MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Polyphonic Substitution Cipher – Part 2

Author: Satoshi Tomokiyo

January 2020

Introduction (1/2)

A polyphonic substitution cipher is a variant of substitution cipher in which one ciphertext character may correspond to two or more plaintext letters. For example, both "o" and "s" may be enciphered as "1", both "n" and "i" may be enciphered as "2", both "e" and "x" may be enciphered as "3". In this particular example, the ciphertext "123" may represent "one" as well as "six". This means a ciphertext encrypted with a polyphonic substitution may not be uniquely deciphered even if one has the correct key.

Introduction (2/2)

Nevertheless, polyphonic substitution was actually used in the 16th century in Italy [1] and France [2]. There are many encrypted historical documents that await deciphering (e.g., [3][4][5]), and one cannot exclude the possibility that some of them are polyphonic. So, it is of interest to see whether polyphonic substitution ciphers can be solved. It is known that Edgar Allan Poe solved a challenge cipher with polyphonic substitution [2]. With today's computerized techniques, the author has been informed by a private email that polyphonic ciphers can be solved with hill climbing, but the details have not been published yet. It will be desirable to establish a methodology to solve polyphonic ciphers without a key.

Challenge (1/3)

Your task is to find a substitution key of the cipher used in the attached ciphertext. The key should be of a format

12345678901234567890123456

i.e., 26 digits corresponding to the substitution digits for a-z. (This particular example indicates "a" is enciphered as "1", "b" is enciphered as "2", ..., and "z" is enciphered as "6".)

Challenge (2/3)

- The challenge ciphertext consists of the numbers 0-9.
- The plaintext is in English.
- Partly because of the author's historical interest, it is assumed j=i, u=v, k=q=x=c, z=s. This reduces the number of letters in the alphabet from 26 to 20. With this assumption, each digit in the ciphertext represents two letters of the alphabet.

Challenge (3/3)

- As exemplified above, there may be cases in which more than one reading is possible. So the solution does not require the plaintext. All you need is to find the substitution key.
- This is Part 2 of the two challenges. The digits in the key for Part 1 tend to represent two letters of similar frequencies, while the digits in the key for Part 2 tend to represent one high-frequency letter and one low-frequency letter.
- The author wishes to discuss whether there are some means to tell whether a given ciphertext is a polyphonic substitution cipher or a homophonic substitution cipher. Every solver can discuss this either in the forum or send an email to: solution[at]mysterytwisterc3[dot]org.

References (1/2)

[1] S. Tomokiyo (2017, 2018), "Polyphonic Substitution in Italian Numerical Ciphers"
http://cryptiana.web.fc2.com/code/polyphonic.htm

[2] S. Tomokiyo (2017, 2019), "A Polyphonic Substitution Cipher of the Catholic League (1592-1593)"
http://cryptiana.web.fc2.com/code/mayenne.htm

[3] George Lasry (2019), "The Vatican Challenge – Part 4"
https://www.mysterytwisterc3.org/en/challenges/level-x/the-vatikan-challenge-part-4

References (2/2)

[4] George Lasry (2019), "The Vatican Challenge – Part 5"
https://www.mysterytwisterc3.org/en/challenges/level-x/the-vatikan-challenge-part-5

[5] S. Tomokiyo (2015, 2019), "Unsolved Historical Ciphers"
http://cryptiana.web.fc2.com/code/unsolved.htm