Chapter 16. The Internet as a Message-Handling Network - 2

Table of Contents

Introduction to the Internet as a Message-Handling Network - 2

Context

This chapter continues the treatment of the Internet as a message-handling network commenced in chapter 15.

Introduction

The conceptual step from data exchange to message exchange is elaborated to show that other forms of messaging can be conceptualised in the same way as e-mail. E-mail supports the exchange of unstructured information, but the step needed to adapt electronic messaging for the exchange of structured information is straightforward. This capability provides the basis of Electronic Data Interchange (E.D.I.). The purpose of E.D.I. in exchanging invoices, delivery notes, receipts and so on in standardised form to enable the automation of commerce is explained. Other benefits of E.D.I. are covered. The thrust of the treatment is to present E.D.I. within a framework of 'e-mail with forms'. Although forms based browser technology is currently widespread, many industrial sectors have adopted other variants of SGML to represent document structure. XML is such a recent variant.

Secure communication is also presented as a form of messaging. Ways in which messages may be processed prior to their transmission and after their reception so as to make message exchange secure are examined to bring out the basic principles of encryption and decryption. Public key encryption is then explained. It is shown that public key encryption can be used for both encryption and authentication. Aspects of electronic commerce, including various forms of electronic payment, are used to illustrate patterns of exchange that require various patterns of authentication and encryption.

Objectives

At the end of this module, you should be able to:

- understand the concepts underpinning E.D.I.;
- appreciate the standards and usage of E.D.I.;
- analyse issues of security and authentication in message exchange;
- understand the basic ideas of different methods of encryption.

Content

In parallel with this chapter, you should read relevant chapters in your textbooks.

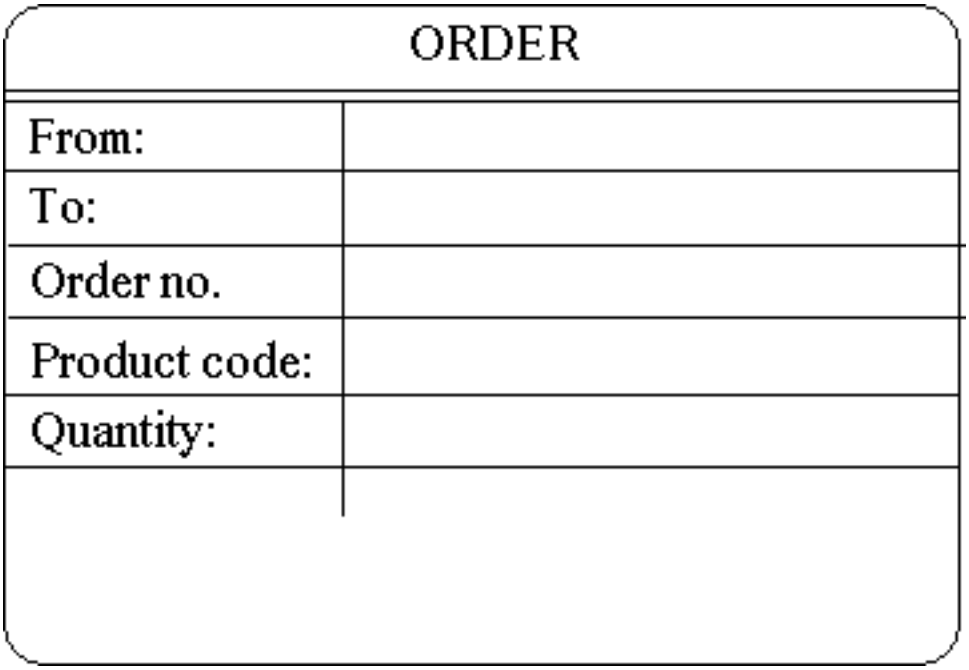
Electronic Data Interchange (E.D.I.)

