Shift Cipher

The Roman ruler Julius Caesar (100 B.C. – 44 B.C.) used a very simple cipher for secret communication. He substituted each letter of the alphabet with a letter three positions further along. Later, any cipher that used this “shift” concept for the creation of a cipher alphabet, was referred to as a Caesar cipher.

Of all the substitution type ciphers, this Caesar cipher is the simplest to solve, since there are only 25 possible combinations.



Often this type of cipher is made on a wheel device. A disk or wheel has the alphabet printed on it and then a movable smaller disk or wheel with the same alphabet printed on it is mounted forming an inner wheel. The inner wheel then can be rotated so that any letter on one wheel can be aligned with any letter on the other wheel.

For example above, the inner wheel is rotated so that the letter N is placed under the letter A on the outer wheel. To code the word ‘yellow’ Find the letters on the outside wheel and change it for the matching one on the inside.

So Y would become L

 E would become R

 L would become Y

And so on so the coded word would be LRYYBJ

To decode a message simply find the letter on the inside and match it with one on the outside. The challenge is finding the correct setting for your Caesar Wheel.