MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

A Cloaked Substitution Cipher – Part 1

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

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

as follows:

Introduction (2/8)

Some permutation of 31 of the 62 characters of A' is chosen as a secret shared 31-character key K, say for example,

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

which is used as the basis of a Simple Substitution Cipher that can be displayed as a substitution table, ξ_{K}

$\mathrm{m}:$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	_	,	-	?
$\xi_{\mathrm{K}}(\mathrm{m}):$	D	x	-	U	M	^	Q	p	K	O	s	.	_	Y	f	B	z	J	r	L	h	A	a	T	C	g	b	N	m	G	W

Introduction (3/8)

A plaintext message M is encrypted into a ciphertext cryptogram C using the key K by means of the following

> ***Simple Substitution Encryption algorithm:*** $\mathbf{C \Leftarrow E(K, M)}$
> Replace each character m of M by $\xi_{\mathrm{K}}(\mathrm{m})$.

and a ciphertext cryptogram C is decrypted into a plaintext message M using the key K by means of the following

> ***Simple Substitution Decryption algorithm:*** $\mathbf{M \Leftarrow D(K, C)}$
> Replace each character c of C by $\xi_{\mathrm{K}}^{-1}(\mathrm{c})$.

Introduction (4/8)

For instance, using the example key above, the message

`THE_QUICK,_BROWN_FOX_JUMPS._OVER_A_LAZY-DOG?`

would be encrypted as

`LpMNzhK-smNxJfaYN^fTNOh_BrbNfAMJNDN.DgCGUfQW`

The 31 characters of A' used by a key are said to be that key's ***signal characters***, and the 31 unused characters are its ***noise characters***, so each key K divides A' into a subset $\mathcal{S}_K$ of signal characters and a complementary subset $\mathcal{N}_K$ of noise characters. For the example key above,

$$\mathcal{S}_K = \{\texttt{ABCDGJKLMNOQTUWY.\_-abfghmprsxz\^{}}\}$$
$$\mathcal{N}_K = \{\texttt{EFHIPRSVXZ,?cdeijklnoqtuvwy*'=+}\}$$

Introduction (5/8)

Now consider the following modification of the Simple Substitution Cipher:

Cloaked Substitution Encryption algorithm: $\mathbf{C \Leftarrow E^*(K, M)}$

1. $C' \Leftarrow E(K, M)$, i.e., encrypt M with the simple substitution algorithm E using K.
2. Randomly intersperse noise characters into C' producing a string C as follows:

```
i ← 0 j ← 0
REPEAT
        Flip a coin
        IF heads
                Randomly choose a noise character n ∈ N_K
                increment i
                C_i ← n
        ELSE
                increment j
                IF j ⩽ |C'|
                        increment i
                        C_i ← C'_j
                ENDIF
        ENDIF
UNTIL j > |C'|
```

Introduction (6/8)

Cloaked Substitution Decryption algorithm: $\mathbf{M \Leftarrow D^*(K, C)}$

1. Drop all noise characters from C, leaving a string C' of signal characters.
2. $M \Leftarrow D(K, C')$, i.e., decrypt C' with the simple substitution algorithm D using K.

Continuing with the previous example key, the message

`THE_QUICK,_BROWN_FOX_JUMPS._OVER_A_LAZY-DOG?`

might be encrypted by the cloaked substitution cipher as

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

Introduction (7/8)

The Cloaked Substitution Cipher is essentially similar to the cipher considered in the MONOALPHABETIC SUBSTITUTION WITH CAMOUFLAGE — Part 2 challenge. The principal differences are:

Substitution With Camouflage	Cloaked Substitution Cipher
key size: 54 chars	key size: 31 chars
key-space: $54! \approx 2.3 \times 10^{71}$ chars	key-space: $31! \times (62!/31!^2) \approx 3.8 \times 10^{51}$ chars
decoy chars added to plaintext	decoy chars added to ciphertext
before simple substitution	after simple substitution

Introduction (8/8)

The last difference suggests a possible vulnerability of the Camouflage cipher: In a hill climbing attack, scoring the correctness of a putative key can utilize the number of common English trigrams or quadgrams revealed simply by omitting all lower case letters from the putative plaintext.

More information about the Cloaked Substitution Cipher can be found at (https://eprint.iacr.org/2019/621.pdf).

Challenge (1/2)

Your task is to decrypt the following 938-character ciphertext generated by encrypting a plaintext message M with the Cloaked Substitution Cipher. 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 followed by a space, and hyphenated words are counted as single words). Please enter the solution with spaces between the words.

Challenge (2/2)

```
HQ=^-nQOhUGBEcjnx.EZvlSMg=E?o'SfE.Rprmc?HpIaZcKSNA^rXfoQ'cKC
?qpvtJm.esEkQh+slIcutRHJkPh.'jHsKQoctihSpdkouuB-QwKcoUPMPVmc
vZnkQcEOCIV.IjKvIScNBpvcBoeXVHYQJcKZkrQPKKQmBlcNfXJQck?Qs.rm
m.mscLpPta^cso^hJuViXcZNnodXQphFuZncVEcCVcg+lowxVNXQ^w'BVN.U
dMV-cj?.EnM.i-.ml^QDgcoNoXB.KvZ?CEAclmpv*W+cBZtaVwIoWBWpH=UE
ncVhN.netdMWx-rQcCjQnrVn?x-Nc*.OK'NXcCUfuVm?cUdQEIEZQmN.VJ--
HFcs'gL+hLLVUiX.ZePoMVfoCf-ciShd'npLk-CQLOwJ,ZrZvcPo-.ANrN-Q
JHc.rwVns.LWmVN.pmtvAOcRkQ.tU?AlmscZhoWQfJz=nUun^lUe.htLQjcN
ZpcIMppumdE.KjQhcgIORNuIXAQCcJYlRVZJUJhI.pOJnB=ECciWB-+KVMPQ
EcNpckQLcY?.E.NgQjc?VEcip.mHZONE,'gBUc'NdXWxQvESQOr?xciJp.??
HtmN^xEelc?kWOQ.mstecM+OlpmmQUUvIMNSCWQjHRIOckFce-.m'QEZ'Uch
IQihQUnEQxWvmLgN.mescNXoIggQckLh.jd^ZdsQEDcIdt.m+jQQjoUrngcN
ILXKQcilhptk-QLLwAc+MVumBckrQOfcJjUhV*oKmlPCIcUp=NufocJpJmci
ViQK+xhc?VEcIiSpv.SmNEI^ocSMZpmevoL'mSQOBMNQjckFcnRRfvf-U.r+
mZWQWAExc*.uUNPXp^?oL=Nc-pgIEEcvp^RghcVjdj.N.pmc'SpacdhZntQO
v-QYUPVmNcnCKJ.'maphrwxVgLNI.pm?rADncn
```

Additional Files

The additional zip archive contains the following files:

- ciphertext-cloakedsub-01.txt
  - ➥ the ciphertext
- program.py
  - ➥ Python 3 script to encrypt or decrypt with this cipher. The usage is described in the Python script itself. The script is called with either "python program.py" or "python3 program.py" depending on the system environment.