FINAL PROJECT REPORT

PARALLEL CRYPTOGRAPHY

[A Program for Parallel Encryption and Decryption]

Group Members:

Muhammad Owais Mushtaq (18K-1177)

Faiq Nadeem (18K-1194)

Syed Haris Ahmed (18K-1162)

Introduction:

The purpose of the project entitled “**Parallel Cryptography**” is to encrypt simple text, to avoid security issues and to be able to communicate in terms of emergency without letting undesirable individuals know the contents of the original message. The process of text encryption has been around from the Ancient Greek period. And military officials use encryption to communicate with each other in war or in a state of emergency. Historically, encryption methods like Morse code and Caesar Cipher were used. But nowadays, due to advanced computers, traditional encryption methods such as Morse code have become weak, so the need for new encryption methods is felt.

Objective:

The objective of our project, **Parallel Cryptography,** is to develop an advanced computer program capable of encrypting any given text such that it cannot be decrypted or deciphered without the use of this software. This program seeks to maximize efficiency by dividing the input text into four components and encrypt each of them using a different key while utilizing parallel programming paradigms.

Scope of the Project:

This software can be used for military purposes, for online data security and to ensure the safe transfer of confidential data over any distributed network.

MODULES:

Main methodology/techniques for both Encryption and Decryption:

- Caesar Cypher
- Keyword Cypher
- Columnar Transposition Cypher
- Affine Cypher

WORKING OF SOFTWARE:

- The Software first asks the user to choose between encryption and decryption from our main menu which also shows one option for an 'about' page, which gives information about program methodology.
- After choosing from encryption or decryption the user will see the choice in input methods like Input through file or Input through type.
- After giving the input to program, The user will see the output in a next few milliseconds
- In these few milliseconds, what our software does:
    - If the users have chosen encryption, our program will break the input text into four parts and with the help of Open MP it will send all of them in parallel to our four different encryption methods randomly. Where each character of sub part of text will be encrypt in parallel again through Open MP. After the encryption of all four methods the subtext will be merged and the information about their encryption technique will be store at start and then the final output will shared with user.
    - Or if the user have chosen decryption, our program first read the starting four characters of input to insure which part of text will be sent to which method of decryption. And then through Open MP first it will send the subparts of text to relevant decryption method in parallel. Where all characters will also decrypt in parallel through Open MP. After the competition of decryption from all the four methods, program will merge the text and shows to user.
- After the output comes on the screen, our program will ask our user, if they want to save the output in a file? If the user says yes then it will save the output in a file whose details were also given by user.
- Our program also handled all possible exception like wrong input of filename while giving input because on output it doesn't matters if the user puts the file name that is not available then our program will make the file on user given file name.

CONCLUSION:

The software achieves parallelism through Open MP while encrypting or decrypting the user's given text. Plus the four different methods of cryptography, makes our output more secure. And the combination of both makes our software program more efficient in terms of speed and security.