户从银行中他的账号取钱时，也要进行类似的操作。客户以r除y，就得到银行对数字硬币序列数m的签字z：

$$z = \frac{y}{r} \equiv \frac{x^d}{r} \equiv \frac{\big(m(r^e)\big)d}{r} = \frac{m^d r^{ed}}{r}$$

$$\equiv m^d r/r \equiv m^d (\mathrm{mod}\, n)$$

- **数字硬币支付：**客户用数字硬币$(m,\ z)$从能接受电子货币的商家购买商品或服务。而后商家可以用相应公钥(n, e)对银行对硬币的签字z进行证实。

二、安全电子支付系统

实用系统:

(1) Chaum 建了 DigiCash 公司 [http://WWW.digicash.com]，将匿名电子货币体制用 **Ecash** 名字推向市场。1995年10月，Missouri St.Louis的 Mark Twain 银行成为首家通过 Internet 提供 Ecash 业务的银行。在Mark Twain 银行之后，同时又有几个银行，例如德国的 Deutsche 银行也开发使用 Ecash。

在 Ecash 系统，数字硬币存在客户的系统中，可以用通行字导出的密钥对数字硬币进行加密，另一种可能是采用智能卡。无论哪种情况，客户都必须将数字硬币通过 Internet 传给商家。在接受硬币之前，商家必须用发行银行相应的公钥检验它的真实性和完整性，并与此银行在线证实此硬币是否已被用过。硬币只能花一次，银行要记录所有的序列号、识别并拒绝第二次使用的硬币。

二、安全电子支付系统

(2) 除了 Ecash 外，**CAFÉ** (Conditional Access for Europe)计划也已开始探索匿名电子货币的思想。此计划假定在线检验硬币不一定总是可行的，脱机系统为电子货币经 Internet 广泛使用提供了一个更好的途径。但是，对脱机系统会立即提出的问题是重复花的问题。如何能避免一个数字硬币被使用了两次？应当指出，脱机模式下，商家没有可能和发行银行核实硬币。一般有两种途径处理这个问题：

第一种途径是采用某种巧妙的数学来保证可以揭露将数字硬币花两次的拥有者的身份。此情况下，硬币的拥有者在支付过程中要提供其识别特征的部分信息，但不给出更多有关身份的信息。只有当与另一部分识别特征信息进行组合时才能披露拥有者的身份

- 第二种途径采用专用硬件存储硬币，并保证数字硬币仅仅能花一次。称这类硬件为**电子钱包**或**观察者** (Observer)

CAFE计划采用特别设计的电子钱包按第二种途径实现

二、安全电子支付系统

(3) Mondex 是另一种以硬件支持的脱机匿名 e-cash 系统。它主要在英国开发。 NetCast 提供一种称作**弱匿名**的 e-cash 系统，是研发原型设计。弱匿名就是若客户将 NetCash 传送给商家，靠商家自己无法决定客户的身份(除非客户通过其它方式泄露)。但是，若商家和计账服务器串通，就可一起确定出客户的身份。 NetCash 系统由南加州大学信息科学研究所研发。 Net Cash 采用 NetCheque 系统去清理现金服务器之间的支付。

二、安全电子支付系统

其他电子货币方案：

- NetCash，North California University, Information Sciences Institute
- CyberCoin，CyberCash Inc., USA 1996.12。
- EMV cash cards，即欧洲发卡银行集团 Euopay 和 MasterCard 及 VISA, 1996.6。
- Server Wallet，GlobeSet。
- Passport，Microsoft。

二、安全电子支付系统

2. 电子支票

在现实世界中已广泛采用支票(至少在美国)，电子支票也可作为电子商务的一种重要支付方案。简单地说，客户商家提供一个电子支票，商家则在银行兑换为钱。因而电子支票系统可包括下述几个部分。

客户和客户的银行；

商家和商家的银行；

交易所，在不同银行之间处理支票。

二、安全电子支付系统

电子支票交易的3个阶段的一些基本步骤：

第 1 阶段，客户购买商品或服务。向商家送一个电子支票。而后商家和他的银行为了对支票进行适当支付授权需要验证支票的合法性。若支票合法，商家就和客户完成这笔交易。

第 2 阶段，为了**兑现**商家将支票送给他的银行。商家要谨慎地采取这个行动。

第 3 阶段，商家的银行将支票送给交易所**兑换为现金**。交易所则与客户的银行合作，对支票清账，并将钱转到商家的银行，商家银行相应更新商家的账目。客户的银行也要根据提款信息更新客户的账目。

