brief explaination of quiz4 109550027紀竺均

1.Using the number of vowels to detect ciphertext rectangles

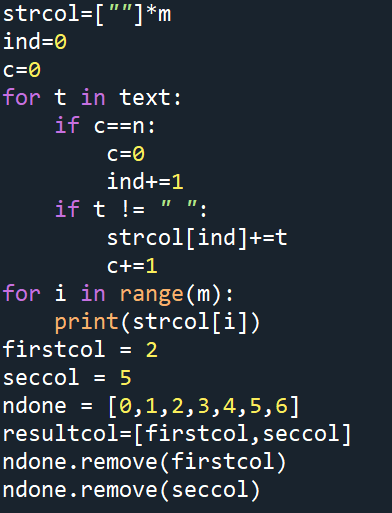


I use the counting function to determine the matrix’s rows and cols. (Same as quiz 2)

As a result, this is a 11\*7 matrix.

2. Using plaintext bigrams and trigrams to calculate conditional probabilities for Markov decision processing (MDP).

I use the markov function to count the probabilities of 2 characters and 3 characters, then, I save them in dictionary d2 and d3.



In this section, I slice the ciphertext into strings of columns. The result is:

‘EOEYEGTRNPS’

‘ECEHHETYHSN’

‘GNDDDDETOCR’

‘AERAEMHTECS’

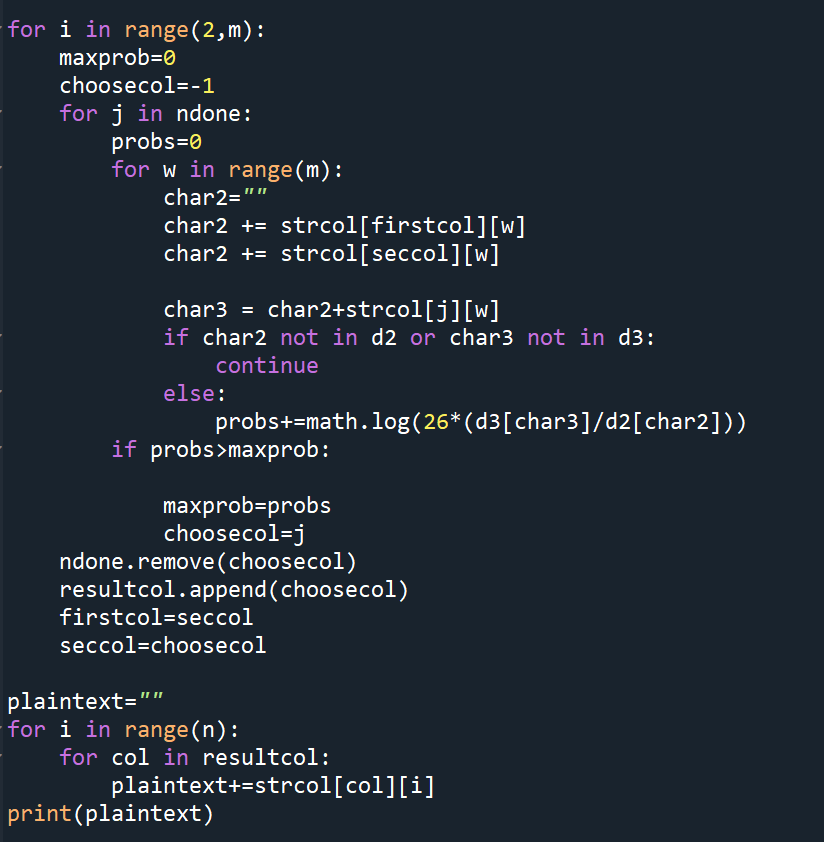
‘EUSIARWKDRI’

‘RNYARANUEYI’

‘NTTCEIETUS’

Followed the hint, the first column should be ‘GNDDDDETOCR’ and the second column should be ‘RNYARANUEYI’

3. Using MDP to recover columnar transposition ciphers



Every time I want to decide the next column, I run through the undone columns and count the total conditional probabilities of the column.

probs += math.log(26\*(d3[char3]/d2[char2]))

Find the most appropriate column with the highest probability, remove it from the undone columns and redo this to find the next column.

Luckily, I find out the origin plaintext: GREECEANNOUNCEDYESTERDAYITHADREACHEDAGREEMENTWITHTURKEYTOENDTHECYPRUSCRISISNS