第 3 章　网络金融安全技术

现代网络金融，许多电子交易和电子支付都是通过网上交易平台和支付平台完成的。由于互联网的开放性和技术上存在的缺陷，加上黑客和病毒的破坏，正常的信息传输常常面临着被非法中断、截取、篡改和伪造的危机。为了保证电子交易、资金汇兑和电子支付的正常进行，保证企业和消费者的利益不受任何损失，保证厂商的重要商业信息、消费者的个人隐私信息不被泄露，需要有安全技术作为保障。其中，作为电子交易和电子支付安全的基础，加密技术起了至关重要的作用。

3.1　网络金融的安全需求

网络金融提供了全新的交易品种和服务方式，通过 Internet 和金融网络，不但能为全球的客户提供丰富的金融信息、简便的交易过程，而且使得交易的成本大为降低。但是，在享受这些好处的同时，人们也碰到了一系列的问题，较为突出的就是有关交易安全的问题。有时，交易系统会遭到各种各样病毒的侵扰、黑客的攻击，导致系统突然崩溃，用户账号被盗，网站页面内容被恶意篡改，偶尔还会产生子虚乌有的合同，等等。在这样的情况下，网络金融业务要能正常地进行下去，必须满足一定的安全需求，具备相应的安全保障。

案例 1　手机在，SIM 卡却被“偷”

2016 年 4 月，一起不同寻常的电信诈骗案吸引了众多的手机安全公司和电信专家的注意，用户回复了一条短信后，手机绑定的网银被盗。最终调查结果显示，这次并非伪基站在“捣鬼”，那骗子是如何得手的呢？

1. 回复验证码短信后网银被洗劫一空

据北京移动用户许先生反映，4 月 8 日，他收到来源为 1065800、10086 的短信提示，说他订阅了某财经杂志的手机报，花费 40 元。许先生以为被运营商摊派业务，在退订的过程中回复了一个 6 位数的校验码之后，自己支付宝、手机绑定的三张银行卡、百度钱包里的所有财产居然被洗劫一空。

2. 骗术过程

手机安全公司和电信专家们对此案进行研究后终于弄清了骗子的诈骗过程。

第一步，掌握手机营业厅账号密码后订购手机报服务。

首先，诈骗嫌疑人在行动前已掌握了许先生的中国移动网上营业厅账号和登录密码，因此可以用许先生的身份订购手机报等服务，如图 3-1 所示。许先生发现自己订购不明业务后便回复 TD 进行退订。

第二步，申请办理“自助换卡”业务。

与此同时，嫌疑人再次利用许先生的账号密码登录中国移动网上营业厅，并办理“自助

换卡”业务。骗子办理“自助换卡”后，中国移动官方系统会给许先生发出短信提示“您的USIM 卡 6 位验证码为××××××”，如图 3-2 所示。

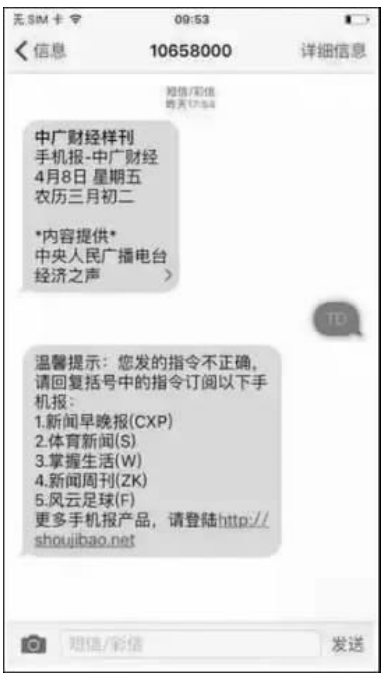

图 3-1　假冒身份订购手机报

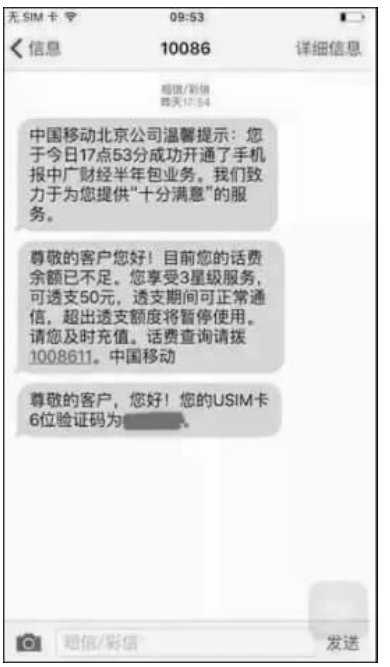

图 3-2　“自助换卡”短信提示

据电信业内人士解释，自助换卡是运营商推广的 4G 业务，客户在网站、手机 APP 上填入姓名、地址、联系方式等信息，运营商就可以将新的 SIM 寄送给客户，收到卡片后按照提示发送短信或验证码，即可开通新的卡片。开通同时旧卡失效，新 SIM 卡插入手机即可享受 4G 服务。

第三步，启用新 SIM 卡转移网银账户钱款

这时骗子再通过中国移动免费邮箱，给许先生发送“退订业务请发送校检码”的短信，因此许先生收到的短信显示来源为 106581390 开头，如图 3-3 所示。许先生一看到“校验码”三个字，就毫不犹豫地把这组数字回复给来源为 106581390 开头的短信。

这时，嫌疑人拿到验证码后完成“自助换卡”，许先生的手机里的 SIM 卡则报废停用。嫌疑人启用 SIM 卡后，可以用自己的手机接收所有许先生的电话、短信信息，然后配合已经获取的支付宝、银行卡账号、身份证信息转移财产。

此案例出现之后，引发了相关思考：

图 3-3　假冒发送“退订业务请发送校检码”的短信

(1) 运营商的业务流程安全吗?

许先生的遭遇让很多人对运营商的业务流程安全性提出质疑。现在人们的手机号大多关联了银行卡、支付宝、微信钱包等至关重要的财产,通过六位校验码就可以完成自助换卡操作,这是否符合电信业务的"可靠性"要求?

对此,中国移动回复:许先生的手机号码是通过海南海口IP、采用客户自设密码登录营业厅,并通过官方系统下发给客户本人手机的验证码换卡成功,业务流程办理正常。

(2) 运营商怎么才能分辨真假?

电信业内人士表示:由于骗子掌握了许先生网上业务大厅的账号和密码,拥有密码最高权限,可以办理包括自助换卡在内的所有业务,因此运营商无法分别真假。

(3) 骗子为什么会掌握到许先生的关键信息?

据许先生介绍,他已半年多未登录手机营业厅官网。手机安全专家认为:可能是用户设置的密码过于简单,或黑客撞库获取了相关信息。

专家介绍:用户经常会在很多平台或网站使用同一个密码,密码一旦在一些安全性较低的网站被黑客盗用,信息就有可能会被放到黑市交易,骗子购买后便会在一些网站进行尝试,得到身份证号、姓名、银行卡等有效信息后再有针对性地对用户进行诈骗。

(4) 如何防范此类诈骗?

① 手机用户收到不了解的业务增订或退订短信,一定要拨打官方客服或去营业厅咨询。

② 手机收到陌生短信及链接切勿轻易点击下载。

③ 骗子会利用伪基站、改号软件等发送短信,用户即使是收到官方客服号码发来的短信也不要轻易相信。

④ 手机卡的补卡换卡业务可通过手机直接办理,并非一定要去营业厅办理,遇到相关问题应提前了解办理流程,以免被骗。

⑤ 保护好个人信息,避免身份证号、银行卡号、密码等敏感信息泄露。

案例2 骗子克隆"公司微信群",女会计被骗85万元

2016年5年14日之前的某天,武汉一家汽车销售公司的会计李女士正在上班,突然发现自己被"董事长"拉进了一个新建的微信工作群里。群内六人都是公司同事,头像、名称也都对得上。"董事长"与"总经理"在群里先是一番热聊。之后,"董事长"发出工作指示,要李女士将公司的85万元转给江苏一名客户。

然而,等李女士打完了款,却发现公司老总就在旁边办公室,压根没有开会。而且,公司老总当面告诉李女士,他没有做出过任何汇款的指示。李女士急忙向警方报案。还好,在银行和警方的通力配合之下,被骗走的85万元当中,有近80万元被拦截了下来。当地警方也已经立案侦查。

1. 骗子行骗的四个关键节点

第一,微信群内的"董事长""总经理"等六位同事,表面看上去,他们的微信头像、名称都对得上,加上"董事长""总经理"等同事在群内讨论工作,这完全是场景模拟,让李女士深信这就是小范围的"内部工作群"。

第二,故意在群里说:"我这边在开会,不方便电话",直接堵死了李女士电话和当面确

认的渠道。

第三，透露与江苏的蒋总（同伙）谈好了合同，并故意告知蒋总的联系方式，叫李女士联系同伙，进一步诱李女士入局。

第四，表明对方也打了保证金到自己的私人账户上。将事先 PS 伪造好的邮件信息和电子版汇款单发给李女士，彻底让她打消疑虑。

2. 详细过程

（1）微信群聊天记录曝光。

2016 年 5 月 6 日，武汉洪山区一公司会计李女士正在上班。突然发现自己被“董事长”拉进了一个新建的微信工作群里，如图 3-4 所示。群内六人都是公司同事，头像、名称都对得上。

