A CLOAKED SUBSTITUTION CIPHER – PART 2

Author: Bruce Kallick
August 2019
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

\[ \mathcal{A} = \{ \text{ABCDEFGHIJKLMNOPQRSTUVWXYZ._,-,} \} \]

and generates ciphertext strings over the 62-character alphabet

\[ \mathcal{A}' = \mathcal{A} \cup \{ \text{abcdefghijklmnopqrstuvwxyz*^}\_\+=} \]
In Part 1, the Cloaked Substitution Cipher was defined and exemplified using the key

$$K : Dx-UM^\wedge QpKO_s._YfBzJrLhAaTCgbNmGW$$

which divides $A'$ into signal characters and noise characters

$$S_K = \{\text{ABCDEFGHIJKLMNOPQRSTUVWXYZ_.-abfghmprsxzˆ}\}$$

$$N_K = \{\text{EFHIPSXVZ,?cdeijklnoqtuvwy*’=+}\}$$
to encrypt the message

```
THE_QUICK_BROWNFOX_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:** $R \leftarrow I(S, T)$

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

- $i \leftarrow 1$
- $j \leftarrow 1$
- $k \leftarrow 1$
- While $i \leq |S| + |T|$
  - Flip a coin
  - If heads
    - If $j \leq |S|$
      - $R_i \leftarrow S_j$
      - Increment $i$
      - Increment $j$
    - Else
      - If $k \leq |T|$
        - $R_i \leftarrow T_k$
        - 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, $S_{K_1} = N_{K_2}$ and $S_{K_2} = N_{K_1}$; i.e., for each key, the subset of $A'$ 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 $M_2 \leftarrow D^*(K_2, C)$. 
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.
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 $M_1$

$$\text{THE\_QUICK,\_BROWN\_FOX\_J}$$

and as $M_2$

$$\text{UMPS.\_OVER\_A\_LAZY\_DOG?}$$
then

\[ C_1 = E(K_1, M_1) = \text{LpMNzhK-smNxFaYN}}^{fTNO} \]
\[ C_2 = E(K_2, M_2) = \text{dHE*yi+?ZtiIoISVl=+ev} \]

and \( C = I(C_1, C_2) \)

\[ = \text{dLpMNHE*zhyK-smNxFj+?aZYN}}^{fTNOtiIoISVl=+ev} \]

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+HPtTnCyeyb+J-dHChq+Oe+sxy-dhJeue gbFp,+qOPdybY+RnogHoQtHy-+, HCMh, sdc+Hn0, F+ubyOHq, HCmlyU+dtOd +h,y^RgqyMHoXQdHsbCxOq+oRgP-yuHdNgTPehbAIoFgge+OA-UP+edty+m HFdVXHbERgeuHVejxJAbGyF+vTMv+iTqyHxGJeqyHFe+EOX-UH, Hz+Ru*, xEHb, fFRmHdh, 0PcqF+xTJqeUh+Hjy+bypPbycFy-, gH, gdHyUe+jfuu+e0 gPR, +wEHbsOpt, hPChxOoQqHPCeHs+FhodbJxVdEJby+TveG+_yHPFcFRuHy -dc, uCHHeGOqq, f+RgeFmHCiuoCHqQoohbH+PIcC-UeHe+dzteH^ORmd+ 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..FQhxoG0pyHM, GU +vbeTHPceoi+hCXdF+pH, CgxdmTHbCsOqho+TMbhCw, CGGR-gMHPchoF^+nC dtMcH+dtyu^R+FPdAcRgJUMHAF+TvR+jC-ObfhA+byq0*RdPCuHr-, gmH AoG G*gRA, PRouHPceohXBHAogu^GehHVec, zRoeH, gmHsuXAcOEoMxBHPoHsho VEeGuHQhoGHVRoEoMX_
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.