MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

A Cloaked Substitution Cipher – Part 2

Author: Bruce Kallick

August 2019

Introduction (1/8)

Like the MONOALPHABETIC SUBSTITUTION WITH CAMOUFLAGE series of challenges, this two-part challenge considers a modification of the classic simple substitution cipher achieved by randomly introducing decoy characters into the ciphertext in encryption which are then ignored in decryption.

Here we consider a cipher system which operates on plaintext strings over the 31-character alphabet

$$A = \{\texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ.\_,-?}\}$$

and generates ciphertext strings over the 62-character alphabet

$$A' = A \cup \{\texttt{abcdefghijklmnopqrstuvwxyz*\^{}'=+}\}$$

Introduction (2/8)

In Part 1, the Cloaked Substitution Cipher was defined and exemplified using the key

$$\mathrm{K} : \texttt{Dx-UM\^{}QpKOs.\_YfBzJrLhAaTCgbNmGW}$$

which divides A' into signal characters and noise characters

$$\mathcal{S}_\mathrm{K} = \{\texttt{ABCDGJKLMNOQTUWY.\_-abfghmprsxz\^{}}\}$$

$$\mathcal{N}_\mathrm{K} = \{\texttt{EFHIPRSVXZ,?cdeijklnoqtuvwy*'=+}\}$$

Introduction (3/8)

to encrypt the message

THE_QUICK,_BROWN_FOX_JUMPS._OVER_A_LAZY-DOG?

as

LqcjpMNFztedhyvK-smNxiJfaVX=YVSqN^w,fTiNkOh'_
BrbFPNo*eZ+fnZAcMJjNDIwN=.DugC'wj=tG'kqZUf?QkW

In Part 2, we proceed very much along the lines followed in the MONOALPHABETIC SUBSTITUTION WITH CAMOUFLAGE — Part 3 challenge, first dividing the plaintext message into two parts, encrypting each part separately, and finally merging the two resulting ciphertexts.

Introduction (4/8)

Two ciphertext strings S and T can be randomly interleaved by the following

Random Interleaving algorithm: $\mathbf{R} \Leftarrow \mathbf{I}(\mathbf{S}, \mathbf{T})$

Given two strings S and T, the string R is constructed as follows:

```
i ← 1 j ← 1 k ← 1
WHILE i ⩽ |S| + |T|
        Flip a coin
        IF heads
            IF j ⩽ |S|
               R_i ← S_j
               increment i
               increment j
            ENDIF
        ELSE
            IF k ⩽ |T|
                   R_i ← T_k
                   increment i
                   increment k
            ENDIF
        ENDIF
ENDWHILE
```

Introduction (5/8)

Let us say that two keys K_1 and K_2 are complementary in case for each key, $\mathcal{S}_{K_1} = \mathcal{N}_{K_2}$ and $\mathcal{S}_{K_2} = \mathcal{N}_{K_1}$; i.e., for each key, the subset of $\mathcal{A}$' comprising its signal characters is the subset comprising the other's noise characters. (So for any given key there will be 31! complementary keys.)

If for two such complementary keys, $C_1 \Leftarrow E(K_1, M_1)$ and $C_2 \Leftarrow E(K_2, M_2)$ for two messages M_1 and M_2, and these two cryptograms are randomly interleaved as $C \Leftarrow I(C_1, C_2)$, then $M_1 \Leftarrow D^*(K_1, C)$ and $M_2 \Leftarrow D^*(K_2, C)$.

Introduction (6/8)

That is, C is one of the infinitely many[1] cloaked substitution encryptions of M_1 using K_1, and at the same time it's one of the infinitely many cloaked substitution encryptions of M_2 using K_2.

This technique can be employed to encrypt a message M by dividing it into two parts M_1 and M_2, encrypting each part with a simple substitution using two complementary keys, and then randomly interleaving the two resulting cryptograms to produce a ciphertext of the same length as M which will be decrypted as M_1 using one key and as M_2 using the other.

[1] *Infinitely many, since there is no upper bound on the length of the character strings randomly generated by the encryption algorithm.*

Introduction (7/8)

To illustrate, let us take the example key above as K_1 and as K_2 the complementary key

IRj=ZXen,cwoH'+Eut*kd?FPVSyiqlv

Now, if we take as M_1

THE_QUICK,_BROWN_FOX_J

and as M_2

UMPS._OVER_A_LAZY-DOG?

Introduction (8/8)

then

$C_1 = E(K_1, M_1) =$ `LpMNzhK-smNxJfaYN^fTNO`

$C_2 = E(K_2, M_2) =$ `dHE*yi+?ZtiIioISVl=+ev`

and $C = I(C_1, C_2)$

$=$ `dLpMNHE*zhyK-simNxJf+?aZYN^fTNOtiIioISVl=+ev`

is decrypted by the Cloaked Substitution Cipher as M_1 using K_1, and as M_2 using K_2.

Challenge (1/2)

Your task is to decrypt the following 799-character ciphertext generated by encrypting a plaintext message M using the technique just described above. You can also find the ciphertext as a text file in the additional zip file.

The solution consists of the third word in every sentence of M (where sentences are defined as character strings ending in either a period or a question mark, and hyphenated words are counted as single words). Please enter the solution with spaces between the words.

Challenge (2/2)

```
CucRd+snuH,OF+uHM-hTd,scuB+HPtTncye'yb+J-dHChq+Oe+sxy-dhJeue
gbfP,+qOPdybY+RnogHoQtHy-+,HCMh,sdc+HnO,F+ubyOHq,HCmlyU+dtOd
+h,y^RgqyMHoxQdHsbCxOq+oRgP-yuHdnRgTPehbAIoFgge+OA-UP+edty+m
HFdVXHbERgeuHVeJxdJAobGyFR+gTMv+iTqyHxGJeqyhFe+EOX-UH,Hz+Ru*
,xEHb,fFRmHdh,OPcqF+xTJqeUh+Hjy+bypPbycFy-,gH,gdHyUe+jfuu+eO
gPR,+wEHbsOpt,hPCHxOoQqHPceHs+FhodbJxVdEJby+TveG+_yHPFcFRuHy
-dc,uCHheGOqq,f+RgeFmHCiuoCHqQOohbH+PIcC-UeHe+dztehH^ORmdeg+
dtRybgyM+nOF+OHh+,gMbeyFJbwy-xHyo+QTv+Hu*CV-LedyAPubHPyFoH^c
d+CRAcHMh,sc-HPceoh+XwHbc,Opt+udtyHTbfNu+Od+RgOAjeTJdHV+dty+
eFegOHQoiy+dCiy*+wbgmH,Ospst+dtyERTbA,VfE+ey..FQhxoGOpyHM,GU
+vbeTHPceoi+hCXdF+pH,CgxdmTHbCsOqho+TMbhCw,CGGR-gMHPchoF*+nC
dtMcH+dtyu^R+FPdAcRgJUMHAf+TvR+jC-ObfhA+byqO*RdPCuHT-,gmHAoG
G*gRA,PRoguHPceohXBHAogu*GehHVec,zRoeH,gmHsuXAcoEoMXBHPoHsho
VEeGuHQhoGHVRoEoMX_
```

Additional Files

The additional zip archive contains the following files:

- ciphertext-cloakedsub-02.txt
    ➥ the ciphertext
- Cloaked-2.py
    ➥ Python 3 script to encrypt or decrypt with this cipher. The script is called with either "python Cloaked-2.py" or "python3 Cloaked-2.py" depending on the system environment.
- instructions_for_syntax-en.txt
    ➥ Description of the usage of the Python script.