在群中，“董事长”与“总经理”等同事进行热聊，讨论工作，进行完全的场景模拟，让李女士深信这就是小范围的“内部工作群”，如图 3-5 所示。

图 3-4　拉进微信工作群

图 3-5　在微信工作群热聊

（2）“董事长”故意在群里说：“我这边在开会，不方便电话，如图 3-6 所示。此举直接堵死了李女士电话和当面确认的渠道。

（3）表明对方也打了保证金到自己的私人账户上。将事先 PS 伪造好的邮件信息和电子版汇款单发给李女士，彻底让她打消疑虑，如图 3-7 所示。

（4）引诱并指示李女士将公司的 85 万元转给江苏一名客户，如图 3-8～图 3-10 所示，并伪造到账信息，如图 3-11 所示。

（5）透露与江苏的蒋总（同伙）谈好了合同，并故意告知蒋总的联系方式，叫李女士联系同伙，进一步诱李女士入局。

图 3-6 “董事长”在微信中的留言

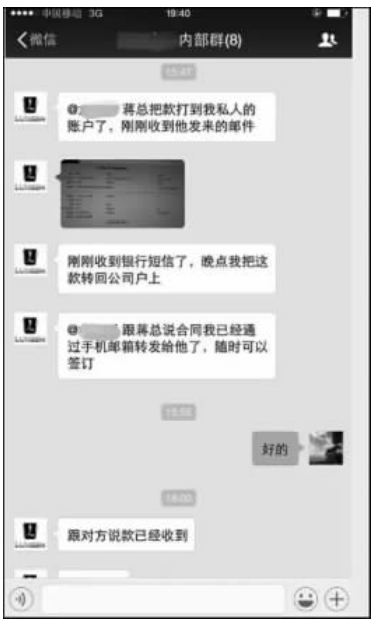

图 3-7 假冒合同保证金已到账

图 3-8 引诱并指示李女士转账(1)

图 3-9 引诱并指示李女士转账(2)

至此，李女士以为圆满完成了领导交代的任务。当天下午 4 时左右，李女士起身外出时，竟然发现董事长在隔壁办公室办公。他不是在外面开会吗？还让我不要打他电话。想到这里，李女士顿时慌了。

图 3-10　引诱并指示李女士转账(3)

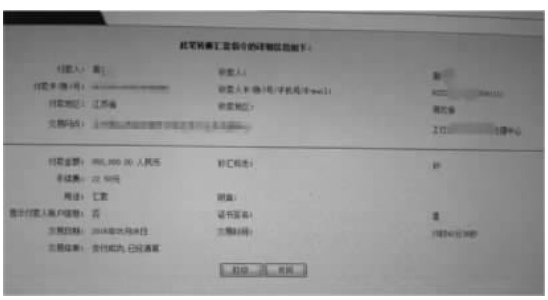

图 3-11　伪造到账信息

(6) 报警后，警察出手追回了近 80 万元。

当天下午 5 时 01 分，在警方介入后，骗子仍在冒充董事长，在微信群点名李女士说道："对方已经收到。"并问："转出这笔后，公司还有多少余款"，如图 3-12 所示。

图 3-12　继续行骗

经调查，该公司是招商银行账户，85 万元巨款已转到江苏的某工商银行账户。当天下午 5 时许，民警带着法律文书与工商银行某支行取得联系，迅速启动冻结程序。由于整个过程十分迅速，骗子仅转走 5 万元并用掉了 9 元手续费，近 80 万元被成功冻结。

案例 3　分不清收款码和付款码，原本进账立刻变成亏损

24 岁的小赵是一名微商，在朋友圈卖化妆品。4 月 24 日上午 11 时 30 分许，一名微信昵称叫“美美”的加了她的微信。一番交谈后，“美美”表示想买一只眼霜，小赵推荐了一款价格是 288 元的眼霜。“美美”同意购买。很快，一单生意就谈妥了。小赵让“美美”通过微信红包将钱汇过来。“美美”称微信转账支付金额超额了，让她发一个二维码，扫码付款。

没多想，小赵就发了一个收款码给她，但“美美”说这不对，让小赵进入微信钱包首页，将付款码的二维码发给她，如图 3-13 和图 3-14 所示。

图 3-13　谎称收款码不对

图 3-14　欺骗索要付款码

“二维码这个我不太懂，就按照她说的发过去了，”小赵说，第一次“美美”说超时，让再发，第二次发过去说网络不好，又发了一次，一共发了三次二维码。

等小赵发完验证码后，再联系“美美”，已经联系不上对方。小赵慌了，此时短信提醒微信绑定的农业银行分三次付款共 1500 元，每次 500 元左右。

相关提示：

（1）当微信支付交易金额小于 1000 元时（支付宝的免密金额是 2000 元），对方通过特定收款工具即可扫描你的付款码扣款，不需要密码。（前提是先展示了自己的付款码，当然，付款码会不断动态更新，被扫过一次后将会失效）。

（2）收款码。

单击微信右上角的“＋”图标，进入“收付款”—“我要收款”，就会出现一个二维码页面，如图 3-15 所示。

图 3-15　收付款下的收款码

属性：二维码。

特点：长期不变。

用途：别人无须加你好友，扫二维码就可以向你转账。

（3）付款码。

单击微信右上角的“＋”图标，进入“收付款”—“向商家付款”或者，打开“钱包”—“付款”，如图 3-16 所示。

属性：由一个条形码＋一个二维码组成。

特点：动态更新。

用途：商家用专用的设备扫一扫，支付过程就完成了。

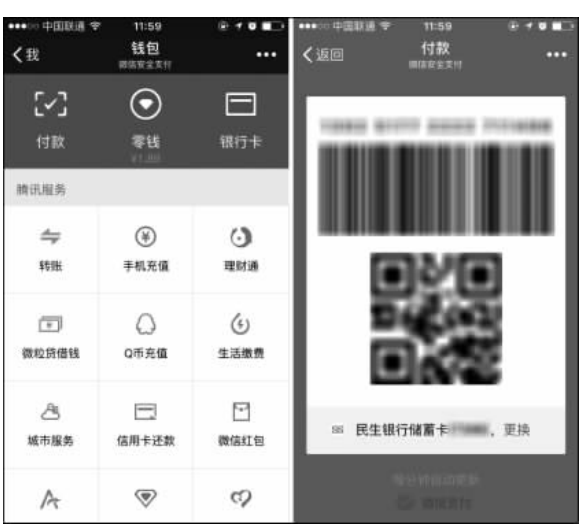

图 3-16　钱包下的付款码

若担心付款码对1000元以内的交易免密支付，建议设置手势密码，这样就算他人拿到你的手机也无法进入钱包进行消费。输入手势密码之后展示出来的条形码＋二维码，可用于向商家付款，但仅限自己使用，切勿截屏分享。

一般来讲，网络金融的安全需求涉及信息安全需求、信用安全需求、管理安全需求和法律保障安全需求这几个方面。只有同时满足了这些安全需求，才能够真正地保障网络金融的顺利实施。但要完全做到这几点，不仅在主观上和客观上存在一定的困难，而且有时也显得没有必要。事实上，在网络金融发展的不同阶段，对网络金融的安全需求也是不一样的。早期对网络金融的安全需求主要是提供计算机安全，也就是要能对信息进行保密，这可以通过加密、访问控制等技术手段解决。之后的网络金融安全需求要求能提供较为全面的信息安全保障，其要解决的问题一是防止不法分子冒名顶替合法交易者参与交易或未经授权地篡改数据；二是防止交易数据丢失或交易数据在通信网络中传输出现问题。此时要求网络金融应具备四个基本安全特性，即数据的保密性、完整性、可用性和身份的确定性。

网络金融发展到今天，其安全需求已不再满足于四个基本安全特性，而是要求更全面的安全保证，包括管理安全和法律保障安全。换句话说，目前对网络金融的安全需求是一个立体的需求，不但要求网络金融能提供数据保密性、完整性、可用性和对交易行为的可控性、身份的真实性等，还要求具备安全的外部交易法律环境，要求制定一系列的有关交易安全的法律法规，以解决管理安全问题和法律保障问题。

总之，除去外部交易环境的安全因素外，网络金融安全应具备以下几个基本特性：

(1) 信息的保密性。

(2) 信息的完整性。

(3) 信息的不可否认性。

(4) 交易者身份的真实性。

(5) 系统的可靠性、可用性、可控性。

3.2 信息的保密性技术

信息的保密性在技术上是通过加密/解密和防火墙等措施来实现的。

3.2.1 加密与解密技术

加密/解密技术是一种用来防止信息泄露的技术。电子商务中的信息在通过 Internet 传送之前，为了防止信息的内容被他人有意或无意地知晓，需要将它的内容通过一定的方法转变成别人看不懂的信息，这个过程就是加密(Encryption)；而将看不懂的信息再转变还原成原始信息的过程称为解密(Decryption)。这里，加密之前的信息称为明文(Plaintext)，加密之后的内容称为密文。加密通常要采用一些算法(对应着加密/解密的程序)，这些算法需要用到不同的参数，这些不同的参数称为密钥，密钥空间是所有密钥的集合。

加密/解密所用方法的种类，按照历史发展阶段可分为手工加密、机械加密、电子机内乱加密、计算机加密四种。手工加密是指以手工完成加解密的过程，或者以简单器具来辅助完成加解密的过程，在第一次世界大战之前主要采用这种加密形式。机械加密是指以机械密

码机或电动密码机来完成加解密过程，它在第一次世界大战到第二次世界大战期间曾得到普遍应用。电子机内乱加密是指通过电子电路，以严格的程序进行逻辑运算，以少量制乱元素来生成大量的加密乱数，最终完成加解密过程。由于制乱是在加解密的过程中完成的，不需要预先制作，所以称其为电子机内乱加密，在 20 世纪 60 年代到 70 年代被广泛应用。计算机加密是指以计算机软件程序来进行加密，程序是公开的，也就是加解密的算法是公开的，密文的保密程度不取决于加密程序，而是取决于加密中用到的参数，即密钥，这种方法适用于对现代计算机中的数据进行保护和通信。

