Protecting digital systems and data (incl. encryption)

5.3.2 · Issues and impact · revision notes

The methods used to protect digital systems and data: anti-malware, encryption, acceptable use policies, and backup and recovery procedures. On Paper 1, expect 'Explain how…' questions, scenario questions about what an organisation should do and 6-mark 'Discuss' questions. You may also be asked to use a simple cipher, such as the Caesar cipher.

Key facts

- **Anti-malware**: finds, quarantines and removes malware using signatures and behaviour checks; keep it updated.
- **Plaintext**: readable data. **Ciphertext**: encrypted data.
- **AUP**: rules users agree to about how they may use an organisation's systems, and the consequences of breaking them.
- Good backups: regular, automatic, off site and offline, several versions, tested.
- Encryption stops data being read, not lost: you still need backups.
- **Encryption**: an algorithm and a key turn plaintext into ciphertext; only someone with the key can decrypt it.
- **Caesar cipher**: shift each letter by the key, wrapping from Z to A; decrypt by shifting back the same number of places.
- **Backup**: a separate copy of data so that it can be restored.
- **Recovery procedure**: isolate, remove the malware, restore from the last clean backup.

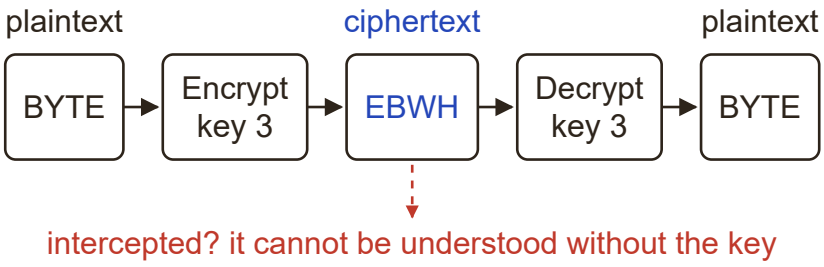
Notes

Anti-malware

- **Anti-malware** software scans files, downloads, emails and USB drives, and quarantines or deletes any malware it finds.
- It compares files with a database of **signatures** of known malware, and watches for suspicious behaviour to catch new malware.
- It must be updated regularly, ideally automatically, because new malware appears all the time. Install software patches promptly too.

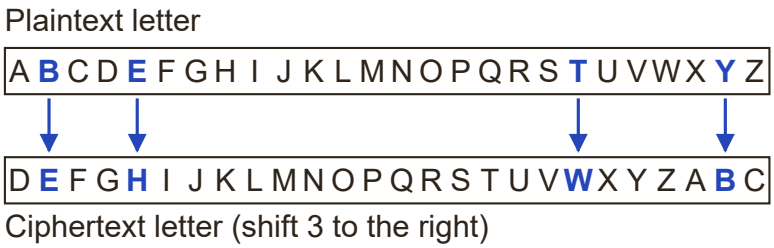
Encryption

- **Encryption** uses an algorithm and a **key** to turn **plaintext** into **ciphertext**, which cannot be understood without the key. **Decryption** turns it back into plaintext.



Encryption with a key turns plaintext into ciphertext; decryption with the key turns it back.

- It protects data sent over a network (if it is intercepted, it cannot be read) and data stored on devices (if a laptop or phone is lost or stolen).
- Encryption does not stop data being intercepted, copied or deleted: it stops it being understood.
- A simple example is the **Caesar cipher**: each letter is shifted a fixed number of places along the alphabet, wrapping round from Z to A. The shift is the key. With a shift of 3 to the right, BYTE becomes EBWH.



Caesar cipher, shift 3: B→E, Y→B (wrapping round), T→W, E→H, so BYTE becomes EBWH.

- The Caesar cipher is easy to break: there are only 25 useful keys, so an attacker can try them all (a brute-force attack). Modern encryption uses keys of 128 bits or more; each extra bit doubles the number of possible keys, so trying every key would take far too long. Grade 7+ only

Acceptable use policies

- An **acceptable use policy (AUP)** is a set of rules that users must agree to before they use an organisation's computer systems.
- Typical rules: do not share passwords; lock your screen when you leave it; do not install software or plug in personal USB drives; only visit appropriate websites; report suspicious emails.
- It protects the system by reducing risky behaviour, making users aware of threats and allowing action to be taken against anyone who breaks the rules.

Backup and recovery procedures

- A **backup** is a copy of data stored separately, so it can be restored if the original is lost, deleted, corrupted or encrypted by ransomware.
- A good backup procedure: back up regularly and automatically; keep at least one copy off site (e.g. in the cloud) and one offline, so ransomware cannot reach it; keep several versions; test that backups can be restored.
- A **recovery** procedure sets out what to do after an attack or failure: isolate the infected devices, remove the malware, then restore the data from the last clean backup.
- A full backup copies all the data; an incremental backup copies only the data changed since the last backup. Incremental backups are quicker, but restoring needs the full backup and then each incremental backup in order. Grade 7+ only

How to answer each type of question

Use a Caesar cipher

1 to 2 marks | Grade 4

1. Write out the alphabet A to Z so you can count along it.
2. Shift every letter by the key in the stated direction, wrapping from Z back to A.
3. To decrypt, shift the same number of places the other way.
4. Check every letter again: one slip loses the mark.

Example. (a) Encrypt the word **BYTE** using a Caesar cipher with a shift of 3 to the right. (1 mark)
(b) State the shift needed to decrypt the ciphertext. (1 mark)

Model answer.

