# Application of MCMC in Cryptography

By: Kathleen
Mentor: Alex

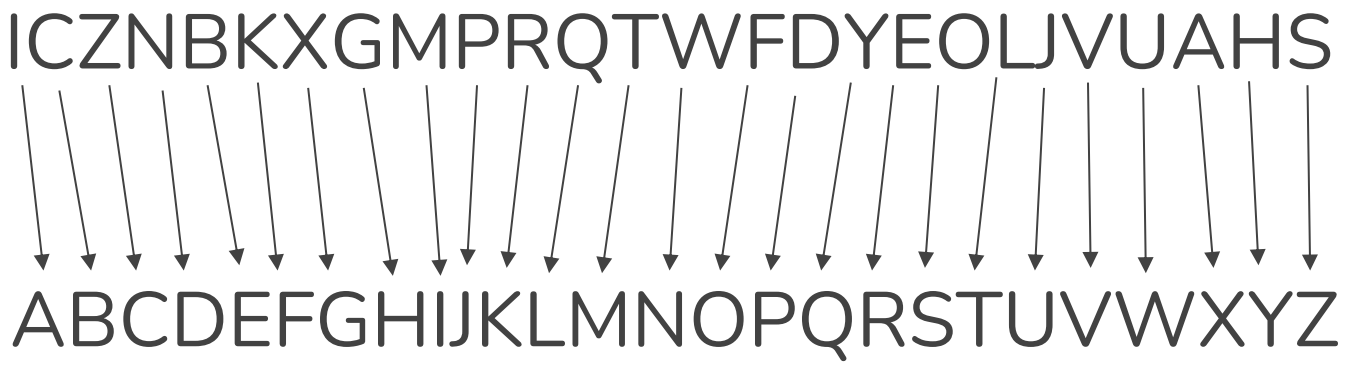
# Problem Description

- We have a encrypted text that looks like a gibberish, but it can actually mean something
- The text that has been decrypted  might be really important to different stakeholders
- The encrypted text looks something like this:

```
[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
```

# Methods

**Decryption key:**




**Text to decode:**
RDHTAZY MRGMZ OSK ERHADDRKZ MS JKXBMABR KRXPADH XDP

**Turns in to:**
KPYMXCQ IKHIC SZF RKYXPPKC IZ UF UFGEIXEK FKGJXPY GPJ

- We will create a decryption key, which is a 26 letter string with all alphabets that appear exactly once, then we will map the decryption key into a string of 26 letters in alphabetical order
  - Decryption key: “ICZNBKXGMPRQTWFDYEOLJVUAHS”
  - For example, “I” maps to “A”, “C” maps to “B”, “Z” maps to “C”, and so on
- To solve this problem, we will be using the monte carlo markov chain
- We will be using the scoring function:

