Sādhanā Vol. 30, Parts 2 & 3, April/June 2005, pp. 89–117. © Printed in India

Building blocks of e-commerce

V RAJARAMAN

Supercomputer Education & Research Centre, Indian Institute of Science, Bangalore 560 012, India
e-mail: rajaram@serc.iisc.ernet.in

Abstract. This article examines the architecture of e-commerce as a set of layers, each supporting the one above it. The layers have clean interfaces, that is, they can be designed independently. We present an architecture with six layers. The lowest layer consists of a physical communication network such as local area network or public switched telephone networks. The next higher layer is the logical layer which describes the protocol used to interconnect communication systems to create internet, intranet and extranet. The services provided over the internet infrastructure, namely, e-mail, world wide web etc., are described in what is called network services layer. It is essential to ensure security of messages, documents etc., which are transmitted using network services. The messaging layer is thus concerned with encryption methods, both private and public key encryption and their applications. We call the layer above this the middleman service, which is concerned with value-added services offered by intermediaries to enable payment for services received, certify digital signatures, safely transmit documents and provide information on behalf of companies. The topmost layer is the application layer which users see. The major applications are customer-to-business (C2B) e-commerce, business-to-business (B2B) e-commerce, customer-to-consumer (C2C) e-commerce etc. We briefly explain these modes.

Keywords. e-Commerce architecture; network services; e-commerce security; encryption; digital signature; information technology act.

1. Introduction

A major revolution has taken place during the last five years in the way business is done. This revolution is primarily due to the convergence of computers and telecommunication technologies and the emergence of a number of Internet Service Providers (ISPs) who facilitate the connection of computers to the internet–the world wide network of computers. Internet has spawned a number of innovations in business between commercial organizations, between individuals and commercial organizations, and between individuals and individuals. These transactions are commonly known as business-to-business (B2B), business-to-customer (B2C) and customer-to-customer (C2C) electronic commerce and is abbreviated as e-commerce. These transactions include orders sent to vendors to supply items, invoices sent by vendors, payment usually made by debiting an organization's account

and crediting the vendor's accounts with banks, and payments made using cre1dit cards. The important point is that all transactions are carried out electronically using a network of computers.

One may define e-commerce as "the sharing of business information, maintaining business relationships and conducting business transactions using computers inter-connected by a telecommunication system". The telecommunication system may be a public network (as used in internet) or a secure private network. There are a variety of e-commerce applications. Some of these are as listed below.

- Retail stores such as those selling books, music, toys etc.
- Auction sites using which an individual buyer/seller can buy/sell goods.
- Cooperating businesses connected using their own private telecommunication network carrying out transactions in a semi-automated way.
- Banks connected to their customers providing services such as deposits, payments, and providing information on status of an account.
- Railways/airlines/cinema theatres permitting booking of tickets on-line and paying for them on-line using credit cards or electronic cash.
- Filing tax returns with government agencies on-line and obtaining immediate acknowledgements.
- Electronic publishing to promote marketing, advertising, sales and customer support.
- Web-based educational material which allow students to learn anytime and anywhere.

One of the earliest B2C e-commerce application was a book shop. Selling books using the internet is an excellent choice for promoting e-commerce as it is difficult and expensive for a physical book shop to stock a large number of books and allow customers to browse before they buy. The catalogue of an e-bookshop can be of very large size and store a huge quantity of information on books, such as excerpts, reviews, summaries, other books by the same author etc., which can be provided to a prospective buyer. A major problem is prompt delivery of books and ensuring the security of a customer's credit card details. This business model can be copied very quickly by others leading to fierce competition.

A major success story in India of B2C is the reservation of railway tickets. Using a site maintained by the Indian Railways (irctc.co.in) one can book train tickets from anywhere, anytime (it is a 24×7 service). Payment is by credit card and the ticket is delivered by courier at a customer's doorstep. It is estimated that currently the monthly volume of ticket sales is Rs. 8 Crores and 4000 tickets are booked on-line everyday.

C2C e-commerce is the one used by two individuals who want to sell/buy items. Such items are usually second-hand things, antiques etc. The seller posts the description of the item and the expected price on a web site maintained by a facilitating company. A website called e-Bay pioneered this idea in USA, and usually acts as an intermediary. In India, a site called bazee.com (since acquired by e-Bay) is a popular C2C auction site. A prospective buyer looks at the postings in bazee.com and enters his offer for the item. When several buyers are interested, the highest bidder (within a specified deadline) wins the auction. The items are collected by the intermediary, delivered to the customer and the payment is then sent to the seller. The intermediary gets a commission from both parties.

B2B is perhaps the most important mode of e-commerce. In the long run, it will be economically the most significant application of e-commerce. In B2B e-commerce, cooperating businesses carry out transactions such as placing an order, receiving an invoice for payment,

paying bills etc., electronically. Typical applications of e-commerce by businesses are listed below.

(1) Publishing on-line catalogues and price lists on their website.
(2) Placing tender requests on their websites.
(3) Tracking supply chains to minimize delays.
(4) Just-in-time supply to minimize inventory. For example, a manufacturer may allow his suppliers to inspect his inventory data base and production schedule. This will allow suppliers to adjust their own production schedules to meet prospective demands for items and supply them just in time.

e-Commerce has a lot of advantages among which are the following.

(1) Businesses using the world wide web have an international presence and can operate (24×7) at low cost.
(2) In several cases, middle men can be eliminated with direct business-to-business contact.
(3) All transactions are very fast as electronic communication is almost instantaneous.
(4) Delay in fund transfer is minimal.

The major disadvantages are as given below.

(1) Issues of security. Viruses and worms are an ever present threat. There is also a possibility of theft of proprietary information, credit card numbers and willful corruption of databases. Special security systems must be carefully installed.
(2) Business models can be quickly copied by competitors.

However, the advantages far outweigh the disadvantages and it is becoming increasingly evident that e-commerce will proliferate rapidly in many areas such as buying tickets, paying bills, ordering goods and transacting most business.

The rest of this article is organized as follows. In § 2, we describe a layered architecture of e-commerce systems (Kalakotta & Whinston 1999). This division of the architecture into layers allows us to organize our discussion of building blocks of e-commerce in a logical sequence. There are 6 layers in the suggested architecture. In succeeding sections each of these layers are described in some detail. In § 3, we very briefly describe what we call the physical layer, namely, the hardware infrastructure for e-commerce. Section 4 describes the logical layer, namely, the internet which is the backbone for e-commerce. In § 5, important applications which use the internet are discussed, of which the important ones are the world wide web and other applications using the web. In § 6, we describe the messaging layer which deals with secure communication on the internet infrastructure. In § 7, we elaborate on the so-called middlemen services, that is, services provided by various entities to facilitate monetary transactions and services that can be outsourced by organizations wanting to participate in e-commerce. The topmost layer, namely, applications of e-commerce, has already been detailed in this section. In § 8, we discuss some emerging applications primarily in mobile commerce. We also examine the legal framework which has become essential for promoting e-commerce. The problems are both legal and ethical, particularly while examining intellectual property rights in the age of internet and e-commerce. India is one of the first countries to have enacted an information technology act with the intention of promoting e-commerce. Some aspects of this act and some gray areas of this act are discussed in this section. We state our conclusions in § 9.

2. Layered architecture of e-commerce systems

When we examine a complex system, it is a good idea to break it up into a number of parts where each part has a specific function to perform. e-Commerce systems may also be thought of as consisting of many layers, each layer providing a service (Kalakotta & Whinston 1999). Each layer has a specific function and can be described separately. The lower layers support the upper ones. This provides us with a logical means of discussing the architecture of e-commerce systems. One possible layered architecture is given in table 1. We have used six layers to logically discuss e-commerce systems. Each layer has a function and supports the layers above it. The bottom-most layer is the physical layer. By this we mean the physical infrastructure such as cables, wires, satellites, mobile phone system etc. Their common function is that they provide the communication infrastructure for e-commerce. In fact, without high speed, reliable electronic communication, e-commerce is not possible. The emergence of wireless communications has enabled one to use mobile hand-held

Table 1. A layered architecture of e-commerce systems.

Application layer	• C2B e-commerce • B2B e-commerce • C2C e-commerce • C2G e-commerce
Middleman services layer	• Value-added networks • Digital signature certifying authority • Electronic payment schemes • Electronic cash • Hosting services
Messaging layer	• Digital encryption standard • Advanced encryption standard • Public key encryption • Digital signature • Electronic data interchange
Network services layer	• E-mail • World wide web services; browsers • Hyper-text transfer protocol: http • Hypertext markup language: html • Extensible markup language: XML • Search engines • Software agents
Logical layer	• Internet • Intranet • Extranet • Firewalls
Physical layer	• Local area networks • Public switched telephone networks • Private communication networks • Optical fibre and coaxial cable networks • Routers • Satellite-based networks • Cellular networks • Wireless networks

computers which is turn has resulted in the emergence of mobile commerce, abbreviated to m-commerce.

We call the next layer the logical layer, as it defines protocols (i.e. a set of mutually agreed rules) to communicate logically between computers connected by the physical network. Internet is a world-wide network of computers that communicate with one another using a particular protocol known as TCP/IP (Transmission Control Protocol / Internet Protocol).

