第 1 章　电子商务概述

1.1　电子商务模式与发展

1.1.1　电子商务的概念

许多组织、公司、学术团体等机构按照各自的理解，给出了对电子商务的诸多诠释。以下是一些权威机构对电子商务的定义：

联合经济合作和发展组织（OECD）：电子商务是发生在开放网络上的包含企业之间、企业和消费者之间的商业交易。

美国政府的“全球电子商务纲要”：电子商务是指通过 Internet 进行的各项商务活动，包括广告、交易、支付、服务等活动。

加拿大电子商务协会：电子商务是通过数字通信进行商品和服务的买卖以及资金的转移，它还包括公司间和公司内利用电子邮件、电子数据交换（EDI）、文件传输、传真、电视会议、远程计算机联网所能实现的全部功能。

全球信息基础设施委员会（GIIC）电子商务工作组：电子商务是运用电子通信作为手段的经济活动，通过这种方式人们可以对带有经济价值的产品和服务进行宣传、购买和结算。

已于 2019 年 1 月 1 日生效实施的《中华人民共和国电子商务法》界定电子商务“是指通过互联网等信息网络销售商品或者提供服务的经营活动”。

综合各方观点和大众理解，电子商务通常是指在网络环境下，买卖双方不需见面，实现网上交易、在线支付以及相关综合服务的一切活动，是完全创新的或者在一定程度上协同了传统商务流程的一种以信息化手段应用为典型特征的商业运营模式。

1.1.2　电子商务的分类

电子商务按交易的内容基本上可分为直接电子商务和间接电子商务。

直接电子商务包括向客户提供的软体商品（又称无形商品）和各种服务。如计算机软件，研究性咨询性的报告，航班、参团出游及娱乐内容的订购、支付，兑汇及银行有关业务，证券及期货的有关交易，全球规模的信息服务等，都可以通过网络直接传送，保证安全抵达客户。直接电子商务突出的好处是快速简便及十分便宜，深受客户欢迎，企业的运作成本显著降低。受限之处是只能经营适合在网上传输的商品和服务。

间接电子商务包括向客户提供的实体商品（又称有形商品）及有关服务。显然这是社会中大量交易的商品和有关服务。由于要求做到在很广的地域范围和严格的时限内送达，一般均交由现代物流配送公司和专业服务机构去完成配送工作，这里所说的现代物流配送公司和专业服务机构远非过去传统商业的仓储货运机构和简单的服务部门，而是一种具有相当规模、拥有很强运输能力、采用自动化手段特别是充分运用互联网进行信息管理的现代企业。

电子商务按网络类型基本上分为 EDI（电子数据交换）商务、Internet（互联网）商务、Intranet（企业内部网）商务、Extranet（企业外部网）商务四种类型。

- EDI（电子数据交换）应用于企业之间、企业与中间商之间的批发业务。较之传统的订货和付款方式，EDI 大大节约了时间和费用，有较好的安全保障、严格的登记手续和准入制度、多级权限的防范措施，实现了包括付款在内的全部交易工作电脑化。
- Internet（互联网）商务是国际现代商业的最新形式。它以计算机、通信、多媒体、数据库技术为基础，通过互联网在网上实现营销、购物服务。它突破了传统的商业、生产、批发、零售及进、销、存、调的流转程序与营销模式，有利于实现少投入、低成本、零库存、高效率，避免了商品的无效转移及搬运，从而实现了社会资源的高效运作和最大节余。对于消费者来说，则可不受时空和厂商的限制，进行广泛的比较和选择，能以较低的价格获得所需的更好的商品和服务。
- Intranet 又称为内联网。这是企业拥有的采用与互联网相同的 TCP/IP 协议的局域网，可将局域网接入，形成一个企业内部的虚拟网络。Intranet 可运用防火墙（firewall）手段构造安全网站，防止外界访问者未经授权随便进入内联网，以保护企业内部需要保密的信息。跨国公司和大中型企业借助 Intranet 商务，可将其分布在世界各地的分支机构以及总部内有关部门联通起来，使企业各级管理人员按级分享内部信息，使在线业务取代一些纸面业务，从而有效地降低交易成本，提高了运营效益。
- Extranet 又称为外联网。它是在企业已有的互联网商务基础上扩展而成的，完全采用互联网技术。企业借助 Extranet 商务与上下游协作厂家建立更加紧密的伙伴关系。由于这些协作厂家的信息化程度各异，本企业往往要拥有多种网络方式，分别同它们连接。对于未建企业网站的伙伴，主要用 E-mail 方式；对于建有企业网站的伙伴，显然可以通过互联网构成 Extranet 商务；对于只拥有 EDI 商务的，最好都采用 Web-EDI，或经过 E-mail 过渡。

除了上述从不同角度分类外，常见的电子商务模式有 B2B、B2C、C2C、O2O 等。

1.1.3　电子商务的发展历程

我国早期的电子商务是以国家公共通信网络为基础，以国家“金关”工程为代表，以外经贸管理服务为重要内容逐步发展起来的。1993 年 3 月国务院会议提出并部署了“金

桥”工程（国家公用经济信息通信网），随后相继实施了金卡、金关等一系列金字工程，为我国电子商务的发展作了良好的铺垫。

1994年9月，中国公用计算机互联网（CHINANET）建设启动。10月，中国教育和科研计算机网（CERNET）启动。1995年1月，中国电信开始向社会提供Internet接入服务。1995年4月，中国科学院启动百所联网工程。在此基础上，网络不断扩展，形成了中国科技网（CSTNET）。同年，作为中国大陆第一家互联网应用服务商，“中国黄页”推出了定位于外向型企业的贸易撮合服务，为国内外企业搭建了全新的贸易桥梁。1996年1月，中国公用计算机互联网（CHINANET）全国骨干网建成并正式开通。接着中国国际电子商务中心（CIECC）正式成立。由中国国际电子商务中心承建并运营的中国国际电子商务网，是国家“金关工程”的骨干网络，是我国外经贸专用网络。1996年9月，中国电子进出口总公司成为中国国际电子商务网的第一个用户。同月中国金桥信息网（CHINAGBN）向社会提供Internet接入服务。1997年，中国公用计算机互联网（CHINANET）、中国科技网（CSTNET）、中国教育和科研计算机网（CERNET）、中国金桥信息网（CHINAGBN）实现了互连互通。以IBM为首的IT大厂商在1998年以前的中国电子商务热中扮演了无可争议的主要角色，它们以各种方式进行电子商务的“启蒙教育”，激发和引导人们对电子商务的认识、兴趣和需求，推动电子商务技术的介绍、应用与发展，使得中国电子商务技术能够在很短时间内跟上世界潮流，并为后来的进一步发展奠定了基础。1998年，对中国电子商务来说，是宣传、启蒙、概念和技术的推广。

1999年中国电子商务迅速扩大，从原先几乎局限于北京、上海、深圳、广州等极少数城市，开始向沿海及东部、中部各大城市发展。5月18日，B2C模式的8848网站建成。同月，中华网成立，并于7月在美国NASDAQ以每股20美元成功上市，成为在美国第一个上市的中国概念网络公司股，上市一周内股价攀至67美元。8月18日，易趣在上海成立。随着B2C、C2C的发展，B2B也有了一定起步。首都电子商城推出企业间电子商务，海尔集团等国内大型企业开始在企业内部和企业间应用电子商务。这一年中国电子商务的主角已经变成了电子商务企业、电子商务网站和致力于电子商务项目的机构。1999年的发展表明，中国电子商务已经开始由表及里，从虚到实，从宣传、启蒙和推广进入到了广泛而务实的发展阶段。