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

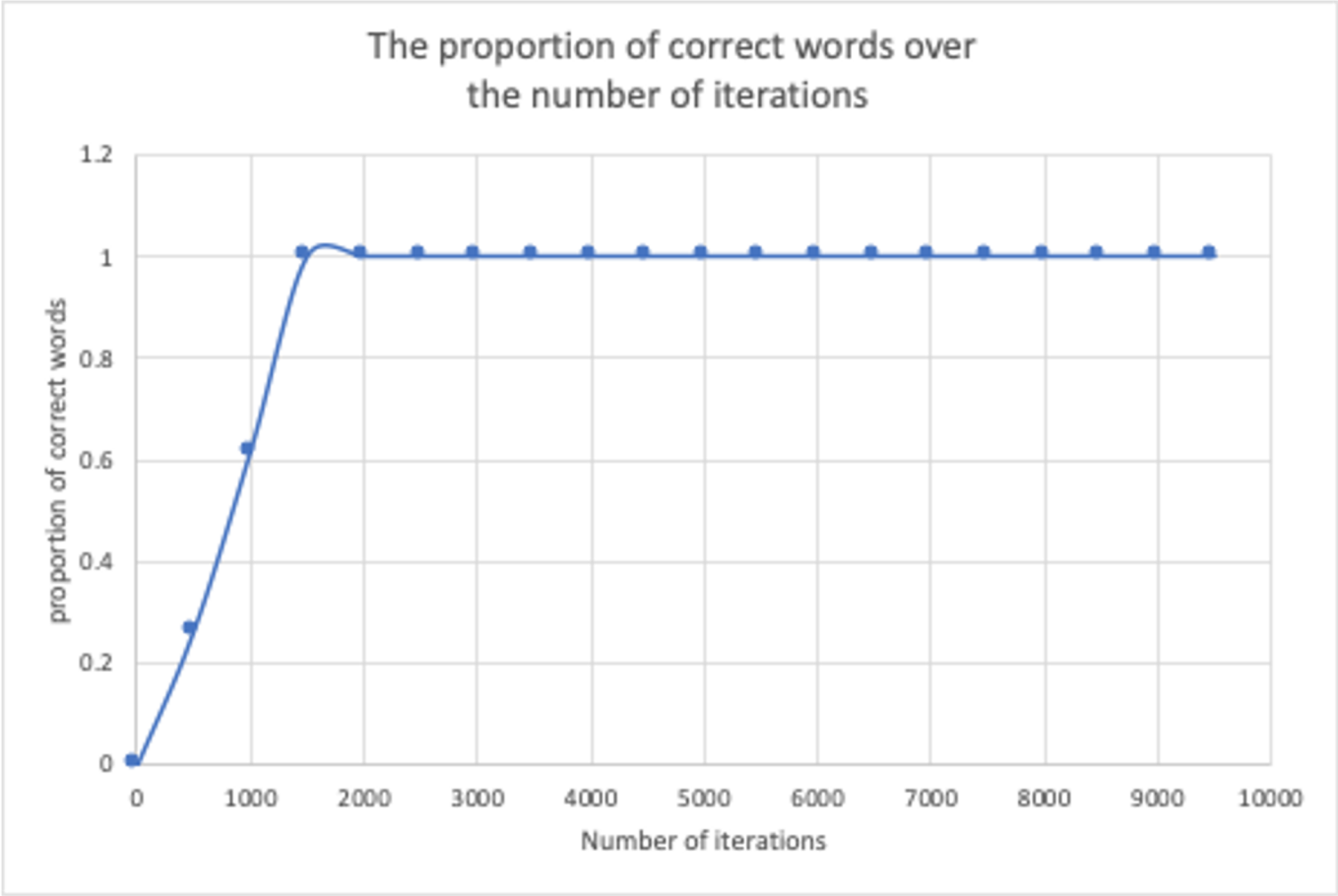
- **R function:** record the number of times that specific pair of letter (e.g. “TH”) appears consecutively in the reference text
- **Fx function:** record the number of times that pair appears when the ciphertext is decrypted using the decryption key x