计算机加密方法，按照保密程度来说，又可分为理论上保密的加密、实际上保密的加密、不保密的加密三种类型。对于理论上保密的加密，不管获取多少密文和有多大的计算机计算能力，对明文始终不能得到唯一解，所以也叫理论不可破的加密，如客观随机一次一密的加密就属于这种；而对于实际上保密的加密，虽然在理论上可破，但在现有客观条件下，无法通过计算来确定密码；至于不保密的加密，当获取一定数量的密文后就可以得到所用的密码，如早期的单表代替密码，后来的多表代替密码，以及明文加少量密钥等。

按照密钥使用方式的不同，计算机加密方法通常又分为对称加密和非对称加密两种类型。对称加密是指加密和解密时使用相同的密码，传统的加密都属此类；而非对称加密，在加密和解密时，分别使用两个不同的密码，一个称为公钥，另一个称为私钥。常见的对称加密和非对称加密方法如表 3-1 所示。

表 3-1　常见的对称加密和非对称加密方法

	方　法	描　　述
对称加密	DES	是美国国家标准局 20 世纪 70 年代开发的一种对称加密算法，采用分组乘积密码体制。数据块 64 位，密码长 64 或 56 位
	IDEA	由瑞士苏黎士联邦工业大学的赖学嘉和 James L. Massey 于 1990 年共同提出。数据块 64 位，密码长 128 位
	FEAL	由日本 NTT 公司的清水和宫口设计
	Rijndael(荣代尔)	一种高级的加密标准(AES)，由比利时的 Joan Daemen 和 Vincent Rijmen 提出，用于代替 DES，其数据块长度和密钥长度可分别为 128、192、256
	RC	由 Ron Rivest 于 1987 年设计，密钥长度可变
非对称加密	RSA	由 MIT 的 Ron Rivest、Adi Shamir、Leonard Adleman 于 1978 年提出。安全性基础是数论和计算复杂性理论中的下述论断："求两个大素数($>10^{100}$)的乘积在计算上是容易的，但若要分解两个大素数的积而求出它的因子则在计算上是困难的"
	EL Gamal	1985 年由 EL Gamal 提出，安全性基于"在有限域上计算离散对数比计算指数更高的困难"(DLP)
	背包系统	第一种出现的公开钥加密算法，由 Ralph Merkle 和 Martin Hellman 于 1978 年基于求解背包问题的难解性而提出
	McEliece	1978 年由 McEliece 提出。基于"将一个译码容易的线性码经过变换而伪装成一个译码困难的线性码"原理
	Diffe-Hellman	1976 年出现，安全性基于"在有限域上计算离散对数比计算指数更高的困难"
	椭圆曲线密码(FEE、ECC)	1985 年由 N. Koblitz 和 V. Miller 提出，利用有限域上的椭圆曲线上点集所构成的群，在其上定义离散对数系统。安全性基于"在有限域上计算离散对数比计算指数更高的困难"

3.2.2 对称加密与解密

对称加密也称共享密钥加密或机密密钥加密，收发双方拥有相同的单个密钥，这个密钥既可用于加密，也可用于解密，即加密和解密使用的是相同的密钥，此密钥又称对称密钥或会话密钥。常见的对称加密方法有 DES、DES3、AES、IDEA、RC2、RC4、RC5、Blowfish、CAST、BASE64 等。

DES(Data Encryption Standard)算法是美国政府机关为了保护信息处理中的计算机数据而使用的一种加密方式，是一种对称加密的方法，其历史可以追溯到 1973 年。1973 年，美国国家标准局开始研究国防部门以外的计算机系统数据加密标准，先后于 1973 年 5 月 15 日和 1974 年 8 月 27 日两次向公众发出了征求加密算法的公告。1977 年 1 月，美国政府采纳了 IBM 公司设计的 DES 方案作为非机密数据的正式数据加密标准。目前，DES 算法在国内的 POS、ATM、磁卡及智能卡(IC 卡)、加油站、高速公路收费站等领域被广泛应用，以此来实现关键数据的保密，如信用卡持卡人的 PIN 的加密传输，IC 卡与 POS 间的双向认证、金融交易数据包的 MAC 校验等。

DES 加密的原理如图 3-17 所示，加密之前，先将明文分成若干数据块，每块的大小为 64 位，每块与 64 位的密钥(包含 8 位的奇偶校验，实际有效长度为 56 位)进行 16 轮的循环置换，得到 64 位的密文，将不同的密文块组合起来，得到最终的密文。1997 年 RSA 数据安全公司发起了一项“DES 挑战赛”活动，志愿者四次分别用四个月、41 天、56 个小时和 22 个小时破解了其用 56 位 DES 算法加密的密文。因此，DES 加密算法在计算机速度提升后的今天被认为是不太安全的。

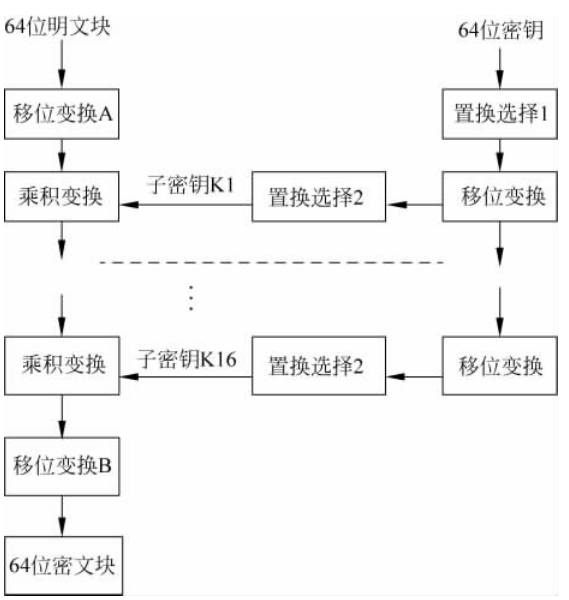

图 3-17 DES 加密原理

DES3 是 DES 算法扩展其密钥长度的一种方法，可使加密密钥长度扩展到 128bit(实际有效位为 112bit)或 192bit(实际有效位为 168bit)。其基本原理是将 128bit 的密钥分为

64bit 的两组，对明文多次进行普通的 DES 加解密操作，从而增强加密强度。

AES(Advanced Encryption Standard)是在 2001 年由 NIST 宣布的一种 DES 后继加密算法。AES 处理以 128bit 数据块为单位的对称密钥加密算法，可以用长为 128 位、192 位和 256 位的密钥加密。NIST 估计如果用能在 1 秒内破解 56bit DES 算法的计算机来破解 128 位的 AES 密密钥，那需要用大约 149 亿万年时间才行。

使用 Openssl 软件，来对某个文件进行 DES3 加密

Openssl 是一个有关安全的自由软件，具有多个版本(可从 www.openssl.org 站点下载)，分别运行在 UNIX、Linux、Windows 平台上。运行在 Windows 平台上的 Openssl 功能主要包括对称加密、非对称加密、SSL 接口及 PKCS 接口(包括 X509 证书、PKCS 标准、ASN.1)等。利用 Openssl 可以直接构建各种有关数据加密和 PKCS 接口的应用，不但如此，用它构建的应用，其加密的强度要比微软(受美国安全产品出口限制)用组件来加密的强度高得多，也安全得多。目前，Openssl 已发展到 0.95 版，功能越来越丰富。

对文件进行加密，其命令为“openssl enc －des －in 明文文件 －out 密文文件”，命令中参数 enc －des 表示用 DES 算法来进行加密。若要进行解密，只需输入命令“openssl enc －des －d －in 密文文件 －out 明文文件”，命令中的参数－d，表示解密。

对称加密具有算法简单、加密与解密的速度较快的特点，能对大量的明文进行加密；但也有一些明显的缺点，最主要的缺点是：由于加解密双方都要使用相同的密钥，因此在发送、接收信息之前，必须完成密钥的分发，密钥不能直接通过网络来传递，在首次通信前，通信方必须通过除网络以外的途径来传递对称密钥给接收方。因而，密钥的分发便成了该加密方法中最薄弱、风险最大的环节，在非对称加密方法出现前，各种基本的手段很难保障安全、高效地完成此项工作。另外，当某个对象需要与多个对象保密通信时，就需要产生多个密钥，因此对密钥的管理难度很大。对称加密是建立在共同保守秘密的基础之上的，在管理和分发密钥的过程中，任何一方的泄密都会造成密钥的失效，因而存在潜在的危险。

3.2.3　非对称加密与解密

对称加密方法遇到了密钥分发管理的难题，不管算法多么优秀，如果密钥在分发时发生泄露，则整个安全将毁于一旦。非对称加密方法则有效地避免了密钥分发的难题。非对称加密方法中使用一对密钥：公钥(Public Key)和私钥(Private Key)组合。用公钥加密的密文只能用私钥解密，反之，用私钥加密的密文只能用公钥解密。在操作过程中，公钥可向外界发布，让其他人知道，私钥则自己保存，只有自己知道。如果 A 要发一份秘密信息给 B，则 A 只需要得到 B 的公钥，然后用 B 的公钥加密秘密信息，此加密的信息只有 B 能用其保密的私钥解密。反之，B 也可以用 A 的公钥加密保密信息给 A。信息在传送过程中，即使被第三方截取，也不可能解密其内容。非对称加密也有许多种方法，常见的有 RSA 加密和椭圆曲线加密等。

RSA(由 Ron Rivest、Adi Shamir 和 Leonard Adleman 三人首创)是一种公开密钥加密方法，其密钥对的产生方法如下：先产生两个足够大的强素数 p、q。可得 p 与 q 的乘积为 $n=p\times q$。由 p 和 q 算出另一个数 $z=(p-1)\times(q-1)$，这里 z 称为 n 的欧拉函数值。然后，再选取一个与 z 互素的奇数 b，称 b 为公开指数；从这个 b 值可以找出另一个值 a，并满

