How does encryption work?

KS3 KS4 Ages 11-16 ⏰ 4 min read

Encryption is the process of scrambling information so that only the intended recipient can read it. It's not new — Julius Caesar used a simple version where each letter was shifted three positions in the alphabet. Modern encryption uses mathematics so complex that breaking it would take longer than the age of the universe, even with the fastest computers we have.

Symmetric encryption

The simplest type: the same key scrambles and unscrambles the message. Both sender and recipient need the same key. The problem is — how do you share that key securely in the first place? If you're sending it over the internet, someone could intercept it. This is called the "key distribution problem," and it stumped cryptographers for centuries.

Imagine you want to send a locked box to someone across the world. You could send the key separately — but what if the key gets intercepted? The brilliant solution (invented in the 1970s) is public-key encryption: you send an open, unlocked padlock to anyone who wants to send you something. They put their message in a box, snap your padlock shut, and send it back. Only you have the key to open it. The open padlock (public key) can be shared with everyone. The key (private key) never leaves you.

Public-key encryption

In 1977, mathematicians invented a system using two mathematically linked keys: a **public key** (shared freely) and a **private key** (kept secret). A message encrypted with the public key can *only* be decrypted by the private key. This means anyone can encrypt a message to you, but only you can read it. The maths behind this relies on a simple asymmetry: multiplying two huge prime numbers is easy; factoring the result back into its prime components is computationally almost impossible. The most common system (RSA) uses key sizes where factoring the number would take billions of years with current computers.

HTTPS and the padlock

Every time you see a padlock icon in your browser, your connection to that website is encrypted using these principles. Your browser and the server do a rapid "handshake" — exchanging public keys, verifying identity certificates, and establishing a shared encryption key — all in milliseconds before you see any content. Your card details, passwords, and messages are scrambled the moment they leave your device and unscrambled only at the destination.