**ESE-3014 Lab 5 - Try to crack Asymmetric cryp-tography**

**Review our slide about the process of asymmetric cryptography (like RSA which have public key and private key), try to find an idea to crack it and get text message between A and B.**

**FRANCIS VIJITH - C0742980**

**VIJAYAPRAKASH - C0744450**

The most popular and common way of cracking an asymmetric cryptographic message is by Brutal force attack. It is defined as trying out several combination of the password so as to guess the combination of the key to decrypt the sent or received message. This method can also be termed as the password -guessing method. The performance of this method depends on the length of the password of the key. Several software tools such as [Aircrack-ng](https://en.wikipedia.org/wiki/Aircrack-ng), [Cain and Abel](https://en.wikipedia.org/wiki/Cain_and_Abel_(software)), [Crack](https://en.wikipedia.org/wiki/Crack_(password_software)) and [DaveGrohl](https://en.wikipedia.org/wiki/DaveGrohl).

This method works by guessing 2^N combination of passwords, where N is the length of the password. When a message is transferred from A to B, with a key K1, the length of the key K1 is known as N and the password is guessed using supercomputers, which may take even days to crack the code. In the future, with the advent of quantum computers, it is assumed to crack the code with a matter of seconds.