足条件 $b\times a=1\ (mod\ z)$。由此而得到的两组数(n,b)和(p,q,a)分别称为公开密钥和秘密密钥,或简称公钥和私钥。

使用 RSA 密钥来对明文 $x(0\leqslant x<n)$进行加密/解密时,其加密算法为 $y=E(x)=x^b \pmod n$,解密算法为 $D(y)=y^a \pmod n$。

RSA 算法的数学基础

剩余类集合:整数集合 $\mathbf{Z}$ 模正整数 n 得到的剩余类集合 $\mathbf{Z}_n$(或 $\mathbf{Z}/(n)$称为剩余类环,即 $\mathbf{Z}_n=\{[0],[1],[2],\cdots,[n-1]\}$。在剩余类环中,存在两类元素:零因子元素和可逆元因子元素。若 $\alpha,\beta\in\mathbf{Z}_n$ 且 $\alpha,\beta\neq[0]$,有 $\alpha\times\beta\equiv[0] \pmod n$,则称 α(或 β)为零因子元素;若 $\alpha,\beta\in\mathbf{Z}_n$,有 $\alpha\times\beta\equiv[1] \pmod n$,则称 α(或 β)为可逆元因子元素。可以证明,剩余类环 $\mathbf{Z}_n$ 中元素 $a=[a]$为可逆元因子元素当且仅当 $\gcd(a,n)=1$,即 a 与 n 互素。

可逆元集合上的封闭除法运算:若 α,β 属于可逆元集合上的两个元素,则定义 $\alpha/\beta=\alpha\times\beta^{-1}$。

欧拉函数(Euler $\varphi(n)$):当 $n=1$ 时,$\phi(1)=1$;当 $n>1$ 时,$\phi(n)$的值为 $\mathbf{Z}_n$ 集合中与 n 互素的元素的个数。利用欧拉函数可判断可逆元因子的个数。例如:$\phi(8)=4$,$\phi(24)=8$。可以看出,若 p 为素数,则 $\phi(p)=p-1$;若 p、q 为不同的素数,则 $\phi(pq)=(p-1)(q-1)=\phi(p)\phi(q)$;若 p 为素数,则 $\phi(pp)=p(p-1)$;若 $ab\equiv ac \pmod n$且 $\gcd(a,n)=1$,则必有 $b\equiv c \pmod n$。

费马定理(Format Formula):如果 p 为素数,a 是任意一个正整数,a 不能被 p 整除(此时 $\gcd(a,p)=1$),则有 $a^{p-1}\equiv 1 \pmod p$。

欧拉定理(Euler Formula):对任意互素的整数 a 和 n,有 $a^{\phi(n)}\equiv 1 \pmod n$。

可以看出,费马定理是欧拉定理的特例,并且可以证明:若 n 为两个素数 p 和 q 之积(即 $n=pq$),整数 a 和 n 在不互素的情况下,也有 $a^{\phi(n)}\equiv 1 \pmod n$这样的结论成立。

例如,设 $p=11$,$q=13$,则 $n=143$,$\phi(n)=(11-1)(13-1)=120$。再令 $a=11$,$b=11$,这里 $ab\equiv[1] \pmod{\phi(n)}$,则公钥为$(n,b)=(143,11)$,私钥为$(p,q,a)=(11,13,11)$。若对信息 $M=7$ 进行加密,密文 $y=M^b \bmod n=106$;若进行解密,得明文 $x=y^a \bmod pq=7$。

椭圆曲线加密的数学基础

1. 无穷远点(θ)

规定欧氏平面上的两条平行的直线,相交于无穷远点,记为 θ。由此得到欧氏平面上的以下结论:

(1) 直线 L 上的无穷远点只能有一个。

(2) 一组相互平行的直线,有一个公共的无穷远点。

(3) 任何相交的两个直线,有不同的无穷远点。

(4) 全体无穷远点,构成一条无穷远直线。

(5) 无穷远直线和欧氏平面一起,构成射影平面。

2. 齐次坐标

类似在欧氏平面上引入欧氏坐标系,在射影平面中也可以引入齐次坐标系,进而能用代数的方法来研究直线性质。

对于两条直线 L_1 和 L_2，若在欧氏平面上的直线方程为 $\begin{cases} L_1: a_1x+b_1y+c_1=0 \\ L_2: a_2x+b_2y+c_2=0 \end{cases}$，其中，$a_1, b_1$ 不同时为 0，a_2, b_2 也不同时为 0，并设 $D=\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}$，$D_x=\begin{vmatrix} b_1 & c_1 \\ b_2 & c_2 \end{vmatrix}$，$D_y=\begin{vmatrix} c_1 & a_1 \\ c_2 & a_2 \end{vmatrix}$。

(1) 若 L_1 和 L_2 相交于点 $P(x,y)$，则有 $\begin{cases} x=\dfrac{D_x}{D} \\ y=\dfrac{D_y}{D} \end{cases}$，这里 $D\neq 0$。设 $x=\dfrac{X}{Z}$，$y=\dfrac{Y}{Z}$，这里 $Z\neq 0$，则有 $\dfrac{X}{D_x}=\dfrac{Y}{D_y}=\dfrac{Z}{D}$，点 $P(x,y)$ 的齐次坐标即为 $P(X,Y,Z)$ 或 $P(X:Y:Z)$。

(2) 若 L_1 和 L_2 相互平行(即相交于无穷远点 θ)，则 $D=0$，$c_1\neq c_2$。也设 $x=\dfrac{X}{Z}$，$y=\dfrac{Y}{Z}$，代入 L_1、L_2 直线方程，有 $\begin{cases} Z=0 \\ a_1X+b_1Y=0 \end{cases}$，无穷远点的齐次坐标为 $\theta(X,Y,0)$ 或 $\theta(X:Y:0)$。

总之，两条直线在射影平面上的交点坐标为 $P(X,Y,Z)$。当 $Z\neq 0$ 时，有 $\dfrac{X}{D_x}=\dfrac{Y}{D_y}=\dfrac{Z}{D}$；当 $Z=0$ 时，有 $\begin{cases} Z=0 \\ a_1X+b_1Y=0 \end{cases}$。

3. 椭圆曲线

在射影平面上满足方程 $Y^2Z+a_1XYZ+a_3YZ^2=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3$ 的所有点构成的集合，形成了椭圆曲线(又称 Weierstrass 曲线)。

由椭圆曲线方程可知，无穷远点 $\theta(0:1:0)$ 在椭圆曲线上。实际上，椭圆曲线是由欧氏平面上所有满足方程 $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$ 的点和 y 轴上的无穷远点 $\theta(0:1:0)$ 组成的。若 $a_1, a_2, \cdots, a_6\in$ 集合 K，则称椭圆曲线为 K 域上的椭圆曲线。实数域 **R** 上的椭圆曲线 ECC，形状类似于计算一个椭圆周长的方程(故得名)。

1) 椭圆曲线在实数域上的⊕运算

设 L 为实数域 **R** 上的一条直线，与椭圆曲线 ECC 相交(交点为 P,Q,R)或相切(P,Q,R 相同)，如图 3-18 所示。

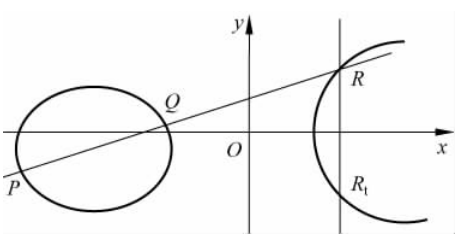

图 3-18　椭圆曲线与直线相交

定义⊕运算为：$P\oplus Q=R_t$，其中 R_t 为直线 $R\theta$(平行于 y 轴)与椭圆曲线 ECC 的交点。

⊕运算的性质：

(1) $\forall P\in \text{ECC}, \forall Q\in \text{ECC}$，有 $P\oplus Q= Q\oplus P$。

(2) $\forall P\in ECC, \forall Q\in ECC, \exists R\in ECC$,使得$(P\oplus Q)\oplus R=\theta$。

(3) $\forall P\in ECC$,有 $P\oplus\theta=\theta\oplus P$。

(4) $\forall P\in ECC$,必定 $\exists P_t\in ECC$,使得 $P\oplus P_t=\theta$。

(5) $\forall P\in ECC, \forall Q\in ECC, \forall R\in ECC$,有$(P\oplus Q)\oplus R=P\oplus(Q\oplus R)$。

由⊕运算性质可知,ECC 对⊕运算形成了一个循环群(Abel 群),其中 θ 为单位元(幺元)。

若 $P(x_1,y_1), Q(x_2,y_2), P\oplus Q=R_t(x_4,y_4)$,则 $\begin{cases}x_4=k^2+a_1k-(a_2+x_1+x_2)\\ y_4=k(x_1-x_4)-y_1-a_1x_4-a_3\end{cases}$,这里 $k=\dfrac{y_2-y_1}{x_2-x_1}(P\neq Q)$ 或 $k=\dfrac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}(P=Q)$。值得一提的是,不仅实数域上的椭圆曲线 ECC 满足这样的条件,其他有限域(如可逆元因子集合)也满足这样的条件。例如,运用此条件公式,可求得椭圆曲线 $y^2=x^3+x+1$ 在 Z_{23} 域上的所有点的集合为{θ,(0,1),(6,19),(3,13),(13,16),(18,3),(7,11),(11,3),(5,19),(19,18),(12,4),(1,16),(17,20),(9,16),(4,0),(9,7),(17,3),(1,7),(12,19),(19,5),(5,4),(11,20),(7,12),(18,20),(13,7),(3,10),(6,4),(0,22)}$=\{\theta,p,p^2,\cdots,p^{27}\}$,这里 $p=(0,1)$。