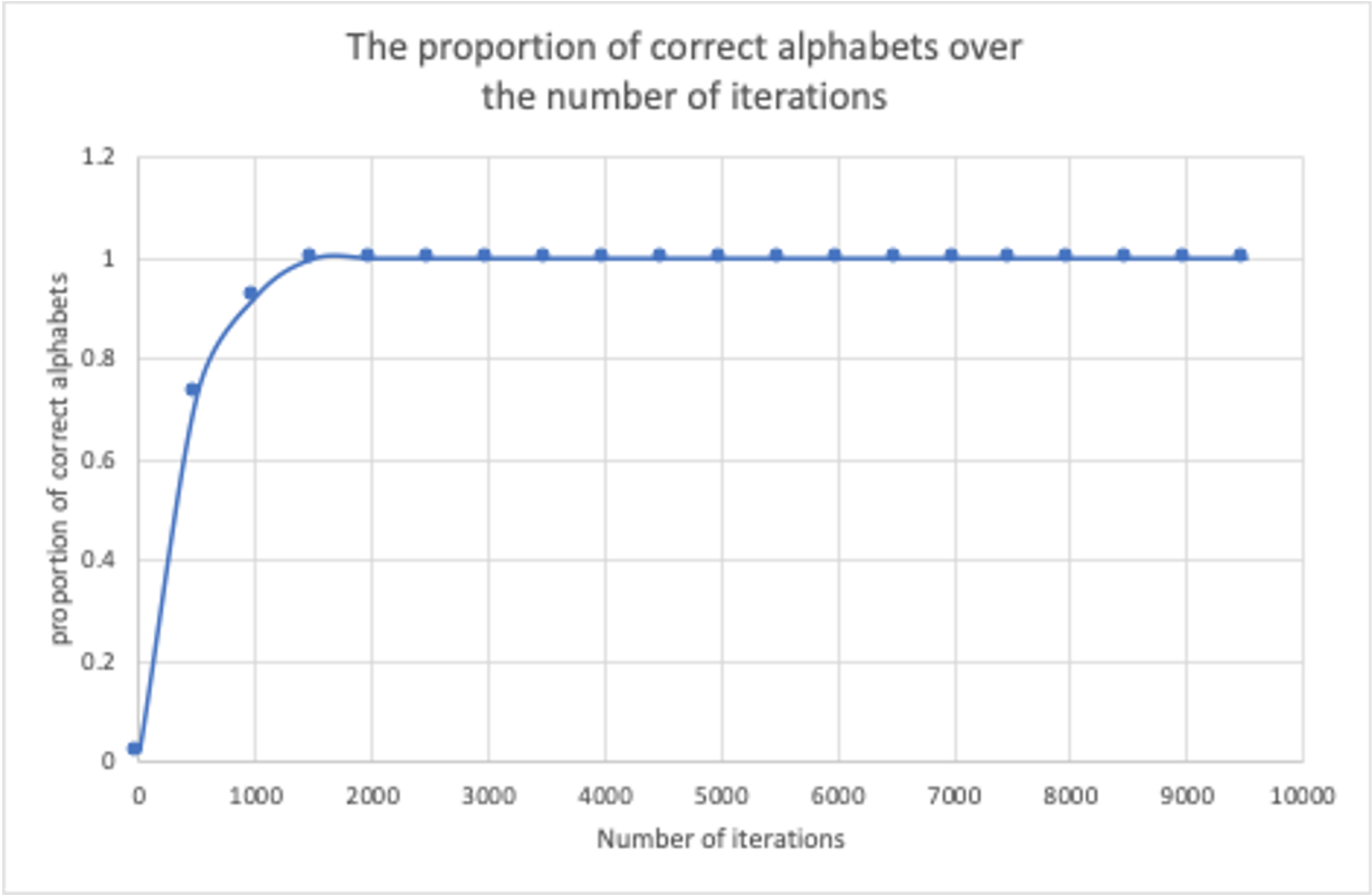
1. chooses a random current state (a pair of random letter)
2. Propose a new state by swapping the two random alphabets in the current state
3. Use the scoring function to determine whether we should stay in the current state or move to the proposed state
    - If score of proposed state > score of current state, we move to the proposed state.
    - Else, we will flip a coin that has a probability of the Score_P/Score_C for the Heads
        - If the probability is > 1, we accept the case, which means that we move to the proposed state
        - Score_P = score of proposed state
        - Score_C = score of current state
4. Then we will repeat this process all over again starting from step 2

