Encryption

Computer systems (Paper 1) · revision notes

How encryption protects data by scrambling it with an algorithm and a key, so that intercepted or stolen data cannot be understood. Questions ask for definitions, why encryption is used on networks and devices, and sometimes a simple cipher such as the Caesar cipher to show the principle.

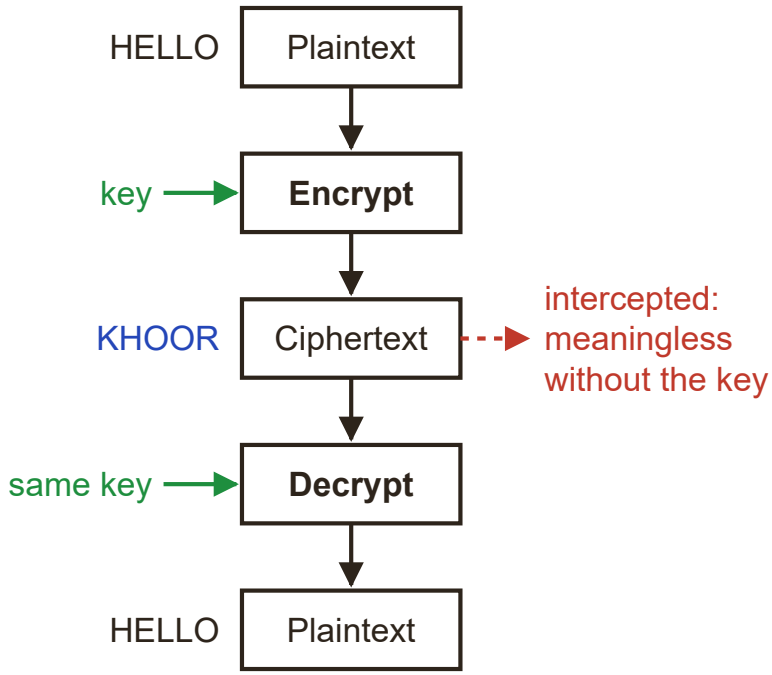
Key facts

- Encryption = scrambling data using an algorithm and a key
- Encryption does not stop interception; it makes intercepted data unreadable
- Caesar cipher: shift each letter by the key; wrap round from Z to A
- Plaintext → (encrypt with key) → ciphertext → (decrypt with key) → plaintext
- Used in: HTTPS, Wi-Fi, encrypted storage on devices
- Grade 7+ only n-bit key → 2^n possible keys

Notes

What encryption does

- **Encryption** scrambles data using an **encryption algorithm** and a **key**, so that it cannot be understood by anyone who does not have the key.
- **Plaintext**: the original, readable data. **Ciphertext**: the scrambled data. **Decryption** turns ciphertext back into plaintext using the key.



Encryption turns plaintext into ciphertext; only someone with the key can turn it back

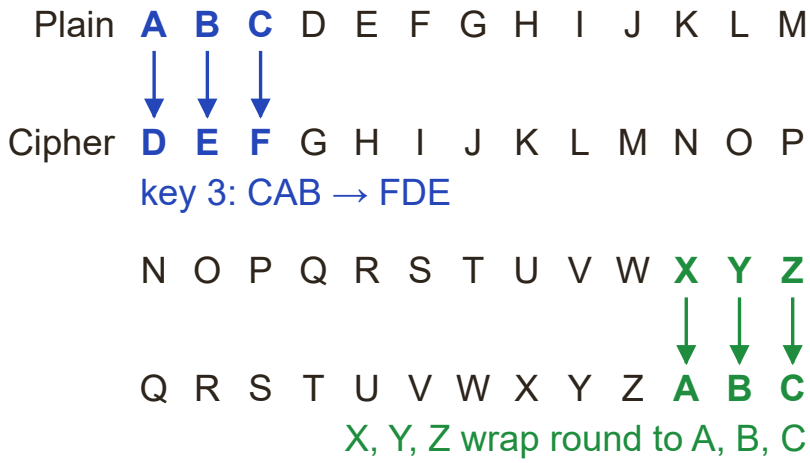
- Encryption does **not** stop data being intercepted or stolen. It makes intercepted or stolen data **meaningless** to the attacker.

