Cambridge IGCSE · Computer Science 0478 · Notes

Encryption

Read online at **pastopic.com/cambridge/computer-science-0478/notes/encryption**

Last checked 30 September 2026

Read first: **Types and methods of data transmission**

What you need to know

By the end of this topic you should be able to:

1. **Explain why data is encrypted before it is transmitted, and what encryption is for.** Data sent over a network can be intercepted. Encryption doesn't stop that, but it makes the intercepted data **meaningless** to anyone without the key, which keeps it secure.
2. **Describe how data is encrypted with symmetric encryption**: one key, shared by the sender and the receiver, both encrypts and decrypts the data.
3. **Describe how data is encrypted with asymmetric encryption**: a **public key** and a **private key**. The public key encrypts the data; only the matching private key can decrypt it.

You should be able to compare the two (similarities, differences, and why you might pick one over the other) and use the words **plain text**, **cipher text**, **key** and **algorithm** correctly.

How HTTPS, SSL/TLS and digital certificates use encryption on websites is in Cyber security; packets and transmission methods are in Types and methods of data transmission.

Understand it

Why encrypt data?

When data travels across a network, especially the internet, it passes through many devices and cables you don't control. Anyone on the way could **intercept** it (copy it as it passes) and look at it. For bank details, passwords, medical records or private messages, that is a problem.

Encryption scrambles the data before it is sent, so that if it is intercepted, it **makes no sense** to the person who took it. Only a device holding the right **key** can turn it back into the original. So the purpose of encryption is to **keep data secure** by making it **meaningless** if it is intercepted or stolen.

Two points examiners care about:

- Encryption **doesn't stop** the data being intercepted, hacked or deleted. It only stops the data being **understood**.

- Encrypted data is not "unreadable": anyone who intercepts it can still read the characters. They just don't **mean** anything. Say **meaningless**.

The same idea protects data **stored** on a device: if a phone is stolen, its encrypted files are meaningless to the thief.

The words you need

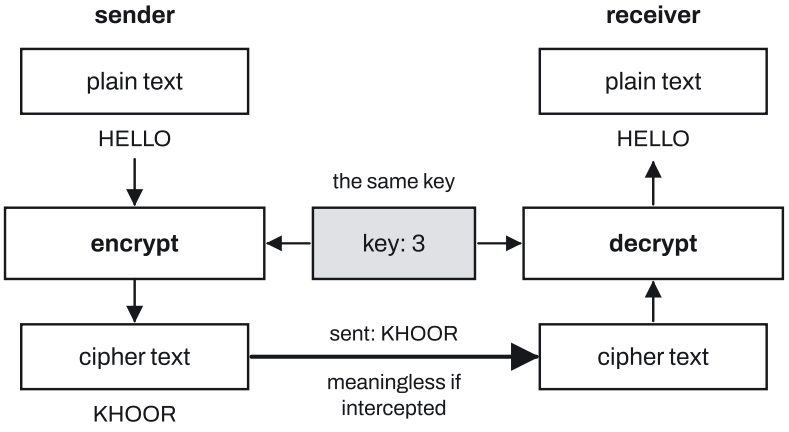
- **Plain text**: the original data, before encryption. It makes sense.
- **Cipher text**: the scrambled data, after encryption. It is meaningless.
- **Encryption algorithm**: the fixed set of steps that scrambles plain text into cipher text.
- **Key**: a value the algorithm uses. The same algorithm with a different key gives different cipher text, so without the right key the cipher text can't be turned back.
- **Encrypt**: plain text → cipher text. **Decrypt**: cipher text → plain text.

$$\text{plain text} \xrightarrow{\text{encrypt (algorithm + key)}} \text{cipher text} \xrightarrow{\text{decrypt (key)}} \text{plain text}$$

A toy example shows how an algorithm and a key work together (real encryption uses far longer keys and harder algorithms, and you won't be asked to use a particular one). The algorithm is "move each letter forward in the alphabet by the key"; the key is 3. The plain text HELLO becomes the cipher text KHOOR. To decrypt, move each letter back by 3. Someone who intercepts KHOOR but doesn't know the key sees nonsense.