The world wide acceptance of this standard has led to the emergence of the internet as the essential infrastructure for e-commerce. The simplicity of connecting computers from diverse manufacturers using TCP/IP protocol led to the explosive growth of the internet and its wide acceptance. Organizations found it attractive to use the same protocol, namely, TCP/IP to interconnect computers within their organization. A major advantage of doing this, besides allowing the organization to interconnect computers made by different manufacturers, is the availability of many services such as e-mail, file transfer, protocol, browsing etc., available on the internet, that may be adopted inexpensively within an organization. Such a local network within an organization is called *intranet*. The internet allows anyone to connect to it. It is thus vulnerable to misuse by anti-social elements who break into others' computers and steal or destroy valuable files. Special precautions are required to prevent unauthorized access. This is provided by what are known as *firewalls* which guard the intranets of organizations. Firewalls do not provide absolute security from intruders. Thus many organizations do not connect their intranet to the internet.

This however would prevent electronic communication among cooperating organizations. Therefore many cooperating organizations lease communication lines and create a private network interconnecting their intranets. The protocol is, of course, TCP/IP. Such a private network interconnecting cooperating organizations is known as an *extranet*. A private network formed by leasing communication lines is expensive compared to using the internet. Thus a method of ensuring secure communication between cooperating organizations using the internet has been designed. This is called a virtual private network (VPN) (Ben-Ameur & Kerivin 2003).

The next higher layer is the network services layer. This provides services on the internet infrastructure. The most important service originally was the e-mail service. Currently, the most important service is the world wide web service which provides users convenient access to information stored in computers anywhere in the world. Other services which make e-commerce possible are: html (hyper text markup language), XML (extensible markup language), browsers and search engines.

Among the most important requirements of e-commerce is exchanging messages and documents between participants in e-commerce. For example, purchase orders, delivery notes etc., have to be sent electronically. The cheapest means of doing it is using the internet. In C2B and C2C e-commerce, internet is the only available system. As was pointed out earlier, the internet being accessible to everyone there is always the danger of messages and documents being maliciously altered by unscrupulous persons. Thus, there is a need to send messages which are coded using a secret code. It is also necessary to have an equivalent of signing in the electronic medium. These requirements namely encrypting messages to ensure security and digital signature to authenticate communications received electronically are provided by the messaging layer.

We call the next layer "middleman services". They are essentially services provided to e-commerce participants to make their dealings easier. Some important middleman services are secure payments using credit cards, imitating cash payments for small purchases and authentication of digital signatures. Value-added networks provide secure electronic transactions

among participants. Hosting services provide among other facilities, web presence for organizations and electronic catalogues and directories etc., to participants.

All the services provided by the layers described above are essential to support e-commerce application, namely, C2B, B2B and C2C e-commerce. This is thus the top layer in the layered architecture.

In the rest of this article, we will describe in greater detail each of these layers and how they cooperate to provide e-commerce solutions for many day-to-day needs of persons and organizations.

3. Physical layer

If computers are to communicate with one another, they should be physically connected. Most businesses have a local area network (LAN) connecting all their computers. The LAN usually connects machines with an unshielded twisted pair (UTP) of copper wires. Computers connected to a LAN using UTP can communicate at the rate of 1 gigabit/second, even though 100 megabits/second is more common. The number of computers that can be connected to a segment of a LAN is limited to around 16. Larger LANs are made by connecting smaller LAN segments by what are known as *bridges*. Besides UTP, one may use fibre optic cables to interconnect computers if higher speed is needed. Mobile computers may also be connected to a LAN using wireless communication. Those interested in detailed information on physical networks may refer to Stallings (1998).

When two businesses want to communicate with each other, their LANs are connected using what is known as a *router* to the telephone network provided by the Department of Telecommunications (DOT). This network is known as a Public Switched Telephone Network (PSTN). PSTNs are not very secure. Thus, if two businesses want to closely collaborate and want high security they have to use their own private leased communication lines.

4. Logical network

The single most important technology which has enabled the growth of e-commerce is the *internet*. The internet connects tens of millions of computers spread all over the world enabling them to exchange information and share resources (Comer 1995). The major applications of internet are exchange of electronic mail, exchange of files (text as well as multimedia), storing information in a form which allows other computers connected to the internet to access it, and remote logging onto a computer and using it to run programs. For two computers in different locations to communicate, it is necessary that the following conditions hold.

(i) Each one must have a unique address.
(ii) messages originating from one computer must be routed to the destination via a public switched telephone network, which may be local, national or international.
(iii) There must be compatible software in each computer to format messages using commonly agreed rules so that all messages are properly routed and interpreted. This commonly agreed set of rules is called the *Internet Protocol* (IP).

The unique address required by a computer in order to access the internet is called its IP address. The IP address is a 4-byte address and is expressed in what is known as the

dotted decimal format, e.g. 202.42.128.3. The IP address for a business or an individual is provided by the Internet Service Provider (ISP). IP addresses are an important and scarce resource particularly because the number of computers connected to the internet is rapidly growing. The IP address is converted into a string of characters for ease of remembering and grouped into *domains*. For example in the address: iisc.ernet.in, the top domain is the country name abbreviated *in*, the ISP is *ernet*, who is the host of *iisc*. IP addresses are controlled by an international authority known as Internet Corporation for Assigned Names and Numbers (ICANN), and a hierarchical organization of addresses allows this authority to decentralise the assigning of addresses. For example, ernet is given a range of IP addresses by ICANN and it allocates a subset of addresses to iisc, which in turn allocates addresses to various departmental servers. The clients connected to the departmental servers are then given their unique address by the department. Domain names are very important in e-commerce as they provide immediate brand recognition. Thus, there has been a problem known as cyber squatting which has led to legal wrangles. Cyber squatting is the registering of a well-recognized name as one's own domain name to prevent an organization or company from using it. Resolution of disputes on domain names is currently done by ICANN. However, there is a move to refer international disputes to the World Intellectual Property organization which currently resolves disputes on copyright, trademark etc.

The internet protocol breaks up a message sent from a source to a destination into a number of *packets*. A packet consists of two parts, the part containing the information which is called the *payload* and a part called the *header* (see figure 1). The header consists of the source and destination addresses, the serial number of the packet, error detection bits and other control bits, and is used to route the packet to the destination address. Messages are broken into packets as this reduces the cost of transmission and improves the fault-tolerance of transmission. The cost of transmission is reduced as a number of packets (that may belong to different messages) can be assembled and sent along any free communication channel. The packets are stored in routers along the path and forwarded to another router when the communication link is free. This is called *packet switching*. It is also fault-tolerant because if a line is not working, the stored packet can be sent along another line which is working. Observe that different packets belonging to a message may travel along different paths. They are finally assembled at the destination using the serial number of each packet. The major disadvantage of packet switching is that the time taken for a message to reach a destination cannot be predicted. This is not a disadvantage for applications such as e-mail, file transfer etc., but is a disadvantage for real-time messages such as telephone conversations and video transmissions. Currently, work is going on to improve the internet protocol to allow real-time data transmission also. One of the major advantages of internet, as already mentioned, is its ability to connect computers from any manufacturer and LANs using different technologies together into a uniform access system by enforcing that the computers use a software layer conforming to the internet protocol known as TCP/IP (Transmission Control Protocol/Internet Protocol).

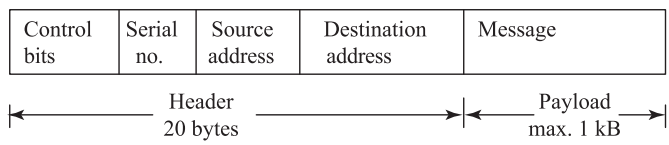


Figure 1. Structure of an internet packet.

5. Network layer

The World Wide Web is a global multimedia information service available on the internet. It consists of linked web pages (or documents). Each web page is prepared using a language known as HTML (Hyper Text Markup Language). HTML has features to embed links within web pages pointing to other web pages, multimedia files and data bases. Web pages are stored on what are known as web servers. A web server can host one or more web pages. Observe that the world wide web is not internet. Internet provides the infrastructure on which the world wide web is built.

To locate a web page stored in the world wide web, a scheme known as uniform resource locator (URL) is used. An example of a URL is given below:
http://www.freesoft.org/connected/index.html

In this example http specifies the protocol to be used. In this case it is hypertext transfer protocol. This is the protocol used for web search. www.freesoft.org preceded by :// is the address (called domain name) of a computer (called a server) which is permanently connected to the internet. The computer may be located anywhere in the world. The part of the URL, namely, /connected/index.html is a path to the required file which stores the information. In this case the document index.html is stored in a folder named "connected".

There are other protocols used in the internet for other services. For example ftp:// is used for transferring files from one computer to another connected to the internet. ftp stands for file transfer protocol. For example ftp://freesoft.org/<filename> transfers the contents of the specified file to a user's computer if he/she has access permission from the server.

The information on a web page can be retrieved by a customer (or user) using a web browser program which runs on his/her desktop computer connected to the internet. There are many web browsers, the most popular of which are Netscape and Internet Explorer. The URL is entered in the location field of the browser screen. The browser program connects to the specified web server, and displays the document on the browser screen. Web browsers have excellent Graphical User Interface (GUI) which simplifies access to web pages. Most organizations now maintain a web page on a server in their organization or on a server which is rented by a service agency. Hosting of the web pages of many organizations has now become an important business. These businesses keep a large number of powerful servers on their network with reliable connection to the internet. They create the web pages for different organizations, based on specifications given by them, and continuously update them on request from the contracting organizations. Web presence is now essential for any business as it publicises their activity. Besides organizations, individuals also create and maintain web pages to "sell themselves".

In order to create a web page, a language is needed which formats the page with pleasant background colours, graphics, links to other parts of the same document and links to other web pages, either in the same server or other servers. This language is called Hypertext Markup Language (HTML). Hypertext markup language adds tags to text which can be interpreted by any program. A simple example is given below.

```
<HTML>
<HEAD>
<TITLE> </TITLE>
</HEAD>
<BODY>
<H1> Analysis and Design of Information Systems </H1>
```

```
<P> This is the <B> second edition </B> of <I> Rajaraman's </I> book </P>
</BODY>
</HTML>
```

will display the following.