Electronic Data Interchange is used by organisations to exchange in a standard way the information needed for trading in electronic fashion. In order to trade with each other, the items that organisations

need to exchange include orders, invoices, bills and receipts. E.D.I. provides what can be thought of as a standard form for each of these. The forms and the information they contain can be sent electronically in essentially the same way as an e-mail, so that E.D.I. can be thought of as e-mail with forms rather than the blank sheets of ordinary e-mail. Whereas e-mail supports the exchange of unstructured information, E.D.I. supports the exchange of information that is not only structured but structured in a way designed to support commercial transactions.

The fact that E.D.I. supports a set of standards ensures that organisations exchanging information with the aid of software conforming to these standards can be confident that they will assign the same meaning to the exchanged messages and their components. There will, for example, be no disagreement that a particular standard message is an order, and that a specific item within the message is a price.

The E.D.I. software provides the forms and ensures that only information of the correct type can be entered in each field of a form. On screen, a form could be presented rather like this:



When a form has been completed, the form and the information on it are encoded in a standard fashion to provide a message for transmission. When a message is received, it can be appropriately decoded by E.D.I. software to recover the form and its contents. This assures that both will be assigned their correct meaning. The information on the form can then be acted upon and passed on to the next stage in the process of progressing the transaction.

In this way, E.D.I. brings to electronic trading many of the same advantages that e-mail brings to personal communication.

To Do

Do Review Questions 1, 2 and 3.

Carry out Activity 1.

E.D.I. and electronic trading

With E.D.I., electronic trading can be automated from the placing of an initial order through the stages of invoicing, delivery, payment and receipt. The data on an E.D.I. form can be used directly as input to an organisation's information systems because its standardised format ensures compatibility. No re-keying of data is necessary.

The following sequence of activities is indicative of what can be triggered automatically on receiving an E.D.I. order form:

- the order can be checked for correctness,
- the order can be passed to the ordering system,
- orders can be passed to warehouses and suppliers,
- the appropriate data can be passed to other databases,
- invoices can be generated, and so on.

In this way, E.D.I. is an enabler for a particular style of electronic commerce.

To Do

Carry out Activity 2.

Electronic payment

Payment can also be made by exchanging electronic forms, in which case all aspects of a transaction can be completed over the network except the delivery of physical goods. The payment form could take any of a number of designs: it could be designed to hold credit card details; it could be designed as a digital cheque. In any event, particular attention needs to be paid to security and authentication. Security is needed to keep secret the amount of the payment, which is confidential to the parties involved, and to ensure that the electronic payment is not tampered with. It is usually provided by some form of encryption. Authentication is needed to ensure that the payment is really made by the purported payer. A form of electronic signature can be used to provide authentication.

There are other circumstances in which secure communication and authentication are required or desired. We examine how they may be provided in the next section.

To Do

Do Review Questions 4, 5 and 6.

Carry out Activities 3, 4 and 5.

Secure communication

Secure communication can be provided by encrypting messages prior to their communication so as to disguise them. After this, even if communicated messages are intercepted, they cannot be read because of their disguised form. Messages to be stored can also be secured by encrypting them prior to their storage. In this section, we first look at simpler methods of encryption before turning to more sophisticated methods.

Simpler methods of encryption

The simpler methods of encryption can be explained by using an analogy with a physical situation. A physical means of securing a message while it is taken from one place to another is to put it in a box, and to lock the box with a key. The secured message can then be transported to its destination, where the recipient can unlock the box and remove the message.

This scenario has three important characteristics.

- It is symmetric. The same key is used is used to secure the message (by locking the box) and to recover it (by opening the box).

- A secret must be shared. For the sender and the recipient to share one secret (the contents of a message) they must share another secret (the key).

- The level of security is proportional to the number of possible keys. Anyone intercepting the secured message can see the lock on the box and infer something about the type of key that opens it. The more keys there are of this type, the harder it will be to guess which one opens the box.

Now let us turn to the encryption of messages to be exchanged over a data network, and see how this aligns with our analogy.

