Mystery Twister G3 THE CRYPTO CHALLENGE CONTEST

HILLY - PART 2

Author: Yahya Almardeny

October 2017

Introduction

Hilly is an improved version of Hill cipher.

In the previous challenge (Hilly Part 1) you were given a plaintext P_1 and its corresponding ciphertext C_1 . The task was to decrypt a ciphertext C_2 and find its plaintext P_2 which was encrypted with the same key that was used for the aforementioned pair (P_1, C_1) .

In this challenge you are given a partly-known key K and a ciphertext C. The task is to decrypt this ciphertext and find its corresponding plaintext P.



Challenge (1/2)

This challenge requires to decrypt a ciphertext C by means of a partly-known key K. This is the given ciphertext C:

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



Challenge (2/2)

You are also given the partly-known key K that was used to encrypt the ciphertext C:

?	?	472	?	?	13
4	?	?	234	?	?
?	-55	?	?	?	75
?	?	?	?	?	?
?	?	?	?	?	?
12	?	?	88	?	?

The solution consists of the plaintext P.

Please enter the solution in capital letters with spaces between the words.

Additional Files

The additional zip archive contains the following files:

- mtc3 hilly description.pdf
 - detailed explanation of Hilly
- ciphertext hilly-02.txt
 - ⇒ the complete ciphertext C
- partly-known-key_hilly-02.txt
- 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.

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.