# Results

```
[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

iter 0 : RDHTAZY MRGMZ OSK ERHADDRKZ MS JKXBMABR KRXPADH XDP BSIJKRYRDZASD SDTADR XDP OSK OKRR JKXBMABADH QS
iter 500 : ONSTUFR LOPLF YEI KOSUNNOIF LE HIACLUCO IOADUNS AND CEGHIORONFUEN ENTUNO AND YEI YIOO HIACLUCUNS ME
iter 1000 : ENTSIFK LEWLF MOR BETINNERF LO HRACLICE READINT AND COGHREKENFION ONSINE AND MOR MREE HRACLICINT YO
iter 1500 : ENGSILY TEPTL FOR BEGINNERL TO HRACTICE READING AND COKHREYENLION ONSINE AND FOR FREE HRACTICING MO
iter 2000 : ENGLISH TEYTS FOR BEGINNERS TO WRACTICE READING AND COKWREHENSION ONLINE AND FOR FREE WRACTICING MO
iter 2500 : ENGLISH TEYTS WOR BEGINNERS TO FRACTICE READING AND COPFREHENSION ONLINE AND WOR WREE FRACTICING MO
iter 3000 : ENGLISH TEFTS WOR BEGINNERS TO PRACTICE READING AND COMPREHENSION ONLINE AND WOR WREE PRACTICING YO
iter 3500 : ENGLISH TEXTS WOR BEGINNERS TO PRACTICE READING AND COMPREHENSION ONLINE AND WOR WREE PRACTICING YO
iter 4000 : ENGLISH TEXTS FOR BEGINNERS TO PRACTICE READING AND COMPREHENSION ONLINE AND FOR FREE PRACTICING YO
iter 4500 : ENGLISH TEXTS FOR BEGINNERS TO PRACTICE READING AND COMPREHENSION ONLINE AND FOR FREE PRACTICING YO
iter 5000 : ENGLISH TEXTS FOR BEGINNERS TO PRACTICE READING AND COMPREHENSION ONLINE AND FOR FREE PRACTICING YO
iter 5500 : ENGLISH TEXTS FOR BEGINNERS TO PRACTICE READING AND COMPREHENSION ONLINE AND FOR FREE PRACTICING YO
iter 6000 : ENGLISH TEXTS FOR BEGINNERS TO PRACTICE READING AND COMPREHENSION ONLINE AND FOR FREE PRACTICING YO
iter 6500 : ENGLISH TEXTS FOR BEGINNERS TO PRACTICE READING AND COMPREHENSION ONLINE AND FOR FREE PRACTICING YO
iter 7000 : ENGLISH TEXTS FOR BEGINNERS TO PRACTICE READING AND COMPREHENSION ONLINE AND FOR FREE PRACTICING YO
iter 7500 : ENGLISH TEXTS FOR BEGINNERS TO PRACTICE READING AND COMPREHENSION ONLINE AND FOR FREE PRACTICING YO
iter 8000 : ENGLISH TEXTS FOR BEGINNERS TO PRACTICE READING AND COMPREHENSION ONLINE AND FOR FREE PRACTICING YO
iter 8500 : ENGLISH TEXTS FOR BEGINNERS TO PRACTICE READING AND COMPREHENSION ONLINE AND FOR FREE PRACTICING YO
iter 9000 : ENGLISH TEXTS FOR BEGINNERS TO PRACTICE READING AND COMPREHENSION ONLINE AND FOR FREE PRACTICING YO
iter 9500 : ENGLISH TEXTS FOR BEGINNERS TO PRACTICE READING AND COMPREHENSION ONLINE AND FOR FREE PRACTICING YO
```


The proportion of correct words over the number of iterations
proportion of correct words
1.2
1
0.8
0.6
0.4
0.2
0
0
1000
2000
3000
4000
5000
6000
7000
8000
9000
10000
Number of iterations


The proportion of correct alphabets over the number of iterations
proportion of correct alphabets
1.2
1
0.8
0.6
0.4
0.2
0
0
1000
2000
3000
4000
5000
6000
7000
8000
9000
10000
Number of iterations

```
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
```

- turns it into something that is readable and meaningful

# Discussions

- This cryptography technique is very important especially for securing information so that no one will be able to access and process the information
- Nowadays cryptography is everywhere, for example, we use it to securely send passwords for online purchases.
- At first, it was pretty hard for me to understand the concept of cryptography and how MCMC plays a role in it

# References


- Agarwal, Rahul. “Applications of MCMC for Cryptography and Optimization.” *Medium*, Towards Data Science, 25 Dec. 2019, towardsdatascience.com/applications-of-mcmc-for-cryptography-and-optimization-1f99222b7132.
- Rizzo, Maria L. *Statistical Computing with R*. CRC Press LLC, 2019.

# THANK YOU!