

A Caesar cipher, shift cipher, or substitution cipher is a simple type of cryptographic algorithm that works by replacing each letter of a plaintext message with another letter from a fixed alphabet. The alphabet is usually the standard 26-letter Latin alphabet, but it can be any alphabet with a fixed number of letters.

The Caesar cipher is named after Julius Caesar, who used it in his private correspondence. The cipher is very easy to break, but it is still used sometimes in educational settings and in recreational cryptography.