Symmetric encryption

In **symmetric encryption** there is **one key**, and it is used both to **encrypt** and to **decrypt**.



The key must also be sent to the receiver, so it could be intercepted.

1. The sender and receiver need the **same key**. It is created (often generated by an algorithm) and **sent to the receiver**, or values are exchanged so both devices can generate the same key.
2. The sender's device uses an **encryption algorithm** with the key to turn the **plain text** into **cipher text**.
3. The cipher text is transmitted.
4. The receiver's device uses the **same key** to **decrypt** the cipher text back into plain text.

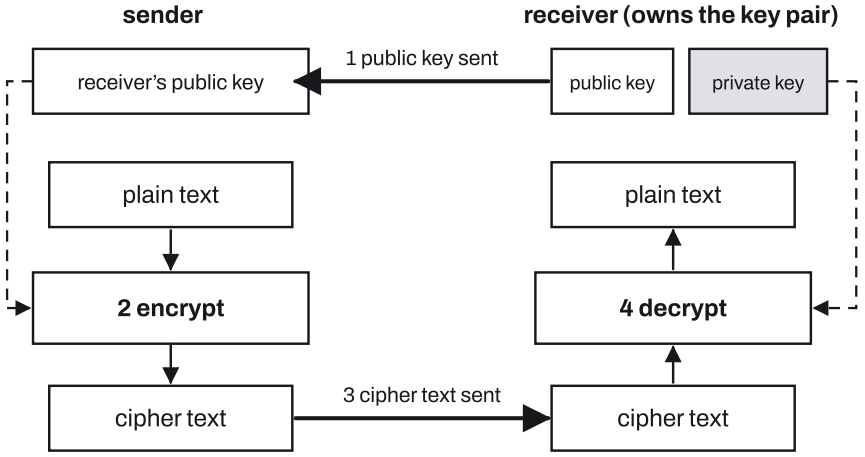
The weakness is the key itself. It has to get from the sender to the receiver, and if someone intercepts the **key**, they can decrypt every message sent with it. This is the "key exchange" problem.

Asymmetric encryption

In **asymmetric encryption** each device has a **pair** of keys that belong together:

- a **public key**, which anyone may have; the device gives it to anyone who asks;
- a **private key**, which never leaves the device and only its owner knows.

The pair is made so that data encrypted with the **public key** can only be decrypted with the matching **private key**. The public key **cannot** decrypt what it encrypted.



The public key can only encrypt. The private key, which decrypts, is never sent, so there is no key to intercept.

1. The sender **requests** the receiver's **public key**, and the receiver sends it.
2. The sender encrypts the **plain text** with the receiver's **public key**, making **cipher text**.
3. The cipher text is transmitted.
4. The receiver decrypts it with its own **private key**.

Think of the public key as an open padlock the receiver hands out to anyone, and the private key as the only key that opens it. Anyone can snap the padlock shut on a box, but only the owner can open it again. Intercepting the padlock (the public key) is no use to an attacker, because it can only lock.

This is why asymmetric encryption is **more secure**: the key that decrypts is **never sent**, so there is no key to intercept on the way.

Comparing them

	Symmetric	Asymmetric
Keys	One key	Two keys: a public key and a private key
Encrypt with	The key	The receiver's public key

	Symmetric	Asymmetric
Decrypt with	The **same** key	A **different** key: the matching private key
Who knows the keys	Sender and receiver both know the one key	Anyone can know the public key; only the owner knows the private key
Key sent across the network?	Yes, so it could be intercepted	Only the public key; the private key is never sent
Security	Less secure	More secure; no worry about key exchange

The same in both: both use a key and an algorithm; both scramble plain text into cipher text; both make the data meaningless if it is intercepted.