2) 椭圆曲线加密原理

1985 年,N. Koblitz 和 V. Miller 分别独立提出了椭圆曲线加密的密码体制,其依据是定义在椭圆曲线循环群上的离散对数具有难解的特性。由前面的原理可以看出,设 $p\in ECC$,必有 $p\oplus p\oplus\cdots\oplus p=\theta$(即 $p^t=\theta$),若 p 的周期 t 足够大,则 $p^m=Q$ $(m<t)$;已知 p、m 求 Q 容易,但若已知 P、Q,求 m 却很难。

椭圆曲线加密的过程如下:

在 ECC 上选一个周期很大的点 P,由点 P 生成的循环群点的集合为 $Z_*=\{\theta,P,P^2,\cdots,P^{t-1}\}$,这里 ECC 曲线、点 P 和周期 t 是公开的信息。

(1) 密钥生成:在区间$[1,t-1]$中随机选取一个整数 d,计算 $P^d=Q$,得到公钥(ECC,P,t,Q)和私钥(ECC,P,t,d)。

(2) 用公钥对信息 m 加密:将 m 看作 ECC 域中的一个元素,并在区间$[1,t-1]$内选取一个随机数 k,计算 $P^k=T(x_1,y_1)$,$Q^k=S(x_2,y_2)$;若 $x_2=0$,则重新取一个随机数 k 并计算 T 和 S,直到 $x_2\neq0$ 为止。当 $x_2\neq0$ 时,计算 $c=mx_2$,得到密文$(T(x_1,y_1),c)$。

(3) 用私钥对密文解密:先计算 $T^d=(x_1,y_1)^d=Q(x_2,y_2)$,然后计算 $cx_2^{-1}=m$,这里 m 为明文,x_2^{-1} 为 x_2 的逆元。

目前的公钥密码算法都是基于一些复杂的数学难题,例如目前广泛使用的 RSA 算法就是基于大整数因子分解这一著名的数学难题。公钥密码体系的优点:能适应网络的开放性要求,密钥管理简单,并且可方便地实现数字签名和身份认证等功能,是目前电子商务等技术的核心基础。其缺点是:算法复杂,加密数据的速度和效率较低。因此在实际应用中,通常将对称加密算法和非对称加密算法混合加以使用,利用对称加密算法来进行大容量数据的加密,而采用 RSA 等非对称加密算法来传递对称加密算法所使用的密钥,通过这种方法可以有效地提高加密的效率并能简化对密钥的管理,如图 3-19 所示。

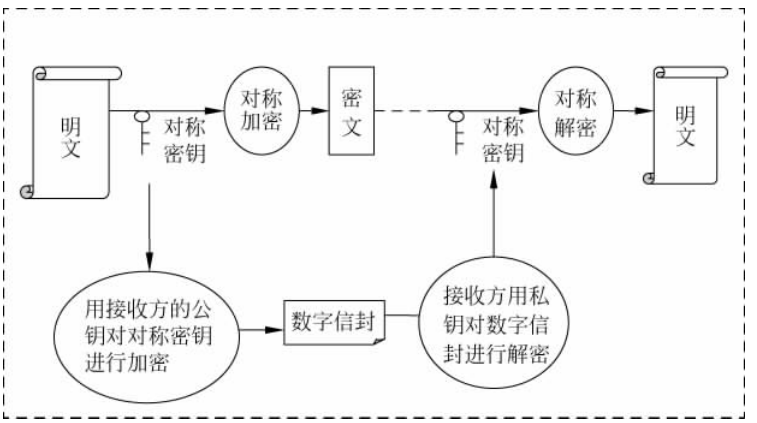

图 3-19　混合加密

使用 Openssl 软件进行加密和解密

首先,使用命令:

```
openssl genrsa -out 密钥存放文件 1024
```

产生长度为 1024 位的一对 RSA 非对称密钥。

有了 RSA 的私钥和公钥,就可以对某个文件进行加密和解密。由于 RSA 算法的复杂性,利用它只能对少量数据内容的文件(一般少于 150 字节)进行加密。RSA 有两种加密方式:

(1) 用公钥加密,以后用私钥解密(加密模式)。

(2) 用私钥加密,以后用公钥解密(签名模式)。

使用命令:

```
openssl rsautl -encrypt -in 明文文件 -inkey 密钥存放文件 -out 密文文件
```

用公钥对明文加密;使用命令:

```
openssl rsautl -decrypt -in 密文文件 -inkey 密钥存放文件 -out 新明文文件
```

用私钥对加密的文件进行解密。

同理,可使用命令:

```
openssl rsautl -sign -in 明文文件 -inkey 密钥存放文件 -out 密文文件
```

用私钥对明文加密;使用命令:

```
openssl rsautl -verify -in 密文文件 -inkey 密钥存放文件 -out 新明文文件
```

用公钥对密文解密。

3.2.4　防火墙技术

实现保密的另外一种方法是进行存取访问控制,对敏感数据的访问实行身份验证,具备合法身份的允许其访问,不合法身份的禁止其访问。防火墙技术正是为实现这一目的而产生的。

“防火墙”是一种形象的说法，其实它是一种计算机硬件和软件的组合，使互联网与内部网之间建立起一个安全网关(Security Gateway)，从而保护内部网免受非法用户的侵入，它其实就是一个把互联网与内部网(通常这局域网或城域网)隔开的屏障，如图 3-20 所示。

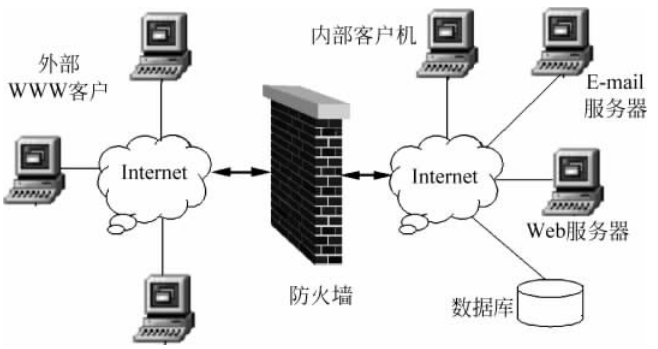

图 3-20 防火墙

防火墙如果从工作原理来看，主要可分为包过滤型和应用网关型两类。包过滤型防火墙可以动态检查通过防火墙的 TCP/IP 报文头中的报文类型、源 IP 地址、目标 IP 地址、源端口号等信息，与预先保存在防火墙中的清单进行对照，按预定的安全策略决定哪些报文可以通过、哪些报文不可以通过。应用型网关使用代理技术，在内部网与外部网之间建立一个单独的子网，该子网有一个代理主机，通过路由器和网关分别与内、外网连接，代理主机对外部和内部用户的网络服务请求进行认证，对于合法用户的服务请求，代理主机则连接内部网与外部网，自己作为通信的中介，外部用户只能获得经过代理的内部网服务，从而保护内部网络资源不受侵害。

防火墙如果从实现方式来看，又分为硬件防火墙和软件防火墙两类，通常软件防火墙属于包过滤型，而硬件防火墙属于应用网关型与包过滤型的综合。硬件防火墙通过硬件和软件的结合来达到隔离内、外部网络的目的，价格较贵，但效果较好，一般小型企业和个人很难实现；软件防火墙采用纯软件的方式，价格很便宜，但这类防火墙只能通过一定的规则来达到限制一些非法用户访问内部网的目的。现有的软件防火墙主要有天网防火墙个人及企业版，Norton 防火墙个人及企业版，以及一些开发杀病毒软件的开发商开发的软件防火墙，如 KV 系列、KILL 系列、金山系列、瑞星系列等。

硬件防火墙又可分为两类，即标准防火墙和双家网关防火墙。标准防火墙系统包括一个 UNIX 工作站，该工作站的两端各接一个路由器进行缓冲。其中一个路由器的接口是外部世界(即公用网)，另一个则连接内部网。标准防火墙使用专门的软件，并要求较高的管理水平，而且在信息传输上有一定的延迟。双家网关 (Dual Home Gateway) 则是标准防火墙的扩充，又称堡垒主机(Bation Host) 或应用层网关(Applications Layer Gateway)，它是一个单个的系统，但却能同时完成标准防火墙的所有功能。其优点是能运行更复杂的应用，同时防止在互联网和内部系统之间建立的任何直接的边界，可以确保数据包不能直接从外部网络到达内部网络，反之亦然。

随着防火墙技术的发展，在双家网关的基础上又演化出两种防火墙配置：一种是隐蔽主机网关方式，另一种是隐蔽智能网关(隐蔽子网)。隐蔽主机网关是当前一种常见的防火

墙配置。顾名思义，这种配置一方面将路由器进行隐蔽，另一方面在互联网和内部网之间安装堡垒主机。堡垒主机装在内部网上，通过路由器的配置，使该堡垒主机成为内部网与互联网进行通信的唯一系统。目前技术最为复杂而且安全级别最高的防火墙是隐蔽智能网关，它将网关隐藏在公共系统之后使其免遭直接攻击。隐蔽智能网关提供了对互联网服务进行几乎透明的访问，同时阻止了外部未授权访问对专用网络的非法访问。一般来说，这种防火墙是最不容易被破坏的。

3.3　数据完整性技术

要保证数据的完整性，技术上可以采用信息摘要的方法或者采用数字签名的方法。与信息摘要相比，数字签名除了能保证完整性外，还能有效防止交易者的交易抵赖，保证交易的不可否认。