Analysis and Design of Information Systems.

This is the **second edition** of *Rajaraman's* book

Observe the various commands introduced with the text. Some of them are:

- Document delimiters such as <HTML>, <HEAD>, <TITLE> and <BODY>
- Section heading <H1>. More levels are available
- Paragraph and other spacing commands such as <P> above
- Character attributes such as <B> for bold face, <I> for italics
- Graphic images to be displayed with the document.
- Listing using bullets or sequence numbers
- "Anchor" commands which specify text or images that can be clicked on to reach another HTML document either in the same server or another server.

Observe that when a web page is designed, selected words are picked and tagged with anchor commands. When these words are clicked on, the tag activates a link to the specified page, graphics file, audio or video file. As the use of inter- and intranets increases, most documents are now created using HTML format. Standard word processor outputs can be converted to HTML format using tools. There are also specialised tools available to create web pages.

HTML is based on a much larger standard language known as Standard Generalized Markup Language (SGML). A dialect of SGML called XML (Extended Markup Language) is now becoming more popular as it allows designing documents tailored to a select audience (Pardi 1999).

The number of web pages in the world wide web runs into tens of millions and is continuously growing. Documents in the web are often poorly structured but do contain very useful information sometimes along with poor quality unauthenticated information. Finding relevant documents is not easy. There are many tools known as search engines (Rajasekhar 1998; Brewer 2002) which aid users in their search. These engines (which are actually search programs) receive a user's query, systematically explore the web to locate documents, evaluate their relevance and return a rank-ordered list of documents to the user. Currently the most popular search engine is www.google.com.

6. Messaging layer

Electronic commerce generally uses a public switched telephone network (PSTN) and often occurs between entities who are not known to one another. Ensuring security of communication between the entities participating in e-commerce is hence an important requirement (Shim *et al* 2004) Apart from ensuring the security of messages, an organization should protect data stored in computers that are connected to the internet from malicious damage. It is also necessary to be able to authenticate messages received via the internet. In this section, we

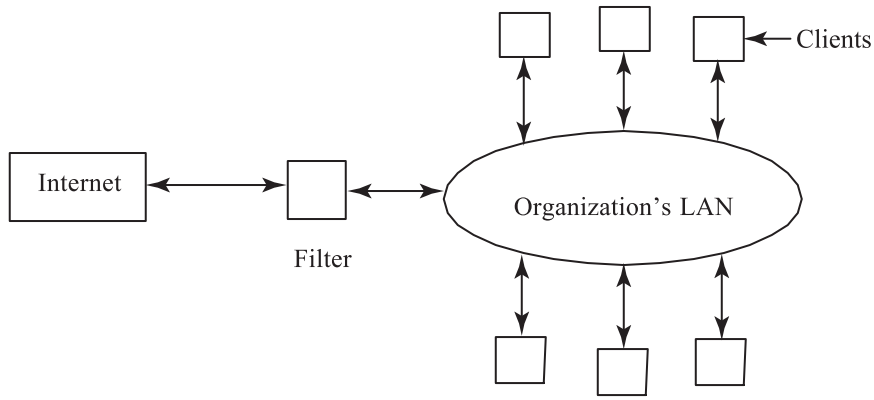


Figure 2. Filter to protect organization's computers.

will describe *filters* which protect an organization's network from intruders, *encryption* methods to ensure secrecy of message contents and stored data and *digital signature* to authenticate messages received from customers or business associates.

6.1 *Filters*

A filter is a computer program or a piece of hardware (with associated software) used to monitor message packets which enter or leave an organization's network (figure 2). One may decide to allow a message packet to enter or leave the network, based either on the information contained in the header of the packet or the contents of the packet. The header contains the internet source and destination addresses (IP addresses) and the port number which identifies the internet service, namely, telnet, ftp, http etc.

A commonly used filter is called a firewall (Cheswick & Belleroin 1994). The simplest firewall allows access to an organization's network only to a specified set of IP addresses. Another screening rule may be to allow outsiders to access only one IP address in the organization which may be hosting its web page. The other two filters that are commonly used are for filtering out junk e-mail (called spam) entering a system and for preventing specified material from entering a system while users are browsing the web. Junk e-mail filters scan the "From", "X-Sender" and "Subject" fields in the header of a message. If these are in a list of unsolicited known junk mailers the messages are deleted. Automatic deletion may sometimes delete legitimate email and careful monitoring is needed.

6.2 *Data encryption with private key*

As a message sent using PSTN may be snooped by unauthorized persons it is necessary to scramble it before sending it on a public network so that even if an outsider is able to read it he will not be able to understand or use it. One should also take precautions to prevent unauthorized persons from accessing a database. If, by some means, he is able to access it, the data stored should be in encoded, i.e., scrambled form, so that he cannot read and use it to harm the organization. For example, sensitive databases are those containing credit card numbers, passwords, financial data etc. Encoding or scrambling data to make it difficult to decode is called *encryption*. Encryption is a transformation of a data in any form (text, audio, video, graphics) into another form which cannot be understood. In order to understand the

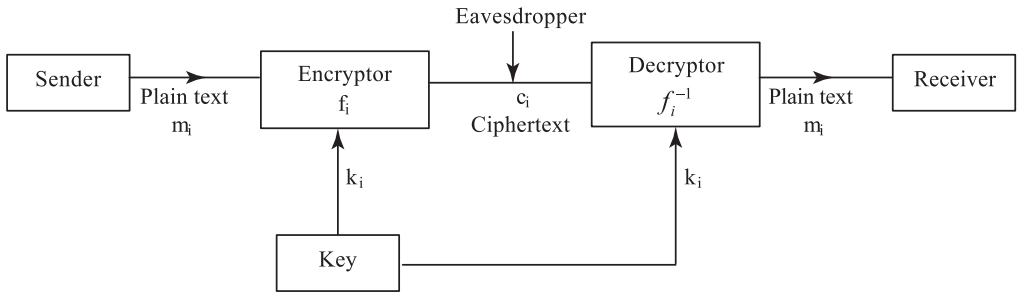


Figure 3. Use of private key for encryption.

data one needs a *key* which is used to decrypt the message. Messages to be encrypted are also known as *plain text* and encrypted messages are known as *cryptograms* or *ciphertext*.

There are two methods of encryption. One of them is called symmetric or private key encryption and the other, public key encryption (Stallings 1999). In symmetric key encryption, a message sent on a PSTN is encrypted using a key (i.e. it is transformed using a transformation). The receiver applies the inverse transformation (as he knows the key) and recovers the message (see figure 3). A common method uses a combination of permutation and substitution on the plain text to obtain the ciphertext.

This general idea is used in a very popular encryption method called the Data Encryption Standard (DES) introduced by IBM in 1975 and standardized by the US Government in 1977. DES was reasonably secure, i.e., trying out all possible keys exhaustively to break the code took too long till recently. However, with the increasing speed of computers, it has now become insecure. A system called triple DES which is based on DES is very secure and is currently used (Stallings 1999). We will first briefly describe DES. DES applies transformations on blocks of 64-bits corresponding to binary encoding (may be ASCII) of a message text. The plain text is exclusive ORed with the key to obtain the ciphertext ($A \oplus B = A.\overline{B} + \overline{A}..\ B$ where $\oplus$ is an exclusive OR operator). If the key is exclusive ORed with the ciphertext we get back the original plain text as shown below.

M = Plain text	01101100	11011000	11011010
K = Key	10101111	00101100	01011011
$E = M \oplus K =$	11000011	11110100	10000001 (encryption)
$E \oplus K =$	01101100	11011000	11011010 (decryption)

This general idea is used in DES. DES encrypts 64-bit blocks. First, the 64-bits are permuted with a secret key. The resulting block is divided into two 32-bit blocks (L_i, R_i) which are the left and right half of each block. The following complex procedure is applied 16 times.

$$L_{i+1} = R_i,$$
$$R_{i+1} = L_i \oplus f(R_i, K_i)$$

where K_i is the secret key used in the i^{th} round and f a complex function which uses both permutation and substitution operations and depends on the key. The resulting block is again permuted using the secret key to obtain the final encrypted block. DES was designed to be implemented in hardware. Integrated circuit chips implementing DES have been marketed. As we stated earlier, with the increasing speed of computers DES is now not secure. Thus triple

DES is now used. Triple DES applies the DES algorithm thrice each time with a different 56-bit key and is expected to be secure in the foreseeable future. As triple DES is an application of DES thrice, the same DES chips technology can be used for its hardware implementation. A new standard has been developed called Advanced Encryption Standard (AES), which uses 128-bit blocks and 128- or 192- or 256-bit keys (depending on the level of security specified) (Landau 2000; Daeman & Rijmen 2002), but is not yet widely used.

The encryption methods we have discussed so far are called *symmetric key* or *private key* encryption as encryption and decryption use the same key known to the two parties exchanging messages. The main problems with this method are the need to have a separate key for each of the organizations with which an organization transacts business and the requirement to securely distribute the keys to all of them. Key distribution must use a different channel to avoid it being stolen. Further, one needs to maintain a table of all keys and keep it secure from snoopers.

