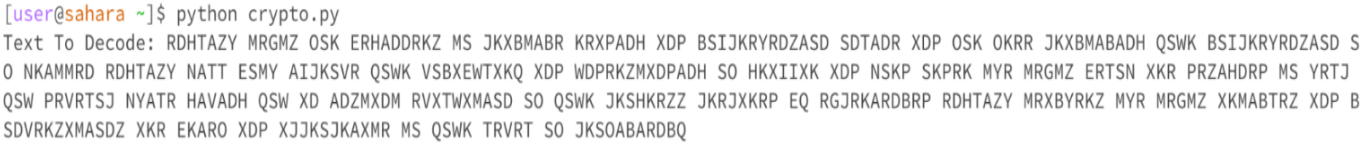
Kathleen Anabelle Cahya
Mentor: Alex Ziyu Jiang
Statistics DRP writeup
06/10/2021

Application of Markov Chains Monte Carlo to Cryptography

Throughout this quarter, I learnt a lot about the Markov Chains Monte Carlo method and how this method plays a role in the study of cryptography. At first, the Markov Chains Monte Carlo method is pretty hard to understand. However, Alex, my mentor, helped me a lot in understanding this concept by assigning me some readings every week. These readings allowed me to understand the concept better. However, there are times where I do not know what the reading is about, and this is where I ask my questions to Alex. Every week Alex and I had a meeting together through zoom to discuss about the reading and to catch up with the materials. In this meeting, Alex will usually explain the concepts that I have not yet understand.

To start off, we learnt about the theory of the Markov Chains Monte Carlo (MCMC) method. I learnt that the MCMC method is basically a method used for sampling from a probability distribution. This method draws samples in which the next sample is dependent on the existing sample. To understand this method better, we also looked at some examples of its applications to different problems in our daily lives, such as how this method relates to music.

After we are familiar with this concept and the theory, we move on to the coding part of the project. In this project, I used the Ed workspace in order to code in real time using python. Basically, in this problem, we were given a gibberish text that we need to decode or decrypt. This gibberish text actually has a hidden message behind it, and this message can be important to different stakeholders. For example, it can be used as a secret communication between military commanders to ensure a successful operation. Here is the text I decided to decrypt:

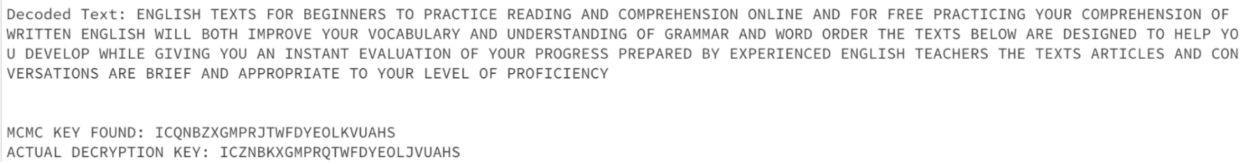


```
[user@sahara ~]$ python crypto.py
Text To Decode: RDHTAZY MRGMZ OSK ERHADDRKZ MS JKXBMABR KRXPADH XDP BSIJKRYRDZASD SDTADR XDP OSK OKRR JKXBMABADH QSWK BSIJKRYRDZASD S
O NKAMMRD RDHTAZY NATT ESMY AIJKSVR QSWK VSBXEWTXKQ XDP WDPRKZMXDPADH SO HKXIIXK XDP NSKP SKPRK MYR MRGMZ ERTSN XKR PRZAHDRP MS YRTJ
QSW PRVRTSJ NYATR HAVADH QSW XD ADZMXDM RVXTWXMASD SO QSWK JKSHKRZZ JKRJXKRP EQ RGJRKARDBRP RDHTAZY MRXBYRKZ MYR MRGMZ XKMABTRZ XDP B
SDVRKZXMASDZ XKR EKARO XDP XJJKSJKAXMR MS QSWK TRVRT SO JKSOABARDBQ
```

To solve this problem, we will be using a scoring function, and this scoring function helps to determine whether we will be staying in the current state or moving to the proposed state. Here is the formula for the scoring function:

$$Score(x) = \prod R(\beta_1, \beta_2)^{F_x(\beta_1, \beta_2)}$$

Beta1 and Beta2 are basically a pair of letter, and the R function records the number of times that specific pair of letter (e.g. “TH”) appears consecutively in the reference text. Meanwhile, the Fx function record the number of times that pair appears when the ciphertext is decrypted using the decryption key x. To solve this problem, we first need to choose a random current state, which is a pair of letter Beta1 and Beta2. Then, we will propose a new state in which we swap the order of Beta1 and Beta2. After that, we will calculate both the score of the current state and proposed state using the scoring function. If the score of the proposed state is bigger than the score of the current state, then we move to the current state. Else, we will flip a coin that has a probability of the Score_P/Score_C for the Heads. We will repeat all this process again until we have reached the end of the text. The process that I have explained here is based on the MCMC method. After running the program, we finally reach our main goal. The test that was once gibberish turned into something that is readable and meaningful. Here is the result:



```
Decoded Text: ENGLISH TEXTS FOR BEGINNERS TO PRACTICE READING AND COMPREHENSION ONLINE AND FOR FREE PRACTICING YOUR COMPREHENSION OF
WRITTEN ENGLISH WILL BOTH IMPROVE YOUR VOCABULARY AND UNDERSTANDING OF GRAMMAR AND WORD ORDER THE TEXTS BELOW ARE DESIGNED TO HELP YO
U DEVELOP WHILE GIVING YOU AN INSTANT EVALUATION OF YOUR PROGRESS PREPARED BY EXPERIENCED ENGLISH TEACHERS THE TEXTS ARTICLES AND CON
VERSATIONS ARE BRIEF AND APPROPRIATE TO YOUR LEVEL OF PROFICIENCY


MCMC KEY FOUND: ICQNBZXGMPRJTWFDYEOLKVUAHS
ACTUAL DECRYPTION KEY: ICZNBKXGMPRQTWFDYEOLJVUAHS
```

In conclusion, the MCMC method does play a role in the study of cryptography, solving and writing codes. Through this project, I have successfully gained in depth knowledge regarding the MCMC method and its application. I would like to thank my mentor, Alex, for guiding me in finishing this project successfully.