信息摘要技术的原理如图 3-21 所示。

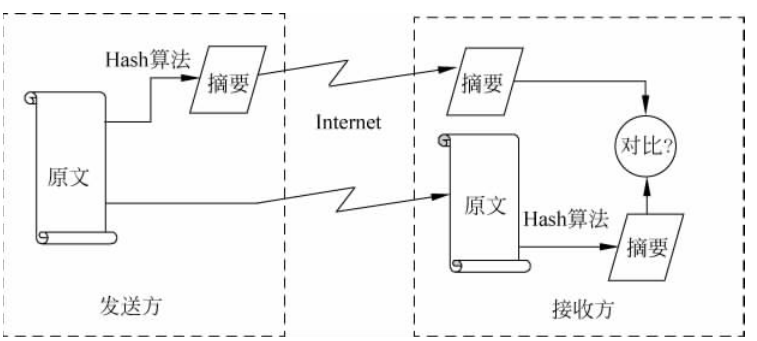

图 3-21　信息摘要

数字摘要采用单向 Hash 函数(如 SHA、MD5 等)对要传送的信息内容进行某种变换运算，得到固定长度的摘要信息，并在传输信息时将它一起送给接收方；接收方收到文件后，用相同的方法进行变换运算，若得到的结果与发送来的摘要信息相同，则可断定信息在传送的过程中未被篡改，反之亦然。在 Openssl 软件中，可使用命令：

```
openssl  dgst  -md5  -out 存放摘要的文件  文件
```

来产生数字摘要。

3.4　不可否认技术

要达到不可否认的目的，可以采用数字签名和数字时间戳等技术。

3.4.1　数字签名

日常生活中，通常用对某一文档进行签名来保证文档的真实有效性，防止其抵赖。在网

络环境中,可以用电子数字签名作为模拟。

把 Hash 函数和公钥算法结合起来产生的数字签名如图 3-22 所示。可以在提供数据完整性的同时保证数据的不可抵赖。完整性保证传输的数据没有被修改,而不可抵赖则保证了是由确定的对象产生的 Hash,而不是由其他人假冒的,自己不可否认。

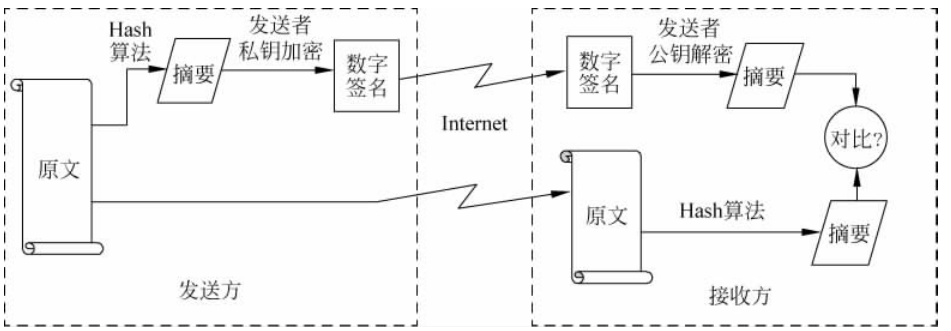

图 3-22 数字签名

在 Openssl 软件中,可使用命令:

```
openssl  dgst -md5  -out 数字签名文件  -sign 密钥文件  需签名的文件
```

来对原件进行签名;使用命令:

```
openssl  dgst -md5  -signature 数字签名文件  -prverify  密钥文件  需验证的文件
```

来对已签名的文件进行验证。

3.4.2 数字时间戳

在电子交易合同中,文件签署的日期和签名一样均是防止文件被伪造和篡改的关键性内容。而在电子交易中,同样需要对交易文件的日期和时间信息采取安全措施,而数字时间戳就能提供电子文件发表时间的安全保护。数字时间戳(DTS)是网络安全服务项目,由专门的机构提供。时间戳是一个经加密后形成的凭证文档,它包括三个部分:需加时间戳的文件的摘要、DTS 收到文件的日期和时间、DTS 的数字签名,如图 3-23 所示。

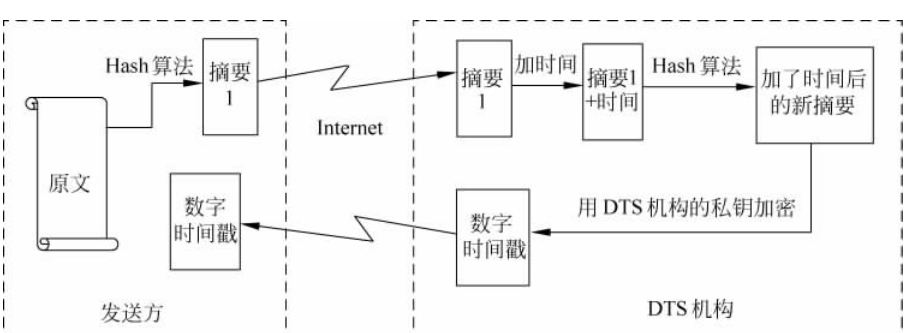

图 3-23 数字时间戳

3.5　身份认证技术

在电子商务的过程中，尤其在交易支付过程中，参与各方必须要能在网上表明自己的真实身份，防止身份的假冒，需要借助于数字证书的技术，设立安全认证中心，制定一系列的安全协议等来实现。

3.5.1　数字证书

数字证书(Digital Certificate)是一种权威性的电子文档，提供了一种在 Internet 上验证身份的方式，其作用类似于司机的驾驶执照或日常生活中的身份证。它利用数字签名技术由一个权威机构——CA 证书认证(Certificate Authority)中心签发。在数字证书认证的过程中，证书认证中心(CA)作为权威的、公正的、可信赖的第三方，其作用是至关重要的。

数字证书概念最早由 MIT 的 Kohnfelder 于 1978 年在他的本科毕业论文中提出，内容是通过数字签名来保护命名的证书(名字/密钥对)，从而可将公钥分散存放和访问，克服将公钥集中存放到一个数据库中而带来的访问性能问题，因此，数字证书除了可用于网上证明交易者的身份，还有另外一个作用，可以利用它来分发交易者的公钥。

数字证书必须具有唯一性和可靠性。为了达到这一目的，需要采用很多技术来实现。通常，数字证书采用公钥体制，即利用一对互相匹配的密钥进行加密、解密。每个用户自己设定一个特定的仅为本人所有的私有密钥(私钥)，用它进行解密和签名；同时设定一个公共密钥(公钥)并由本人公开，为一组用户所共享，用于加密和验证签名。当发送一份保密文件时，发送方使用接收方的公钥对数据加密，而接收方则使用自己的私钥解密，这样信息就可以安全无误地到达目的地了。通过数字的手段保证加密过程是一个不可逆过程，即只有用私有密钥才能解密。公开密钥技术解决了密钥发布的管理问题，用户可以公开其公开密钥，而保留其私有密钥。

数字证书颁发过程一般为：用户向注册中心提出申请，注册中心首先为用户产生密钥对，然后生成一个称为 csr(数字证书请求)的文件，内含公钥及部分用户身份信息；认证中心收到注册中心的 csr 文件后，执行一些必要的核实步骤，以确信请求是真实的，然后进行签名，生成数字证书。这样该证书内包含有用户的个人信息和他的公钥信息，同时还附有认证中心的签名信息。数字证书各不相同，可用于不同的目的，每种证书可提供不同级别的可信度。

目前的数字证书按用途可分为个人数字证书、服务器数字证书、代码签名证书；按证书的格式可分为 X.509、PGP、SDSI/SPKI、X9.59(AADS)、AC 等类型的证书；按证书所用于的协议可分为 SSL 证书(服务于银行对企业或企业对企业的电子商务活动)、SET 证书(服务于持卡消费、网上购物)等。SSL 证书通过公开密钥可证明持证人的身份，而 SET 证书则是通过公开密钥，证明了持证人在指定银行确实拥有该信用卡账号，同时也证明了持证人的身份。常见的 X.509 数字证书，其内容含有数字证书的版本号、数字证书的序列号、证书拥

有者的姓名、证书拥有者的公钥、公钥的有效期、颁发数字证书的单位、颁发数字证书单位的数字签名等。

下面是一个 X.509 数字证书的数据结构：

```
        Version: 3 (0x2)
        Serial Number: 288 (0x120)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C = CN, ST = SH, L = sh, O = usst, OU = Certification Services Division, CN =
MyCa/emailAddress = myca@sh.cn
        Validity
            Not Before: Jun 8 12:12:36 2005 GMT
            Not After : Jun 8 12:12:36 2006 GMT
        Subject: CN = User/emailAddress = zhang_bm@citiz.net
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:ca:87:bb:d8:b0:6e:15:30:73:5a:c0:6e:f5:49:
                    42:c7:26:38:15:d8:74:6c:a3:f0:a2:91:12:fb:4a:
                    1e:88:73:d4:1b:f1:b7:5a:64:41:0a:ae:57:d6:d9:
                    31:a7:3c:08:18:4c:c4:8a:52:47:bd:84:be:1a:f7:
                    9b:a0:dd:5f:64:40:98:ee:05:93:93:19:4d:c2:63:
                    59:76:29:92:1d:ba:5b:5e:ce:d9:b0:0b:b4:d7:fe:
                    41:34:f2:6e:e3:27:e3:c1:1f:e3:f0:17:ce:82:10:
                    85:47:a8:d0:97:de:c4:cd:65:2d:8a:3a:49:4c:1e:
                    ac:e9:b2:00:ae:c1:c5:ae:cb
                Exponent: 65537 (0x10001)
            X509v3 extensions:
            X509v3 Subject Alternative Name:
                email:zhang_bm@citiz.net
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Authority Key Identifier:
                keyid:69:9B:A8:8A:93:8C:68:8D:38:16:ED:80:36:BF:91:CE:AE:3F:C9:DC
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, E-mail Protection
    Signature Algorithm: md5WithRSAEncryption
        14:11:27:83:10:bf:bd:35:43:71:dc:04:e4:9d:8f:de:2a:a8:
        3e:1e:8e:51:39:97:5b:a0:17:ae:2b:c9:3a:52:e5:19:91:69:
        26:99:a3:b5:ac:e1:13:a8:dd:80:f4:0e:99:6f:99:cd:50:91:
        59:9a:ec:f9:a1:4a:a9:1a:4e:d5
```