6.3 *Data encryption with public key*

Public key cryptography allocates two keys to each organization wanting to communicate with another. One of the keys is called a *public key* of the organization as it is available to any one wanting to send a ciphertext to that organization. The organization has another key which it uses to decrypt the ciphertext it receives (see figure 4). A popular public key system is known as the RSA system named after its three inventors – Rivest, Shamir and Adleman. The procedure has been described in detail by Sarkar (2000). There are two important points to note regarding RSA. First, if a message is encrypted by a sender S with his *private key*, it can be decrypted by a receiver R using S's *public key*. Second, RSA derives its strength from the fact that, given a number n which is a product of two large prime numbers, it is difficult to factor n and get the two prime components. Compared to DES, the RSA encryption technique is computationally complex. Thus, for large plain texts RSA is not applied in practice. The plain text is encrypted using triple DES and the secret key necessary to decrypt the ciphertext is sent using RSA (see figure 5). There are two advantages in following this procedure. First, encrypting using triple DES is faster as it is normally done using hardware. Second, the secret key used in triple DES can be unique for each message as it is sent along with the message in encrypted form. Thus, even if a snooper gets hold of a large number of messages exchanged between the sender and the receiver he cannot decode them as the key is changed for each message transmitted. If a message is long, it can be broken into several parts and each part encrypted with a separate secret key.

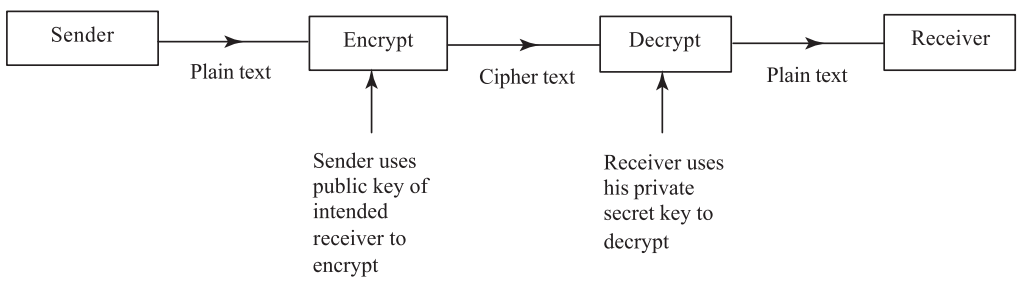


Figure 4. Public key encryption system.

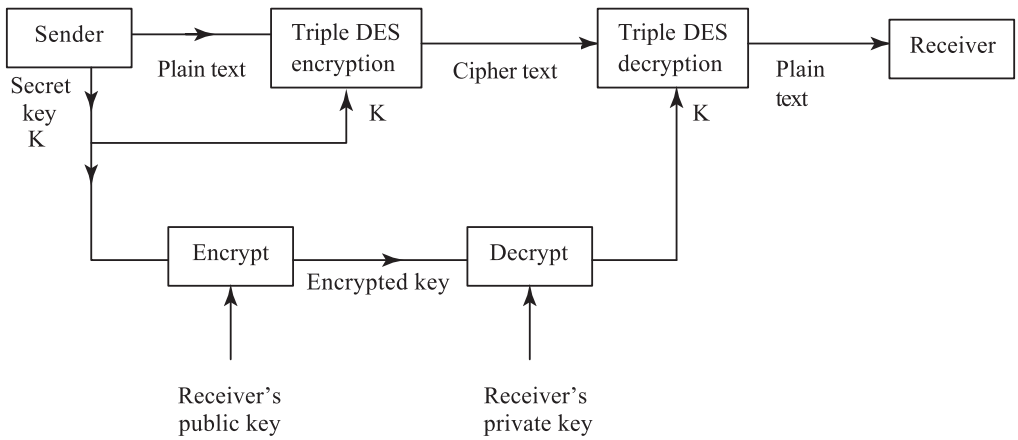


Figure 5. Combining private and public key encryption.

6.4 *Digital signature*

There are two important aspects of a signed paper document that has to be imitated by an electronic signed document. First, the letterhead and the signature convince a receiver about the authenticity of the sender. Second, the signature appears physically following the text and this ties it to the matter typed. In legal documents, every page is signed and every correction is also signed.

The RSA system is used primarily to protect messages being sent on a public network from illegal snoopers. There are two problems which may occur. First, if a sender S sends a message to R, unless it is signed by S, R cannot be sure of its authenticity. Physical signatures are unique and can be verified. We need a similar method of signing an e-mail message or document, so that S cannot claim later on that he never sent the message. In other words, S should not repudiate, say, a purchase order after sending it to R. Second, a person say, W, should not be able to impersonate R and receive messages intended for R. The public keys of all potential participants in e-commerce are known. If W somehow is able to convince S that R's public key is his, S will be sending messages intended for R to W and W can read it using his private key. There is thus a need for a third party to authenticate public keys of all the participants. We will first explain how a digital signature system works (see figure 6). Assume that a sender S wants to send a message to a receiver R and sign it. The following steps are carried out by S.

(1) S picks a *random key* K, encrypts the plain text message (M) to be sent to R using K, and sends the ciphertext ME to R. The encryption normally uses a private key system such as triple DES.
(2) S encrypts the random key K using $R's$ public key and sends it to R. We will call the encrypted key KE. Observe that K is encrypted using the RSA system.
(3) R will be able to decrypt KE using his private key and get K.
(4) Having obtained K, R can decrypt the ciphertext ME sent by S and get M
(5) Now R has to be convinced that S sent the plain text. This can be done only if S signs the message. Signing of the message is done as follows:
(6) The message M is hashed using a hashing function, which compresses M to H. The hashing function should try to avoid collisions. In other words, two messages M1 and

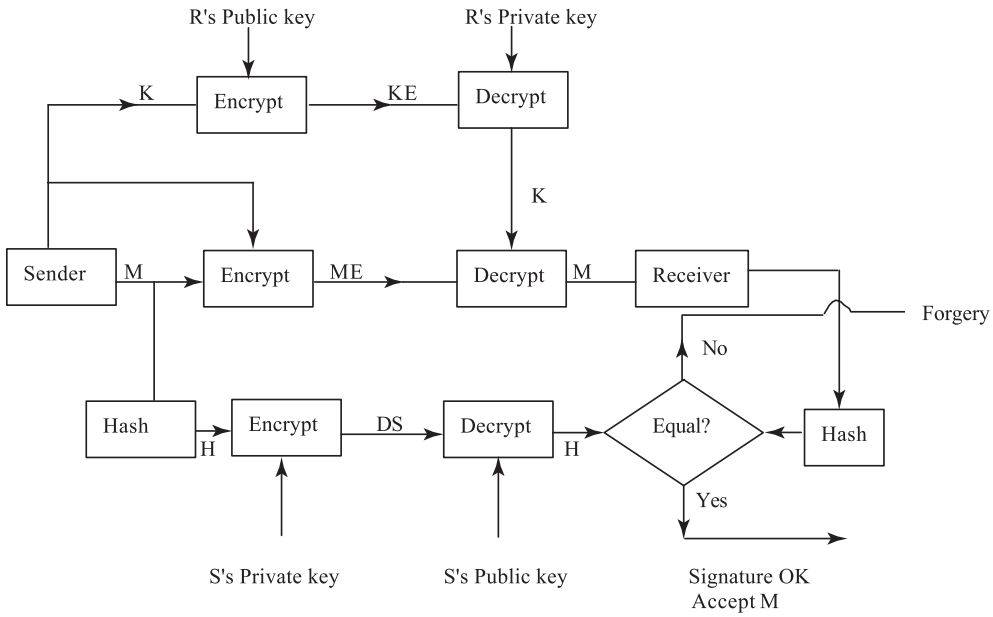


Figure 6. Signing a message using digital signature.

M2 when hashed should give unique hashed values H1 and H2. H should also be much shorter compared to M. Hashing is done primarily to reduce the size of the signature. (A hashing method called MD5 (Message Digest 5) is popular.) Also hashing the message M ties H to M. In other words, the signature uses H, which is tied to the document being sent.

(7) H is encrypted by S using his *private key* and transmitted to R. This is his *digital signature* DS.
(8) As R already has M he can hash it using the known hash function to obtain H.
(9) When R receives DS, he decrypts it using the *public key* of the sender S.
(10) The decrypted value must be H. If it is not, then it is a fake message. If it is H then R is convinced that it is signed by S. S cannot repudiate (i.e. say that he did not send the message) as he has encrypted H using his *private key* which is known only to him.

The procedure works because the RSA algorithm is symmetric, i.e., if encryption is done with a private key decryption can be done with the corresponding public key.

The second question we raised at the beginning of this section was about the authenticity of public keys. This is done by some organizations (identified by governments) which issue public key certificates after verifying the credentials of an organization or individual. Thus, if an organization A wants to do business with another organization B electronically, B can send an email to the certification authority requesting certification of A's public key, email identity etc. Once the certifying authority certifies the public key, transactions can proceed. The certification authority takes on the legal responsibility in case of disputes on identity.

7. Middleman services

Payment is an important component in e-commerce. In day-to-day commercial dealings there are many modes of payment, each with its own advantages and disadvantages. The most common mode of payment, especially for low value purchases, is by cash. For higher value purchases credit cards are preferred by customers. If a customer is a trusted party, merchants often accept cheques. Payment for services such as telephone bills, electricity bills etc., and settlement of bills between businesses is normally by cheque. In e-commerce also we need systems which are equivalent to these three modes of payment. Of these three modes, a cash transaction is the one which is most difficult to mimic. Large electronic cash transactions are discouraged by most governments. It is thus still in a fluid state.