2000年，中国电子商务网站数量、规模都进入了高度膨胀期，商务网站超过2500家。门户网站的概念被进一步演绎为水平门户、垂直门户。其中网上购物类为数最多，达到1500家以上。2000年下半年，NASDAQ股票市场持续跌落，综合指数由最高峰时的近6000点跌至不足3000点，多数公司的股票市值折损近半，以网络为基础的新经济受到沉重的打击。在投资者心目中，门户这种商业模式已令人质疑，赢利结构单一，经营模式简单，在线广告成为几家中国门户网站的主要收入来源。三大门户的广告收入占总收入的比重均超过85%，搜狐更是高达95%。股市的变化反映了人们对电子商务公司的评价更加务实。

2002 年，我国互联网发展迅速，为电子商务的大行其道奠定了基础。2002 年 7 月，中国用户的互联网使用率占全球互联网总流量的 6.63%，达到 5900 万，超过日本跃居世界第二，网民的分布和层次都有了较大的改善。此外，全年上网计算机数、CN 下注册的域名数、网站数等都继续保持了超过 20%的高增长速度。

2003 年我国发生非典疫情，严重影响了社会生活和经济发展。但是这一灾难却使电子商务寒冬逐渐回暖，并迎来新的发展。由于疫情迫使人们尽可能远离商场、超市、办公大楼等公共场所，而电子商务不需要人员的直接接触就可以方便地完成交易的优势得到充分展现，这让电子商务迅速进入人们的日常生活，诞生了在中国电子商务发展史上比较重要的两家网络零售公司，即京东和淘宝。

2004 年至 2007 年，物流、支付、信用、政策法规等电子商务支撑环境获得实质性改善，电子商务取得了一系列的突破性进展：交易额持续增长，网络购物人数飞速上升，一些 B2B 企业开始盈利，B2C 企业蓄势待发，C2C 企业竞争格局基本形成，传统企业对电子商务的认识逐步深入，中小企业信息化和农村信息化开始起步。这期间，阿里巴巴、中国化工网和携程网分别上市。B2C 市场与 B2B 市场结构不同，市场份额仍然比较分散，当当和卓越网仍处于领先地位。B2C 综合类网站学习亚马逊商业模式，追求长尾效应，将网站越做越大，把经营的商品种类越做越全，细分的产品类型也越来越多。C2C 成为当时我国网络购物市场（包括 B2C 和 C2C）的主流商业模式。这期间我国 C2C 电子商务从无到有，从 2001 年的交易额 4 亿元，增长到 2007 年的 581 亿元，显示出市场巨大的发展潜力。淘宝网、eBay 易趣、拍拍网三足鼎立的 C2C 市场格局中，淘宝网市场龙头老大地位加强。

2008 年“金融危机”再次爆发。金融危机对我国经济影响很大，但电子商务成功地利用金融危机带来的种种机会，多角度突围，发展势头比以往更加强劲：电子商务年度交易额连续突破新高，中国网购市场取得突破性进展；基础设施、电子支付等电子商务环境逐步改善；中小企业信息化稳步推进；农村信息化进程加快；电子商务服务市场在创新中发展；移动电子商务布局初见成效；新技术不断推动电子商务模式和应用创新。2009 年我国电子商务交易额达到 3.7 万亿元，同比增长 19.12%，相比国内生产总值 8%左右的增速高出 2.4 倍。

2010 年销售衬衫的凡客诚品异军突起。农村电子商务的沙集模式引起了社会的广泛关注，农民通过网店生意，走出了一条以信息化带动工业化和农业发展的新路。在政策利好、技术进步、市场需求和社会化投资的多重因素驱动下，2011—2014 年我国电子商务交易额继续高速增长，其中网络购物市场依然火爆，占社会商品零售总额的比例大幅度提高。一批国家级电子商务示范基地启动，传统行业不断尝试电子商务应用，农村电子商务起步，跨境电子商务崛起，移动电子商务崭露头角。这期间，每年的 11 月 11 日成为人们期待的网络购物节，苏宁易购、京东、国美等电商巨头发起了“史上最大规模”的电商价格战。

2015 年我国电子商务交易额达到 21.79 万亿元人民币，同比增长 32.9%，相比国内生产总值 6.9%的增速，电子商务成为中国经济增长的新动力。B2C 交易额首次超过 C2C 交易额，网络零售主流商业模式由 C2C 转变为 B2C。网络零售交易规模为 3.88 万亿元，同比增长 33.3%。跨境电商交易总额达 4.56 万亿元，同比增长 21.7%，成为我国进出口贸易的重要渠道。工业企业电子商务采购和销售普及率进一步提升，平均达到 37.24%，部分行业接近 60%。农村电子商务发展进入快车道，建设电商村级服务点 25 万个，新增网店 118 万家，农村网购交易额达 3530 亿元，同比增长 96%，农产品网络零售额 1505 亿元。2015 年，以国务院《关于大力发展电子商务加快培育经济新动力的意见》《关于推进线上线下互动加快商贸流通创新发展转型升级的意见》为代表的一系列支持电子商务发展的政策密集出台。各级政府部门按照“积极推动、逐步规范、加强引导”的原则继续加大对电子商务的支持力度，完善电子支付、物流快递等新商业基础设施，积极促进和引导电子商务服务业的发展。电子商务成为中国经济社会实现“创新、协调、绿色、开放、共享”发展的重要驱动力量，成为“互联网+”行动计划的先导产业，成为大众创业、万众创新的一片热土。

2017 年我国电子商务交易额达 29.16 万亿元，同比增长 11.7%。网络零售额 7.18 万亿元，同比增长 32.2%。与其他国家相比，我国电子商务优势进一步扩大，网络零售规模全球最大、产业创新活力世界领先。

截至 2018 年底我国网民数达到 8.29 亿，普及率达 59.6%，通过手机接入互联网比例高达 98.6%，互联网覆盖范围进一步扩大，贫困地区网络基础设施“最后一公里”逐步打通，“数字鸿沟”加快弥合，数字经济发展态势良好。电子商务领域首部法律《中华人民共和国电子商务法》正式出台并于 2019 年 1 月 1 日实施，对促进行业持续健康发展具有重大意义。

在经历多年高速发展后，网络消费市场在 2019 年逐步进入提质升级的发展阶段，供需两端“双升级”正成为行业增长新一轮驱动力。在供给侧，线上线下资源加速整合，社交电商、品质电商等新模式不断丰富消费场景，带动零售业转型升级；大数据、区块链等技术深入应用，有效提升了运营效率。在需求侧，消费升级趋势保持不变，消费分层特征日渐凸显，进一步推动市场多元化。

1.1.4 电子商务模式

1．B2B 模式

1）B2B 模式的内涵

B2B 即 Business To Business（商家对商家），就是企业与企业之间通过互联网进行产品、服务及信息的交换。B2B 是电子商务按参与对象分类中的一种。这种形式的电子商务是在企业与企业之间进行的，一般以信息发布与撮合为主，主要是建立商家之间的桥梁。B2B 模式主要是通过互联网平台聚合众多的企业，形成买卖的大信息海洋，买家与

卖家在平台上选择交易对象，通过在线电子支付完成交易。传统的企业间的交易往往要耗费企业的大量资源和时间，无论是销售和分销还是采购都要占用产品成本。通过 B2B 的交易方式买卖双方能够在网上完成整个业务流程，从建立最初印象，到货比三家，再到讨价还价、签单和交货，最后到客户服务。B2B 使企业之间的交易减少许多事务性的工作流程和管理费用，降低了企业经营成本。网络的便利及延伸性使企业扩大了活动范围，企业发展跨地区跨国界更方便，成本更低廉。

2）B2B 模式的分类

（1）面向制造业或面向商业的垂直 B2B 模式。垂直 B2B 可以分为两个方向，即上游和下游。生产商或商业零售商可以与上游的供应商形成供货关系，例如 Dell 电脑公司与上游的芯片和主板制造商就是通过 B2B 这种方式进行合作。生产商与下游的经销商可以形成销货关系，例如 Cisco 与其分销商之间就是通过 B2B 这种方式进行交易。

