

# MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

## MODIFIED CAESAR CIPHER

Author: Viktor Veselovsky

August 2011

# Description

A Caesar cipher is one of the simplest encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter a fixed number of positions down the alphabet. Decryption is done by simply shifting the letters in the ciphertext into the opposite direction.

To make it a little more complicated cipher, in this challenge the usually ordered alphabet has been changed and each word of the plaintext has been shifted differently.

# Example

How to create a ciphertext:

1) Choose an alphabet:

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

2) Choose a plaintext: "One two three"

3) There are three words whose letters are going to be shifted towards right by 3, 1 and 4 positions in the alphabet respectively. First word by 3: One-Rqh (O-P-Q-R, n-o-p-q, e-f-g-h), second word by 1: two-uxp (t-u, w-x, o-p), third word by 4: three-xlvii (t-u-v-w-x, h-i-j-k-l, r-s-t-u-v, e-f-g-h-i)

4) In this way you get the ciphertext: Rqhuxpxlvii

To decode this cipher we have to move the letters of the three words by either 3, 1, 4 positions to the left or by 49, 51, 48 positions to the right since the alphabet has 52 letters.

The answer, that is to be entered, to this example would be: One two three,49,51,48

(Clear text with the numbers of shifts to the right separated by a comma is to be provided as an answer, there are spaces between the words and no spaces before or after each comma)

# Assignment

Use the following 52-character alphabet:

aZbYcXdWeVfUgThSiRjQkPIOmNnMoLpKqJrIsHtGuFvEwDxCyBzA

This is the ciphertext:

PrdbejitgjcuiFFWFHVWlgYJILXELWWLYXsjuqsxHPMADYIHWHY  
IHYSANNSGREIPElgixczcyxcVRDVEUOHPSFypaSGXRGXIGIXQM  
ATQHGFmzpgvnoexmmxkXNh

The plaintext is in English. Please enter it in the format described in the example.