**National University of Computer & Emerging Sciences**

**Karachi Campus**



**Project Proposal**

**EE229 Computer Organization and Assembly Language**

**Section: G**

*RSA Algorithm Based Encryption & Decryption*

**Group Members:**

19k-1475: Syed Ahsan Akhtar Naqvi

19k-1273: Mustafa Bawany

19k-1440: Ajar Sarmad

# **SECURE ENCRYPTION OF DATA IN ASSEMBLY USING THE RSA ALGORITHM**

## **INTRODUCTION:**

* An advanced encryption system that incorporates a variety of encryption methods for increased security. It will use multiple variables in one given method for increased scrambling and also pseudo random factors to minimize unauthorized cracking.

## **PROJECT DESCRIPTION:**

* RSA is an asymmetric system, which means that a key pair will be a public key and a private key, you keep your private key secure and pass around the public one.
* RSA is rather slow so it’s hardly used to encrypt data, more frequently it is used to encrypt and pass around symmetric keys which can actually deal with encryption at a faster speed.

## **TOOLS & TECHNOLOGIES:**

Programming language: Assembly x86

Operating System: Windows