（2）面向中间交易市场的水平 B2B 模式。这种交易模式是水平 B2B，它是将各个行业中相近的交易过程集中到一个场所，为企业的采购方和供应方提供了一个交易的机会，如像 Alibaba、中国制造网、环球资源网、中国化工网、中国网库、ECVV、中国供应商、慧聪网、敦煌网、万国商业网等。水平 B2B 只是企业实现电子商务的一个开始，它的应用会得到不断发展和完善，并适应所有行业企业的需要。

（3）自建 B2B 模式。行业龙头企业自建 B2B 模式是大型行业龙头企业基于自身的信息化建设程度，搭建以自身产品供应链为核心的行业化电子商务平台。行业龙头企业通过自身的电子商务平台，串联起行业整条产业链，供应链上下游企业通过该平台实现资讯、沟通、交易。但此类电子商务平台过于封闭，缺少产业链的深度整合。

（4）关联行业 B2B 模式。关联行业 B2B 模式是相关行业为了提升目前电子商务交易平台信息的广泛程度和准确性，整合水平 B2B 模式和垂直 B2B 模式而建立起来的跨行业电子商务平台。

3）B2B 模式的演进

B2B 电子商务发展经历了四个阶段：电子数据交换（EDI）、基本的电子商务、电子交易集市、协同商务。

- 第一阶段：电子数据交换（EDI）。在此阶段中，企业与组织之间，通过制定各种通信标准来管制数据传输的工作。在此阶段中企业和厂商所形成的网络是封闭的，因为信息技术并未普及、所需的费用昂贵，并不是所有的企业均有足够的资金引进 EDI，在此阶段，电子商务弹性低、成本高。
- 第二阶段：基本的电子商务。在此阶段中，买卖双方直接在网站上进行交易，并不依赖中间交易商，是从网站一对一进行，在网站上设置在线目录，卖给专业的厂商。在此阶段，弹性变高、成本降低，但互动仍是单向，同时市场的效率并不高，且市场透明度也不高。
- 第三阶段：电子交易集市。在此阶段中，产生了第三方供应者，目的在于形成一

个电子交易集市，提供大家一起交易的地方，在流程方面，由单向交易发展到双向交易，随着订单的复杂性增强，互动性更加丰富，沟通协调也增强。

- 第四阶段：协同商务。在此阶段中，扩大了企业运作的范围，在作业流程中引入了事前、事中、事后流程，除了注重自己企业运作的内部流程，还通过上下游一起协商合作的一种商业合作，市场更加透明化。

4）B2B 的盈利模式

（1）会员费。企业通过第三方电子商务平台参与电子商务交易，必须注册为 B2B 网站的会员，每年要交纳一定的会员费，才能享受网站提供的各种服务，目前会员费已成为我国 B2B 网站最主要的收入来源。

（2）广告费。网络广告是门户网站的主要盈利来源，同时也是 B2B 电子商务网站的主要收入来源。这一领域的典型代表有 TOXUE 外贸网、阿里巴巴、ECVV 等。

（3）竞价排名。企业为了促进产品的销售，都希望在 B2B 网站的信息搜索中将自己的排名靠前，而网站在确保信息准确的基础上，根据会员交费的不同对排名顺序做相应调整。

（4）增值服务。B2B 网站通常除了为企业提供贸易供求信息以外，还会提供一些独特的增值服务，包括企业认证、独立域名、提供行业数据分析报告、搜索引擎优化等。例如现货认证，由于电子采购商比较重视库存，就产生了针对电子采购行业的这样一个特殊的增值服务。另外针对电子型号做的谷歌排名推广服务，是搜索引擎优化的一种，企业都比较感兴趣。所以，可以根据行业的特殊性去深挖客户的需求，然后提供具有针对性的增值服务。

（5）线下服务。其主要包括展会、期刊、研讨会等。通过展会，供应商和采购商面对面地交流，一般的中小企业还是比较青睐这种方式。期刊主要是关于行业资讯等信息，期刊里也可以植入广告。环球资源的展会现已成为重要的盈利模式，占其收入的三分之一左右。而 ECVV 组织的各种展会和采购会也已取得不错的效果。

（6）商务合作。它包括广告联盟、行业协会合作、传统媒体的合作等。广告联盟通常是网络广告联盟，亚马逊通过这个方式已经取得了不错的成效，国内做得比较成熟的几家广告联盟有：百度联盟、谷歌联盟、淘宝联盟等。

（7）按询盘付费。它区别于传统的会员包年付费模式，按询盘付费模式是指从事国际贸易的企业按照海外推广带来的实际效果，也就是海外买家实际的有效询盘来付费。其中询盘是否有效，主动权在消费者手中，由消费者自行判断，来决定是否消费。“按询盘付费”有四大特点：零首付、零风险；主动权、消费权；免费推、针对广；及时付、便利大。广大企业不用冒着“投入几万元、十几万元，一年都收不回成本”的风险，零投入就可享受免费全球推广，成功获得有效询盘后，辨认询盘的真实性和有效性后，只需在线支付单条询盘价格，就可以获得与海外买家直接谈判成单的机会，主动权完全掌握在供应商手里。

2．B2C 模式

1）B2C 模式的内涵

B2C 即 Business To Consumer（商家对个人），就是电子商务按参与对象分类中的一种，即表示企业对消费者的电子商务，这种形式的电子商务一般以网络零售业为主，主要借助于 Internet 开展在线活动，是企业通过互联网为消费者提供的一个新型的购物环境——网上商店。消费者通过网络进行全部的贸易活动。

B2C 以完备的双向信息沟通、灵活的交易手段、快捷的物流配送、低成本高效益的运作方式等在各行各业展现了其极大的生命力。这种模式节省了消费者和企业的时间和空间，大大提高了交易效率。这种商业模式在我国已经基本成熟，其代表有当当网、卓越网等。

2）B2C 模式的分类

（1）综合型 B2C。发挥自身的品牌影响力，积极寻找新的利润点，培养核心业务。如卓越亚马逊，可在现有品牌信用的基础上，借助母公司亚马逊国际化的背景，探索国际品牌代购业务或者采购国际品牌产品进行销售等新业务。网站建设要在商品陈列展示、信息系统智能化等方面进一步细化。对于新老客户的关系管理，需要精细客户体验的内容，提供更加人性化、直观的服务。选择较好的物流合作伙伴，增强物流实际控制权，提高物流配送服务质量。

（2）垂直型 B2C。核心领域内继续挖掘新亮点。积极与知名品牌生产商沟通与合作，化解与线下渠道商的利益冲突，扩大产品线与产品系列，完善售前、售后服务，提供多样化的支付手段。个别垂直型 B2C 运营商开始涉足不同行业，可以尝试探索“物流联盟”或“协作物流”模式，若资金允许也可逐步实现自营物流，保证物流配送质量，增强用户的粘性，将网站完善后再寻找其他行业的商业机会。

（3）传统生产企业网络直销型 B2C。首先要从战略管理层面明确这种模式未来的定位、发展与目标。协调企业原有的线下渠道与网络平台的利益，实行差异化的销售。如网上销售所有产品系列，而传统渠道销售的产品则体现地区特色；实行差异化的价格；线上产品也可通过线下渠道完善售后服务。在产品设计方面，要着重考虑消费者的需求感觉。大力吸收和挖掘网络营销精英，培养电子商务运作团队，建立和完善电子商务平台。

