MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

# Monoalphabetic substitution with camouflage – Part 4

Author: Viktor Veselovsky

December 2011

# Introduction

Two friends Alice and Bob communicated using the cipher as it had been described in part 3 of this challenge.
They had chosen a secret key for the encryption process. Usually they got a response from the friend within a day after sending a message. But one day Alice did not get a reply to her message for more than a day, so she thought something had gone wrong and sent her message again. After another day she finally got a reply from Bob.

# First Message

Here are the two messages $m_1$, $m_2$ sent as ciphertexts $c_1$, $c_2$ and $c_3$:

Alice encrypts the message $m_1$ and gets
$c_1$ = kLyUpJ*yNvgrNvjjginjCpglCylzvln*h+gOnoynboinkOJgyJVr
mgwklNDWhZzygDxnrCgZzyVplcgaNCzqgyVplU*gmJnyIUgN*vyig
vVgpylxiCplvlnTh*g+npyuMV*lrUugTNUigNUkghLVyiVWvsygz*v
V+gyxV*coqNCnoGyZrpgyUJinpUgyZsV*lcygrmVlyhKipyqigpUJN
yCWgxUidJdnUygCIVrUxJNkCbgy*mnvkygzm*oV+CbgmyNUjJg*
yNURgn+UgnhYhgHnyCp*qyigpNyCganrDkIUygCVUpJNcCzbgyNv
gz*N+UgNvcglyjCGildvlndhjgUyJrVlbJgmpyJsZgvUlqZgiNL+UcgUi
JNCkWLygnMVliUgpy*NU+gpnCyLq**gZIVlgPydn+ZguaNCGqygV
Il*yUgkMlU*gpyKNdgn*PxgyzC*V+Ucygu**dbVN

# Second and Thrid Message

Alice encrypts the message $m_1$ once again and gets
$c_2$ = ruUJpNyk*vpTigkNLvyijgynCipyigjy+klC+jlv+rdlnyphTg*+O
LnTyoxTzynjp+IbzoyinOJpgyJpTVimkgGywrKl*+pyNiDWpyrkIyhzZ*
+yYgrzDysniCkIgyZ*V+pylgK+apyiNyrCYyqk*pgyVlL*UikLgmypJ*n
yrjjijUpgyzN*v+yigkvVgyrklzyxCrzlypvclzypn*yIh*ygniMpyxViplTU*
g+pyNu*rUugTikNLyisUygzhV*V+yx*WcGvygrpvyiVpys*cygryKViop
qyNipCyxnioddyIZrxkgyU*kyJz*nUg+ZyVj*yR+lYgHymVp*lyiphqyrg
kUIypJcNzyzCWgU*J+ncyjGUigdCVUdjJyrNpysCiLbg+cimkLynivpgy
*+moVpyL**CbIydgm+NUuGJygI*NUykg*npUygKnd*hhgxynCzq*
+cgyNu*C*gda

Bob encrypts his answer $m_2$ and gets
$c_3$ =*U+yJIfigIyhkf*pUUfyAtogHAEgupypNvTgrPNpvyuvNdCAFA
bgcNyrkgbljfxvAcvyIgIIZ

Later they had a discussion in person. Bob explained that he had not been able to send a reply because his computer was out of order. Then he said that he suspected that what Alice did might be a security risk. Alice agreed that it had been risky and said that she should have sent the same ciphertext again instead of encrypting the same message $m_1$ again and then sending its ciphertext.

Finally they found out that the security was degraded so much that any attacker would be able to decrypt the ciphertexts without using a computer. Can you decipher the communication using only pen and paper like Alice and Bob envisaged? Then it will be easy for you to provide the plaintext of the last ciphertext $c_3$ written in capital letters as the solution.

# Hint

The ciphertexts $c_1$ and $c_2$ contain the same message $m_1$. The same cipher and the same key has been used but the random place to set the line break was chosen differently.