MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Cipher ID – Part 1

Author: Miles Stamp

November 2019

Challenge (1/4)

In this challenge you have to identify different ciphers that were used for encrytion of a given dataset of ciphertexts.

The dataset for this challenge consists of 500 ciphertext samples, each of which is 100 characters in length. Your goal is to determine the type of cipher used to encrypt each message. The 500 ciphertext messages comprise 100 ciphertexts from each of the following classic ciphers: simple substitution, Vigenére cipher, columnar transposition, Playfair cipher, and the Hill cipher [1].

Challenge (2/4)

The plaintext messages were taken from random locations in the Brown Corpus [2]. Each key was randomly generated, with restrictions (for some of the ciphers) to ensure that no padding was needed to encrypt a message of exactly 100 characters. In addition, for ciphers that use key "words" (e.g., Vigenére), these key words are not necessarily actual English words, but rather random strings of characters. More details on the keys used for each type of cipher is included in the additional file README.txt.

Challenge (3/4)

Give your solution in the form of one string of 500 upper-case letters with no separators (i.e., no spaces, commas, etc.). Use the following letters to identify each type of cipher:

S	Simple Substitution
V	Vigenére Cipher
C	Columnar Transposition
P	Playfair Cipher
H	Hill Cipher

Challenge (4/4)

For example, if you determine that the first two ciphertexts are simple substitutions, the next two are columnar transpositions, the next two are Vigenére, the next two are Playfair, and the next two are Hill, then your 500 character solution would begin with

```
SSCCVVPPHH...
```

When you submit a putative solution, you will receive a number that represents the percentage of ciphertext messages correctly identified. For example, if you receive 98, that would mean that your solution is 98% correct, and hence you only misidentified 10 of the 500 ciphers.

Again, the challenge is to simply identify the type of cipher used to encrypt each message. It is not necessary to actually decrypt any of the messages.

Additional Files

The additional zip archive contains the following files:

- ciphertext_cipher-id.txt
  - ➥ the 500 ciphertexts
- README.txt
  - ➥ details on the keys used for each type of cipher

References

[1] J. Lyons, Practical Cryptography, http://practicalcryptography.com/ciphers/hill-cipher/ https://en.wikipedia.org/wiki/Hill_cipher

[2] Brown University Standard Corpus of Present-Day American English, available for download at http://www.cs.toronto.edu/~gpenn/csc401/a1res.html