7.1 *Payment using credit cards*

In manual credit card transactions, the transaction is validated using the physical card and the customer's signature on the card. In e-commerce there is no physical contact between the merchant and the customer making it impossible to verify a physical signature. Also it is necessary for the merchant to verify the genuineness of the customer and for the customer to be assured that he is not dealing with a fake merchant. Thus a customer would be reluctant to reveal his credit card number and details using the internet as the merchant may be a fake or the number may be stolen by eavesdroppers on the internet. Further, if the merchant is careless, a hacker may access the merchant's data base and steal credit card numbers. There have been cases reported in the press of credit card numbers being stolen by hackers as well as by disgruntled employees of the merchants themselves. Thus, a protocol is required in which the credit card number is not revealed to a merchant but only to the acquirer who authorises sale based on the credit card validity and available credit. In addition to this, the acquirer and the bank need not know what was bought by a customer (to protect the privacy of customers). They need to know only the bill amount.

7.2 *Secure electronic transaction (SET) protocol*

A protocol called Secure Electronic Transaction (SET) has been standardised for credit card payments by major credit card companies such as Visa and Mastercard in the USA. To use the SET protocol for credit card transactions the following are assumed.

(1) Public key encryption systems (such as RSA) are used by both customers and merchants. Thus each of the parties involved in e-commerce transactions have a pair of keys: a private and a public key.
(2) All parties have their public keys certified by a certification authority and these certificates accompany requests for service sent by them. This is to assure both customers and merchants that they are dealing with genuine parties.
(3) A standard hashing algorithm is used to create message digests for digitally signing purchase orders.

The main features of this protocol are as below.

(1) It ensures that a customer's credit card number is not revealed to a merchant. It is revealed only to the acquirer who authorizes payment.
(2) Purchase invoice details are not revealed to the credit card issuing company called acquirer and the controlling bank. Only the credit card number and total amount is revealed.

(3) A purchase invoice, coupled with the credit card number, is digitally signed by the customer so that disputes, if any, on purchase invoice and cost can be settled by an arbitrator.

The complete protocol is given in detail in a formal SET protocol definition. We will present the simplified essentials of the protocol in what follows. Readers interested in learning about the detailed protocol are referred to Stallings (1999) in the suggested reading list and the website www.redbooks.ibm.com/SG244978.

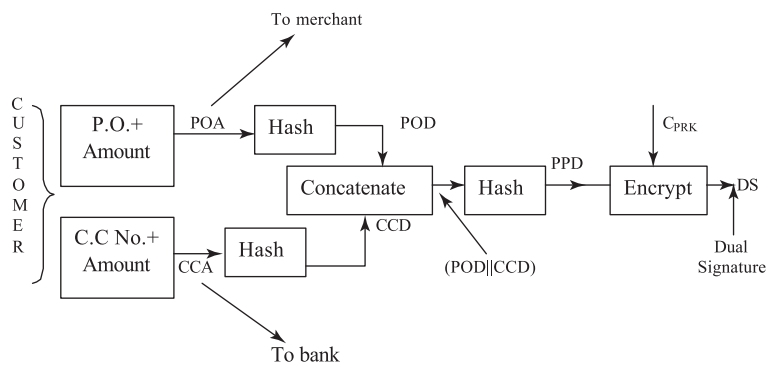
7.3 *Dual signature scheme*

SET protocol depends on an innovation called dual signature whose main purpose is to give to a merchant the purchase order and amount only (without revealing the credit card number) and give the credit card number and the amount to be paid (without revealing the purchase order details) to the acquirer. It also will ensure that the payment is for the actual purchase made. The essentials of the idea are explained below (figure 7). A customer's purchase information consists of a purchase order (PO) accompanied by credit card number (CCN) and amount to be paid. This is divided into two parts (PO + amount) and (CCN + amount). The two parts are separately hashed using a standard one-way hash algorithm (such as MD5 explained earlier). Let us call these POD and CCD respectively. The two are concatenated (i.e. stringed together) and hashed again giving a PCD (see figure 7). The PCD is encrypted using the customer's private key C_{PRK}. This is the customer's digitally signed copy of the purchase order + credit card number. Let us call it DS. The formula to get DS is given as,

$$DS = C_{PRK}\{H(POD||CCD)\} \tag{1}$$

where || is the concatenation operator and H a hashing function.

The purchase order and the amount, namely POA, are separately encrypted using the *merchant's public key* and sent to the merchant. He can decrypt it using his private key to



POA: (Purchase order + amount)
CCA: (Credit card No. + amount)
‖ : Concatenation operator which strings together POD and CCD
POD: Purchase order digest
CCD: (Credit card no. + amount) digest
PPD: Purchase payment digest
C_{PRK}: Private key of customer

Figure 7. Dual signature system.

obtain POA. CCD and DS are also sent to him separately. Remember that given CCD he cannot find CCA as hashing is a one way function. Thus, credit card number is not available to the merchant. The merchant can compute

$$H(H(POA)||CCD) = H(POD||CCD). \tag{2}$$

The signature DS received by the merchant can be decrypted by him using the *public key of the customer* to obtain,

$$C_{PUK}(DS), \tag{3}$$

where C_{PUK} is the certified public key of the customer which is sent to the merchant by the customer along with his purchase order. If (2) equals (3), then the merchant has verified the customer's signature. If payment is authorized by the acquirer, he can ship the order.

As far as the bank is concerned, it receives the CCA encrypted by the customer with the bank's public key forwarded by the acquirer. It can decrypt it using its private key and obtain the CCA. The bank also receives POD and DS. Remember that POA cannot be found from POD as it is obtained by hashing POA with a one-way hash function. The bank will not thus know the purchase details. It can however compute

$$H(POD||H(CCA)) = H(POD||CCD), \tag{4}$$

and C_{PUK} (DS). If (4) equals C_{PUK} (DS), the signature of the customer is verified by the bank. If the customer's balance in the credit card account is adequate, the bank can authorise the merchant to honour the purchase order.

Observe that the customer cannot repudiate his purchase order as it has been signed by him and deposited with the bank. The merchant also cannot substitute a customer's purchase order with some other purchase order as the signature contains a unique digest of the customer's purchase order as deposited with the bank.

We summarise the procedure below.

Step 1: Customer fills purchase order, amount payable and credit card number in his PC. A software in the PC strips it into two parts: purchase order with amount and credit card number with amount. Let us call them POA and CCA.
POA is encrypted using the merchant's public key and CCA with the bank's public key. Both are sent to the merchant along with CCD and dual signature (DS). Merchant verifies signature and proceeds further if signature is OK.

Step 2: Merchant forwards encrypted CCA, POD and DS to acquirer who forwards it to customer's bank.

Step 3: The bank decrypts CCA with its private key, checks the validity of the credit card and available balance in the credit card account. If it is OK and the customer's digital signature is OK it authorises the acquirer the to proceed with the transaction.

Step 4: The acquirer in turn okays the transaction to the merchant and credits his account.

Step 5: The merchant accepts the customer's purchase order and informs him about delivery details.

Step 6: At the end of the month, the bank issuing the credit card sends a consolidated bill to the customer.

It should be remembered that all the operations are carried out by software stored in the respective computers and effected by clicks of their mouse buttons!

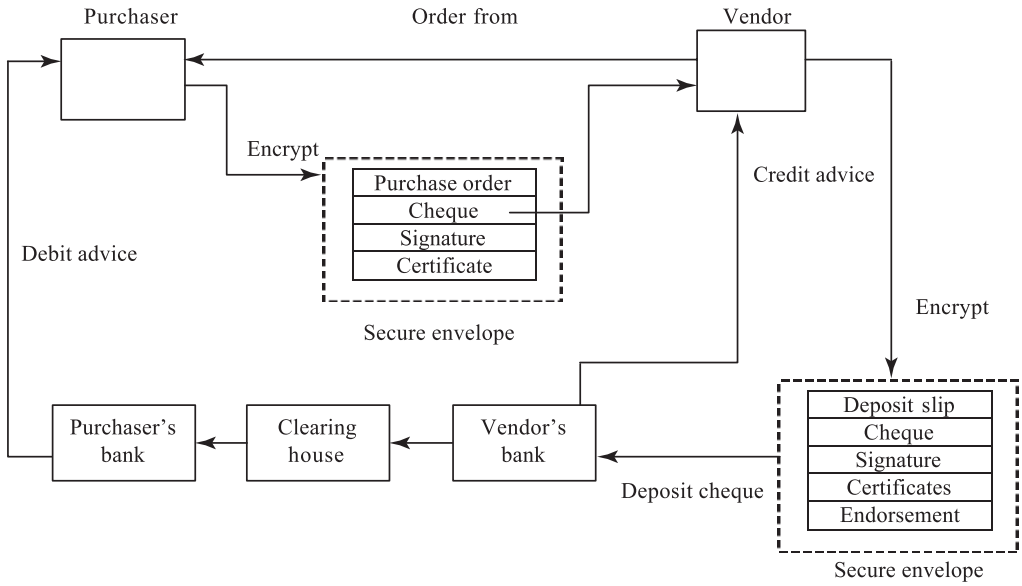


Figure 8. Clearing cheque payment electronically.

7.4 *Electronic cheque payment*

We now describe an electronic cheque clearance system developed by a company called Financial Services Technology Consortium Inc. (FSTC), which is supported by a number of American banks. Most of the cheque-based transactions are between businesses and therefore this mode of payment is relevant in B2B e-commerce. It is assumed that the businesses are willing to invest in special hardware (normally an electronic circuit attached to a PC) to sign payments. Hardware encryption of signatures are secure as it is difficult for hackers to steal keys stored in hardware. The system is shown in figure 8. This system assumes that all organizations participating in the system use public key encryption schemes such as RSA and have their public keys certified by certification agencies. It is also assumed that banks have trusted relationships among themselves as well as with the clearing house which settles cheque payments. In India, the Reserve Bank of India is the clearing house and all scheduled banks use RBI's services via a private secure network. The transaction proceeds as follows.