Any message to be exchanged over a data network consists of a sequence of binary digits. If the message contained just the ASCII code for 'A', it would be:

01000001

To encrypt this, a key is needed. The key also consists of a sequence of binary digits, such as:

10101010

The message and the key must now be combined to give the encrypted message. This can be done bit by bit, combining the first bit of the message and the first bit of the key, then the second bit of the message and the second bit of the key, and so on until all the bits have been dealt with. A combination rule such as the following (which is the exclusive-or rule) can be used:

Message	0	0	1	1
Key	0	1	0	1
Encrypted Message	0	1	1	0

The first bit of the encrypted message is given by the third column of the table as 1, the second bit of the encrypted message is given by the fourth column of the table as 1, and so on.

Encrypting the message has secured it so that it can be safely sent. On reception, it must be decrypted, but the symmetry of the scenario means that it must be decrypted with the same key as that used for encryption. Consequently, decryption proceeds as follows. The encrypted message is:

11101011

The key is still:

10101010

The combination rule is also the same, but for decryption it reads as:

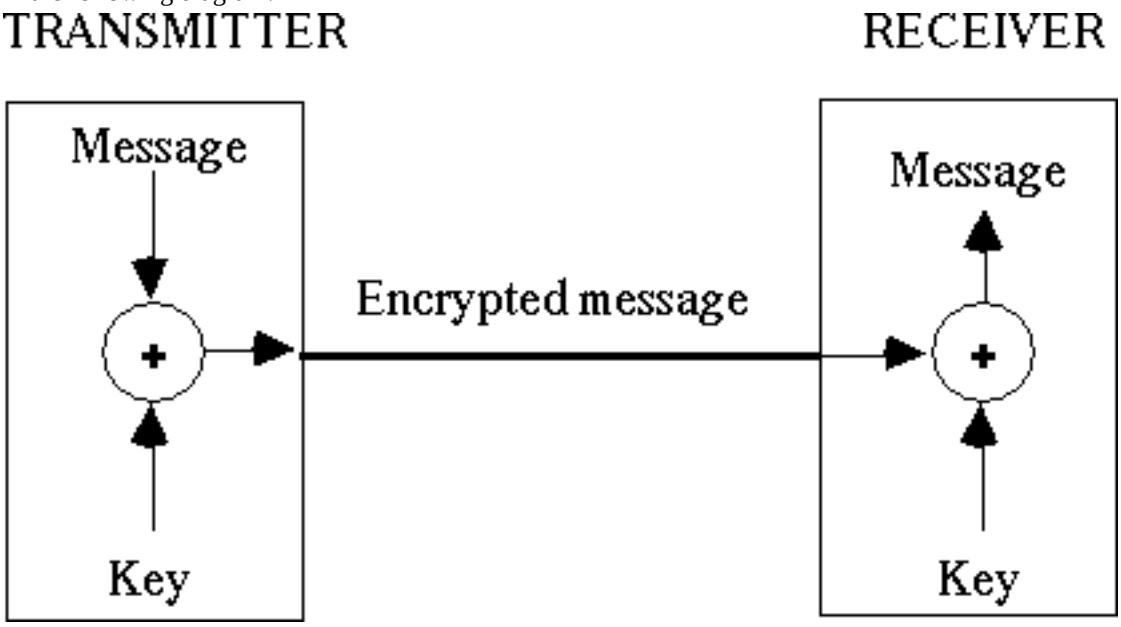
Encrypted Message	0	0	1	1
Key	0	1	0	1
Message	0	1	1	0

The first bit of the decrypted message is given by the fifth column of the table as 0, the second bit of the encrypted message is given by the fourth column of the table as 1, and so on.

To Do

Do Review Question 8.

The complete process of communicating a message securely with the use of encryption is represented in the following diagram.



To Do

Carry out Activities 6 and 7.

More-sophisticated methods of encryption

The encryption methods used in practice incorporate techniques that are more sophisticated than those illustrated in the previous section. In particular, they are less constrained because they do not require either symmetry or the sharing of a secret. This extra freedom makes them more secure by making it harder to guess the key.

