MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Hilly – Part 1

Author: Yahya Almardeny

January 2017

Introduction

Once upon a time, there was a student, who listened to a lecture of linear algebra. He got to know the classical Hill cipher and thought: "I like the idea, but it has a few weaknesses, which could be improved."
At first he modified the substitution table for the plaintext-character alphabet, so that it is addicted to the key matrix.
After he understood the problem of computing an inverse modulo 26, he decided to find a way to avoid it. He found a possibility, at which the determinant of the key matrix may just not have an inverse mod 26.
The result of the thoughts of this student is Hilly, an improved version of Hill cipher.

Challenge (1/3)

This challenge consists of the decryption of a ciphertext by means of a given plaintext-ciphertext pair (P_1, C_1).
You are given the ciphertext C_1:

```
L?%$^-@-?%J%-?&*-#^&P%^*$$-#$%P?+-&^%#%*
Z%*%^*---+X?%%$?^*@-T%&?-?@@&?F%?+&$+&##
B%$*%$#-#-H?%%*?#+&^X%-##$??@-N%^@-?^*^*
P%#%%**#?-Z$+%@*&^%Z*-#^?^??J%?&$@+-#@
Z***+-&?@F&-?&$#$$V%+%$*?-%^N&--%@@-%
Z%#+$$^-^*F%-*@#^#*-T%##@@#$@@X%?$^@?*%%
Z%@$-&#%$$Z&*$^*^$#D%?-??#-&@T%$@&%^++^
Z%%&*&$-%@V%@+-^*&^*P%##&$^?--F$^$%*%&^
D*^^^-*@?D%?-+#%&#$T$&?@@*%+N&@@*+&+$
```

You are also given the related plaintext P_1 to the ciphertext C_1:

```
HILLY IS AN IMPROVED VERSION OF HILL CIPHER
```

MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

Challenge (2/3)

Your task is to decrypt the ciphertext C_2:

```
L%-+^---#+D&$@%#*@^B%++**@$$-H%$&#%^@%%V%+*?$-$-^
R%--#@?@%^J%-^?#?-%-R%%##??##+X%?+&$&^&-N%&-%?*&%@
L%?@$*@+#*N%-+$&$&$^P%^$$$??*?X%++$@?&%+V%-?+?$??+
N?%&-***^$L%+$-*-*@?D%**^*-+-*B%^?&-$*@^X%%*#^#@&+
R%-**&%^%*H?#+?%+^?&V%@++-^@^@Z%*$&?%%+#D%&?-?+%$%
R%?^*$%+?-Z%$-@^#^$*Z?#*$&$+%-J%--*$@$$&T%^@*-*@%$
T**+@?%#$Z-^##*@#&J-@?#?^$^L%%%$+$$?*F$^@?-@+&
L^?#@#%@#D%?-^#-*?#R^$$&*?+&P%#?^*@%#+V%@^++*#$?
J&@#^$&^^J%?##@*^#*P%+++*-%@#F%#$@??^%@X%#$$+%%$$
Z%$#^&#@**L%%-$*^^&^H%+-^*#&@?D%%^%^@$$$T^-#@-&-%
J^^$-%?^#J%-?-%@@?-T%#%+^%#&%B%?%&#&?&%H&$&%%$@#
D$#?%%#%$H**+###&#P%%^??---*F$%*-%-$?B^**+%$#&
H%#$?%@@$+F*#$*-*^-H^$^+#*%+X%?+@^-%?&R$^&+*&-&L&-*+%#**
```

Challenge (3/3)

The ciphertexts C_1 and C_2 have been encrypted with the same key K.

The solution consists of the plaintext P_2 to the ciphertext C_2.
Please enter the solution with spaces between the words.

Remark:
This is not a partly-known-plaintext challenge, because ciphertext C_1 is not part of ciphertext C_2.

Additional Files

The additional zip archive contains the following files:

- mtc3_hilly_description.pdf
  - ➥ detailed explanation of Hilly
- known-plaintext_hilly-01.txt
  - ➥ the plaintext P_1
- ciphertext_hilly-01.1.txt
  - ➥ the ciphertext C_1
- ciphertext_hilly-01.2.txt
  - ➥ the ciphertext C_2
- hilly.zip
  - ➥ Python code and test files for Hilly

References

In the document "`mtc3_hilly_description.pdf`" the cipher is explained in detail. You can find it within the additional zip file.

Remark:
To avoid any confusion: The order of the symbols in the substitution table T_A in this challenge is different from the order in the example in the description file.