Chapter 8 Data security, Privacy and Integrity

Syllabus sections covered: 1.6 (1.6.1–1.6.2)

8.05 Answers to coursebook questions and tasks

Task 8.01

1 The password should contain upper and lower case characters, a number and a symbol to be secure.

2 There are 128 ASCII characters of which 96 are graphic characters. The number of different passwords is therefore 96^8, which is about 7×10^{15}. In words this is about seven million billion.

3 If a password could be tested every second, the time taken to test every possibility in years would be this value divided by 3600 then divided by 24 then divided by 365. The result is still a very large number. To get the time down to less than a year the password would have to be tested every nanosecond. Clearly the password is secure from this type of attack.

Question 8.01

1 The following would be the eight bytes that include the original seven with the parity bit set appropriately and byte 8 created from a parity bit for each column.

Byte 1	0	1	0	0	1	0	0	0
Byte 2	1	1	0	0	0	1	0	1
Byte 3	0	1	1	1	0	0	1	0
Byte 4	0	1	1	0	0	0	1	1
Byte 5	1	0	1	0	1	1	0	0
Byte 6	0	1	0	1	0	1	0	1
Byte 7	1	0	1	1	0	0	1	0
Byte 8	1	1	0	1	0	1	1	1

Figure 8.01

2 **a** The eight bytes have to be examined in the following matrix presentation:

0 1 0 0 1 0 0 0	
1 1 0 0 0 1 0 1	
1 1 1 1 0 0 0 1	x
0 1 1 0 0 0 1 1	
0 1 0 0 1 0 1 0	x

0 1 0 1 0 1 0 1	
0 1 1 1 0 0 1 0	
0 1 1 1 0 0 1 0	
✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	

Figure 8.02

Each of the columns needs to be checked. For each of these the parity is correct assuming even parity. This would indicate that the transmission has taken place with no error. However, checking the rows reveals that two have odd parity (indicated by the x) while the remaining five data bytes and the last (parity) byte have even parity. This would indicate that the process of setting the parity bits at the transmitting end has been in error.

b The only option is to ask for re-transmission of the data.

Exam-style Questions (with mark allocation in brackets):

1 a i accuracy (1).

ii Validation concerns checking that the data is of the right type (1) and format (1) whereas verification is checking data that has been input (1).

iii Any from the coursebook list (1) with a sensible example (1).

iv It is possible to enter data with the correct format and of the correct type (1) but it can still be incorrect (1).

b Unauthorised access to a system (1) can be made more difficult by creating usernames and passwords (1), strong passwords (1), biometric tests (1), security tokens (1). (Max 2). Unauthorised access to data once a user is logged in (1) can be controlled by only authorising certain users (1) by setting access rights (1). (Max 2)

2 a i Accidental deletion (1), disk problem (1), system failure (1), location forgotten (1), storage device lost (1), file deleted or corrupted because of a virus (1). (Max 3)

ii Encryption (1) possibly when storing data but certainly when transmitting it, authorisation policy controlling access to data (1), giving different users different access rights (1). Controlling access to the system (1), by setting user ids and passwords (1), using methods to authenticate users (1), biometric methods (1). (Max 3; note that the question says ‘describe’ so three names of features would not get three marks).

b i A disaster such as earthquake, fire or flood (1), which destroys the system or makes it completely non-functional (1).

ii A risk assessment (1), which considers the effect on the organisation of having systems out of commission (1),and the likelihood of a disaster occurring (1) (Max 2) OR a choice of type of standby system (1), dependent on the urgency of the need to get back into operational mode (1).

c A firewall (1), to restrict what transmissions can enter (1) or leave the system (1), to check all transmissions that have entered the system (1) (Max 2), authentication of sender of email (1), by insisting on a digital certificate (1), virus checker (1), used regularly (1), intrusion detection (1), auditing system use (1). (Overall Max 4 for two measures and two descriptions).

3 **a** **i** The transmitting end must define parity to be even or odd (1), then for each individual byte (1) the number of 1 bits in the 7-bit code is counted (1) and the parity bit is chosen so that the number of bits in the byte is even or odd (1) . At the receiving end the choice of parity defined must be known (1), the bits in each individual byte are counted (1), if for any byte the number of bits does not match the defined parity (1) a re-transmission is requested (1). (Max 5 provided there is detail for both transmitter and receiver)

ii At the transmitting end a block is defined as a certain number of bytes (1), each byte is treated as a binary number (1), the binary numbers are added for the bytes in each individual block (1), the value obtained is added to the data transmitted for each block (1). At the receiving end the same calculation is carried out for each block (1) and the value obtained compared to the transmitted one (1). (Max 3)

b If two errors occur these could effectively cancel each other out so the errors would not be detected (1). The position of an error cannot be identified (1).

c

Byte 1	0	1	0	1	0	0	1	1	
Byte 2	1	0	1	1	0	0	0	1	
Byte 3	1	1	0	1	0	0	0	0	*
Byte 4	1	0	0	1	1	1	0	0	
Byte 5	1	0	1	1	0	0	1	0	
Byte 6	1	0	1	1	0	0	0	1	
Byte 7	1	0	1	1	0	0	0	1	
Byte 8	0	0	0	1	0	1	0	0	
					*				

Figure 8.03

The columns should be checked first. The fifth one as indicated in the diagram has an odd number of 1 bits, and all of the others have an even number. This suggests an error in transmission (1). The rows should then be checked. The third one as indicated in the diagram has an odd number so is in error (1). The bit at the intersection of the fifth column and the third row must be wrong (1). The receiver program will change the 0 to a 1 (1).