（4）第三方交易平台型 B2C。B2C 受到的制约因素较多，但中小企业在人力、物力、财力有限的情况下，这不失为一种拓宽网上销售渠道的好方法。关键是中小企业要选择具有较高知名度、点击率和流量的第三方平台；其次要聘请懂得网络营销、熟悉网络应用、了解实体店运作的网店管理人员；再次是要以长远发展的眼光看待网络渠道，增加产品的类别，充分利用实体店的资源、既有的仓储系统、供应链体系以及物流配送体系来发展网店。

（5）传统零售商网络销售型 B2C。传统零售商自建网站销售，将丰富的零售经验与电子商务有机地结合起来，有效地整合传统零售业务的供应链及物流体系，通过业务外包解决经营电子商务网站所需的技术问题，典型代表就是国美。

3）B2C 电子商务网站主要形式

（1）综合商城。它有庞大的购物群体，有稳定的网站平台，有完备的支付体系和诚信安全体系，促进了卖家进驻卖东西，买家进去买东西。如同传统商城一样，淘宝自己是不卖东西的，仅提供完备的销售配套。综合商城中有许多店，如同现实生活中的大商场。

（2）百货商店。商店，只有一个卖家；而百货即是满足日常消费需求的丰富产品线。这种商店具有自有仓库，会库存系列产品，以备更快进行物流配送和更好地进行客户服务。这种店甚至会有自己的品牌。就如同线下的沃尔玛、屈臣氏、百佳百货。

（3）垂直商店。这种商城的产品存在着更多的相似性，要么都是满足于某一人群的，要么是满足于某种需要，要么是服务于某种平台的（如电器）。互联网上的垂直商店数量取决于市场的细分。一般是细分的种类 3 到 5 倍，正因为有了良好的竞争格局，从而促进了服务的完善。常见的电子商务网站除了综合商城、百货商店、垂直商店外，还包括复合品牌店、轻型品牌店、服务型网店以及导购引擎型网店。

4）B2C 的盈利模式

（1）产品销售营业收入模式。以产品交易作为收入主要来源是多数 B2C 网站采用的模式。这种 B2C 网站又可细分为两种：销售平台式网站和自主销售式网站。

①销售平台式网站。网站并不直接销售产品，而是为商家提供了 B2C 的平台服务，通过收取虚拟店铺出租费、交易手续费、加盟费等来实现盈利。淘宝 B2C 购物平台——淘宝商城就是典型代表。淘宝提供淘宝商城这一 B2C 平台，收取加入淘宝商城商家一定费用，并根据提供服务级别的不同收取不同的服务费和保证金。

②自主销售式网站。与销售平台式网站不同，自主销售式需要网站直接销售产品。与销售平台相比运营成本较高，需要自行开拓产品供应渠道，并构建一个完整的仓储和物流配送体系或者发展第三方物流加盟商，将物流服务外包。

（2）网络广告收益模式。网络广告收益模式是互联网经济中比较普遍的模式，B2C 网站通过免费向顾客提供产品信息或服务信息吸引足够的“注意力”从而吸引广告主投入广告，通过广告盈利。相对于传统媒体来说，广告主在网络上投放广告具有独特的优势：一方面，网络广告投放的效率较高，一般是按照广告点击的次数收费。另一方面，B2C 网站可以充分利用网站自身提供的产品或服务来区分消费群体，对广告主的吸引力也很大。

（3）收费会员制收益模式。B2C 网站对会员提供便捷的在线加盟注册程序、实时的用户购买行为跟踪记录、准确地在线销售统计资料查询等。网站收益量大小主要取决于自身推广努力。例如，网络可以适时地举办一些优惠活动并给予收费会员更优惠的会员价，与免费会员形成差异，以吸引更多的长期顾客。

（4）网上支付收益模式。当 B2C 网上支付拥有足够的用户，就可以借助其他途径来获取收入。以淘宝为例，有近 90%的淘宝用户通过支付宝，带给淘宝巨大的利润空间。淘宝不仅可以通过支付宝收取一定的交易服务费用，而且可以充分利用消费者存款和支

付时间差产生的巨额资金进行其他投资盈利。

3．C2C 模式

1）C2C 模式的内涵

C2C 即 Consumer To Consumer（个人对个人），就是消费者和消费者之间通过互联网进行交易的一种商务模式，换句话说就是由提供商品的消费者与需求商品的消费者在线达成交易的方式。举个例子来说吧，张三有一件衣服，放到淘宝网上进行拍卖，被李四买到，这种交易的方式就是 C2C。由于是个人跟个人的交易，大众化交易成为了 C2C 最大的特点。从字面上看，C2C 的构成要素包括买卖双方，即消费者。消费者是 C2C 的主体，扮演着提供商品者和购买商品者的角色。除此之外还包括电子交易服务平台，它将买卖双方聚集在一起，扮演着管理者的角色，保障交易的顺利进行，也起着极为重要的作用。例如淘宝、易趣、拍拍、有啊这些网站，它们都是极具有代表性的电子交易服务平台。

2）C2C 模式的优势

C2C 模式具有如下优势：

（1）我国人数众多，且是使用互联网人数最多的一个国家，这给 C2C 市场的发展奠定了群众基础。我国的科技技术日新月异，不断提高，这给 C2C 市场的发展奠定了技术基础。

（2）利用互联网进行交易，大大地节约了成本。例如，店铺租金、商品展示成本等等。

（3）网络交易平台的安全和信用制度的不断完善。例如，淘宝的支付宝、有啊的百付宝等等，解决了人们交易支付的问题。

（4）有更多的年轻人喜欢追随时尚的潮流，喜欢尝试新的购物体验，这促进了 C2C 市场的发展。

C2C 模式具有如下劣势：

（1）C2C 与中国原有的消费方式大大不同。人们已经习惯了实物的面对面的购买，而 C2C 模式的商品是看不见摸不着的，不能确定是否满足消费者的需求。

（2）买卖双方在交易支付的过程中缺乏信任。虽然现在有了第三方支付，一定程度上促进了 C2C 业务的发展，但是减缓了交易效率，使卖家不能及时收到钱导致经营成本过高。这样在一定的程度上延缓了 C2C 市场的发展速率。

（3）人们的消费观念难以改变，尤其是年龄稍大的人群。中国人已经习惯了一手交钱一手交货的消费模式，即现金交易，虽然有支付宝、安付通等便利的支付方式，有些人却选择了在网下完成交易。

（4）物流体系发展不成熟。人们常常遇到买货容易收货难的问题，尤其是在特殊节日，如双 11、双 12 等，给买卖双方都带来了不便。我国物流主要靠传统的邮政和快递企业，效率比较低，难以很好地满足网上购物快速交易的需求。

（5）商品质量得不到保证。网上购物是虚拟的，不能与商品零距离接触，会出现假货的可能，使网民承担了一定的风险性。

3）C2C 的商业模式

（1）盈利模式。C2C 市场的盈利方式有广告收入、交易提成、增值服务、黄金铺位的推荐费等等。

（2）信用模式。网络作为一种交易手段，应创建一个诚信的环境。其中应包括注册认证、交易实名认证、设立诚信指数、奖惩制度、在线支付、在线交流等等。

（3）支付模式。交易中支付的安全是每个用户所关心的内容，随着第三方支付的出现，凭借其信用度，解除了用户的忧虑。支付工具的出现，所建立起来的制度和采取的措施，大大地提高了交易的安全性。

（4）配送模式。为了买家能够及时迅速地收到商品，C2C 网站推荐了物流服务。邀请物流公司为第三方支付平台用户提供特别服务和优惠价格，卖家可以应买家要求或自行选择推荐的物流公司。

4．O2O 模式

1）O2O 模式的内涵

O2O 即 Online To Offline（线上购买线下商品与服务，实体店享受），就是把线上的消费者带到现实的商店中去——在线支付线下商品、服务，再到线下去享受服务。通过打折（如团购）、提供信息、服务（预定，如 Opentable）等方式，把线下商店的消息推送给互联网用户，从而将他们转换为自己的线下客户。该模式最重要的特点是：推广效果可查，每笔交易可跟踪，相对传统网购更强调互动。模式简称为线上线下电子商务，即 O2O。这个模式中必须包含“线下商户的发现或推荐”“在线支付”“营销效果的监测”这三大块。