There is a physical method of providing security that provides an analogy with these methods of encryption. The message is still secured by placing it in a box, but this time the box is secured with a snap lock and, on its receipt, the box is unlocked with the appropriate key.

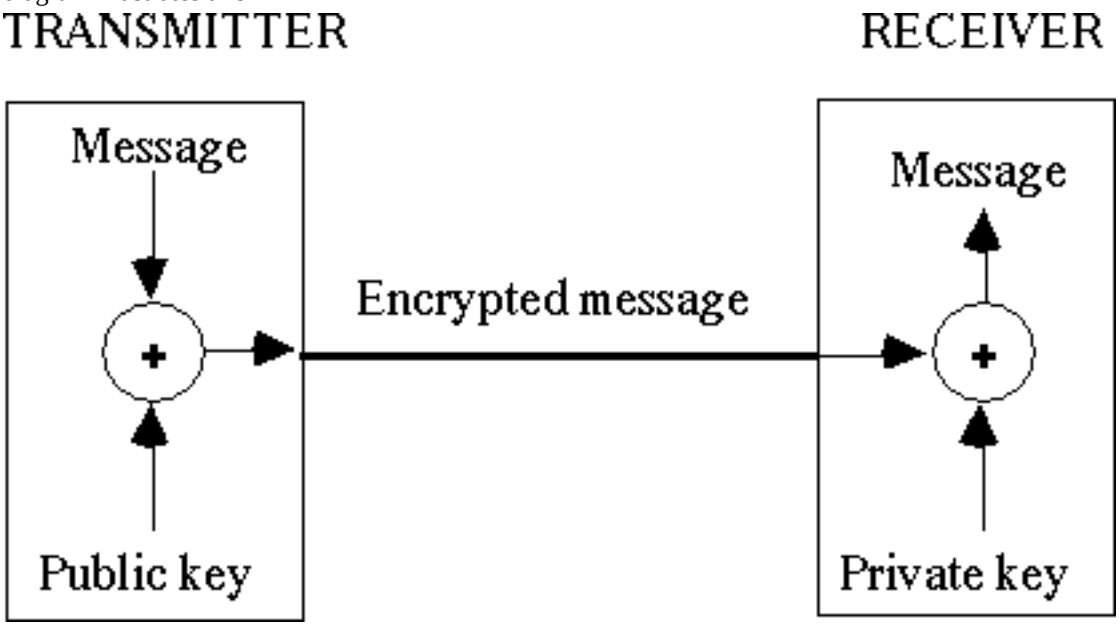
We can note that:

- The situation is not symmetric. The security of the message is ensured by snapping a lock and the message is removed by using a key to open the lock.
- Ensuring security is easy (just snap the lock) while removing the message is hard (unless you have the key).
- There is no shared secret
- In fact, the locks can be made publicly available. To send someone a message, you use their lock, safe in the knowledge that they have the key to their own lock.

This analogy provides the basic idea of the widely used method known as public-key encryption. This form of encryption uses two keys (since it is not symmetric). The snap lock corresponds to the 'public key' that is made public. The physical key corresponds to the 'private key' which is the secret of its owner.

All the subscribers to public-key encryption have their own public and private keys: they all publish their public key. For secure communication, a message is encrypted prior to transmission with the

