

# MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

## MONOALPHABETIC SUBSTITUTION WITH CAMOUFLAGE – PART 1

Author: Viktor Veselovsky

October 2011

A monoalphabetic substitution is a classical symmetric encryption method. Every plaintext letter is replaced by a ciphertext letter. There are two alphabets: a plaintext alphabet and a ciphertext alphabet.

In this challenge, another alphabet has been added: a camouflage alphabet.

## Example (1/3)

This example illustrates the encrypting process.

We choose as plaintext alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZ

and as camouflage alphabet abcdefghijklmnopqrstuvwxyz.

The encryption key can be any permutation of all 52 letters of both alphabets. In this example we have chosen

jsEqWiZCTXzKdMynkullVmFhpyBtQSwgrcoUAXGORefbJaYHNDPL.

The letter A in the plaintext is replaced by j.

B is replaced by s.

C is replaced by E.

...

z is replaced by L.

## Example (2/3)

The plaintext is "MONOALPHABETIC SUBSTITUTION". Now the letters of the camouflage alphabet are randomly inserted between the letters of the plaintext. This results in the following string: acMONxOALqqPHAwBETmIC iSIUBdSTluebTUfTlcON. Afterwards the usual monoalphabetic substitution is performed, so that we get the following ciphertext: BQdyMDyjKffnCjNsWIGTE olxVsSIITYwtlVgITQyM

## Example (3/3)

The decryption is performed by reversing all the steps listed before, i.e. monoalphabetic substitution is performed with the key for the decryption and then all letters of the camouflage alphabet are removed and pure plaintext remains.

The key for decryption is the reversed key for the encryption (just like in normal monoalphabetic substitution). In this example the decryption key associated to the given encryption key is:  
kaHxCWmvSsLzNwnycodljUEJuGtrhMpqfXFAQ TVPiYDgBbRZelOK

# The Challenge

Two sentences have been encrypted by the above described monoalphabetic substitution cipher with camouflage. The first one is an English sentence, the second one is a German sentence:

BWVeUCWMN MdadaVEMC NEFCYYRARWQIUSH  
aMYFFWVCUQEVF FYJ TdXEOMEQN eYXF QdJF FdWJ  
SRWJUQN

YOVQWNbdTVQ QVUTOEVQ YRdO IVWIVQENMFB BUXY  
SJVEGEVQ WBVUeCWMN dMESN MYXZZMSYSVUQP  
IVdOXENFUVCF GYMTCW

Please enter the two sentences in capital letters and separate them by a single space. The first sentence is the English plaintext, the second one is the German plaintext.

# Hints

Spaces were not removed before performing the encryption, i.e. a word in ciphertext represents a word in plaintext.

The camouflage alphabet consists of only 5 letters: abcde

All five letters of the camouflage alphabet have been used.

Both plaintext sentences have the same meaning.

Both plaintext sentences have been encrypted using the same key.