O2O 模式的诞生，会促进很多新生网络公司提供该服务，尤其是团购类网站，以及本地信息生活服务类平台。对于传统企业来说，下列几类企业适合利用 O2O 模式。

（1）连锁加盟型的零售企业，如：流行美、卡顿、哎呀呀，或者大型渠道流通品牌商，因为加盟门店分布广，并且有线下服务优势等各种原因，这时候借助 O2O，能迅速促进门店销售，及进一步扩大连锁加盟商数量。

（2）连锁类餐饮公司，如小肥羊之类，因为产品无法快递，只能在线下体验服务，所以可以通过线上下单，线下体验服务的方式抢占更多消费者。

（3）本地生活服务企业，如：酒吧、会所、餐饮、电影等，通过 O2O 进行电子商务。事实上很多企业就是这么做的。

对于传统企业来说，开展 O2O 电子商务，主要有以下方式：

（1）自建官方商城+连锁分店铺的形式，消费者直接向最近门店的网络店铺下单购买，然后线下体验服务，而在这过程中，品牌商提供在线客服服务，及随时调货支持（在缺货情况下），加盟商收款发货，适合全国连锁型企业。可以线上和线下店铺一一对应。但是投入大，需要的推广力度很大。

（2）借助全国布局的第三方平台，如：赶集、拉手或窝窝等，实现加盟企业和分站

第 2 章　电子商务信息安全

2.1　电子商务信息安全威胁与防范

2.1.1　信息安全概述

1．信息安全的定义

信息安全是一个广泛而抽象的概念，不同领域、不同角度对其概念的阐述都会有所不同。建立在网络基础之上的现代信息系统，对于信息安全的定义是：保护信息系统的硬件、软件及相关数据，使之不因为偶然或者恶意侵犯而遭受破坏、更改及泄露，保证信息系统能够连续、可靠、正常地运行。在商业和经济领域，信息安全主要强调的是削减并控制风险，保持业务操作的连续性，并将风险造成的损失和影响降低到最低程度。

2．信息安全面临的威胁

信息安全面临的威胁主要包括信息截取和窃取、信息篡改、信息假冒、信息抵赖。

1）信息截取和窃取

攻击者可能通过搭线窃听、安装数据截收装置等方式获取传输的机密信息，或通过对信息流量和流向、通信频度和长度等参数的分析，推理出有用信息，如消费者的银行账号、密码以及企业的商业机密等。

2）信息篡改

攻击者可能通过各种技术方法和手段对网络传输的信息进行中途修改，破坏信息的完整性。信息篡改主要表现为三种方式。

（1）篡改。改变信息流的次序或更改信息的内容。

（2）删除。删除某个消息或消息的某些部分。

（3）插入。在消息中插入一些信息，让接收方读不懂或接收错误的信息。

3）信息假冒

当攻击者掌握了网络信息数据规律或解密了商务信息以后，可以假冒合法用户或发送假冒信息来欺骗其他用户，如冒充竞争对手发布虚假信息；冒充网络控制程序，套取或修改使用权限、通行字、密钥等信息；冒充合法用户行使授权等。

4）信息抵赖

信息抵赖涉及多个方面，如信息发送者事后否认曾经发送过某条信息或内容；信息接收者事后否认曾经收到过某条信息或内容；购买者发了订货信息却不承认；销售者卖

出商品却因价格差而不承认原有交易等。

3．信息安全需求

信息安全面临的威胁，带来信息安全需求。在电子商务活动中，信息安全需求涉及保密性、完整性、不可否认性、身份可认证性、可用性和可控性。

（1）保密性。保密性也称为机密性，是指网络中的信息不被非授权的实体（包括用户和进程等）获取与使用。

（2）完整性。完整性是指数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。

（3）不可否认性。不可否认性也称为不可抵赖性，是指在信息交换过程中，确信参与方的真实同一性，即所有参与者都不能否认和抵赖曾经完成的操作和承诺。例如信息发送方不能否认发送过的信息，信息接收方不能否认接收过的信息。

（4）身份可认证性。身份可认证性是指通过安全认证技术实现对信息交流双方身份真实性的确认，保证交易对象的身份真实性。电子商务活动过程中，信息交流双方互不见面，确认对方的真实身份，是电子商务交易活动过程中保证交易安全的重要环节。

（5）可用性。可用性是指对信息或资源的期望使用能力，即可授权实体或用户访问并按要求使用信息的特性。简单地说，就是保证信息在需要时能为授权者所用，防止由于主、客观因素造成的系统拒绝服务。

（6）可控性。可控性是指人们对信息的传播路径、范围及其内容所具有的控制能力，即不允许不良内容通过公共网络进行传输，使信息在合法用户的掌控之中。

2.1.2　电子商务安全体系

电子商务的交易过程面临着信息截取和窃取、信息篡改、信息假冒、信息抵赖等威胁，对电子商务的交易信息安全提出了保密性、完整性、不可否认性、身份可认证性、可用性和可控性的安全需求。如何实现和保证电子商务的安全需求，从组织、技术、管理以及法律等多方面入手，构建全方位的电子商务安全体系，全面采取电子商务安全防范措施是关键。

电子商务的安全性研究从整体上可分为两大部分：计算机网络安全和商务交易安全。

1．计算机网络安全

常见的计算机网络安全威胁有：

（1）黑客攻击。黑客非法进入网络，非法使用网络资源。例如，通过网络监听获取网上用户的账号和密码，非法获取网上传输的数据，破坏防火墙等。

（2）计算机病毒。计算机病毒侵入网络，破坏资源，使网络不能正常工作，甚至造成网络瘫痪。

（3）拒绝服务。典型的拒绝服务如“电子邮件炸弹”，它的破坏方式是让用户在很短

的时间内收到大量的无用邮件，从而影响正常业务，严重时造成系统关闭、网络瘫痪等。

（4）身份窃取。用户的身份在通信时被他人非法截取。

（5）非授权访问。对网络设备及信息资源进行非正常使用或越权使用。

（6）冒充合法用户。利用各种假冒或欺骗手段非法获取合法用户资源的使用权限，以达到占用合法用户资源的目的。

（7）数据窃取。非法用户截取通信网络中的某些重要信息。

（8）物理安全。网络的物理安全是整个网络系统安全的前提，包括计算机、网络设备的功能失常，电源故障，由于电磁泄漏引起的信息失密，搭线窃听等，还有自然灾害的威胁（如雷电、地震、火灾等），操作失误（如删除文件、格式化硬盘、线路拆除等），都是造成计算机网络不安全的因素。

（9）软件的漏洞和“后门”。程序设计者为了后期便于维护或是疏漏，在操作系统、应用软件设计时往往会留有一些安全漏洞或“后门”，这也是网络安全的主要威胁之一。例如，大家熟悉的 Windows 操作系统、UNIX 操作系统几乎都存在或多或少的安全漏洞，众多的各类服务器、浏览器、一些桌面软件等都被发现过存在安全隐患。

（10）网络协议的安全漏洞。网络安全协议也会产生漏洞，成为黑客攻击的目标。如一些路由协议漏洞、DNS 协议漏洞、ARP 协议漏洞等都对网络安全造成了威胁。

计算机网络安全是一个复杂和多面性的问题，除上述讲到的影响网络安全的因素外，计算机犯罪等人为因素都会使网络面临安全威胁。解决这些问题，涉及很多的网络安全技术，如防火墙技术、虚拟专用网技术、各种反黑客技术和漏洞检测技术等。此外，网络行为的规范化管理及安全意识也是很重要的方面。

