Project Report - CS691

The project is the development of parallel version of Hill Cipher decryption. In this project, we use MPI for distributing the work load among different processes and find if the plain text is retrieved from the cipher text alone.

Hill cipher is a substitution cipher where the plain text is stored in a matrix format and multiplied with the key to generate the cipher text. The cipher text is then performed with modulo 26 operation to encode. The resultant cipher text is a complex substitution cipher with the complexity of 26^{d^2} where d is the number of diagonal elements.

In our case the diagonal elements are 2 for the base case therefore resulting in the complexity of 26^4.

The average time for each process to complete decryption is 0.0144 seconds on an average when the number of tasks specified are 10.

For the specific experiment the we assumed plain text and cipher text to be a 2x2 matrix. The workflow of the project is given below

Each process calculates its own key based on it's offset value. It then calculates the inverse of the key and multiply with the cipher text to generate probable plain text.

The plain text is then compared with the floating value and printed if the value matches with the plain text

Size	CPU	MPI
2x2	34 seconds	0.014seconds