

**(**KARACHI CAMPUS)

Department of Computer Science

Fall 2020

[Project Proposal for PDC]

Project Title:

Parallel Cryptography

**(Project on Fast and Secure Encryption and Decryption of Messages)**

By:

Muhammad Owais Mushtaq (18K-1177)

Faiq Nadeem (18k-1194)

Syed Haris Ahmed (18k-1062)

Objective:

The purpose of this project is to understand, research and develop a computer program capable of taking a certain amount of text as input, break it down or **divide** it into a of smaller texts and encrypt each of them in **parallel** and finally make that massage available for transmission and also capable of doing decryption in same way.

Methodology:

The program breaks down the given text into smaller parts in specific range, and then it precedes to encryption each part in **parallel** using different keys. It may then rearrange individual blocks of text with the reference of its key (which will also hidden in decrypted text). In order to decrypt the text, the program will firstly find all the unique keys with their range and finally it will decrypt all sub text and again join them in order to understand easily.

**Example of Encryption:**

**Input:**

Muhammad Owais Mushtaq is coming to Karachi on Saturday

Note: For understanding purpose we are assuming sequential key (like 1,2,3..) and same range of 11 for division of text But in actual Program both will assign randomly.

Step of Procedure:

* Input will firstly breakdown into sub parts with the range of 11 as:

Substr1: “Muhammad Ow”

Substr2: “ais Mushxtaq”

Substr3: “ is coming ”

Substr4: “to Karachi ”

Substr5: “on Monday”

* We will now increment the ASC II of Substr1 by 2 and Substr2 by 3 … Substr5 by 6 in parallel as:
* Substr1: “Owjcoocf”Qy” , k=2
* Substr2: “dlv#xvkwdt” ,k=3
* Substr3: “ mw$gsqmrk$ ” , k=4
* Substr4: “yt%Pfwfhmn%” ,k=5
* Substr5: “ut&sutjq\*” ,k=6

Now we will merge these decrypted texts into one starting with their key and then range and then text.

**Output:**

211Owjcoocf”Qy311dlv#xvkwdt411mw$gsqmrk$511yt%Pfwfhmn%611ut&sutjq\*

Platform:

We are thinking to work on C++ using Open MP. And the tool (IDE) which we will use for our project will be DevC++.