2．商务交易安全

在电子商务交易活动过程中，交易双方（商家和消费者）都面临不同的安全威胁。

1）商家面临的主要威胁

- 中央系统安全性被破坏。例如入侵者假冒合法用户改变用户数据（如商品送达的地方）、解除用户订单或生成虚假订单等。
- 竞争者检索商品递送状况。例如恶意竞争者以他人名义订购商品，了解有关商品的递送状况、货物和库存情况等。
- 被他人假冒。例如假冒销售者建立与真实销售者服务器名字相同的另一个服务器，进而造成可能的损害，使公司信誉受到损失等。
- 其他威胁。例如客户资料被竞争者获悉等。

2）消费者面临的主要威胁

- 虚假订单。例如假冒者可能会以客户的名字订购商品，客户却被要求付款或返还商品等。
- 付款后不能收到商品。例如在要求客户付款后，恶意销售商可能不供给客户商品等。

- 机密性丧失。例如客户可能将个人身份等秘密数据（如 PIN、口令等）发送给冒充销售商的机构，或是在信息传递的过程中被假冒者窃听等。

电子商务交易过程中交易双方面临各种安全威胁，解决其安全问题涉及多种安全技术及其应用，包括加密技术、认证技术、电子商务安全协议等。

3．电子商务安全体系

电子商务安全涉及的计算机网络安全和商务交易安全，二者相辅相成，缺一不可。电子商务安全体系反映了电子商务安全涉及的内容和相关技术，其结构如图 2-1 所示。

图 2-1　电子商务安全体系结构

电子商务安全体系由网络服务层、加密技术层、安全认证层、安全协议层、应用系统层组成。

在电子商务安全体系结构层次中，下层是上层的基础，为上层提供技术支持；上层是下层的扩展与递进。层次之间相互依赖、相互关联构成统一整体。每一层通过各自的安全控制技术，实现各层的安全策略，保证电子商务系统的安全。

网络服务层为电子商务系统提供基本、灵活的网络服务，是各种电子商务应用系统的基础，提供信息传送的载体和用户接入的手段。通过 Internet 网络层的安全机制（如入侵检测、安全扫描、防火墙等技术）保证网络层的安全。

加密技术层、安全认证层和安全协议层确保电子商务交易安全。加密技术是保证电子商务交易安全所采用的最基本的安全措施，它用于满足电子商务对保密性的需求。安全认证层对加密技术层中提供的多种加密算法进行综合运用，进一步满足电子商务对完整性、不可抵赖性等要求。安全协议层是加密技术层和安全认证层的安全控制技术的综合运用和完善，为电子商务安全交易提供保障机制和交易标准。

2.1.3　电子商务安全策略

电子商务安全策略是提供安全服务的一套准则，它定义了系统要实现的安全目标和

实现这些安全目标的途径。电子商务安全策略的内容应该有别于技术方案。安全策略是原则性的并且不涉及具体细节，对于整个组织提供全局性指导，为具体的安全措施和规定提供一个全局性框架。

电子商务安全策略主要包括电子商务安全技术及安全管理两部分内容。安全技术为电子商务安全提供基本的技术支持，安全管理为电子商务安全提供严格的组织与管理制度。

1．安全技术策略

（1）计算机及网络安全技术。计算机和网络是开展电子商务活动的基础，因此计算机和网络安全是保障电子商务安全的基础。计算机和网络安全技术涉及的内容很多，包括计算机硬件安全、软件安全、操作系统安全、数据库安全、防火墙技术、虚拟专网技术、入侵检测技术、漏洞检测技术和病毒防范技术等。

（2）信息加密技术。信息加密技术是实现电子商务交易安全保密性、完整性、不可抵赖性、身份可认证性的基础。信息加密技术主要有单钥密码体制和公开密钥密码体制两大类。单钥密码体制中加密密钥和解密密钥相同，算法简单、速度快，但密钥发布与管理安全性较低；公开密钥密码体制中加密密钥和解密密钥不同，分为公钥和私钥，公钥用于加密，私钥用于解密。相对于单钥密码体制，公开密钥密码体制的密钥便于管理，安全性更高，但算法复杂，速度慢，实际应用中普遍采用两种体制相结合的方式。典型的单钥密码体制和公开密钥密码体制算法分别是DES算法和RSA算法。

（3）数字摘要和数字签名技术。数字摘要技术用于验证信息的完整性，应用信息加密技术生成数字签名，表明签署者身份，签署者承认所签署的文件内容，保证交易的真实性和有效性。如果当事双方关于签名的真伪发生争执，能够由公正的第三方仲裁机构通过验证签名来确认其真伪，有效防止交易抵赖和伪造行为的发生。

（4）认证中心（Certificate Authority，CA）。认证中心是一个权威的、受信任的第三方机构，其核心职能是发放和管理数字证书，用于证明和确认交易参与者的身份，保证电子商务交易过程中身份可认证性。认证中心以数字证书的方式为采用公开密钥的用户分发公开密钥，承担公钥体系中公钥的合法性检验等任务。为了建立信任关系，认证中心用它的私钥对数字证书进行签名，防止数字证书的伪造和篡改，从而保证了认证信息的完整性和数字证书的权威性，并且认证中心不能否认自己所颁发的证书。

（5）安全协议。信息加密技术、数字摘要和数字签名技术、认证中心等电子商务安全技术如何与电子商务交易的各参与方充分地结合起来，以保证安全、有序、快捷地完成交易流程，需要安全交易协议规范各方的行为与各种技术的应用。电子商务安全协议主要有SSL协议和SET协议。

2．安全管理策略

电子商务是一个复杂的系统，涉及很多参与角色和活动环节。因此，电子商务的安全除了靠安全技术保障外，还必须加强监管，建立健全相应的安全管理制度，有相关的法律法规作保障。

（1）交易安全管理制度。交易安全管理制度主要是为电子商务活动提供安全交易环境，制定相应管理制度和策略，提高信用，规避风险，保证商务活动的公平、公开和公正。

（2）风险管理与控制机制。通过风险管理与控制机制的建立能够对潜在风险及其发生的可能性进行分析，从而及时有效地实施应对策略来规避风险。风险管理与控制是一个封闭的连续过程。首先是主动检查系统内外工作环境，找出潜在风险。其次是对潜在风险及其发生的可能性进行分析，在此基础上对可分配的资源进行评估，制定评估计划与实施方案，并予以实现。最后利用实现过程中所获得的监控信息对风险管理的计划与控制进行调整。应对风险要考虑成本效益的问题，应当认真研究和制定风险管理与控制机制，正确把握投入的度，以最小的投入，获得最大的效益。

（3）运行、维护和安全监控管理制度。建立日常的电子商务系统运行、维护和安全监控管理制度，定期检查系统日志，对系统的日常工作情况进行记录与监控。特别要对关系系统安全的重大相关事件、操作状况和运行情况进行记录，以便分析查找发现问题，及时妥善解决问题。

（4）授权、访问控制策略和责任。授权是指赋予本体（用户、终端、程序等）对客体（数据、程序等）的支配权利，即规定了谁可以对谁进行什么操作。例如，规定某个文件只能由特定人员阅读或修改；人事记录只能由人事部职员进行新增和修改，并且只能由人事部职员、执行经理以及该记录所属于的那个人阅读；在多级安全系统中，只有所持的许可证级别等于或高于相关密级的人员，才有权访问该密级中的信息等。这些安全策略的描述也对各类防护措施提出了要求。在计算机和通信系统中，主要是以一种被称为“访问控制策略”的系统安全策略反映出来的。访问控制策略隶属于系统安全策略，它迫使在计算机系统和网络中自动地执行授权。例如，基于身份的策略，该策略允许或者拒绝执行对明确区分的个体或群体进行访问；基于任务的策略，它是基于身份的策略的一种变形，它给每一个体分配任务，并基于这些任务来使用授权规则；多等级策略，它是基于信息敏感性的等级以及工作人员许可证等级而制定的一般规则的策略。支撑所有安全控制策略的一个根本原则是责任。受到安全策略制约的任何个体在执行任务时，需要对他们的行动负责。

