Chapter 17 answers

What you should already know

1 i) **Data integrity** – data stored on a computer should always be accurate/consistent and kept up to date.

ii) **Data privacy** – this refers to the need to ensure a user's data remains private and unauthorised access to their data is prevented.

iii) **Data security** – this refers to the recovery of data if it is lost/deleted, but also refers to ways of preventing unauthorised access to data on a system.

2 Data recovery refers to:

Accidental loss of data:

- use of back-ups in case the data is lost or corrupted through an accidental operation.
- save data on a regular basis
- use of passwords and user ids to restrict access to authorised users only.

Hardware malfunction:

- use of back-ups in case the data is lost or corrupted through an accidental operation
- save data on a regular basis
- use of passwords and user ids to restrict access to authorised users only.

Software malfunction:

- use of back-ups in case the data is lost or corrupted through the software fault
- save data on a regular basis in case the software suddenly "freezes" or "crashes" whilst the user is working on it.

Incorrect computer operation:

- use of back-ups in case the data is lost or corrupted through wrong operation
- correct training procedures so that users are aware of the correct operation of hardware.

In all cases the regular backing up of data is a key component to data recovery. If data becomes corrupted or lost by one of the methods describe above, it is possible to reinstall the affected data from the back-ups. Back-ups should be made on a regular basis (either automatically or manually at the end of the day) onto another medium (such as cloud storage, CD/DVD, memory stick or removable HDD/SSD) and the back-up should be stored in a separate location in case of fire, etc. A person should be appointed to do the back-ups to make sure it is done. It is important to realise that backing up data may not be a suitable method of recovery in the case of data loss or corruption through a virus infection. Unfortunately, the backed-up data may contain strands of the virus which would simply re-infect the 'cleaned' computer if an attempt was made to reinstate this data. Increasingly the preferred method of storing data in another location is the use of managed cloud storage.

3 **Protect against data loss by:**

- user accounts which authenticate the user (account number/name and password)
- use of access rights (level of access to data)
- digital signatures
- firewalls (to monitor traffic and help reduce hacking and other eavesdropping risks)
- use of anti-spyware, anti-virus software, for example
- encryption can help in prevention of data loss
- biometrics (fingerprint, facial, recognition, for example) can restrict access to sensitive data

- backups to guard against loss due to software crash; hardware failure or power loss
- multiple backups in case of back up failure
- use of uninterruptable power supply (UPS) or power filters to protect against data loss through power failure
- ensuring system warns user it is still writing to a removable device.

4 a) i) Hacking

- Hacking can lead to loss of data or illegal use of data (e.g. access to bank details) with serious consequences for data security, data privacy and data integrity.
- Hacking is illegal access to a computer without user's permission.

ii) Malware

- There are many forms of malware (e.g. virus, Trojan horses and spyware, for example).
- The effects of malware can vary from
  - corrupting data/exec files stored on a computer
  - replacement of legitimate software with malicious software
  - to monitoring a user's key presses.
- All of these can lead to loss/corruption of data, allowing access to personal data and so on.

iii) Phishing

- This occurs when a user opens an email (or attachment) from what seems to be a legitimate source/company only to be redirected to a fake website where personal details can be accessed.

iv) Pharming

- This is slightly more alarming than phishing since it doesn't require any action by a user.
- Code is placed on a user's hard drive or on the web server and when user types in a targeted website, they are sent to a fake website without their knowledge – this again can lead to personal data being accessed by a hacker, for example.

b) methods of guarding against the above include:

- use of passwords
- authentication techniques
- running up-to-date virus checkers/spyware checkers
- encryption
- only open emails from secure sources, and so on.

Activity 17A

1 A
2 B
3 B
4 E
5 A
6 A
7 C
8 D
9 C
10 B

Extension activity 17A

a)

sender	recipient
X = 3	Y = 5
7^3 (MOD 11) = 343 (MOD 11) = 31 remainder 2	7^5 (MOD 11) = 16807 (MOD 11) = 1527 remainder 10
10^3 (MOD 11) = 1000 (MOD 11) = 90 remainder 10	2^5 (MOD 11) = 32 (MOD 11) = 2 remainder 10

giving 10 as the encryption key

b)

sender	recipient
X = 7	Y = 6
7^7 (MOD 11) = 823543 (MOD 11) = 74867 remainder 6	7^6 (MOD 11) = 117649 (MOD 11) = 10695 remainder 4
4^7 (MOD 11) = 16384 (MOD 11) = 1489 remainder 5	6^6 (MOD 11) = 46656 (MOD 11) = 4241 remainder 5

giving 5 as the encryption key

End of chapter questions

1 a) QKD is a protocol used when sending encryption keys over a fibre optic network using quantum cryptography technology

(b) Order: 10, 2, 6, 1, 5, 9, 3, 11, 8, 4, 7

(2) (a) SSL = secure socket layer

TLS = transport layer security

- TLS is a more modern version of SSL.
- They are client-server applications.
- They are standard cryptographic protocols …
- … to ensure security, authenticated communication.
- SSL encrypts the data.
- User knows if SSL secure due to HTTP and closed padlock.

b) i) Record protocol

- can be used with or without encryption
- contains data being transferred over Internet.

ii) Handshake protocol

- permits website and client to authenticate each other and to make use of encryption algorithms
- secure session between client and website is established.

iii) Session caching

- avoids need to utilise computer time during each TLS connection
- TLS can establish either a new session or attempt to resume existing session …
- … the latter can save considerable computer time.

c) Differences between SSL and TLS

- It is possible to extend TLS by adding new authentication methods.
- TLS can make use of session caching which improves overall performance of computer compared to using SSL.
- TLS separates handshaking process from record protocol layer (which holds all the data).

3 a) Order: 6, 1, 4, 5, 3, 2

b) Items on a digital certificate

- serial number
- CA that issued the certificate
- CA digital signature
- name of company/organisation
- subject's public key
- period during which certificate is valid
- version number
- expiry date of certificate
- algorithm identification
- signature algorithm used
- company details/identifier.

(c) All certificate details condensed and put through a hashing algorithm (e.g. MD4/5) then encrypt the number using the CAs private encryption key.