# Number-based Ciphers

The earliest ciphers were simple **substitution ciphers**, where letters were swapped for different letters or symbols.

If we **represent** letters as numbers we can use maths to create ciphers. They are much more flexible. We can easily turn letters into numbers using the following table, for example.

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

We can encrypt whole messages using a maths-based cipher based on this.

Here is a simple maths-based cipher. To encrypt a letter:

**STEP 1.** Replace it by its equivalent number.

**STEP 2.** Add 10 to the number.

**STEP 3.** If the result is greater than or equal to 26, then subtract 26.

The last step uses **clock arithmetic**. It works like the hands on a big clock that, here, has 26 hours instead of just 12. When we get to 26, we go back to 0 just like a clock. It disguises patterns.

Let's encrypt an example word:

CIPHER

It is encrypted by each step as follows:

STEP 1: 2-8-15-7-4-17

STEP 2: 12-18-25-17-14-27

STEP 3: 12-18-25-17-14-1

Representing letters as numbers allows us to make complex ciphers that are hard to crack.

## Things to try

1. Encrypt the following message using this cipher.

   I AM A PRISONER

2. Write your own message and then encrypt it using the cipher
3. Work out the steps to decrypt a message using the cipher. Check it works by decrypting the messages encrypted so far.
4. Invent your own number-based cipher. Use clock arithmetic to always end up with a number between 0 and 25. You need a way to decrypt messages too.