二、安全电子支付系统

从技术上看，电子支票是相当简单的。一个电子支票就是由客户用其秘密钥签署的一份文件，接收者 (商家或商家的银行) 或用客户相应的公钥证实此数字签字。

电子支票的优点：

- 无须填写就能发出，商家将电子支票收集起来并送给商家的银行。利用电子支票商家可以立即将支票送给银行，并将得到的钱计入他的账上。这样，电子支票可以大大降低处理时间。
- 电子支票系统也可设计成在接受支票之前可以从客户银行得到适当的授权。这与出纳员 (Cashier) 支票方法很类似。

二、安全电子支付系统

3. 信用卡支付

最近，电子信用卡支付系统已成为 Internet 用户和客户所选择的支付系统。这些系统必须提供一些安全性要求。例如，机制必须能提供对各参与方的**认证**，如**客户**、**商家**和参与的**各银行**。另一个机制必须能提供对信用卡和 Internet 中传送的**支付信息的保护**。最后，过程必须制定解决信用卡支付中各参与方之间的**纠纷**。已有几种电子信用卡支付方案设计能满足这些要求。大多数方案都有一些附加优点。例如，在某些方案中可以不向商家泄露信用卡信息。因而，电子信用卡支付系统可以提供比传统信用卡支付系统更高的安全性。

二、安全电子支付系统

一个电子信用卡支付方案可以设计得使商家能几乎瞬间可从信用卡得到对商品的支付。传统信用卡方案商家需要将信用卡收据递送给银行，银行再处理这些支付，一般要用很多时间。

安全电子信用卡支付的五个参与方：

- 持信用卡者。
- 商家。
- 商家的银行。
- 证书管理中心 (CMC) 。
- 信用卡发行银行。

二、安全电子支付系统

持卡人用他的信用卡从商家购买商品或服务。商家和他的银行，称作商家银行交互作用。这类银行也称作**获得者** (Acquirer) 或**获得者银行**。在电子信用卡支付方案中，获得者一般看作是一个金融机构，它有商家的账号并处理信用卡授权和相应的支付。在这种安排下，获得者运行一个支付网关以处理商家的支付消息。任何安全电子信用卡支付方案都有一个非常重要的参与者，它是**证书管理中心** (CMC) ，提供**公钥基础设施** (PKI) 业务，并向各参与者发放公钥证书。此外，一个电子信用卡支付方案还包括**两个网络：公共网** (典型的是 Internet) 和**专用网**，专用网由银行界拥有和运行(因而又称为**银行网**，Banknet) 基本上假定经由银行网的通信有足够高的安全性，而经由Internet的通信是不安全的，必须采用密码进行保护。因此，电子信用卡支付协议主要集中于经过 Internet 的通信，不涉及通过银行网的通信。

二、安全电子支付系统

电子信用卡支付交易的3个主要阶段：

- **第1阶段**，客户通过商家所提供信息进行浏览并购买某些商品或服务。他提供信用卡进行支付，商家访问获得者得到对客户的信用卡授权和购物的钱数。一般仅当钱数超过某个设定的门限值时才要求这种授权。此情况下，获得者完成这一授权并通知商家是否进行交易。最后，商家通知客户是否已处理这笔交易。
- **第2阶段**，商家访问获取者并向它提供各种电子信用卡售货收据。获取者访问信用卡发行银行，代表商家得到售货款。
- **第3阶段**，信用卡发行银行更新信用卡持卡人的账目，将他购货款转出给商家的银行。客户每月可以从邮局或安全电子邮递收到有关的更新的账目。

二、安全电子支付系统

4. 微支付

评价一个支付系统的重要因素是为处理支付所需的**开销**在整个支付额中所占的比例。除了这个开销外，还要支出实现一个支付方案的额外花费，此外银行还要收取一定的服务费。当一个账户或信用卡被接纳时，这些银行服务或交易费可能要收费，在实现支付方案整个费用中可能占很大比例。在微支付系统中，其总的支付一般不超过几分钱，交易的开销至多仅以厘计算。设计有效微支付系统仍是一个有待研究的问题。其基本想法是用密钥控制的单向杂凑函数来代替公钥密码。这种代换的主要优点是有效性高，其主要缺点完全不能提供不可否认业务。注意，密钥控制的单向杂凑函数不能计算和证实数字签字，而签字主要是能提供不可否认性，然而，由于微支付一般不会超过几分钱，商家可以承受个别客户稍后拒绝支付的风险。

二、安全电子支付系统

- **SubScript**，由澳大利亚 Newcastle 大学 Furche, A.和 Wrightson, G.于1996年提出，为 Internet 上按每次阅读或观看付款的有效预支付系统。
- **Millicent**，由 Digital Equipment Corporation1995 开发，可精确到$0.001。
- **PayWord** 和 **Micro Mint**，由 Revist, R.和 Shamir, A.于1996设计的微支付系统，采用公钥密码体制。
- **iPK 微支付协议**，Bellare, M.等1996年提出。
- **MicroMint**，由 Revist, R.和 Shamir, A.于1996设计的微支付系统，不采用公钥密码。
- **NetBill**，Carnegie Mellon大学。
- **CyberCoin**，CyberCash公司。