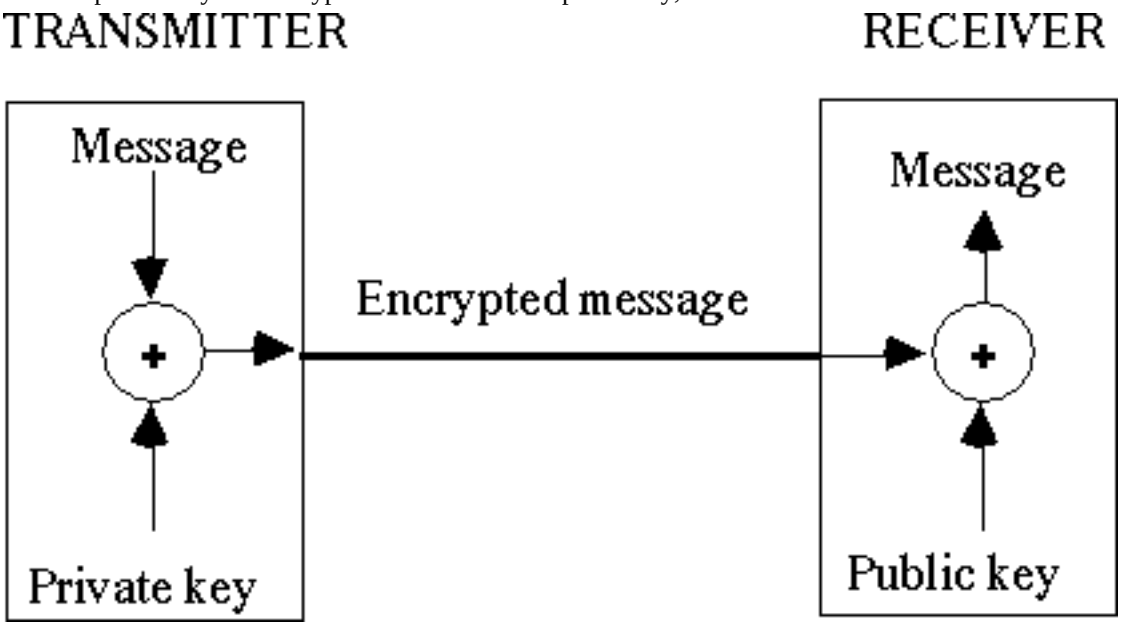
recipient's public key. On receipt, it can be decrypted with the recipient's private key. The following diagram illustrates this



To Do

Do Review Question 9.

Public-key encryption also supports authentication. To achieve it, the message is encrypted with the sender's private key and decrypted with the sender's public key, as shown.



To Do

Do Review Question 10.

The basic idea behind the determination of a pair of public and private keys is a 'trap-door' problem, that is a problem that is easy in one direction, but hard in the other. The hard version of the particular problem used in practice is: Given a very large number, N, with only two factors, P and Q, find the factors. The reverse, and easy, problem is: given two factors, P and Q, of a very large number, N, find N. The solution to this is P*Q = N.

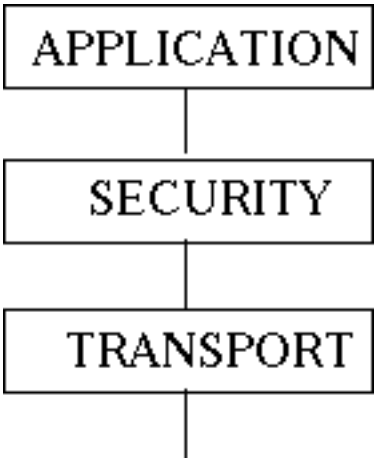
This problem provides a public key (N) and a private key (P and Q). The public key (N) can be published because it is hard to find the private key (P and Q) from it. But from the private key (P and Q), it is easy to find the public key (N). Now secure communication is possible because messages can be encrypted using N, which is public knowledge, but can only be decrypted with a knowledge of P and Q, which is private knowledge and very hard to determine.

To Do

Do Review Questions 11 and 12.

The provision of secure communication on a network

One way to provide secure communication on a network such as the Internet, which makes no such provision itself, is to add a layer with responsibility for it to the communications software. This layer needs to be placed between the Application layer, which produces the messages needing to be secured, and the Transport layer, which is beginning the process of preparing the messages for transmission over the network. In this position, the layer can accept messages, encrypt them, and then pass on encrypted messages for transmission.



A security layer would typically provide public-key encryption, in which case it would be able to communicate with the public-key servers that hold the published public keys.

On the Internet, the so-called Secure Sockets layer is one example of a layer located in this position with responsibility for the automatic provision of security.

Summary

Public-key encryption can be used to assure both secure and authenticated communication.

