17 Encryption – Part 1

Name: _____ Class: _____ Date: _____

Vocabulary

Write each word three times.

English	**Write it 3 times** (English)		
Encryption			
plaintext			
ciphertext			
decryption			
Symmetric encryption			
key distribution			

Recall

Encryption turns readable text into unreadable text using a key, so only someone with the key can read it.

New ideas

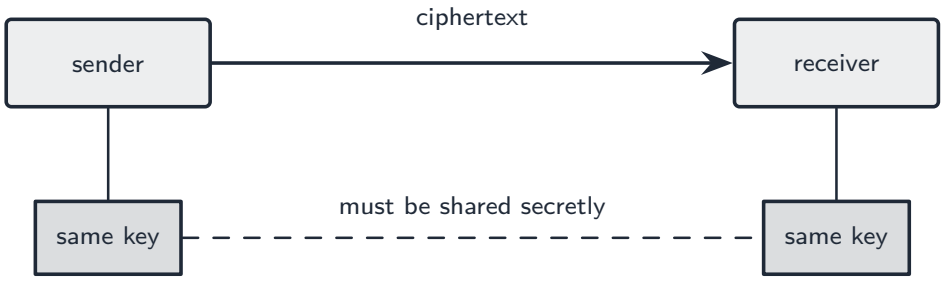
Read these first. Each idea has a short worked example. Then do the Practice.

1 The idea

Encryption turns **plaintext** into **ciphertext** using a key; **decryption** reverses it. Without the key, the ciphertext is meaningless.

Worked example. A simple Caesar cipher shifts each letter by 3: "HELLO" becomes "KHOOR". Here the key is "shift by 3"; to decrypt, you shift back by 3. Anyone without the key just sees "KHOOR".

2 Symmetric encryption



Symmetric encryption uses the *same* key to encrypt and decrypt. It is fast, but raises the problem of **key distribution** – how to share the key safely.

Worked example. Two people agree on one secret key. The sender encrypts with it; the receiver decrypts with the *same* key. The hard part is getting that key to the receiver without anyone else seeing it.

Watch out: the *algorithm* can be public – it is the *key* that must stay secret. Symmetric encryption's weakness is sharing the key, not hiding the method.

Practice

Try these in order.

17.1 What does *encryption* turn plaintext into? [1]

17.2 What is needed to reverse encryption? [1]

17.3 How many keys does *symmetric* encryption use? [1]

17.4 Give one strength of symmetric encryption. [1]

17.5 What is the main problem with symmetric encryption? [1]

17.6 A Caesar cipher shifts letters forward by 3, turning ”CAT” into ”FDW”. Decrypt the ciphertext ”FDW” and explain how. [2]

17.7 Challenge. Two people want to use symmetric encryption, but they have never met and can only talk over the open internet. Explain why this is a problem, and name the issue. [2]