在浏览器窗口中，选择“工具”→“Internet 选项”命令，在“Internet 选项”对话框中，单击选项卡“内容”下的“证书”按钮，在出现的。证书对话框中将会看到若干数字证书，任选一个数字证书，将会看到如图 3-24 所示的数字证书的具体内容。

图 3-24　一个数字证书

3.5.2　认证中心

认证中心(Certificate Authority,CA)作为电子交易中受信任的第三方,负责为网络金融环境中各个实体颁发数字证书,以证明各实体身份的真实性,并负责在交易中检验和管理证书;数字证书的用户拥有自己的公钥/私钥对。证书中包含有证书主体的身份信息、其公钥数据、发证机构名称等。发证机构验证证书主体为合法注册实体后,就对上述信息进行数字签名,形成证书。在公钥证书体系中,如果某公钥用户需要任何其他已向 CA 注册的用户的公钥,可直接向该用户索取证书,而后用 CA 的公钥解密即可得到认证的公钥;由于证书中已有 CA 的签名来实现认证,攻击者不具有 CA 的签名密钥,很难伪造出合法的证书,从而实现了公钥的认证性。数字证书认证中心是整个网上电子交易安全的关键环节,是电子交易中信赖的基础。它必须是所有合法注册用户所信赖的具有权威性、信赖性及公正性的第三方机构。

CA 的核心功能就是发放和管理数字证书。概括地说,CA 的功能主要有证书发放、证书更新、证书撤销和证书验证。具体描述如下:

(1) 接收验证用户数字证书的申请。

(2) 确定是否接受用户数字证书的申请,即证书的审批。

(3) 向申请者颁发(或拒绝颁发)数字证书。

(4) 接收、处理用户的数字证书更新请求。

(5) 接收用户数字证书的查询、撤销。

(6) 产生和发布证书的有效期。

(7) 数字证书的归档。

(8) 密钥归档。

(9) 历史数据归档。

VeriSign是最大的公共CA，也是最早广泛推广PKI并建立公共CA的公司之一。VeriSign除了是公认的最可信公共CA之一，还提供专用PKI工具，包括称为OnSite的证书颁发服务，这项服务充当了本地CA，而且连接到了VeriSign的公共CA。国内常见的认证中心有中国金融认证中心、中国商务在线、北京数字证书认证中心等。

中国金融认证中心(China Financial Certification Authority，CFCA)，是经中国人民银行和国家信息安全管理机构批准成立的国家级权威的安全认证机构，是重要的国家金融信息安全基础设施之一，成立于2000年6月29日。2004年底，CFCA建成了“国家金融安全认证系统”，为网上银行、电子商务、电子政务等金融机构、税务、政府机关和大企业集团提供第三方安全认证服务。

3.5.3 安全协议

要保障电子商务的安全可靠，除了需要依靠上述的一些基本的安全技术外，还需要制定一系列的安全规范，只有依据这些规范，系统与系统之间才能更好地协调工作，安全才能有所保障，这些规范就是所谓的安全协议。常用的安全协议有安全套接层协议、安全电子交易协议、安全超文本传输协议、安全多媒体Internet邮件扩展协议等。

1. 安全套接层协议

安全套接层(Secure Sockets Layer，SSL)协议最初是由Netscape Communication公司设计开发的，主要用于提高应用程序之间的数据的安全系数。SSL协议的整个概念可以被总结为：一个保证任何安装了安全套接字的客户和服务器间事务安全的协议，它涉及所有TC/IP应用程序。

SSL安全协议主要提供三方面的服务：一是用户和服务器的合法性认证。认证用户和服务器的合法性，使得它们能够确信数据将被发送到正确的客户机和服务器上。客户机和服务器都有各自的识别号，这些识别号由公开密钥进行编号，为了验证用户是否合法，安全套接层协议要求在握手交换数据进行数字认证，以此来确保用户的合法性。二是加密数据以隐藏被传送的数据。安全套接层协议所采用的加密技术既有对称密钥技术，也有公开密钥技术。在客户机与服务器进行数据交换之前，交换SSL初始握手信息，在SSL握手信息中采用各种加密技术对其加密，以保证其机密性和数据的完整性，并且用数字证书进行鉴别。这样就可以防止非法用户进行破译。三是保护数据的完整性。安全套接层协议采用Hash函数和机密共享的方法来提供信息的完整性服务，建立客户机与服务器之间的安全通道，使所有经过安全套接层协议处理的业务在传输过程中能全部完整准确无误地到达目的地。

需要说明的是，安全套接层协议是一个保证计算机通信安全的协议，对通信对话过程进行安全保护。例如，一台客户机与一台主机连接上了，首先是要初始化握手协议，然后就建立了一个SSL。对话进段。直到对话结束，安全套接层协议都会对整个通信过程加密，并且检查其完整性。这样一个对话时段算一次握手。而HTTP协议中的每一次连接就是一次握手，因此，与HTTP相比，安全套接层协议的通信效率会高一些。

安全套接层协议的通信过程如下：

(1) 接通阶段：客户通过网络向服务商打招呼，服务商回应。

(2) 密码交换阶段：客户与服务器之间交换双方认可的密码，一般选用RSA密码算法，也有的选用Diffie-Hellmanf和Fortezza-KEA密码算法。

(3) 会谈密码阶段：客户与服务商间产生彼此交谈的会谈密码。

(4) 检验阶段：检验服务商取得的密码。

(5) 客户认证阶段：验证客户的可信度。

(6) 结束阶段，客户与服务商之间相互交换结束的信息。

当上述动作完成之后，两者间的资料传送就会加密，另外一方收到资料后，再将编码资料还原。即使盗窃者在网络上取得编码后的资料，如果没有原先编制的密码算法，也不能获得可读的有用资料。

发送时信息用对称密钥加密，对称密钥用非对称算法加密，再把两个包绑在一起传送过去。接收的过程与发送正好相反，先打开有对称密钥的加密包，再用对称密钥解密。

在电子商务交易过程中，由于有银行参与，按照 SSL 协议，客户的购买信息首先发往商家，商家再将信息转发银行，银行验证客户信息的合法性后，通知商家付款成功，商家再通知客户购买成功，并将商品寄送客户。

SSL 协议是国际上最早应用于电子商务的一种网络安全协议，至今仍然有很多网上商店使用。在传统的邮购活动中，客户首先寻找商品信息，然后汇款给商家，商家将商品寄给客户。这里，商家是可以信赖的，所以客户先付款给商家。在电子商务的开始阶段，商家也是担心客户购买后不付款，或使用过期的信用卡，因而希望银行给予认证。SSL 协议正是在这种背景下产生的。

SSL 协议运行的基点是商家对客户信息保密的承诺。但在上述流程中也可以注意到，SSL 协议有利于商家而不利于客户。客户的信息首先传到商家，商家阅读后再传至银行，这样，客户资料的安全性便受到威胁。商家认证客户是必要的，但整个过程中，缺少了客户对商家的认证。在电子商务的开始阶段，由于参与电子商务的公司大都是一些大公司，信誉较高，这个问题没有引起人们的重视。随着电子商务参与的厂商迅速增加，对厂商的认证问题越来越突出，SSL 协议的缺点完全暴露出来。SSL 协议将逐渐被新的电子商务协议(如 SET)所取代。

2. 安全电子交易协议

在开放的因特网上处理电子商务，保证买卖双方传输数据的安全成为电子商务的重要问题。为了克服 SSL 协议的缺点，满足电子交易持续不断地增加的安全要求，达到交易安全及合乎成本效益的市场要求，VISA 国际组织及其他公司(如 Master Card、Micro Soft、IBM 等)共同制定了安全电子交易(Secure Electronic Transaction，SET)协议。这是一个为在线交易而设立的一个开放的、以电子货币为基础的电子付款系统规范，它采用公钥密码体制和 X.509 数字证书标准，主要应用于 B2C 模式中保障支付信息的安全性。SET 在保留对客户信用卡认证的前提下，又增加了对商家身份的认证，这对于需要支付货币的交易来讲是至关重要的。由于设计合理，SET 协议得到了许多大公司和消费者的支持，已成为全球网络的工业标准，其交易形态将成为未来“电子商务”的规范。

SET 协议比 SSL 协议复杂，因为前者不仅加密两个端点间的单个会话，而且可以加密和认定三方间的多个信息。

SET 主要使用电子认证技术，其认证过程使用 RSA 和 DES 算法，因此，可以为电子商务提供很强的安全保护。由于安全电子交易规范是由信用卡发卡公司参与制定的，一般认为，安全电子交易规范的认证系统是有效的。当一位供货商在计算机收到一张有 SET 签证

的订单时，供货商就可以确认该订单背后是有一张合法的信用卡支持，这时他就能放心地接下这笔生意；同样，由于有 SET 作保障，发出订单的客户也会确认自己是在与一个诚实的供货商做买卖，因为该供货商受到万事达或维莎发卡组织的信赖。