Step 1: A purchaser fills a purchase order form, attaches a payment advice (electronic cheque), signs it with his private key (using his signature hardware), attaches his public key certificate, encrypts it using the vendor's public key and sends it to the vendor.

Step 2: The vendor decrypts the information using his private key, checks the purchaser's certificates, signature and cheque, attaches his deposit slip, and endorses the deposit attaching his public key certificates. This is encrypted and sent to his bank.

Step 3: The vendor's bank checks the signatures and certificates and sends the cheque for clearance. The banks and clearing house normally have a private secure data network.

Step 4: When the cheque is cleared, the amount is credited to the vendor's account and a credit advice is sent to him.
Step 5: The purchaser gets a consolidated debit advice periodically.

We have not described the signing process in detail as it has been described already.

7.5 *E-cash transactions*

The cost of credit card transactions is high and not suitable for small payments. Thus e-commerce tries to mimic cash payments using what is known as e-cash. We will now describe a simple method that has been used for e-cash transactions (Lynch & Lundquist 1996). It is being used by some banks in the United States and Europe. No such system is in place in India as of now. It is primarily intended for small cash transactions. The procedure is as follows (see figure 9)

Step 1: A customer withdraws "cash" in various denominations from the issuing bank (or financial institution) and stores it in his PC. The withdrawal takes place by the customer giving a unique identification number and denomination of each coin and requesting the bank to digitally sign it. The bank signs a coin by encrypting <id#,denomination> with its private key. The signed e-coins are of the form <id#,denomination, bank's signature>
Step 2: The customer pays a vendor for goods ordered using the signed e-coins.
Step 3: The vendor sends the e-coin to the issuing bank for authorization.
Step 4: The bank checks whether the e-coin is signed by it and whether it has not been already spent. If it is a valid e-coin it okays the transaction and credits the amount to the vendor's account. It puts the e-coin details in a spent e-coin data base so that if the e-coin is presented again it can dishonour it.

Communications between customer, vendor and the bank are also encrypted as the internet is used. As the amounts involved are small, symmetric cryptography is used for these communications as it is faster. There are two points which need clarification. The first is the cost of servicing e-coins. Normally banks charge a small commission for the service from vendors. The second is whether a vendor who receives an e-coin from a customer can use it to

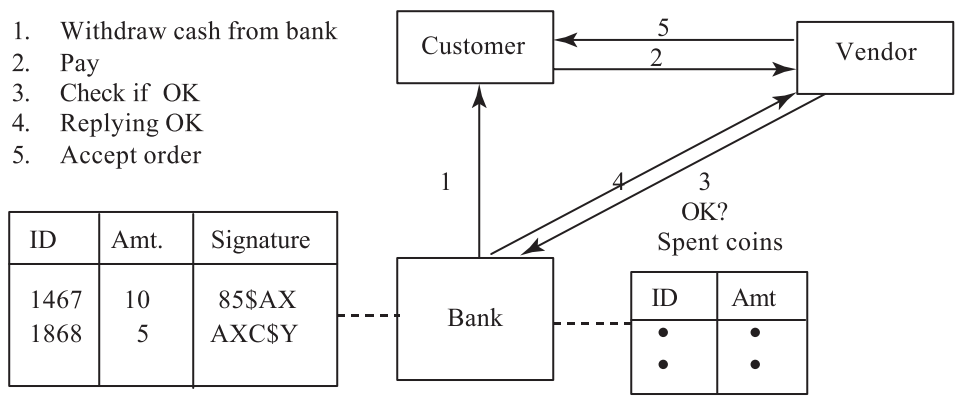


Figure 9. Electronic cash payment.

purchase goods from another vendor. This is not possible as the issuing bank has to authenticate the e-coin and, while doing it, it has marked the coin as "spent". Thus, it is not really like good old cash!

The simple protocol used above does not preserve the anonymity of cash. The bank will know which customer and vendor are involved in the cash transaction and can link the two. There is another protocol called "transaction blinding" in which it is possible for a customer to get e-coins issued by a bank without revealing his identity. The protocol called Chaum's blinding protocol is complicated and, as of now, is not used widely. Chaum invented the idea of blinding (Chaum 1992).

7.6 *Electronic data interchange standards*

We saw that in business-to-business e-commerce, electronic documents are exchanged between business partners by using either a private network or a public switched network. We also stated that in order to interpret them correctly we need standard notation which is agreed to by both parties. This is called electronic data interchange (Minoli & Minoli 1999; Awad 2002) or EDI for short. EDI is defined as the exchange of business documents between organizations in standardized electronic form which can be interpreted and used directly by application programs. The major advantages of using EDI are the following.

(1) Handling of paper documents is eliminated.
(2) There is no need to manually re-key data in documents such as purchase orders, invoices etc., by participating businesses.
(3) Elimination of manual data entry reduces cost, improves accuracy and reliability.
(4) Time is saved due to elimination of manual handling and also due to direct application-to-application movement of data at electronic speeds.

We now describe the steps a business A should follow to establish an EDI partnership with business B (figure 10).

(1) The first step is to agree on a standard format for commonly used documents such as purchase orders, invoices, payment advices, delivery notes etc. Formatting information or data type definition, as it is called, should include description of various fields used such as quantities, price, currency used, delivery date, field lengths, character type, ordering of fields in the document, units used etc. As companies may transact business with many partners, it is desirable to have a universally agreed standard form for all business documents. This realisation led to industry groups such as the automobile industry, shipping and transport industry to adopt standards for inter-company transactions. This later evolved into national and international standards. The two standards are ANSI X.12 standard adopted by the American National Standards Institute for electronic transactions in

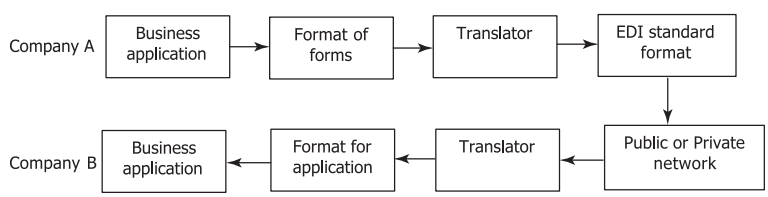


Figure 10. Steps in electronics data interchange.

Table 2. A sample EDI message for a book purchase order.

EDIFACT form	Meaning
UNH000002 + ORDERS; DD96A UN; EAN 008	Header
BGM + 220 − A000512-9'	Order No: A000512
DTM − 137 − 20010204 : 102'	Message date YR MM DD
NAD + BY Universal Book Traders:	Purchaser's name and address
2 + N.S.C.Road, Bangalore ++560022'	
REF + API : UBT4578'	Purchaser's identity code
NAD + SU + + + PHINC'	Supplier's name
CUX + 2 : USD:9'	Order currency: US dollars

the United States of America and EDIFACT (Electronic Data Interchange For Administration, Commerce and Transport) standardised by the United Nations Economic Commission for Europe.

(2) Once an EDI standard is agreed on, company A should send business documents to company B using this format. This would require translation of company A's documents such as purchase order to the EDI format. The EDI messages are text with special characters such as ' , + and : as field separators. There are special tags defined in the EDIFACT dictionary for message header, date etc. The EDI message is meant to be interpreted by computer programs and is thus not easily understood by people unless they are trained in understanding the standard. A purchase order for a book using the EDIFACT standard is given in table 2. In fact EDIFACT standard defines several hundred transaction sets for various types of transactions between organizations and it requires an expert to understand it and convert commonly used documents (which are meant for people to understand) to EDIFACT form using a program.

(3) The last decision to be taken is how the data is to be exchanged between the participating businesses. There are three alternatives. One can use the internet or extranet or a Value-Added Network provided by some vendors for reliable, secure communications of business data among participating businesses.

We discuss next the advantages and disadvantages of the three methods.

7.7 *Using internet and extranet for EDI transactions*

The major advantage of using the internet is its universal availability. All businesses are now connected to the internet. The cost of exchanging messages using the internet is very small. The major disadvantages are poor reliability and lack of security. Internet protocol does not provide guaranteed delivery of messages and hackers are a perpetual problem. In B2B e-commerce it is important to ensure reliable, guaranteed and secure receipt of electronic documents by the intended receiver. Acknowledgement of receipt, non-repudiation (i.e. sender cannot deny later that he did not send a document such as a purchase order) and tracing transactions later, if necessary, are required. If internet is used, the appropriate protocol for EDI is called Secure Multipurpose Internet Mail Extension abbreviated S/MIME. MIME specifies how EDI messages can be sent using the Simple Mail Transfer Protocol (SMTP) of the internet. S/MIME uses a combination of private and public key encryption, public key certification and digital signature. Encryption enhances security, public key certificate and digital signature is used for non-repudiation. If internet is used for EDI, the following steps are followed.

(1) Agree on EDI format to be used.
(2) Cooperating businesses should establish e-mail addresses for sending/receiving EDI messages and for other communications related to EDI.
(3) Method of encrypting messages, digital signature standard and acknowledgement of EDI messages.
(4) Computers which receive EDI messages must always be powered up with a standby system in case of failure. They must be protected from hackers.

Extranet also uses the same method as internet as the protocol used in extranet is also TCP/IP. The main difference is better security as it is more difficult for hackers to enter an extranet which is a private network or a Virtual Private Network (VPN) connecting cooperating businesses.