Key facts and formulas

There is no formula list for this subject, so you must learn all of these.

Formula	Status
Purpose of encryption: keep data secure by making it meaningless if intercepted (it doesn't stop interception)	Learn it
Plain text (before) → encryption algorithm + key → cipher text (after)	Learn it
Symmetric: one key both encrypts and decrypts; the key is sent to (or generated by) the receiver	Learn it
Asymmetric: public key encrypts, matching private key decrypts; the public key cannot decrypt	Learn it
Public key: anyone can request it; private key: never shared, only the owner knows it	Learn it
Asymmetric is more secure: no key exchange, the private key is never transmitted	Learn it

How to do it

In the Paper 1 questions we have tagged for this topic (8 questions, 2022–2025), the types came up this often. 5 of the 8 questions mix types, so the counts add up to more than 8.

Question type	Questions
State the purpose of encryption	5
Compare symmetric and asymmetric encryption	3

Question type	Questions
Describe how symmetric encryption works	2
Complete a paragraph about asymmetric encryption	2
Choose the correct statement or name the other type	1

1. State the purpose of encryption (5 questions)

Usually 1 mark. Give **one clear idea**:

- "If the data is intercepted, it will be **meaningless**" (or "can't be understood"); or
- "To keep the data **secure**, because it is **sensitive** or **confidential**."

Don't say it stops the data being intercepted, hacked or stolen: it doesn't. Don't say "unreadable".

Variations you will meet:

- **"State why encryption helps keep the data safe"** or **"how encryption keeps the data on a device more secure"**: same answer, the data is meaningless to anyone who steals it without the key.
- **"Give one reason why the data is encrypted"**: it is sensitive or confidential, so it must be kept secure; or, to make it meaningless if intercepted.

2. Compare symmetric and asymmetric encryption (3 questions)

1. Read whether it asks for a **similarity**, **differences**, or a **reason** to choose one.
2. **Similarity** (any one): both use a key; both use an algorithm; both turn plain text into cipher text; both make the data meaningless.
3. **Differences**: write each as a pair, symmetric **whereas** asymmetric:
   - symmetric uses **one key**, whereas asymmetric uses **two** (a public and a private key);
   - symmetric **decrypts with the same key**, whereas asymmetric decrypts with a **different** key (the private key);
   - symmetric **sends the key** to the receiver, whereas asymmetric never sends the private key;
   - in symmetric both sides know the key, whereas in asymmetric anyone can know the public key but only the owner knows the private key;
   - symmetric is **less secure** than asymmetric.
4. **Reason to choose asymmetric**: it is **more secure**, because there is no need to worry about **key exchange** (the private key is never sent).

Variations you will meet:

- **"Describe the differences"** (4 marks): describe both sides fully: "symmetric has one shared key that encrypts and decrypts, and both the sender and receiver know it; asymmetric has a public key that encrypts and a private key that decrypts, and anyone can know the public key but only the receiver knows the private key."

3. Describe how symmetric encryption works (2 questions)

Usually 4 marks: one for the key idea, then three for the process. Write each as a separate sentence.

1. The data is encrypted and decrypted using the **same key** (this is the key mark).
2. The key is **generated** using an algorithm,
3. and **sent to the receiver** (or values are sent that let the receiver generate the same key).
4. An **encryption algorithm** uses the key to turn the **plain text** into **cipher text**.
5. The cipher text is sent, and the receiver uses the **same key** to decrypt it back into **plain text**.

4. Complete a paragraph about asymmetric encryption (2 questions)

1. Read the whole paragraph first, then fill each gap from the list.
2. Use the pattern: the **algorithm** scrambles the **plain text** into **cipher text**, which is **meaningless**; the **public key** encrypts; the **private key** decrypts; anyone can request the **public** key; only your device knows the **private** key.
3. Check which gaps say "encrypt" and which say "decrypt", and whether a term may be used more than once.