SET 协议要达到的目标主要有五个：

（1）保证电子商务参与者信息的相互隔离。客户的资料加密或打包后边过商家到达银行，但是商家不能看到客户的账户和密码信息。

（2）保证信息在因特网上安全传输，防止数据被黑客或被内部人员窃取。

（3）解决多方认证问题，不仅要对消费者的信用卡认证，而且要对在线商店的信誉程度认证，同时还有消费者、在线商店与银行间的认证。

（4）保证了网上交易的实时性，使所有的支付过程都是在线的。

（5）规范协议和消息格式，促使不同厂家开发的软件具有兼容性和互操作功能，并且可以运行在不同的硬件和操作系统平台上。

SET 安全协议的工作原理主要包括以下七个步骤：

（1）消费者利用已有的计算机通过因特网选定物品，并下电子订单。

（2）通过电子商务服务器与网上商场联系，网上商场做出应答，告诉消费者的订单的相关情况。

（3）消费者选择付款方式，确认订单，签发付款指令（此时 SET 介入）。

（4）在 SET 中，消费者必须对订单和付款指令进行数字签名，同时利用双重签名技术保证商家看不到消费者的账号信息。

（5）在线商店接受订单后，向消费者所在银行请求支付认可，信息通过支付网关到收单银行，再到电子货币发行公司确认，批准交易后，返回确认信息给在线商店。

（6）在线商店发送订单确认信息给消费者，消费者端软件可记录交易日志，以备将来查询。

（7）在线商店发送货物或提供服务，并通知收单银行将钱从消费者的账号转移到商店账号，或通知发卡银行请求支付。

3.6 PKI 技术

为解决 Internet 和网络金融的安全问题，世界各国对其进行了多年的研究，初步形成了一套完整的解决方案，即目前被广泛采用的 PKI（Public Key Infrastructure）体系结构。PKI 体系结构采用证书来管理公钥，通过第三方的可信机构 CA，把用户的公钥和用户的其他标识信息（如名称、E-mail、身份证号等）捆绑在一起，来验证网上用户的身份。同时，在 PKI 体系结构中，通过使用 SSL 协议和 SET 协议，实现密钥的自动管理，并保证数据的机密性、完整性。

从广义上讲，所有提供公钥加密和数字签名服务的系统都可称为 PKI 系统。PKI 的主要目的是通过自动管理密钥和证书，为用户建立起一个安全的网络运行环境，使用户在多种应用环境下能方便地使用加密和数字签名技术，从而保证数据的机密性、完整性、有效性。一个典型、完整、有效的 PKI 应用系统至少应具有以下部分：公钥密码证书管理、黑名单的发布和管理、密钥的备份和恢复、自动更新密钥、自动管理历史密钥、支持交叉认证。为此，

由 RSA 实验室牵头制定了一个 PKCS 标准(Public-Key Cryptography Standard,公开钥密码标准)。PKCS 共包括 15 个标准,如表 3-2 所示。

表 3-2　PKCS 标准

标准名	说　明
PKCS#1	RSA Cryptography Standard RSA 密码标准
PKCS#2	已合并入 PKCS#1
PKCS#3	Diffie-Hellman Key Agreement Standard DH 密钥交换标准
PKCS#4	已合并入 PKCS#1
PKCS#5	Password-Based Cryptography Standard 基于口令的密码标准
PKCS#6	Extended-Certificate Syntax Standard 证书扩展语法标准
PKCS#7	Cryptography Message Syntan Standard 密文信息语法标准
PKCS#8	Private-Key Information Syntax Standard 私钥信息语法标准
PKCS#9	Selected Attribute Types 属性种类
PKCS#10	Certification Request Syntax Standard 认证请求语法标准
PKCS#11	Cryptographic Token Interface Standard 密码令牌接口标准
PKCS#12	Personal Information Exchange Syntax Standard 个人信息交换语法标准
PKCS#13	Elliptic Curve Cryptography Standard 椭圆曲线密码标准
PKCS#14	Random Number Generation Standards 伪随机数生成标准
PKCS#15	Cryptography Token Information Format Standard 密码令牌信息格式

由于 PKI 体系结构是目前比较成熟、完善的 Internet 网络安全解决方案,国外的一些大的网络安全公司纷纷推出一系列的基于 PKI 的网络安全产品,如美国的 Verisign、IBM、Entrust 等安全产品供应商为用户提供了一系列的客户端和服务器端的安全产品,为电子商务的发展提供了安全保证,为电子商务、政府办公网、EDI 等提供了完整的网络安全解决方案。PKI 安全结构如图 3-25 所示。

图 3-25　PKI 安全结构

3.7 口令身份验证

网上交易者身份的识别，除了使用数字证书之外，还可使用口令验证的方法。利用口令来验证身份是一种较为传统的方法，在交易过程中普遍使用。

3.7.1 常规口令验证

最早的口令验证出现在网络诞生之前，口令是以明文方式表达的，用于计算机用户访问单机系统。后来，这种技术又被广泛用于网络的远程访问。用户访问时，系统出现提示符，用户遵照要求输入自己的用户名和口令，系统查看用户账号数据库，如果输入的用户名和口令与数据库中的内容相匹配，系统就允许该用户访问。

常规口令验证的过程分为三步：首先，用户将口令传送给计算机，计算机完成口令单向函数值的计算，并将单向函数值和存储在后台文件或数据库中的值进行比较，若相符则说明口令正确，否则口令不正确。常规口令验证机制具有自身的弱点：口令不能随着时间的变化而发生随机的改变，具有弱鉴别特性，因而容易产生许多问题，如外部泄露、被猜测、通信过程中被窃取、被重放，甚至危及验证的主机或数据库的安全。

为了防止发生以上这些安全问题，除了需要加强教育和严密组织管理外，还要求口令定期进行更改，口令的长度和内容应满足一定要求。为了防止口令被非法程序进行猜测和非法截取，在口令验证的过程中应插入实时延迟，并对口令进行变换（如进行散列变换）。另外，为了防止含有口令的信息包的网络重放，每次验证时，验证者都应发送随机的验证码，以增加口令验证时的不可预测性和不重复性。

3.7.2 动态口令验证

常规口令验证方法由于其本身的弱点，或多或少会存在一些安全隐患。相比较而言，动态口令（又称一次性口令）是一种更为安全的身份验证方法，近年被广泛使用。

动态口令的基本特征是：在应用过程中，用户必须持有一个用于产生动态口令的设备，用设备产生动态口令后，交给应用系统，再由应用系统转交给认证系统进行认证。这样可有效地防止信息重放、信息窃取和危及验证者的事故发生。目前，基于使用方式的不同，动态口令主要有三种工作模式：基于时间同步机制、基于事件同步机制、基于提问/应答（异步）机制。

1. 基于时间同步机制的动态口令

在这种工作模式中，客户手中掌握着一个令牌卡，里面装有微处理器芯片、有时钟和电源。令牌的形状有多种，如图 3-26 所示。在客户端以时间作为变量，使用对称密钥，进行密码运算，得出一个结果，称为伪随机数，长度可为 128 位。为了操作方便，只截取一定的位数（如 8 位十进制数），显示在令牌卡的液晶屏上，这就是动态口令。用户读取这 8 位数字后，把它输入终端，传给认证服务器。认证服务器使用同样的对称密钥，对时间加密形成另一个

伪随机数。显然，因为双方的时间是同步的，两个伪随机数也会相同，认证服务器截取 8 位数字后把它与收到的动态口令进行比较，如果相同，这就实现了认证。黑客或非法程序因为不掌握相同的密钥，产生不出正确的伪随机数和口令，也就通不过认证。而如果靠窃听截获了这个动态口令，想用它来通过下一次认证，也是无法得逞的。因为下一次认证的时间变量已经改变，密码运算得到的伪随机数和动态口令也变了，上一次的口令已经作废了。

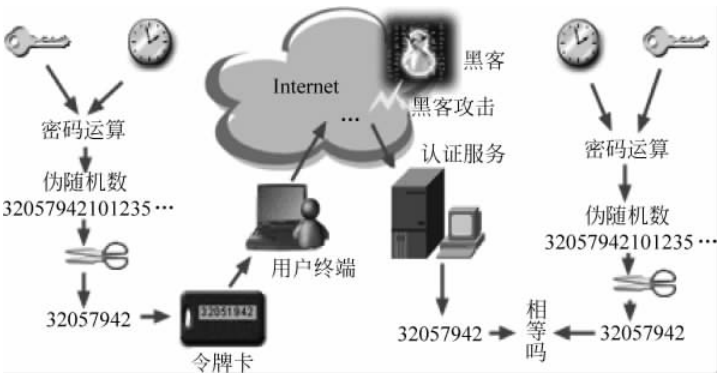

图 3-26　时间同步机制的动态口令

2. 基于事件同步机制的动态口令

在这种工作模式中，通过执行一个 n 次的单向函数来对口令进行变换，用户每登录一次，n 的值就减 1，这样每次产生的变换口令都不相同。由于在验证者处保存了 n 的值和最后一次使用的变换口令，因而正常情况下能够正确地进行验证。若产生变换口令的 n 值与验证者处保存的 n 不一致，则也就通不过认证。

3. 基于提示/应答机制的动态口令

在这种工作模式中，每次由认证系统给出一个挑战数，客户将挑战数输入客户端设备后产生一个应答数，应答数传送给认证系统，由认证系统来判断其真伪。

以上三种模式的动态口令，其后台的认证系统结构非常类似，功能也基本相同，提供着同一级别的安全认证管理。但三种模式的客户端则有着较大的不同。对于时间同步机制，由于以时间做变量，因此客户端设备必须具有时钟，从而对设备精度要求高，成本高，耗电量大，应用模式单一，很难支持双向认证及“数字签名”等应用需求。对于提示/应答机制，由于挑战数是由认证系统提出，客户端设备将挑战数输入后产生应答数，因此应用模式可设计得较丰富，可支持不同的应用需求，如双向认证、数字签名等。但由于需要运算，因此客户端设备必须具备运算功能，同样难以降低成本，而且由于其认证步骤复杂，对旧的应用系统的改造工作量很大。而对于事件同步机制，由于这一机制与应用逻辑相吻合（都是以次数为计算单位），因此客户端的设备设计简单，在使用动态口令表时甚至可不需要运算设备，成本极低，并可支持丰富的应用需求。

习题与思考

1. 计算机加密有何特点？
2. 身份验证有哪些常用的方法？
3. 何谓数字信封？何谓数字摘要？何谓数字签名？
4. 搜寻有关资料，了解双重签名的原理。
5. 收集有关资料，了解网上银行系统所采用的安全协议？