（5）人员管理制度。人员管理在电子商务安全管理中处于非常重要的地位，管理的对象包括在职人员和离职人员，管理的内容包括无意的操作失误、有意的攻击与破坏、错误的判断等。内部人员对系统攻击的危害性及发现的难度要远远大于外部人员，因此如何防止系统内部人员对电子商务系统有意的攻击与破坏是重中之重。制定严格的管理制度，加强教育和监督，明确职责和权限，严禁越权操作和使用。建立离职人员的审计和监督制度，杜绝因人员的离职给单位造成不必要的损失。建立在职人员个人情况（特别是经济状况、工作业绩、道德品行等）档案，及时了解在职人员的思想和工作状况，防止蓄意破坏情况的发生。另外，还要在人员录用、安全教育、岗前培训等方面制定相应的管理制度，消除安全隐患，杜绝安全漏洞，防患于未然。

（6）保密制度。建立安全保密制度，加强工作人员的安全教育，提高安全意识。严格执行信息披露制度，保证企业的有价值信息、关键性商务运作信息、客户私人信息以及内部重要信息等不被泄露。

（7）病毒防范机制。建立病毒的检测与防范机制，通过采用网络防火墙、防病毒软件、控制访问权限等技术和措施，增强安全意识，严格制度管理。认真执行病毒的检测与清理、系统漏洞检查等制度，杜绝安全隐患，防患于未然。

（8）安全计划、应急机制和灾难恢复机制。任何系统都会受到自然灾害或者是人为灾害的影响，使系统处于不安全或者不稳定的状态。因此，需要制定安全计划、应急机制和灾难恢复措施。评估系统薄弱环节，防止和减少系统风险。制定完善的安全解决方案，在系统出现突发性事故或不安全事故发生的情况下，能够尽快排除故障，恢复系统正常运行，最大限度地减少损失。制定灾难恢复措施，经常对重要数据进行备份。采用数据恢复技术，以便灾难发生时，能够及时恢复与使用数据。

2.2 加密技术

2.2.1 基本概念

加密技术是实现信息保密性的重要手段。早在远古时期，人们就能够使用简单的加密技术传递重要的机密信息。20 世纪 70 年代，随着人们对加密技术的深入研究，逐渐形成一门学科——密码学。密码学包括密码编码学和密码分析学。密码编码学主要研究密码体制的设计；密码分析学主要研究密码体制的破译，二者既相互对立，又相互促进。

加密技术涉及信息、算法和密钥等相关概念。信息包括明文和密文，加密技术采用数学方法（算法）对原始信息（明文）进行再组织，使得加密后在网络上公开传输的内容对于非法接收者来说成为无意义的文字（密文），而对于合法的接收者，因为其掌握正确的密钥，可以通过解密过程得到原始数据（明文）。加密和解密的一般过程如图 2-2 所示。

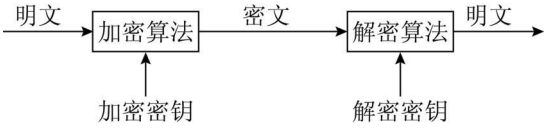

图 2-2 加密和解密的一般过程

加密技术中，算法和密钥是两个核心要素。它们与密码系统的安全有着密切关系。理论上讲，只要采用穷举法去试每种可能的密钥，则几乎所有的密码系统都是可以破译的。但采用穷举法所花费的代价可能是现有计算条件下难以实现的，因此，密码学判断一个密码算法是否安全，更关心的是该密码算法在现有计算条件下是不是不可破译的。

如果一个密码算法不能被现有的计算资源所破译，那么这种密码体制在计算上就可以说是安全的。此外，密钥安全也是密码系统安全的一个重要因素。因为同一加密算法，采用不同的密钥，可以对同一明文加密出不同的密文。只要密钥保密好，他人就不能破译密文。密钥安全主要涉及的是管理问题。密钥的保护与管理，包括密钥的产生、分发、使用和销毁等过程，对信息系统的安全性来说是极其重要的。

按照所使用的密钥不同，可将密码体制分为两类：对称密钥密码体制和非对称密钥密码体制。

2.2.2　对称密钥密码体制

1．对称密钥密码体制原理

对称密钥密码体制的基本原理是加密密钥与解密密钥相同，或者加密秘钥与解密密钥虽不相同，但可以从其中一个推导出另一个。对称密钥密码体制也被称为单钥密码体制，其优点是算法简单，加密和解密速度快，效率高，但也存在一些问题：

（1）密钥传递安全问题。双方传递信息前需要事先通过某个安全渠道传递密钥，而密钥在此过程中可能会泄漏。另一方面，密钥的安全性还取决于传递信息的双方对密钥的保护。

（2）密钥管理问题。为了保证信息传递的安全，当一方与多方（N 方）传递信息时，需要 N 个不同的密钥。当 N 比较大时，密钥的管理和分发难度就会增大。

（3）身份识别问题。对称密钥算法无法实现数字签名技术，因此不能鉴别交易参与者的身份。

2．DES 算法

对称密钥密码体制的典型算法是 DES（Data Encryption Standard）算法。

DES 算法是 IBM 公司研制的一种数据加密算法，1977 年被美国国家标准局颁布为商用数据加密标准，后又被国际标准化组织 ISO 定为国际标准，广泛应用于金融行业的电子资金转账（EFT）等领域。

DES 算法的基本原理是每次取明文中的连续 64 位数据，通过 64 位密钥，对明文进行 16 轮的替代、移位和异或操作，最终得到转换后的 64 位数据（密文），如图 2-3 所示。连续对明文执行上述过程，最终得到全部明文的密文。

图 2-3 中，一组 64 位的明文块首先经过一个初始置换（IP）后，被分成左半部分和右半部分，每部分 32 位，分别以 L_0 和 R_0 表示。然后经过 16 轮变换，第 i 轮变换结果的左半部分为上一轮变换结果的右半部分，即 $L_i = R_{i\text{-}1}$；第 i 轮变换结果的右半部分为上一轮变换结果的左半部分与上一轮变换结果的右半部分经过函数（算法）f 处理后所得结果的异或，即 $R_i = L_{i\text{-}1} \oplus f(R_{i\text{-}1}, K_i)$，$K_i$ 为第 i 轮变换时的子密钥。经过 16 轮变换之后，左右两部分再连接起来，最后经过一个逆初始置换（IP^{-1}）得到 64 位密文块，算法结束。