Distractors to avoid: "unreadable" (use **meaningless**), "compression", "error", "hexadecimal", "binary", "certificate", "symmetric". A word list may offer both "public key" and "private key" and both "plain text" and "cipher text": check the direction (before or after encryption).

5. Choose the correct statement or name the other type (1 question)

- **Tick the true statement about symmetric encryption**: the key is **shared** with the device receiving the data. Not true of symmetric: "two different keys" (that's asymmetric), "the most secure form" (asymmetric is more secure), "encrypted text is plain text" (it's cipher text).
- **"Give one other type of encryption"**: if the question used symmetric, the answer is **asymmetric**, and the other way round.

Worked examples

The bold codes show where marks are earned, as in Cambridge mark schemes. The number is how many marks.

- **B1** mark for a correct result on its own, with no method needed.

Example 1

A doctor sends patients' test results from a clinic to a hospital over the internet. The results are encrypted before they are sent.

(a) Give **one** reason why the results are encrypted. **[1]**

(b) The clinic uses symmetric encryption. Explain how the results are encrypted using symmetric encryption. **[4]**

(a) The results are confidential, so encrypting them means that if they are intercepted they are meaningless **B1**.

(b) The results are encrypted and decrypted using the same key **B1**.

Any three of: the key is generated using an algorithm **B1**; the key is sent to the hospital's computer **B1**; the clinic's computer uses an encryption algorithm with the key **B1** to turn the plain text into cipher text **B1**; the hospital's computer uses the same key to decrypt the cipher text back into plain text.

Example 2

A shop's website sends customers' card details to the bank using asymmetric encryption.

(a) Tick (✓) **one** box to show the true statement about asymmetric encryption. **[1]**

	Statement
A	The private key is sent to the device that encrypts the data.
B	Data encrypted with the public key can be decrypted with the same public key.
C	Any device can request the public key.
D	Encrypted data is called plain text.

(b) Give **one** similarity between symmetric and asymmetric encryption. **[1]**

(c) Give **two** differences between symmetric and asymmetric encryption. **[2]**

(a) C **B1**. A is wrong because the private key is never sent; B is wrong because the public key cannot decrypt; D is wrong because encrypted data is cipher text.

(b) Any one of: both use a key; both use an algorithm; both turn plain text into cipher text; both make the data meaningless if intercepted **B1**.

(c) Any two of **B1** **B1**:

- symmetric uses one key, whereas asymmetric uses two keys, a public key and a private key;
- symmetric decrypts with the same key that encrypted the data, whereas asymmetric decrypts with a different key, the private key;

- symmetric sends the key to the receiver, whereas asymmetric never sends the private key;
- symmetric is less secure than asymmetric.

Example 3

Complete the paragraph about asymmetric encryption. Use the terms from the list. Some terms will not be used. You may use a term more than once. **[6]**

binary · cipher text · compressed · meaningless · plain text · private · public · symmetric · unreadable

An office computer sends a report to a head office using asymmetric encryption. First, the office computer requests the head office's ..... key. The report, which is currently in ..... , is encrypted with this key and becomes ..... . If it is intercepted it is ..... . The head office decrypts the report with its ..... key. The key that encrypted the report cannot decrypt it, and only the head office knows its ..... key.

Answers in order, one mark each: public **B1**; plain text **B1**; cipher text **B1**; meaningless **B1**; private **B1**; private **B1**.

"Unreadable" is not accepted for the fourth gap: the data can still be read, it just has no meaning.

Example 4

A student stores coursework on a laptop and sends it to a teacher by email.

(a) The student encrypts the files on the laptop. State how encryption keeps the files more secure if the laptop is stolen. **[1]**

(b) Give **one** reason why the student might choose asymmetric encryption instead of symmetric encryption for the email. **[1]**

(c) Describe the differences between symmetric and asymmetric encryption. **[4]**

(a) The files will be meaningless to the thief, who does not have the key **B1**.