(a) EBWH (1)
(b) 3 to the left, or 23 to the right (1)

Explain how a method protects data

2 marks | Grade 5

1. Say what the method does.
2. Explain how that stops the threat in the question, using 'so'.

Example. Explain how encryption protects customers' card details when they are sent to an online shop. (2 marks)

Model answer. The card details are turned into ciphertext using a key before they are sent (1), so if they are intercepted, the attacker cannot understand them without the key (1).

Describe a backup and recovery procedure

3 to 4 marks **Grade 6**

1. Say how often and how backups are made (regularly, automatically).
2. Say where copies are kept (off site, offline) and why.
3. Mention keeping several versions and testing restores.
4. For recovery, give the steps in order.

Example. A veterinary surgery keeps all its animal and owner records on one server. Describe a suitable backup and recovery procedure. (4 marks)

Model answer. Back up the server automatically every night (1). Keep one copy off site or in the cloud and one copy disconnected from the network, so that ransomware cannot encrypt it (1). Keep several older versions and regularly test that they can be restored (1). After an attack, disconnect and clean the infected server, then restore the records from the most recent clean backup (1).

Explain why one method is not enough on its own

2 marks **Grade 7**

1. State what the method cannot do.
2. Name another method and explain the gap it fills.

Example. A company has up-to-date anti-malware on every computer. Explain why it also needs an acceptable use policy. (2 marks)

Model answer. Anti-malware cannot stop staff being tricked into giving away passwords, or doing risky things such as plugging in unknown USB drives (1). An AUP sets rules, such as never sharing passwords or installing unapproved software, which reduces risky behaviour that software cannot prevent (1).

6-mark 'Discuss' how to protect an organisation

6 marks **Grade 8**

1. Identify what needs protecting and the likely threats in the context.
2. Recommend methods (anti-malware, encryption, AUP, backup and recovery) and explain what each one prevents here.
3. Mention limitations or costs, and how the methods work together.
4. Conclude with the most important measures.

Example. A small estate agent stores clients' names, addresses, bank details and scanned identity documents on three office computers. Staff often take laptops to house viewings. Discuss the methods the estate agent could use to protect its data. (6 marks)

Model answer. Marked in levels: the top level recommends a range of methods, explains each in the context and reaches a conclusion. A strong answer might say: Anti-malware on every computer and laptop, updated automatically, would detect and remove malware such as key loggers that could steal clients' bank details. Encrypting the laptops' storage means that if one is left at a viewing or stolen, the identity documents cannot be read without the key. An acceptable use policy could ban staff from installing unapproved software and require them to lock laptops when they are not in use, reducing careless mistakes. Because ransomware could encrypt every file, the agent needs automatic daily backups kept off site and offline, with a tested recovery plan, so it could keep trading without paying a ransom. These measures cost money and staff time, but a breach of clients' bank details could lead to fines and lost trust. Overall, no single method is enough: encryption and backups protect the data itself, while anti-malware and the AUP reduce the chance of an attack succeeding.

Don’t lose marks

- Saying encryption stops hackers getting the data: it stops them understanding it.
- Saying a backup prevents malware: it lets you restore the data afterwards.
- Keeping backups on the same computer, or always connected to the network, where ransomware can encrypt them too.
- Forgetting to wrap round the alphabet (from Z back to A) in Caesar cipher questions.
- Describing an AUP as software: it is a set of rules that users agree to.

More tips

Memory tricks

- The four methods: Anti-malware, Encryption, AUP, Backup: 'Always Encrypt And Back up'.
- Match method to threat: malware → anti-malware; stolen or intercepted data → encryption; careless users → AUP; lost or ransomed data → backup.
- Caesar check: a shift of 3 to the right turns A into D and X into A.
- To decrypt a shift of n to the right, shift n to the left (the same as 26 − n to the right).

Exam technique

- For 'Explain how…', say what the method does, then how it stops the specific threat in the question.
- Match each method to a threat in the scenario rather than listing every method you know.
- In 6-mark answers, show that the methods work in layers and mention a limitation or cost.

What each grade needs

What you need to be able to do, from the first marks up to the top grade.

Grade 3 — **Give ways to protect against malware**
Up-to-date anti-malware, installing patches promptly, and not opening unexpected attachments or links.

Grade 3 — **Define encryption, plaintext, ciphertext and key**
Encryption uses an algorithm and a key to turn plaintext into ciphertext that cannot be understood without the key.

Grade 4 — **Encrypt and decrypt with a Caesar cipher**
Shift each letter a fixed number of places along the alphabet, wrapping round from Z to A.

Grade 4 — **Describe what an acceptable use policy contains**
Rules users agree to, such as never sharing passwords or installing software, and the consequences of breaking them.

Grade 5 — **Explain how anti-malware and encryption protect data**
Anti-malware detects and removes malware; encryption makes stolen or intercepted data unreadable without the key.

Grade 6 — **Describe a backup and recovery procedure**
Regular automatic backups kept off site and offline, several versions, tested restores and a recovery plan.

Grade 7 — **Explain the limits of each protection method**
For example, encryption does not stop data being deleted or locked by ransomware, so backups are still needed.

Grade 8 — **Discuss how an organisation should protect data**
Recommend layered measures that fit the organisation's data, threats and budget, with reasons.

Free notes, Full packs, practice papers and mock exams at chhetriacademy.com. Written for this site; not taken from past papers. Stuck? 1-to-1 tutoring with a free 30-minute trial lesson.