= Caesar cipher =

In cryptography , a Caesar cipher , also known as Caesar 's cipher , the shift cipher , Caesar 's code or Caesar shift , is one of the simplest and most widely known encryption techniques . It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet . For example , with a left shift of 3 , D would be replaced by A , E would become B , and so on . The method is named after Julius Caesar , who used it in his private correspondence .

The encryption step performed by a Caesar cipher is often incorporated as part of more complex schemes , such as the Vigenère cipher , and still has modern application in the ROT13 system . As with all single @-@ alphabet substitution ciphers , the Caesar cipher is easily broken and in modern practice offers essentially no communication security .

= = Example = =

The transformation can be represented by aligning two alphabets ; the cipher alphabet is the plain alphabet rotated left or right by some number of positions . For instance , here is a Caesar cipher using a left rotation of three places , equivalent to a right shift of 23 (the shift parameter is used as the key) :

Plain : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher : XYZABCDEFGHIJKLMNOPQRSTUVW

When encrypting , a person looks up each letter of the message in the " plain " line and writes down the corresponding letter in the " cipher " line .

Plaintext : THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
Ciphertext : QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD

Deciphering is done in reverse , with a right shift of 3 .