MCMC for Cryptography

Steps for MCMC

1. Start by picking up a random current state.
2. Create a proposal for a new state by swapping two random letters in the current state.
3. Use a Scoring Function which calculates the score of the current state $Score\_C$ and the proposed State $Score\_P$.
4. If the score of the proposed state is more than the current state, Move to Proposed State.
5. Else flip a coin which has a probability of Heads $Score\_P/Score\_C$. If it comes heads move to the proposed State.
6. Repeat from 2nd.

Scoring Function

- English has a particular structure to it. We assume that the number of times a certain pair of alphabets occur together may follow some particular pattern. Thus “TH” is more probable of occurring then “ZF”.
- $R(\beta_1, \beta_2)$ record the number of times that specific pair(e.g. “TH”) appears consecutively in the reference text.
- $F_{\mathrm{x}}(\beta_1, \beta_2)$ record the number of times that pair appears when the ciphertext is decrypted using the decryption key x.
- Score Function for Decryption key x

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

Tasks

- You will need to implement a python program that reads the ciphertext from a file named “ciphertext.txt” and save the plaintext into a file named “plaintext.txt”
- A template will be given and you can follow the template or design your own MCMC
  - For more detail, please reference the given template
  - Reference text is war_and_peace.txt

Submission

- Please zip the directory and upload the .zip file to E3.
- Filename format: “YOUR_STUDENT_ID.zip"

- Example:
- 309000000.zip
  |- 309000000.py

- Note: Don’t include the reference text and ciphertext