SPECIALIST READING

A **Find the answers to these questions in the following text.**

1 What does data encryption provide?
   a privacy
   b integrity
   c authentication
2 A message encrypted with the recipient's public key can only be decrypted with:
   a the sender's private key
   b the sender's public key
   c the recipient's private key
3 What system is commonly used for encryption?
4 What is the opposite of 'encrypt'?
5 A message-digest function is used to:
   a authenticate a user
   b create a MAC
   c encrypt a message
6 What information does a digital certificate give to a client?

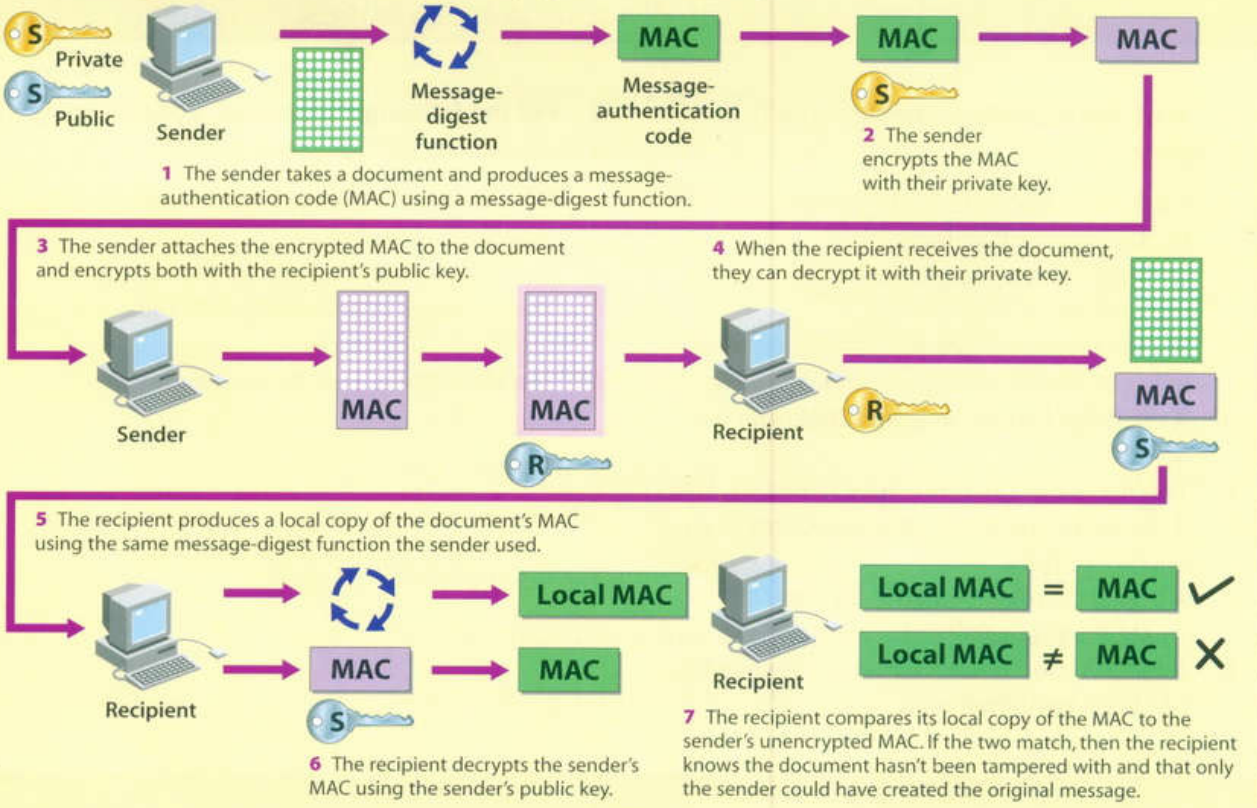
Safe Data Transfer

Secure transactions across the Internet have three goals. First, the two parties engaging in a transaction (say, an email or a business purchase) don't want a third party to be able to read their transmission. Some form of data encryption is necessary to prevent this. Second, the receiver of the message should be able to detect whether someone has tampered with it in transit. This calls for a message-integrity scheme. Finally, both parties must know that they're communicating with each other, not an impostor. This is done with user authentication.

Today's data encryption methods rely on a technique called public-key cryptography. Everyone using a public-key system has a public key and a private key. Messages are encrypted and decrypted with these keys. A message encrypted with your public key can only be decrypted by a system that knows your private key.

For the system to work, two parties engaging in a secure transaction must know each other's public keys. Private keys, however, are closely guarded secrets known only to their owners. When I want to send you an encrypted message,

This shows the complex process that's required to send data securely across open communication lines while satisfying the three basic tenets of secure transfer: data encryption, interference prevention, and user authentification.



I use your public key to turn my message into gibberish. I know that only you can turn the gibberish back into the original message, because only you know your private key. Public-key cryptography also works in reverse – that is, only your public key can decipher your private key's encryption.

To make a message tamper-proof (providing message integrity), the sender runs each message through a message-digest function. This function within an application produces a number called a message-authentication code (MAC). The system works because it's almost impossible for an altered message to have the same MAC as another message. Also, you can't take a MAC and turn it back into the original message.

The software being used for a given exchange produces a MAC for a message before it's encrypted. Next, it encrypts the MAC with the sender's private key. It then encrypts both the message and the encrypted MAC with the recipient's public key and sends the message.

When the recipient gets the message and decrypts it, they also get an encrypted MAC. The software takes the message and runs it through the same message-digest function that the sender used and creates its own MAC. Then it decrypts the sender's MAC. If the two are the same, then the message hasn't been tampered with.

The dynamics of the Web dictate that a user-authentication system must exist. This can be done using digital certificates.

A server authenticates itself to a client by sending an unencrypted ASCII-based digital certificate. A digital certificate contains information about the company operating the server, including the server's public key. The digital certificate is 'signed' by a trusted digital-certificate issuer, which means that the issuer has investigated the company operating the server and believes it to be legitimate. If the client trusts the issuer, then it can trust the server. The issuer 'signs' the certificate by generating a MAC for it, then encrypts the MAC with the issuer's private key. If the client trusts the issuer, then it already knows the issuer's public key.

The dynamics and standards of secure transactions will change, but the three basic tenets of secure transactions will remain the same. If you understand the basics, then you're already three steps ahead of everyone else.

[Jeff Downey, 'Power User Tutor', PC Magazine, August 1998]

B **Re-read the text to find the answers to these questions.**

1 Match the functions in Table 1 with the keys in Table 2.

Table 1

a to encrypt a message for sending
b to decrypt a received message
c to encrypt the MAC of a message
d to encrypt the MAC of a digital signature

Table 2

i sender's private key
ii trusted issuer's private key
iii the recipient's private key
iv the recipient's public key

2 Match the terms in Table A with the statements in Table B.

Table A

a Gibberish
b Impostor
c Decipher
d MAC
e Tenets
f Tamper

Table B

i Message-authentication code
ii Principal features
iii Meaningless data
iv Person pretending to be someone else
v Make unauthorised changes
vi Convert to meaningful data

► Additional exercises on page 129