The idea of public-key encryption is that two keys are needed, one for encryption and one for decryption. Anyone wanting to receive messages publishes a key - their public key. They also have a private key. After this,

- security is ensured if the sender uses the recipient's public key to encrypt and the recipient uses his or her private key to decrypt.
- authentication is achieved if the sender uses his or her private key to encrypt and the recipient uses the sender's public key to decrypt.

With security and authentication in place, electronic payment can be carried out with 'digital cheques', in this way:

1. The payer makes out a digital cheque for a certain amount (creates a message promising to pay a certain amount), adds a 'digital signature' for authentication, encrypts the cheque and sends it to the payee.

2. The payee decrypts the cheque, adds a 'digital signature', encrypts the endorsed cheque and sends it to the bank.

3. The bank decrypts the endorsed cheque, authenticates the signatures and transfers funds accordingly.

Note that this sequence of events can be automated, and that 'digital cheques' should be numbered to ensure that they are not cashed more than once.

To Do

Carry out Activity 8.

Encryption: a formal description

The process of encryption with a public key and a secret key can be represented using the following notation:

D data to be encrypted

X_p public key of entity X

X_s secret key of entity X

Thus, X_p(D) and X_s(D) denote the results of encrypting D with, respectively, the private and secret keys of X. It is also necessary that:

X_p(X_s(D)) = X_s(X_p(D)) = D

In fact, for T to send data securely to U the process is:

T has data D;
T encrypts the data with the public key of U to get U_p(D);
T sends this encrypted data to U;
U receives the encrypted data and decrypts it with its secret key: U_s(U_p(D)) = D.

For U to authenticate itself to T, the process is:

U encrypts some data with its secret key, U_s(D);
U sends this encrypted data to T;
T receives the encrypted data and decrypts it with the public key of U: U_p(U_s(D)) = D.

Activities>

Activity 1 - electronic commerce

Identify the major benefits that electronic commerce brings with it.

You can find a discussion of this activity at the end of the chapter.

Activity 2 - commercial transactions

Explain the reason that it is possible to automate commercial transactions in general, and with the aid of E.D.I. in particular.

You can find a discussion of this activity at the end of the chapter.

Activity 3 - encryption and authentication

Give a further example of a situation where there is a need for encryption and one where there is a need for authentication.

You can find a discussion of this activity at the end of the chapter.

Activity 4 - electronic payment

With the aid of your textbooks and other resources, find out what methods are currently used for electronic payment on the Internet.

Activity 5 - encryption 2

One simple encryption method for use with text is to replace each letter in a text by the letter occurring, say, five places later in the alphabet. So A is replaced by F, B by G, and so on. By taking the alphabet as cyclical, with A following Z, the letters at the end of the alphabet also have replacements.

Now encrypt the message MESSAGE. Give the rule for decryption.

You can find a discussion of this activity at the end of the chapter.

Activity 6 - keys

On the assumption that an 8-bit key is being used, determine the number of possible keys. What is the likelihood the a randomly selected 8-bit sequence is a correct guess at the key? How can the system be made more secure?

You can find a discussion of this activity at the end of the chapter.

Activity 7 - encryption and decryption

Explain how the two versions given for the table, one to be used during encryption and one during decryption, are essentially the same.

You can find a discussion of this activity at the end of the chapter.

Activity 8 - digital signatures

Find out what a 'digital signature' is.

You can find a discussion of this activity at the end of the chapter.

Review Questions

Review Question 1

How can E.D.I. be characterised?

You can find an answer/comment for this review question at the end of the chapter.

Review Question 2

Why is it important to have an agreed standard for E.D.I.?

You can find an answer/comment for this review question at the end of the chapter.

Review Question 3

What advantages does E.D.I. bring to electronic trading?

You can find an answer/comment for this review question at the end of the chapter.

Review Question 4

What is encryption?

You can find an answer/comment for this review question at the end of the chapter.

Review Question 5

What is authentication?

You can find an answer/comment for this review question at the end of the chapter.

Review Question 6

If you were sending your credit card number over the Internet, would you protect it? If so, how would you protect it?

