= 0 , B =
1 , ... , Z = 25 . Encryption of a letter <formula> by a shift n can be described mathematically as ,
<formula>
Decryption is performed similarly ,
<formula>
(There are different definitions for the modulo operation . In the above , the result is in the range 0 ... 25 . I.e. , if x + n or x @-@ n are not in the range 0 ... 25 , we have to subtract or add 26 .)

The replacement remains the same throughout the message , so the cipher is classed as a type of monoalphabetic substitution , as opposed to polyalphabetic substitution .

= = History and usage = =

The Caesar cipher is named after Julius Caesar , who , according to Suetonius , used it with a shift of three to protect messages of military significance . While Caesar 's was the first recorded use of this scheme , other substitution ciphers are known to have been used earlier .

If he had anything confidential to say , he wrote it in cipher , that is , by so changing the order of the letters of the alphabet , that not a word could be made out . If anyone wishes to decipher these , and get at their meaning , he must substitute the fourth letter of the alphabet , namely D , for A , and so with the others .

His nephew , Augustus , also used the cipher , but with a right shift of one , and it did not wrap around to the beginning of the alphabet :

Whenever he wrote in cipher , he wrote B for A , C for B , and the rest of the letters on the same principle , using AA for Z.

There is evidence that Julius Caesar used more complicated systems as well , and one writer , Aulus Gellius , refers to a (now lost) treatise on his ciphers :

There is even a rather ingeniously written treatise by the grammarian Probus concerning the secret meaning of letters in the composition of Caesar 's epistles .

It is unknown how effective the Caesar cipher was at the time , but it is likely to have been reasonably secure , not least because most of Caesar 's enemies would have been illiterate and others would have assumed that the messages were written in an unknown foreign language . There is no record at that time of any techniques for the solution of simple substitution ciphers . The earliest surviving records date to the 9th century works of Al @-@ Kindi in the Arab world with the discovery of frequency analysis .

A Caesar cipher with a shift of one is used on the back of the mezuzah to encrypt the names of God . This may be a holdover from an earlier time when Jewish people were not allowed to have mezuzot . The letters of the cryptogram themselves comprise a religiously significant " divine name " which Orthodox belief holds keeps the forces of evil in check .

In the 19th century , the personal advertisements section in newspapers would sometimes be used to exchange messages encrypted using simple cipher schemes . Kahn (1967) describes instances of lovers engaging in secret communications enciphered using the Caesar cipher in The Times . Even as late as 1915 , the Caesar cipher was in use : the Russian army employed it as a replacement for more complicated ciphers which had proved to be too difficult for their troops to master ; German and Austrian cryptanalysts had little difficulty in decrypting their messages .

Caesar ciphers can be found today in children 's toys such as secret decoder rings . A Caesar shift of thirteen is also performed in the ROT13 algorithm , a simple method of obfuscating text widely found on Usenet and used to obscure text (such as joke punchlines and story spoilers) , but not seriously used as a method of encryption .

A construction of 2 rotating disks with a Caesar cipher can be used to encrypt or decrypt the code .

The Vigenère cipher uses a Caesar cipher with a different shift at each position in the text ; the value of the shift is defined using a repeating keyword . If the keyword is as long as the message , chosen random , never becomes known to anyone else , and is never reused , this is the one @-@ time pad cipher , proven unbreakable . The conditions are so difficult they are , in practical effect , never achieved . Keywords shorter than the message (e.g. , " Complete Victory " used by the

Confederacy during the American Civil War) , introduce a cyclic pattern that might be detected with a statistically advanced version of frequency analysis .

In April 2006 , fugitive Mafia boss Bernardo Provenzano was captured in Sicily partly because some of his messages , clumsily written in a variation of the Caesar cipher , were broken . Provenzano 's cipher used numbers , so that " A " would be written as " 4 " , " B " as " 5 " , and so on .

In 2011 , Rajib Karim was convicted in the United Kingdom of " terrorism offences " after using the Caesar cipher to communicate with Bangladeshi Islamic activists discussing plots to blow up British Airways planes or disrupt their IT networks . Although the parties had access to far better encryption techniques (Karim himself used PGP for data storage on computer disks) , they chose to use their own scheme (implemented in Microsoft Excel) , rejecting a more sophisticated code program called Mujhaddin Secrets " because ' kaffirs ' , or non @-@ believers , know about it , so it must be less secure " .

The animated series Gravity Falls uses the Caesar cipher as one of three different ciphers (the other two being Atbash and an A1Z26 cipher) during the end credits of the first six episodes .

= = Breaking the cipher = =

The Caesar cipher can be easily broken even in a ciphertext @-@ only scenario . Two situations can be considered :

an attacker knows (or guesses) that some sort of simple substitution cipher has been used , but not specifically that it is a Caesar scheme ;

an attacker knows that a Caesar cipher is in use , but does not know the shift value .

In the first case , the cipher can be broken using the same techniques as for a general simple substitution cipher , such as frequency analysis or pattern words . While solving , it is likely that an attacker will quickly notice the regularity in the solution and deduce that a Caesar cipher is the specific algorithm employed .

In the second instance , breaking the scheme is even more straightforward . Since there are only a limited number of possible shifts (26 in English) , they can each be tested in turn in a brute force attack . One way to do this is to write out a snippet of the ciphertext in a table of all possible shifts ? a technique sometimes known as " completing the plain component " . The example given is for the ciphertext " EXXEGOEXSRGI " ; the plaintext is instantly recognisable by eye at a shift of four . Another way of viewing this method is that , under each letter of the ciphertext , the entire alphabet is written out in reverse starting at that letter . This attack can be accelerated using a set of strips prepared with the alphabet written down in reverse order . The strips are then aligned to form the ciphertext along one row , and the plaintext should appear in one of the other rows .

Another brute force approach is to match up the frequency distribution of the letters . By graphing the frequencies of letters in the ciphertext , and by knowing the expected distribution of those letters in the original language of the plaintext , a human can easily spot the value of the shift by looking at the displacement of particular features of the graph . This is known as frequency analysis . For example , in the English language the plaintext frequencies of the letters E , T , (usually most frequent) , and Q , Z (typically least frequent) are particularly distinctive . Computers can also do this by measuring how well the actual frequency distribution matches up with the expected distribution ; for example , the chi @-@ squared statistic can be used .

For natural language plaintext , there will , in all likelihood , be only one plausible decryption , although for extremely short plaintexts , multiple candidates are possible . For example , the ciphertext MPQY could , plausibly , decrypt to either " aden " or " know " (assuming the plaintext is in English) ; similarly , " ALIIP " to " dolls " or " wheel " ; and " AFCCP " to " jolly " or " cheer " (see also unicity distance) .

Multiple encryptions and decryptions provide no additional security . This is because two encryptions of , say , shift A and shift B , will be equivalent to an encryption with shift A + B. In mathematical terms , the encryption under various keys forms a group .