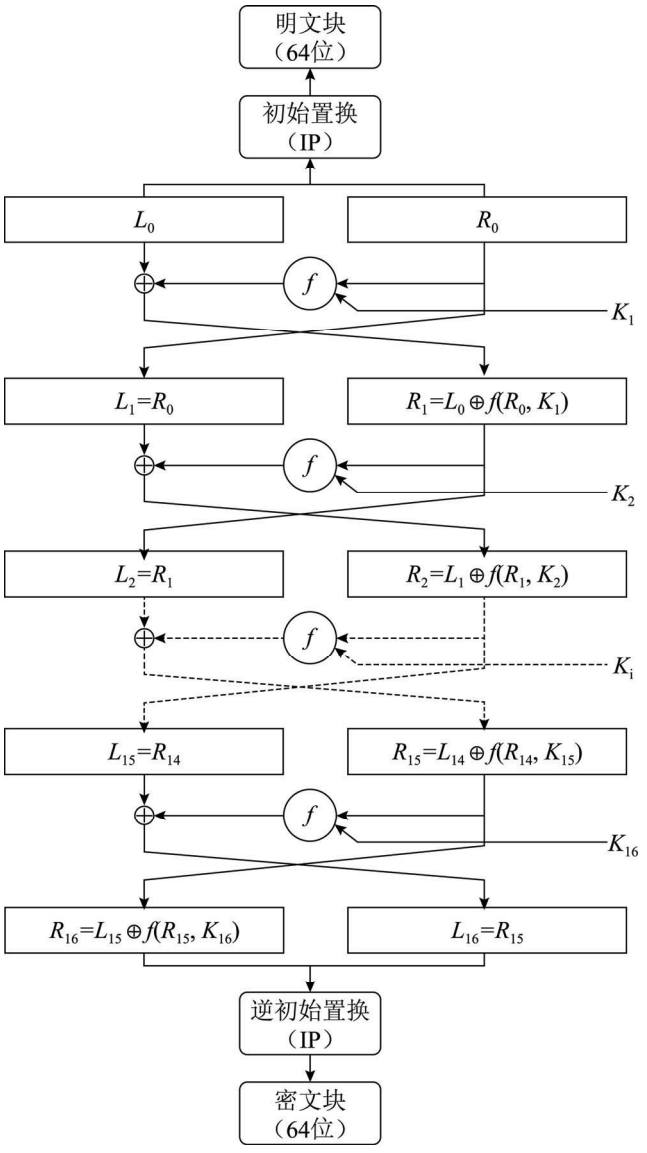

图 2-3　DES 算法原理示意

DES 算法的加密密钥与解密密钥相同，加密算法也与解密算法相同，只是解密时逆向取用加密时所用密钥顺序。加密时第 1～16 轮迭代使用的子密钥顺序是 $k_1, \cdots, k_{16}$，解密时使用的子密钥顺序是 $k_{16}, \cdots, k_1$，产生子密钥时循环移位向右。需要说明的是，64 位密钥中有 8 位是奇偶校验位，所以实际有效密钥长度是 56 位。

DES 算法在密码学的发展过程中具有重要意义，在信息加密方面起了重要作用。但是，进入 20 世纪 90 年代以来，DES 算法的安全性越来越受到了威胁。1997 年，美国科

罗拉多州的程序员 Verser 与 Internet 上数万名志愿者协同工作，用了 96 天时间找到了 DES 密钥；1998 年 7 月，电子前沿基金会（EFF）使用计算机在 56 小时内破译了 DES 密钥；1999 年 1 月，EFF 又只用了 22 小时 15 分钟就宣告破解了 DES 密钥。

DES 算法不再是不可破的，人们加以研究和改进，提出了新的基于分组思想的加密算法，如 3DES 算法、IDEA 算法、RC5 算法、AES 算法等。

2.2.3　非对称密钥密码体制

1．非对称密钥密码体制原理

为了克服对称密钥密码体制存在的问题，密码学专家提出了新的加密体制——非对称密钥密码体制，又称为双钥密码体制或公钥密码体制。非对称密钥密码体制的基本原理是加密和解密采用不同的密钥，使用时其中一个密钥公开，称为公钥；另一个密钥由用户私有保存，称为私钥。传递信息时，发送方用接收方的公钥加密信息，接收方用自己的私钥对信息解密。由于接收方的私钥只有接收方自己知道，因此只要其私钥保存完好，即使信息被截取，截取者也因为没有解密密钥，无法获知信息内容，从而保证了信息的机密性。例如，在电子商务交易过程中，商家可以公开其公钥，保留其私钥；客户用商家的公钥对发送的信息进行加密，安全地传送到商家，然后由商家用自己的私钥进行解密得到原文信息。

非对称密钥密码体制克服了对称密钥密码体制的缺点，解决了密钥的分发和管理问题。另外，非对称密钥密码体制能够实现数字签名技术，解决了参与者身份识别问题，但由于算法复杂，算法的运算速度不高，加密信息的效率降低。

2．RSA 算法

非对称密钥密码体制的典型算法是 RSA 算法。它是由三位发明者 Ron Rivest、Adi Shamir 和 Leonard Adleman 名字的第一个字母组合而成。RSA 算法的基本原理是基于大素数难分解原理，即寻找两个大素数比较简单，而将两个大素数的乘积分解非常困难。

具体算法如下：

①选取两个足够大的质数 p 和 q；

②计算 p 和 q 的乘积，记为 n = p*q；

③计算 p−1 和 q−1 的乘积，记为 m =(p−1)*(q−1)；

④寻找一个与 m 互质的数 e，且满足 1＜e＜m；

⑤寻找一个数 d，使其满足(e*d)mod m = 1；

⑥(n，e)为公钥，(n，d)为私钥。

如果用 M 表示明文，C 表示密文，则

加密过程可表示为：$C=M^e \bmod n$

解密过程可表示为：$M=C^d \bmod n$

传递信息时发送方用接收方的公钥加密信息，接收方用自己的私钥对信息进行解密。

RSA 算法的工作原理可结合一个简单的算例说明。

假设发送方要传送明文 M=19 给接收方，按照 RSA 算法描述，密钥对的生成过程为：

①假设选择两个质数 p=3，q=11；

②计算 n= p*q=33；

③计算 m=(p−1)*(q−1)= 20；

④寻找一个与 m 互质的数 e，且满足 1＜e＜m，取 e=3；

⑤寻找一个数 d，使其满足(e*d)mod m = 1；

此处取 d=7，满足(3*7)mod 20 = 1；

⑥得出公钥(n，e)，即(33，3)；

私钥(n，d)，即(33，7)。

发送方用接收方的公钥加密信息得到密文 $C=M^e \bmod n =19^3 \bmod 33=28$。接收方收到消息后用自己的私钥解密信息得到明文 $M=C^d \bmod n =28^7 \bmod 33=19$。

从所基于的数学难题来讲，RSA 算法基于大整数因子分解系统。除 RSA 算法外，椭圆离散对数系统（ECC）和离散对数系统（代表性算法 DSA）也属于非对称密钥密码体制算法。

2.2.4 数字信封

对称加密技术与非对称加密技术各有利弊，实际应用中，往往扬长避短，将二者结合起来应用。对原文信息采用对称密钥进行加密，再利用非对称密钥加密传递对称密钥。这样既保证了信息传递的安全性，也考虑到了信息加密的时间效率。

以发送方向接收方传递一段交易信息（如电子合同、支付通知单等）为例，发送方先在本地用对称密钥对交易信息进行加密，形成密文；再用接收方的公钥将用于加密交易信息的对称密钥加密，并将加密后的对称密钥信息和密文一同传递给接收方；接收方接收信息后，先用自己的私钥解密加密后的对称密钥信息，得到用于加密交易信息的对称密钥，再用其解密密文得到交易信息原文，其应用示意如图 2-4 所示。

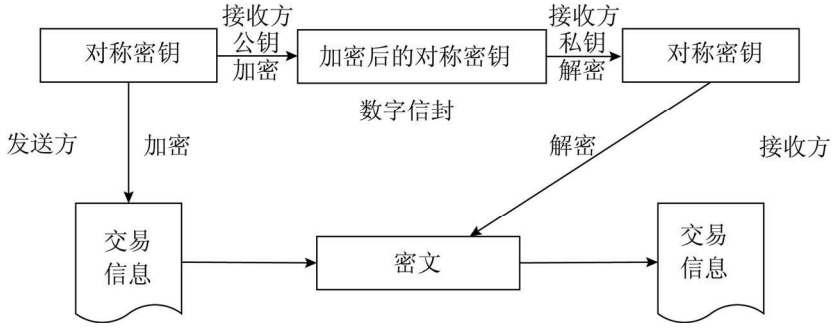

图 2-4 数字信封应用