Solutions

Chapter 2: Understanding encryption

Skill builder: Programming and cracking a symmetric Caesar Shift code, pages 12–13

The spreadsheet solution for this Skill builder is provided online: see Caesar_code.

Page 12: How would this method of using frequencies work?

Some letter substitutions could be deduced by finding which letters occur most often, then next most often and so on. The letter with the highest frequency is likely the letter ‘e’, then ‘a’ and ‘t’ and so on. Once they are replaced the message will be easier to crack.

Skill builder: using letter frequency analysis to crack code, page 14

3 Some letter substitutions could be deduced by finding which letters occur most often, then next most often and so on. The letter with the highest frequency is likely the letter ‘e’. Since the shift is the same for each letter, all that is needed is to identify a single case to decipher the whole message.

Knowledge probe: How public–private key encryption works, page 16

Table 2.3

M7	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Review, pages 17–18

Identify

1 Caesar shift, pictographs, acronyms, mirror writing, morse code.

2 A process in cryptography of encoding (converting) data, using mathematical formulas, into a form that only an intended recipient can decode.

3 To protect data from being accessed and decrypted by unauthorised persons.

4 In cryptography a hash function could be used by two people to confirm each possesses identical information, but where neither is willing to reveal it first! Imagine both Alice and Bob are spies and claim to know the identity of a traitor among them. Alice and Bob could both calculate the hash for the name of the traitor and check that their two hashes are the same.

Analyse

5 Each letter in the English language have known frequencies of occurrence. If a code uses direct substitution, or even if it does not, the frequency of occurrence of a letter can suggest the original data it replaces.

6 Symmetric encryption uses the same key for both encryption and decryption whereas asymmetric method uses two different keys consisting of a public key, which is shared, and a private key, which is not shared. The public key is used to encrypt data that can then only be decrypted using the private key.

7 Both Alice and Bob would share their public keys with each other. Each would then use the other's key to encode their message and send it. Each would then use their private key to decode the message they received.

Research

8 Cracking the Enigma code allowed the Allied powers to read the encrypted radio communications of the Axis powers to learn troop movements and strategy. Weaknesses in the design of the Enigma encryption system were exploited by the work of Polish codebreakers, but it was still a time-consuming process and the code was changed on a daily basis, meaning it had to be continuously re-cracked. Alan Turing's Bombe machine at Bletchley Park in the United Kingdom, significantly reduced the time it took to decrypt the code, allowing codebreakers to set up an Enigma machine with the correct code each day to decrypt intercepted messages.