MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Monoalphabetic substitution with camouflage – Part 3

Author: Viktor Veselovsky

December 2011

On the one hand using letters of a camouflage alphabet increases the security of a cipher but on the other hand it also increases the length of the ciphertext.

If it is important to keep the ciphertext as short as possible for some reasons, there is a way to use the same cipher which produces a ciphertext as long as the plaintext.

Example

These two alphabets will serve as plaintext and camouflage alphabet at the same time.
Alphabet 1: `ABCDEFGHIJKLMNOPQRSTUVWXYZ*`
Alphabet 2: `abcdefghijklmnopqrstuvwxyz+`

Once again a space in the plaintext is used as a character of alphabet, which decreases the security of the cipher. The characters "*" and, respectively, "+" represent a space.

We choose the plaintext "THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG".

The plaintext is split into two parts at any random position (but perhaps it would be wise to choose the difference between the lengths of the two parts not too large in order to maximize the camouflage effect).

Part 1 of plaintext: `THE QUICK BROWN FOX JUMP`
Part 2 of plaintext: `S OVER THE LAZY DOG`

Both parts of plaintext are rewritten in the corresponding alphabet.

Part 1: `THE*QUICK*BROWN*FOX*JUMP`
Part 2: `s+over+the+lazy+dog`

Now both parts are mixed together randomly but in a way that the order of characters of both parts is preserved.

One possibility is:
THs+ovE*QeUrICK+*BtRhOWNe+*lFOazyX*J+UdoMPg

Now a monoalphabetic substitution is applied to it using a key that is formed by a permutation of all 54 characters of both alphabets.

The result of the encryption can be for example:
bXjxASVrpuTvMtNxrZCoDa+LuxrlQahkmHrJxTyAIEw

For the example above, we used the following key:

Plaintext	A	B	C	D	E	F	G	H	I	J
Ciphertext	?	Z	t	?	V	Q	?	X	M	J

K	L	M	N	O	P	Q	R	S	T	U
N	?	I	L	a	E	p	o	?	b	T

V	W	X	Y	Z	*	a	b	c	d	e
?	+	H	?	?	r	h	?	?	y	u

f	g	h	i	j	k	l	m	n	o	p
?	W	D	?	?	?	l	?	?	A	?

q	r	s	t	u	v	w	x	y	z	+
?	v	j	C	?	S	?	?	m	k	x

A person who knows this key is able to decrypt the ciphertext because all of the steps are easily reversible.

The Challenge

tisLJLwfSERnvLnpIGiECCpfWMnFAEsqCrLVLiFbpntSpvLnELqWVLMSnCznSvs
LinvAbpFsFLfnSVLwymkpEQtmVLnymfpFInFAZZAfZnGFtCI*pfnGqyJLnSCnSiv
pLnGTQJtxnkCpzntZgCTFnyfFknESCpTLcnAwSn+SuvGLnJIAptELVnCfpnmvA
Enf+LOWRSpnwrAUEpASunzwCmkQfpKFnGSvLnvCTMLnHLGJpxSGanyfFnipj
LcZy+fnSbCnMSLyiVknpvMAEnvyAVgnyfpFnStCnJyopLnGTwCmQFnTyJiLpfM
SgySACpIfEnGynfLipAZvjCuVnELLAbfZw+nvgAJnCkrpLVqcCJLdpIn*ASvnZGV
ALzipnsyMkfiFpwnTLUyVfptAfZngpSvLwmnqykQEpLnEKytAFmmnxpVtyganFk
CnpfKCiSnZVgIALprILwpnECmnwjQwSneZCptnIyfpFkntSMymodLpnywngESCf
LnyifFnxpTyqLwnASUnAfnpSGvLnvCTMLnsyfpKFnwzybfqaenWigSpvywcSsnS
viLnZbCTPFniAEkpnESGAMsTTpnTaAfZUnSbivLVLnNASn*ATTn+FCnaCQinX
QgASILpnPMSvLsnEyJMLnIELVrAqsLnpIwzCpVIn*GivLfpsnRSvLnwZIpCtTFn*y
gkEnSvLVLnpaCkiQnvyFnASHnfCMSkinyEnaCkQnFApIFwnfpCSKnJyoLntISHvG
LnETAZvSLESpnQEGLnMspCzWwnAPS

Find the English plaintext and provide the longest word in capital letters as solution.