三、电子投票

与传统的选举方式相比较，电子投票一个显著的优点是投票者无须到一个指定的投票箱投票。随着Internet的迅速发展，电子投票已成为电子商务的一个主要内容，许多学者对其作了大量的研究，而且Cranor 等人最近设计并实现了一个适用于Internet 投票协议 Sensus。按选票发送的方式电子投票可分为两种：一种是投票者以加密的形式发送选票，另一种是投票者通过匿名的通讯信道发送选票。

三、电子投票

电子投票一般包括以下的参与者：投票者，管理机构，计票机构。一般还假定协议中还有一个可信赖的注册机构。假定只有在必要的时候才追踪投票者（比如不诚实的投票者提交无效的选票，或只注册而不投票）。投票者和计票机构通过一个匿名的通讯信道交换信息。

三、电子投票

安全的投票方案的性质：

- **秘密性：**除了投票者外，选票的内容不能被其他人知道。
- **公平性：**在选举的中间过程，任何人的行为都无法影响选举的结果。
- **匿名性：**任何人都无法将一张选票和某一投票者联系起来。
- **唯一性：**只有有资格的人能提交一张合法的选票，冒充他人选举则一定能被追踪到。
- **完整性：**所有合法的选票都能被正确计入。
- **稳固性：**不诚实的投票者不能破坏选举。
- **可验证性：**选举的结果可以被检验，任何人无法伪造选举结果。狭义的可验证性保证合法的选票被计入，而广义的可验证性可以使任何感兴趣的第三方参与检验，同时不泄露投票者的隐私。

四、电子拍卖

拍卖是一种特殊的现货交易方式，一个由拍卖群体决定价格及分配的过程。一般情况下，拍卖企业接受委托，在规定的时间和地点，按照一定的规则和程序，由拍卖师主持，买方、卖方之间产生一个合理的参与各方都认可的价格，最后把商品卖给出价最高的竞买者。现在，各种拍卖行、拍卖代理系统如 eBay，Amazon.com 已相继成立。随着科技的发展和保密系统的完善，人们必将进入一个完全崭新的网上交易时代。

四、电子拍卖

拍卖的分类

- 按拍卖叫价的方式分为：价格递增拍卖 (英式拍卖)，价格递减拍卖 (荷式拍卖)。英式拍卖及荷式拍卖的优点是尽可能的使商品以真实的最高价出售。然而，英式拍卖有许多缺点：拍卖时间与最终的出售价成正比；通信时间随最终出售价的增加而呈超线形的增加。荷式拍卖也存在通信时间过长，效率过低的缺点。
- 按标价的是否公开分为：公开标价拍卖及密封式标价拍卖。在电子拍卖中，一般使用密封式标价拍卖。它的优点是可以在单轮通信中完成，拍卖效率高。然而，拍卖行一般会知道各投标者的出价，而且不支持商品最优分配。
- 按拍卖进行的轮数可分为：单轮拍卖 (如密封式标价拍卖) 与多轮拍卖 (如英式拍卖，荷式拍卖)。我们期望能实现一个真正意义上的单轮拍卖以减少拍卖的通讯费用及提高拍卖效率，但实际上一般不能在一轮中完成拍卖。

四、电子拍卖

- 按获胜价位可分为：第一价位 (最高价位) 拍卖 (英式拍卖、荷式拍卖) 和第二价位拍卖。经济学家 Vickrey 结合了英式拍卖与密封式标价拍卖的优点，设计出一种新的拍卖方式--第二价位拍卖。象密封式标价拍卖一样，投标者将标价送给拍卖行，第一价位中标，但中标者只付出第二价位的价格。第二价位原理支持商品分配最优化，Vickrey 因此获得1996年Nobel经济学奖。这种拍卖方式通讯时间固定，并且使投标者尽可能的以真实的最高价投标，但是它仍不保持标价的匿名性。许多学者对 Vickrey 拍卖的性质进行了研究，如何在不暴露投标者的标价的前提下求出第二价位以及尽可能的减少拍卖的通讯时间及费用是一个困难问题。

四、电子拍卖

- 按投标次数可分为：单标价拍卖和多标价拍卖。单标价拍卖投标者只进行一次投标，通讯时间少，效率高。然而风险也高。多标价拍卖进行实时考虑，风险低，但通讯时间长。
- 按拍卖成交的次数可分为：单级拍卖和分级拍卖。在某些情况下，有必要先进行子拍卖，子拍卖的胜者进入下一级拍卖。