Where encryption is used

- Data sent over networks: **HTTPS** encrypts data between a browser and a web server, e.g. passwords and card details.
- **Wi-Fi** networks encrypt the data sent through the air, because anyone within range could pick up the signal.
- Stored data: if the storage on a laptop or phone is encrypted, a thief cannot read the files, even by removing the drive.
- Encryption helps organisations keep personal data secure, which the Data Protection Act 2018 requires.

The principle: Caesar cipher and keys

- A **Caesar cipher** shifts every letter a fixed number of places along the alphabet. The shift is the key. With a key of 3, CAB becomes FDE; after Z it wraps round to A.



A Caesar cipher with key 3: each letter moves 3 places along

- A Caesar cipher is easy to break: there are only 25 useful keys, so trying them all takes seconds.
- Real encryption uses much longer keys made of bits. An n-bit key has 2^n possible values, so each extra bit doubles the number of keys a **brute-force attack** would have to try. Grade 7+ only
- Encryption only protects data from people without the key. If you type your password into a fake website, it is encrypted on the way, but the attacker running the site can still read it. Grade 8+ only

How to answer each type of question

Explain how encryption protects data — 2 to 3 marks — Grade 5

1. Say what happens: the data is scrambled using an algorithm and a key.
2. Say the effect: it cannot be understood without the key if it is intercepted.
3. Say who can read it: only the intended receiver, who has the key.

Example. Explain how encryption protects a customer's card details when they are sent to an online shop. [3]

Model answer. The card details are scrambled using an encryption algorithm and a key before they are sent (1). If the data is intercepted, it cannot be understood without the key (1). Only the shop's server, which has the key, can decrypt the details (1).

Use a Caesar cipher

1 to 3 marks | Grade 5

1. Write out the alphabet so you can count the shift accurately.
2. Encrypt: move each letter forward by the key. Decrypt: move each letter back.
3. Wrap round: after Z comes A (and before A comes Z).

Example. A Caesar cipher with a key of 4 is used.
(a) Encrypt the word WAY. [1]
(b) Decrypt the ciphertext PSKMR. [1]

Model answer.

(a) AEC (1)
(W wraps round to A, A becomes E, Y wraps round to C)
(b) LOGIN (1)

Explain why a longer key is more secure

2 marks | Grade 7

1. Say that a longer key has many more possible values.
2. Link to brute force: trying every key would take far too long.
3. If numbers are asked for, an n-bit key has 2^n possible keys.

Example. Explain why a 16-bit key is much more secure than an 8-bit key. [2]

Model answer. A 16-bit key has 2^{16} = 65,536 possible values, compared with 2^8 = 256 for an 8-bit key (1). So a brute-force attack that tries every key would take 256 times as long (1).

Don’t lose marks

- Saying encryption stops data being intercepted. It stops intercepted data being understood.
- Mixing up plaintext (readable) and ciphertext (scrambled).
- Forgetting to wrap round the alphabet in a Caesar cipher.
- Confusing encryption with a password or with compression. A password controls access; encryption scrambles the data itself.

More tips

Memory tricks

- Encryption is a lock, not a wall: people can still grab the box, but they cannot open it without the key.
- Caesar check: decrypt your answer with the same key to see if you get back to the start.
- Each extra bit of key doubles the number of keys: 8 bits → 256, 9 bits → 512, 10 bits → 1,024.

Exam technique

- Use the key words: algorithm, key, plaintext, ciphertext, decrypt.
- Finish an 'explain' answer with the effect: intercepted data is meaningless without the key.
- Show your shifting in Caesar cipher questions and check each letter twice.

What each grade needs

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

Grade 3 — **Define encryption**
Scrambling data using an algorithm and a key so it cannot be understood without the key.

Grade 4 — **Use plaintext, ciphertext and key correctly**
Plaintext is the original data, ciphertext is the encrypted data, and the key is used to encrypt and decrypt.

Grade 5 — **Explain how encryption protects intercepted data**
Intercepted data is meaningless without the key; only the intended receiver can decrypt it.

Grade 5 — **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 6 — **Give examples of where encryption is used**
HTTPS web pages, Wi-Fi networks and the storage on laptops and phones.

Grade 7 — **Explain why longer keys are more secure**
Each extra bit doubles the number of possible keys, so a brute-force attack takes far longer.

Grade 8 — **Explain what encryption cannot protect against**
It does not stop data being intercepted or deleted, and does not help if the attacker has the key.

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.