ICT2213—Applied Cryptography

Puzzle #1: Running key cipher

1 Introduction

The *running key cipher* is very similar to Vigenère, except that the key is *not* repeating. Typically, the sender and receiver agree on a book where the book's text is used as a *keystream.* In particular, the two parties pre-select the page, line, and character number where the keystream begins, and the exchanged message is then encrypted in a way identical to Vigenère. Although this looks very similar to the OTP cipher, note that the key is not truly random and can be cryptanalyzed or brute-forced. As an example, consider the following plaintext:

```
thisisarunningcipherexample
```

Assume that the keystream comes from the novel "Moby Dick" and that the sender and receiver have agreed to start the keystream from the 36th character of the following book excerpt:

```
There now is your insular city of the Manhattoes, belted round by
wharves as Indian isles by coral reefs-commerce surrounds it with her
surf. Right and left, the streets take you waterward. Its extreme
downtown is the battery, where that noble mole is washed by waves, and
cooled by breezes, which a few hours previous were out of sight of
land. Look at the crowds of water-gazers there.
```

Then, the plaintext will be encrypted with the following key, where all the whitespaces, punctuation, symbols, and numbers are removed from the text (i.e., only alphabet characters are allowed as part of the keystream):

```
TTOESBELTEDROUNDBYWHARVESAS
```

The resulting ciphertext is:

```
MAWWATECNRQZBAPLQFAYEOVQHLW
```

Note that, if the plaintext was longer, then more consecutive characters from the book would be used in the keystream, i.e., the key is never repeated.

2 Your task

You must write a Python script that accepts two command-line arguments. The first one is a file that contains the ciphertext, and the second one is a text file of a book that may (or may not) contain the keystream. The script should output only one of the following: (i) the decrypted plaintext **and** the key; or (ii) a message that the key was not found. A sample command to execute your code looks as follows:

```
$ python3 break.py ciphertext.txt book.txt
```

To test your code, use the following ciphertext and the `txt` file of "Moby Dick" that can be found at `https://www.gutenberg.org/cache/epub/2701/pg2701.txt`. If your code is correct, you should be able to decrypt it. Be careful when copy/pasting the ciphertext from the pdf into a text file; make sure you remove all whitespaces, such as space or newline characters.

```
RVZASIOSXPWRXDEMCLHWWIXWFEWBZRZDMOLBPIDUFBPSPJUCIRJGWKCFOUINWSNKCGB
NEGEHHAFSZZVEDNSUVYTWEPKFSPWZUEFNPJHZTETAJNVQZALPNWVOHNVOBBXFJTYHMG
PZHFMFLBRLWHZLXFOICBLQPTEGRVCZGJPOMSDVGXTPLQPDDNGKQGFMLGKAEXDLRWBHO
MAWLHXNMETDZECIPVUHVNVWDTZGEPEPSBXKSIPPBFWFWVVVORGBTNRUTUEUAGKWZAZT
GFBVRDLQHRVPNYZWEDWCDAKHIZATUCHIDPVREPEKHEELMSQRLHNWWHCTSAEDEDOSKBM
EZAIZQZMOIVKJVXTPWLWHMJJDGNRLXNIVECMWLHRUBGNEWLPTPETKRWBFPALGOEUCZG
HTAGYVMETFGWODWGBUIBXITNIIGNMFWGSSVLZLUOLWLTPTLUHWAUFXTCRIAJTJHBKUS
VTNIFKDHAGUQRGAMEYHCDWBCNREQKRVTJKHVSKCCMMEB
```