(b) It is more secure, because the key that decrypts (the private key) is never sent, so there is no need to worry about the key being intercepted during key exchange **B1**.

(c) Any four of:

- symmetric has one key, shared by the sender and receiver **B1**,
- ... which is used both to encrypt and to decrypt **B1**;
- both the student and the teacher know the key **B1**;
- asymmetric has two different keys, a public key and a private key **B1**,
- ... the public key encrypts the data and the private key decrypts it **B1**;
- ... anyone can know the public key, but only the teacher knows the private key **B1**.

Common mistakes

- **Writing "unreadable" instead of "meaningless".** Encrypted data can still be read; it is scrambled, so it has no meaning to someone without the key (June 2025 report).
- **Saying encryption stops data being intercepted or hacked.** It doesn't stop interception. It makes the intercepted data meaningless.
- **Mixing up plain text and cipher text.** Plain text is the data **before** encryption; cipher text is **after**. "Encrypted text is plain text" is a common wrong statement.
- **Saying the private key is shared or sent.** Only the **public** key is given out. The private key stays with its owner.
- **Saying the public key decrypts.** In the process you describe, the public key encrypts and cannot decrypt the data it encrypted; the matching private key decrypts.
- **Calling symmetric "more secure".** Asymmetric is more secure, because symmetric has to send its one key to the receiver, where it could be intercepted (June 2025 report: most candidates got this right).
- **One-sided differences.** "Asymmetric uses two keys" on its own is weaker than a full comparison: "symmetric uses one key, whereas asymmetric uses two".

How to get the marks

- **Use the key words**: key, algorithm, plain text, cipher text, public key, private key, meaningless, encrypt, decrypt. These are what the mark schemes look for.
- **"State the purpose"** (1 mark): one precise idea, "meaningless if intercepted" or "keep sensitive data secure". Don't add wrong extras.
- **"Explain how data is encrypted using symmetric encryption"**: the first mark is almost always "the **same key** encrypts and decrypts". Then give the process, one step per sentence: key generated, key sent to the receiver, algorithm with the key turns plain text into cipher text.
- **"Give two differences"**: two **different** points, each written as a contrast (symmetric ... whereas asymmetric ...). Two ways of saying "one key vs two keys" earn one mark.
- **"Give one similarity"**: something true of **both**, such as both use a key.
- **"Describe"** (4 marks): describe each type fully, not just a list of words.
- **Gap-fills**: each term is worth one mark in the right place only. Read the sentence both sides of the gap. Check the question says whether a term can be used more than once.
- **Tick one box**: ticking two scores nothing.

Quick check

1. What is the name for data (a) before it is encrypted and (b) after it is encrypted?
2. State the purpose of encryption.
3. In asymmetric encryption, which key encrypts the data and which key decrypts it?
4. Give one reason why symmetric encryption is less secure than asymmetric encryption.

5. Data is sent using asymmetric encryption. Tick one: the data is decrypted with (A) the sender's public key, (B) the receiver's public key, (C) the receiver's private key, (D) the same key that encrypted it.

Answers

1. (a) Plain text. (b) Cipher text.
2. To keep the data secure: if it is intercepted, it is meaningless to anyone without the key.
3. The receiver's public key encrypts the data; the receiver's matching private key decrypts it.
4. The one key has to be sent to the receiver, so it could be intercepted and used to decrypt the data. In asymmetric encryption the private key is never sent.
5. C. The receiver's public key encrypted the data and cannot decrypt it; only the matching private key can. D describes symmetric encryption.

Past questions to try

- **0478/11/O/N/22 Q4**: why encryption keeps stolen bank details safe, and how symmetric encryption works.
- **0478/11/M/J/24 Q7**: complete a paragraph about asymmetric encryption.
- **0478/11/M/J/22 Q7**: how encryption keeps data on a phone more secure.