= ROT13 =

ROT13 (" rotate by 13 places " , sometimes hyphenated ROT @-@ 13) is a simple letter substitution cipher that replaces a letter with the letter 13 letters after it in the alphabet . ROT13 is a special case of the Caesar cipher , developed in ancient Rome .

Because there are 26 letters (2 × 13) in the basic Latin alphabet , ROT13 is its own inverse ; that is , to undo ROT13 , the same algorithm is applied , so the same action can be used for encoding and decoding . The algorithm provides virtually no cryptographic security , and is often cited as a canonical example of weak encryption .

ROT13 is used in online forums as a means of hiding spoilers , punchlines , puzzle solutions , and offensive materials from the casual glance . ROT13 has been described as the " Usenet equivalent of a magazine printing the answer to a quiz upside down " . ROT13 has inspired a variety of letter and word games on @-@ line , and is frequently mentioned in newsgroup conversations .

= = Description = =

Applying ROT13 to a piece of text merely requires examining its alphabetic characters and replacing each one by the letter 13 places further along in the alphabet , wrapping back to the beginning if necessary . A becomes N , B becomes O , and so on up to M , which becomes Z , then the sequence continues at the beginning of the alphabet : N becomes A , O becomes B , and so on to Z , which becomes M. Only those letters which occur in the English alphabet are affected ; numbers , symbols , whitespace , and all other characters are left unchanged . Because there are 26 letters in the English alphabet and 26 = 2 × 13 , the ROT13 function is its own inverse :

<formula> for any basic Latin @-@ alphabet text x .

In other words , two successive applications of ROT13 restore the original text (in mathematics , this is sometimes called an involution ; in cryptography , a reciprocal cipher) .

The transformation can be done using a lookup table , such as the following :

For example , in the following joke , the punchline has been obscured by ROT13 :

Why did the chicken cross the road ?

Gb trg gb gur bgure fvqr !

Transforming the entire text via ROT13 form , the answer to the joke is revealed :

Jul qvq gur puvpxra pebff gur ebnq ?

To get to the other side !

A second application of ROT13 would restore the original .

= = Usage = =

ROT13 was in use in the net.jokes newsgroup by the early 1980s . It is used to hide potentially offensive jokes , or to obscure an answer to a puzzle or other spoiler . A shift of thirteen was chosen over other values , such as three as in the original Caesar cipher , because thirteen is the value for which encoding and decoding are equivalent , thereby allowing the convenience of a single command for both . ROT13 is typically supported as a built @-@ in feature to newsreading software . Email addresses are also sometimes encoded with ROT13 to hide them from less sophisticated spam bots .

ROT13 is an example of the encryption algorithm known as a Caesar cipher , attributed to Julius Caesar in the 1st century BC .

In encrypted , normal , English @-@ language text of any significant size , ROT13 is recognizable from some letter / word patterns . The words " n " , " V " (capitalized only) , and " gur " (ROT13 for " a " , " I " , and " the ") , and words ending in " yl " (" ly ") are examples .

ROT13 is not intended to be used where secrecy is of any concern ? the use of a constant shift means that the encryption effectively has no key , and decryption requires no more knowledge than the fact that ROT13 is in use . Even without this knowledge , the algorithm is easily broken through frequency analysis . Because of its utter unsuitability for real secrecy , ROT13 has become a

catchphrase to refer to any conspicuously weak encryption scheme ; a critic might claim that " 56 @-@ bit DES is little better than ROT13 these days " . Also , in a play on real terms like " double DES " , the terms " double ROT13 " , " ROT26 " , or " 2ROT13 " crop up with humorous intent , including a spoof academic paper " On the 2ROT13 Encryption Algorithm " . As applying ROT13 to an already ROT13 @-@ encrypted text restores the original plaintext , ROT26 is equivalent to no encryption at all . By extension , triple @-@ ROT13 (used in joking analogy with 3DES) is equivalent to regular ROT13 .

In December 1999 , it was found that Netscape Communicator used ROT13 as part of an insecure scheme to store email passwords . In 2001 , Russian programmer Dimitry Sklyarov demonstrated that an eBook vendor , New Paradigm Research Group (NPRG) , used ROT13 to encrypt their documents ; it has been speculated that NPRG may have mistaken the ROT13 toy example ? provided with the Adobe eBook software development kit ? for a serious encryption scheme . Windows XP uses ROT13 on some of its registry keys . ROT13 is also used in the Unix fortune program to encrypt potentially offensive dicta .

= = Letter games and net culture = =

ROT13 provides an opportunity for letter games . Some words will , when transformed with ROT13 , produce another word . Examples of 7 @-@ letter pairs in the English language are abjurer and nowhere , and Chechen and purpura . Other examples of words like these are shown in the table . The pair gnat and tang is an interesting example which are both ROT13 reciprocals and (taken together) a palindrome .

The 1989 International Obfuscated C Code Contest (IOCCC) included an entry by Brian Westley . Westley 's computer program can be encoded in ROT13 or reversed and still compiles correctly . Its operation , when executed , is either to perform ROT13 encoding on , or to reverse its input .

The newsgroup alt.folklore.urban coined a word ? furrfu ? that was the ROT13 encoding of the frequently encoded utterance " sheesh " . " Furrfu " evolved in mid @-@ 1992 as a response to postings repeating urban myths on alt.folklore.urban , after some posters complained that " Sheesh ! " as a response to newcomers was being overused .

= = Variants = =

ROT5 is a practice similar to ROT13 that applies to numeric digits (0 to 9) . ROT13 and ROT5 can be used together in the same message .

ROT47 is a derivative of ROT13 which , in addition to scrambling the basic letters , also treats numbers and common symbols . Instead of using the sequence A ? Z as the alphabet , ROT47 uses a larger set of characters from the common character encoding known as ASCII . Specifically , the 7 @-@ bit printable characters , excluding space , from decimal 33 ' ! ' through 126 ' ~ ' , 94 in total , taken in the order of the numerical values of their ASCII codes , are rotated by 47 positions , without special consideration of case . For example , the character A is mapped to p , while a is mapped to 2 . The use of a larger alphabet produces a more thorough obfuscation than that of ROT13 ; for example , a telephone number such as + 1 @-@ 415 @-@ 839 @-@ 6885 is not obvious at first sight from the scrambled result Z` \ c`d \ gbh \ eggd . On the other hand , because ROT47 introduces numbers and symbols into the mix without discrimination , it is more immediately obvious that the text has been enciphered .

Example :

The Quick Brown Fox Jumps Over The Lazy Dog .

enciphers to

% 96 " F : 4 < qC @ H ? u @ I yF > AD ~ G6C % 96 { 2KJ s @ 8]

The GNU C library , a set of standard routines available for use in computer programming , contains a function ? memfrob ( ) ? which has a similar purpose to ROT13 , although it is intended for use with arbitrary binary data . The function operates by combining each byte with the binary pattern 00101010 (42) using the exclusive or (XOR) operation . This effects a simple XOR cipher . Like

ROT13 , XOR (and therefore memfrob ( )) is self @-@ reciprocal , and provides a similar , virtually absent , level of security .

= = Implementation = =

The ROT13 and ROT47 are fairly easy to implement using the Unix terminal application tr ; to encrypt the string " The Quick Brown Fox Jumps Over The Lazy Dog " in ROT13 :
and the same string for ROT47 :
In Emacs , one can ROT13 the buffer or a selection with the following commands :
M @-@ x toggle @-@ rot13 @-@ mode
M @-@ x rot13 @-@ other @-@ window
M @-@ x rot13 @-@ region
and in the Vim text editor , one can ROT13 a selection with the command :
g ?