Value-added networks (VAN) are private networks (see figure 11) maintained by vendors such as IBM info exchange and General Electric Infoserver which provide EDI services to its customers. VANs provide post boxes for each of its subscribers who want to use their services. A sender wanting to send, say a purchase order, addresses it to a vendor and deposits it in a "postbox" maintained by VAN. The VAN service software receives this, converts it to the required EDI standard format (if requested) and deposits it in a post box which has the recipients' address. VANs operate 24 hours a day, 7 days a week. They have back-up systems to provide fail-safe operations. VANs guarantee delivery of EDI messages, provide acknowledgement to senders, ensure security of messages, and audit trails and non-repudiation. Logs of all activities are maintained and backed up for a reasonable length of time to ensure an effective dispute settlement mechanism. Despite all these services offered by VAN, they have not been popular primarily due to their high cost. Only larger businesses can afford to use their services. Internet-based EDI, on the other hand, is relatively inexpensive. It also provides connections to all businesses large and small. Businesses have also found it expensive to implement ANSI X.12 or EDIFACT standard as they are quite complex to learn and use. Thus, fewer than 15% of businesses using e-commerce for their transactions have adopted the EDIFACT/ANSI standards for EDI. Further, EDIFACT as well as ANSI X.12 EDI standards are low-level machine-oriented documents. They were developed almost 25 years ago when networks were slow and processors also were slow. With the emergence of networks which can transfer data at the rate of gigabits/second and processors with 2GHz clocks, speed is no

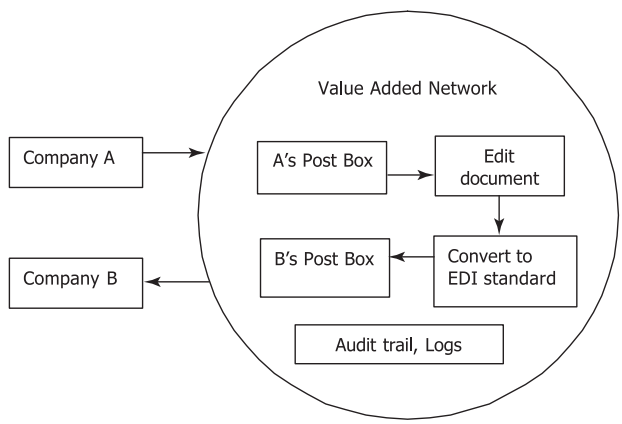


Figure 11. Value-added network.

more a concern. Currently, the major concern is to enable all businesses, big and small, to participate in B2B e-commerce cost effectively. Electronic business documents to be exchanged must have flexible structures as businesses find it impossible to adhere to a common format as they have been using their own business documents for a long time and are reluctant to change their formats as it involves expensive redesign of systems and also the retraining of people. Now-a-days firms across the world transact business with one another. Each country has its own taxation structure, rules and regulations and to expect all firms to adopt a common standard for all business documents is unrealistic. This is the main reason why EDI standards such as EDIFACT and ANSI X.12 are not widely used. This has led to the development of XML (E*X*tended *M*arkup *L*anguage) for describing business documents. We discuss this next.

7.8 *XML for EDI*

As was pointed out in the last section, implementing and operating EDIFACT or ANSI-based EDI system is inflexible and expensive. Thus most businesses, particularly small ones that would like to participate in B2B e-commerce, require cheaper alternatives which are easy to implement and use the internet rather than VAN for communication. The rapid growth of the internet with increase in band width and availability of faster processors has made efficiency less important as compared to flexibility, ease of understanding and good documentation. This led to the development of a flexible and easily implementable messaging system known as XML. XML and HTML (Hyper Text Markup Language), as was stated earlier in this article, are both based on what is known as SGML (Standard Generalised Markup Language), which provides standard notation for defining documents. HTML uses tags to describe the format in which a document is *presented*, for example, spacing, headings, italicizing etc. It does not include tags to represent *logical structure of data*. Thus, it is very difficult to isolate and access data from an HTML page and use it in an application. XML, on the other hand, is a *logical representation* in which we define a structure that directly represents data. A grammar to represent documents called "Document type definition" is used to define various tags used in XML. XML is gaining popularity owing to the following reasons.

(1) XML can be used to define the format, and layout of multimedia documents on a web page. It allows use of hyper-links and is thus a good language to design web pages. As it follows a stricter syntax compared to HTML, it is easier to design browsers to retrieve and view XML documents compared to HTML documents.
(2) Tags used in XML are user-defined and are usually meaningful. Thus users can understand the nature of the document.
(3) XML has the capability to enforce a common structure for large documents which simplifies editing. The emphasis of structure in XML ensures better stability of documents.
(4) Use of XML simplifies EDI, as XML can define the structure, syntax and semantics of documents. It also supports extending and changing the documents if necessary.
(5) As an XML document structure is clearly defined, it is possible to write a program to retrieve contents of fields such as item code, quantity ordered, price per unit etc., from a document such as an invoice received electronically, and use it in an application.

In figure 12 we have given the EDI document defined in table 2 using XML. Observe how easily the XML description can be read and understood. When a company uses XML to describe business documents, it also gives a set of statements which define the syntax of the XML program. This is called a *document type definition* (DTD). This is published in the

```
<order>
    <order-no>A000512</order-no>
    <date>
        <year>2001</year>
        <month> 04</month>
        <day>15</day>
    </date>
    <purchaser>
           <name> Universal Book Traders </name>
           <address>
                  <street> 2 N.S.C. Road </street>
                  <city> Bangalore </city>
                  <pin-code> 560022 </pin-code>
           </address>
           <purchaser-ID> UBT4578 </purchaser-ID>
    </purchaser>
    <supplier>
               <name> PHINC </name>
    </supplier>
    <currency-type> USD </currency-type>
</order>
```

Figure 12. XML definition of book purchase order given in table 2 in EDIFACT notation.

company's website so that any application program wanting to use the XML document can download and interpret the XML document correctly. The DTD corresponding to the XML description of figure 12 is given in figure 13. In this definition #PCDATA means that the element contains a text. There are other key words used in DTD, which we will not discuss in this article. A reference to where the DTD is available (e.g. a file name) should be given at the beginning, as in the XML program of figure 12. The two statements which should be placed at the beginning of the XML program of figure 12 are given in figure 14. It is assumed that the file order.dtd contains the DTD of order.

For details of XML and its application in web design and EDI the reader should read Maruyama *et al* (2000) and Marchal (2001).

We have given a very brief overview of EDI in this article. Those interested in e-commerce must have a good knowledge of XML and Java as Java is used to access XML documents and process data using it. Apart from EDI, e-commerce also requires publication of price lists on a company's web page, business forms to be filled by customers which are made available on-line and managing customer relations (such as attending to information request, complaints, suggestions, etc.) All these also require use of XML which is more flexible than HTML.

8. Emerging applications and some legal issues

So far we described the evolution of e-commerce and some of the technologies crucial in its development. The area of e-commerce is very young and dynamic. Not only has it introduced

```
< !.. This is a comment with delimiters ..>
<! ELEMENT order (entry +)>
<!..order is top-level element and is a listof 1 o
more entries ..>
<!..an entry is an order-no followed by date, purchaser,
supplier and currency type ..>
<! ELEMENT order-no (# PCDATA)
<.. #PCDATA means a character string ..>
<! ELEMENT date (year, month, day)>
<! ELEMENT year (# PCDATA)>
<! ELEMENT month (# PCDATA)>
<! ELEMENT day (# PCDATA)>
<! ELEMENT purchaser (name, address, purchaser-ID)>
<! ELEMENT name (# PCDATA)>
<! ELEMENT address (street, city, pin-code)>
<! ELEMENT street (# PCDATA)>
<! ELEMENT city (# PCDATA)>
<! ELEMENT pin-code (# PCDATA)>
<! ELEMENT purchaser-ID (# PCDATA)>
<! ELEMENT supplier (name)>
<! ELEMENT name (# PCDATA)>
< ! ELEMENT currency-type (# PCDATA)
```

Figure 13. Document type definition for order.

new technologies but has also brought in its wake a number of new social and legal issues. In this section we describe some of the emerging technologies. We also discuss some aspects of the information technology act passed by our parliament in 2000 (Duggal 2000) whose primary purpose is to promote e-commerce and e-governance. We first briefly describe mobile commerce, commonly known as m-commerce.

8.1 *Mobile commerce*

Mobile commerce (Unbaczewski *et al* 2003) is defined as the conduct of business and providing services using portable wireless devices which can communicate with computers connected to the internet. The number of mobile phones and portable personal digital assistants is increasing rapidly and it is predicted that by 2005, 40% of C2B e-commerce will be from mobile phones and mobile personal digital assistants. In table 3 we give a layered architecture (Varshney *et al* 2000) of m-commerce. We will focus our attention on the top layer, namely, novel applications. A number of innovations are possible when we introduce mobility. One of the most interesting applications is tracking and routing goods in transit. In this application each package being shipped has a small broadcast device embedded in it which continuously

```
<? XML version = "1.0"?>
<! DOCTYPE order SYSTEM "order.dtd.">
```

Figure 14. Statement to be set at the beginning of the XML program of figure 12.

Table 3. Layered architecture of m-commerce (adapted from Varshney *et al* 2000).

Mobile user applications (Mobile inventory control, product location, mobile entertainment, mobile information, mobile distance education).	Application layer
Wireless user infrastructure (browsers, hand held devices)	Software layer
Mobile middle ware. Wireless application protocol (WAP)	Middle ware
Wireless network infrastructure. Cellular systems, wireless access points, satellite, IEEE 802.11 a/b/g standards	Hardware layer

broadcasts its unique identity code. With the help of a cellular wireless infrastructure, its location can be found. One can use this to trace packages and inform customers when they can expect to receive a package. This information can also be used to reroute a package where it is critically needed.