You can find an answer/comment for this review question at the end of the chapter.

Review Question 7

What is the complete encrypted message?

You can find an answer/comment for this review question at the end of the chapter.

Review Question 8

What is the complete decrypted message? Is it the same as the original message?

You can find an answer/comment for this review question at the end of the chapter.

Review Question 9

Why does encrypting a message with a public key and decrypting it with a private key provide security?

You can find an answer/comment for this review question at the end of the chapter.

Review Question 10

Why does encrypting a message with a private key and decrypting it with a public key provide authentication?

You can find an answer/comment for this review question at the end of the chapter.

Review Question 11

If N=45, what are P and Q?

You can find an answer/comment for this review question at the end of the chapter.

Review Question 12

How is authentication achieved using N, P and Q?

You can find an answer/comment for this review question at the end of the chapter.

Discussion Topics

1. It has been claimed that E.D.I. is to inflexible and cumbersome for use in electronic commerce on the Web. In what sense could it be 'flexible and cumbersome'? Is it being used, or has something else emerged to fill its potential role in e-commerce.

2. The Internet has had security features 'bolted on' to it. Is this a good idea or, on the basis that security should be 'built in' to the design of a system, would anyone wanting really good security be well advised to wait for the deployment of IP Version 6?

3. The government of the United States has sought to impose limits on the level of security that may be employed on the Internet and elsewhere. Is this a good idea? Is it possible to impose such limits?

Answers and Comments

Activity 1

Electronic commerce brings with it the ability to automate the entire process of carrying out a transaction. It also allows the information provided during the transaction to be collected and used for other purposes, such as tracking sales, monitoring warehouse contents, re-ordering, identifying customer preferences, and so on.

Activity 2

A commercial transaction requires the exchange of a specific set of messages in a specific order. A sale for example, is initiated by placing an order, which is acknowledged. Then an invoice is sent to indicate that the goods have been despatched, after which payment is completed and, finally, a receipt is despatched. this simplified account should make clear that there is a definite protocol associated with a particular type of transaction. A protocol provides a sequence that can be followed automatically. Each stage in the sequence will be triggered by the occurrence of the appropriate event.

With its forms, E.D.I. provides a set of standard messages. When used in the correct sequence, they will create the protocol appropriate to a particular type of transaction.

Activity 3

Encryption is needed in any situation where the content of a transmitted message needs to be kept secret, whether for reasons of commercial security or for personal reasons. Authentication is needed in any situation where one person is sending instructions or orders to another.

Activity 5

The encrypted version of MESSAGE is RJXXFLJ. It is decrypted by replacing each letter of the alphabet by the letter five places before it.

Activity 6

There are 256 possible keys. The chance of a randomly selected 8-bit sequence being correct is 1 in 256. The level of security can be increased by using a longer key (and then selecting, say, its first eight bits).

Activity 7

The tables both give the same rule for converting two inputs to one output: one input and the output are labelled differently in the two cases.

Another way to see that they are the same is to note that by taking the second table, swapping its first and third rows and then rearranging its columns will convert it to the first table.

Activity 8

It is an agreed identifier that has been encrypted with its owner's private key.

Review Question 1

As e-mail with standard forms.

Review Question 2

To ensure compatibility.

Review Question 3

Speed, cheapness and efficiency.

Review Question 4

A way of disguising a message so that it is difficult to see through the disguise unless you know how.

Review Question 5

A way of ensuring that the alleged sender of a message really is the sender.

Review Question 6

I would protect mine, by ensuring that it was encrypted.

Review Question 7

11101011

Review Question 8

01000001, which is the original message.

Review Question 9

Because the intended recipient is the only holder of the private key with which the message must be decrypted.

Review Question 10

Because the recipient can only decrypt it with the alleged sender's public key if it was first encrypted with the private key of that sender, who is the only person to know it.

Review Question 11

P=9, Q=5.

Review Question 12

The sender needing authentication encrypts with her private key, P and Q. The recipient achieves authentication by decrypting with the sender's public key, N.