Your notes

GCSE Computer Science: revision notes

Encryption and ciphers

Contents

1. Start here: why encrypt?
2. Symmetric and asymmetric encryption (Cambridge IGCSE)
3. Caesar and Vigenère ciphers (Edexcel IGCSE)
4. Rail fence and pigpen ciphers (Edexcel IGCSE)
5. Common mistakes
6. Worked examples
7. Key terms
8. Quick questions
9. What to do next

Start here: why encrypt?

- Encryption scrambles data so that anyone who intercepts it can't understand it. It doesn't stop data being stolen, but it makes stolen data useless without the key.
- The original data is the **plaintext**. The encrypted data is the **ciphertext**. An algorithm and a key turn one into the other, and back.
- It protects passwords, payments, messages and files on lost devices.

Symmetric and asymmetric encryption (Cambridge IGCSE)

- **Symmetric encryption** uses the same key to encrypt and decrypt. It is fast, but the key has to be shared safely first; anyone who intercepts the key can read every message.
- Asymmetric encryption uses two keys: a **public key**, which anyone can have and which encrypts data, and a **private key**, which only the receiver has and which decrypts it.
- Because the **private key** is never sent, asymmetric encryption is safer for sending data to someone you haven't met, such as a website.

Caesar and Vigenère ciphers (Edexcel IGCSE)

- A **Caesar cipher** shifts every letter the same number of places along the alphabet. With a shift of 3, A becomes D, B becomes E, and X wraps round to A.
- It is easy to break: there are only 25 possible shifts, and common letters such as E show through.
- A Vigenère cipher uses a keyword. Each letter of the keyword gives a different shift (A = 0, B = 1 ...), so the same **plaintext** letter can be encrypted differently each time. This makes it much harder to break.

Rail fence and pigpen ciphers (Edexcel IGCSE)

- A rail fence cipher writes the message in a zigzag across a number of rows (rails), then reads each row in turn. The letters are rearranged, not replaced.
- A pigpen cipher swaps each letter for a symbol: part of a grid or an X shape, with or without a dot.

Common mistakes

- Forgetting to wrap round the alphabet: with a shift of 3, Y becomes B.
- Saying encryption stops data being intercepted. It only stops it being understood.

Worked examples

Encrypt HELLO with the Vigenère keyword KEY.

Write the keyword under the message, repeating it. **HELLO over KEYKE**

Shift each letter by its keyword letter (K = 10, E = 4, Y = 24). **H + 10 = R, E + 4 = I, L + 24 = J, L + 10 = V, O + 4 = S**

Answer: RIJVS

Encrypt MEETATNOON with a rail fence cipher on 2 rails.

Write the letters in a zigzag on two rows. **Top row: M E A N O. Bottom row: E T T O N**

Read the top row, then the bottom row. **MEANO then ETTON**

Answer: MEANOETTON

Key terms

Plaintext	Data before it is encrypted.
Ciphertext	Data after it has been encrypted.
Key	The value an algorithm uses to encrypt or decrypt data.
Symmetric encryption	Encryption that uses the same key to encrypt and decrypt. (Cambridge IGCSE)
Public key	A key anyone can have, used to encrypt data sent to its owner. (Cambridge IGCSE)
Private key	A key only its owner has, used to decrypt data encrypted with their public key. (Cambridge IGCSE)
Caesar cipher	A cipher that shifts every letter the same number of places. (Edexcel IGCSE)

Quick questions

Cover the answers and test yourself: remembering is what makes it stick.

Your notes

1. What is ciphertext?
2. Does encryption stop data being intercepted?
3. In symmetric encryption, how many different keys are used? (Cambridge IGCSE)
4. In asymmetric encryption, which key decrypts the data? (Cambridge IGCSE)
5. Why is asymmetric encryption safer for sending data to a website you haven't used before? (Cambridge IGCSE)
6. Using a Caesar cipher with a shift of 3, what does CAT become? (Edexcel IGCSE)
7. Using a Caesar cipher with a shift of 3, what does Y become? (Edexcel IGCSE)
8. Why is a Caesar cipher easy to break? (Edexcel IGCSE)

Answers

1. Data after it has been encrypted
2. No, it stops intercepted data being understood
3. One, for both encrypting and decrypting
4. The receiver's private key
5. The private key is never sent, so it can't be intercepted
6. FDW
7. B
8. There are only 25 possible shifts to try

What to do next

Practise 10 questions on this topic

Try 3 exam questions, with mark schemes

Read the lesson, one step at a time

Free revision for GCSE and KS3 at lycolearn.co.uk. Some notes are for one exam board only, and say so in brackets.

Your notes