Another application is to inform a chemist or a hospital about expiry dates of drugs in their inventory. This is done by embedding a small wireless device (called a radio frequency identification tag) in the packing of expensive drugs which have a short life. These packets broadcast their status once a day which is monitored by a server in the shop or hospital and appropriate action is initiated. An emerging application is to provide information on delays in flight schedules, traffic jam reports etc., to mobile users. Mobile commerce is also used for providing to customers who are in transit, information on nearby stores which have an item they need and also comparative prices to let them decide where they want to shop.

8.2 *Intellectual property rights and electronic commerce*

The advent of internet which allows easy distribution and copying of all types of information, text, audio and video has alarmed publishers of books, music and films. The copyright issue has also plagued the spread of the digital library movement. The major problem with content available in digital form is the ease with which they can be copied. Digital information can flow across national boundaries freely at electronic speed and is practically impossible to monitor and control. Many content providers encrypt material they store in the web to prevent easy access and copying. Such encryption impedes free flow of information and the "fair use doctrine" which governs the existing copyright laws for print media, tapes and CD. Users have thus been trying to find methods of decrypting encrypted material. In a new landmark law enacted by United States Congress in October 1998, called the Digital Millenium Copyright Act, it has been made illegal to circumvent access controls used by copyright owners to protect their work and *even to develop technologies* which may be used to circumvent protection. There is raging debate on this issue as it seems to prevent "fair-use" which is the basis of agreements arrived at in the World Intellectual Property treaty (Samuelson 1999; Paulson 2001). Copyright issues get highly complicated when it comes to computer software. The issues are not yet fully resolved and it is still being argued by lawyers and ethicists (Johnson 2001).

8.3 *Information technology act, 2000*

Our parliament passed the Information Technology Act, 2000, which provides the legal infrastructure for e-commerce in India. It received the President's assent and is now a law. The object of the Act has been stated as:

"To provide legal recognition for transactions carried out by means of EDI and other means of electronic communication commonly referred to as e-commerce which involves the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1891, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act 1934 and for matters connected therewith or incidental thereto" (Duggal 2000).

This act is a landmark one which now provides legal status to e-mail correspondence and soft copies of documents. The major interesting aspects of the act are the following.

(1) E-mail correspondence has legal status and thus can be used in evidence. Digitally signed documents are now recognized.
(2) A controller of public key-certifying authorities has been appointed by the Government of India. The controller recognizes certifying authorities who will have the authority to issue public key certificates and verify digital signatures.
(3) All applications to Government bodies can be filed in electronic form. Government can issue licences, permits, sanctions, approvals etc., online, in electronic form.
(4) Many archival documents which companies and government departments are required, by law, to keep for a specified period can now be stored in CD-ROM or tapes, saving precious space and enabling easy retrieval. Care must be taken that such electronically stored documents also keep details which identifies the origin of the document, date and time of despatch or receipt.
(5) The IT Act provides statutory remedy to companies whose networks are illegally accessed and stored information is stolen or damaged. Monetary claims up to one crore of rupees can be made against intruders.
The Act provides for punishment to a hacker who

(i) downloads, copies or extracts data from a database without permission of the owner,
(ii) introduces any soft-contaminant or computer virus into any computer or computer network,
(iii) damages programs or data residing in a computer or network or illegally copies them,
(iv) disrupts a computer or network,
(v) denies access to a computer or a network by authorised persons,
(vi) charges for services availed of by a person to another person by tampering or manipulating accounts in a computer or network.

Hacking has now been classified as a crime under the Indian Penal Code. Punishment for hacking is imprisonment of up to 3 years or fine up to Rs. 2 lakhs or both. Teenagers who hack "for fun" should realise that they will have fun in jail up to 3 years!

Even though the IT Act has a number of laudatory features it still has some flaws as listed below.

(i) It is not clear how cyber crimes affecting computers in India committed from outside India using the internet will be handled;

(ii) It is not clear how many of the provisions in the Act will be enforceable;
(iii) The Act does not apply to a number of important legal documents, such as a power of attorney, a will, any contract for the sale of immovable property and a negotiable instrument;
(iv) The Act does not have any provision regarding domain names and resolving disputes on such names;
(v) It does not deal with intellectual property rights, trademarks and patents;
(vi) Many cyber crimes are not defined in the Act such as cyber defamation, cyber harassment and cyber stalking;
(vii) Statutory bodies may at their discretion not accept electronic documents. In other words a person cannot insist that he/she will submit only an electronic document.

Besides the above, there are some aspects of privacy and individual freedom, which these laws dilute by giving enormous power to the executive. For instance, it allows any agency of the government to intercept any information transmitted through any computer resource, if the same is necessary in the interest of the sovereignty or integrity of India, the security of the state, friendly relations with foreign governments, maintaining public order or for preventing incitement to commit a cognizable offence. Another draconian provision is the powers given to police officers not below the rank of a Deputy Superintendent of Police to enter any public place and search and arrest *without warrant* any person found therein, who is reasonably suspected of having committed or of committing or of *being about to commit* any offence under the IT Act. This provision is supposed to prevent software piracy and hacking but has enormous scope for harassment.

It is heartening to note that India is one of the few countries in the world which now has an IT law in place even though it is not "perfect". This is expected to boost e-commerce in the country.

9. Conclusion

Electronic commerce is rapidly growing in the world and is expanding into what is known as e-services (Stafford 2003). A number of technologies have converged to facilitate the proliferation of e-commerce. Rapid advances in computer technology exemplified by the availability of very powerful personal computers at low cost, coupled with rapid acceleration in communication networks, have enabled computers worldwide to be interconnected and thus have revolutionized the way business is done. The mere availability of hardware infrastructure is not sufficient to proliferate applications. We require several software layers on the basic hardware and international standards to promote applications such as e-commerce. In this article, we have given a flavour of these software systems which constitute the building blocks of e-commerce. Even though technology is essential to enable the emergence of e-commerce it is not sufficient to promote and proliferate e-commerce applications. We need an appropriate legal framework. We have thus discussed the enabling legal framework which has been enacted in India. In the age of internet, national boundaries are becoming meaningless. Data can travel at the speed of light across national boundaries; they can flow not only along wired networks but also by wireless. Governments find it very difficult to stop data flow. Applicability of national laws in international e-commerce has become impractical. This is exemplified particularly by the emergence of vandals who disrupt the internet by proliferating

viruses, worms etc., which affect all countries. International cooperation in standardization of not only technology but also laws is needed. It is evident that the cost of doing business has come down and the reach of business has increased with the emergence of e-commerce. With international cooperation, e-commerce is bound to improve the quality of life of individuals all over the world.

References

Awad E M 2002 *Electronic commerce* (New Delhi: Prentice Hall of India)
Ben-Ameur W, Kerivin H 2003 New economical virtual private networks. *Commun. ACM* 46(6): 69–73
Brewer E A (ed.) 2002 The consumerside of search. *Commun. ACM* 45(9): 40–56
Chaum D 1992 Achieving electronic privacy. *Sci. Am.* 96–101
Cheswick W R, Belleroin G M 1994 *Firewalls and internet security* (Reading, MA: Addison Wesley)
Comer D E 1995 *Internetworking with TCP/IP* (New Delhi: Prentice Hall of India) vol. 1
Daemen J, Rijmen V 2002 *The design of Rijndael. AES – The advanced encryption standard* (New York: Springer-Verlag)
Duggal P 2000 *Cyberlaw in India – An analysis* (New Delhi: Saakshar)
Johnson D G 2001 *Computer ethics* (New Delhi: Pearson Education Asia)
Kalakota R, Whinston A B 1999 *Frontiers of e-commerce* (Reading, MA: Addison-Wesley/Longman)
Landau S 2000 Designing cryptography for the new century. *Commun. ACM* 43(5): 115–120
Lynch D C, Lundquist L 1996 *Digital money: The new era of internet commerce* (New York: John Wiley)
Marchal B 2001 *XML by example* (New Delhi: Prentice Hall of India)
Maruyama A, Tamura K, Uramoto N 2000 *XML and Java* (Reading, MA: Addison-Wesley)
Minoli E M, Minoli D M 1999 *Web commerce technology handbook* (New Delhi: Tata McGraw Hill)
Pardi W J 1999 *XML in action* (Seattle, WA: Microsoft Press)
Paulson L D 2001 Copyright ruling generates concern. *IEEE Comput.* 34(1): 30
Rajasekhar T B 1998 Web search engines. *Resonance* 3(11): 40–53
Samuelson P 1999 Why the anticircumvention regulation needs revision. *Commun. ACM* 42(9): 17–21
Sarkar P 2000 A sketch of modern cryptography. *Resonance* 5(9): 2–40
Shim S S Y *et al* (ed.) 2004 Securing the high speed internet. *IEEE Comput.* 37(6): 33–67
Stafford T F (ed.) 2003 e-Services. *Commun. ACM* 46(6): 26–67
Stallings W 1998 *Data and computer communications* 5th edn (New Delhi: Prentice Hall of India)
Stallings W 1999 *Cryptography and networking security – Principles and practice* 2nd (edn) (New Delhi: Prentice Hall of India)
Urbaczewski A *et al* (eds) 2003 Mobile commerce. *Commun. ACM* 46(12): 31–65
Varshnay V, Vetter R J, Kalakota R 2000 Mobile commerce: A new frontier. *IEEE Comput.* 33(10): 32–38