四、电子拍卖

理想的拍卖应具有的性质：

- 标价的秘密性：拍卖行在收到所有的合法标价之前无法知道投标者的标价。最理想的情况是在拍卖结束后只有中标者的价位公开（第二价位的拍卖只公开第二价位）。
- 不可否认性：中标者中标后不能反悔，必须支付与获胜标价相等数量的货币。卖者将标的（货物）给中标者。
- 投标者身份的秘密性：投标者的身份在拍卖期间不能泄露。在拍卖结束后，只有中标者的身份泄露（现在进一步研究如何保护中标者的身份）；在第二价位拍卖中，即使计算出第二价位，该价位的投标者的身份也不能泄露。
- 高效实用性：拍卖时间及通讯费用少，拍卖效率高。
- 第二价位原则：拍卖最好达到商品最优分配。
- 公平性：每次拍卖有唯一的中标者，最高价位者中标。

五、公平交换

电子商务是基于 Internet 的双方或多方之间进行的有形商品或无形服务的交换。交换一个很基本的要求就是交换双方的公平性。

假如 Alice 想在 Bob 公司购买一张机票。Alice 首先发出一个预定请求， Bob 公司确认后向 Alice 发出一个通知。如果 Alice 和 Bob 公司不能相互信任，那么将存在以下的问题： Alice 发出了预定请求，但后来没有购买机票，Bob 公司就没有卖出机票而受损；另一方面，Bob 公司虽然收到了预定请求，然而将机票卖给了别人，则 Alice 就无法登机。所以，只有一方诚实的执行协议，无法保证双方的利益不受损失。

五、公平交换

公平的定义：

当一个系统涉及到多个互不信任的主体，一个很自然的问题就是满足所有主体的安全性。从主体利益的角度考虑，如果一个系统不会损害一个诚实主体的利益，那么该系统具有公平性。从交换的结果考虑，如果在交换结束后，要么每一方都得到了他所期待的物品（或服务），要么每一方都没有得到任何有意义的东西。此时，我们认为该系统具有公平性。

五、公平交换

分类：

- 按第三方是否参与可分为：无第三方参与的公平交换，交换双方通过逐步的交换秘密（“同时”交换不可否认的tokens）来达到交换的公平性；第三方在线参与的公平交换，第三方参与交换的每一轮协议；最优公平交换，第三方只是在发生纠纷时参与协议。
- 按交换方的数目可分为：双方公平交换与多方公平交换。
- 按交换物品的种类可分为：机密数据交换，公开数据的交换，支付的交换。机密数据指的是在交换前数据不公开，然而在交换协议完成时公开的数据，如数字化产品或消息等。公开数据指的是即使协议没有成功，交换双方也知道的数据，如数字合同。而支付是指将一笔“价值”(value) 从支付方发给接收方。

五、公平交换

基本要求：

- 有效性 (effectiveness)：如果 Alice 诚实的执行协议，而且她和 Bob 都没有中止协议，那么在协议结束后， Bob 就可以得到他所期待的物品。
- 秘密性 (privacy)：交换必须保护用户的秘密隐私信息。
- 不可否认性 (non-repudiation)：在进行有效的交换后，交换的任何一方都不能对他所传递和收到的信息进行否认。
- 高效实用性 (efficiency)： 协议的效率要高，以保证实用。
- 公平性 (fairness)：如果在交换结束后，要么每一方都得到了他所期待的物品（或服务），要么每一方都没有得到任何有意义的东西。

五、公平交换

- 时限性 (timeless)：协议必须保证在某一时刻中止。协议结束时，无论交换处于何种状态，都不能影响协议的公平性。
- 第三方可验证性 (verifiability)：发生纠纷时第三方可进行仲裁，对不诚实的一方可进行制裁。同时，如果第三方不诚实使得该协议对Alice不公平，则Alice可向仲裁者 (arbiter) 证明第三方的不公正行为。
- 无滥用性 (abuse-free)：在多方公平交换模型中，参与交换的任一子集在协议的任何时刻，都无法向第三者证明他们有能力中止（或完成）协议。

考试：论文

- 2000-4000字；
- 页面要求：A4纸，手写，或打印；
- 题目
- 姓名、学号
- 中文摘要要求；
- 正文 **(要有个人见解与心得体会，如发现抄袭、或雷同论文一律计0分)**；
- 参考文献；
- 讨论以下密码学技术问题。

考试：论文

1. 有关 AES 算法的研究和讨论，并与 DES 相比较。
2. 有关 SHA1 或其它杂凑算法及其安全性讨论。
3. 有关快速短签名技术的研究。
4. 特殊签名技术的研究与应用
5. 金融密码学相关的安全性与隐私保护。
6. 有关 RSA 公钥加密算法及其安全性讨论。
7. 零知识证明相关协议的研究与讨论
8. 有关 PKI 在无线网络安全中的应用。
9. 课堂相关内容自定论题。

thank you