592 Course **Spring-2020**
Project #1 **Due: **.**.****

Name: Dursun Oylum Seriner
Student ID: 2022697

RSA Algorithm

Generate the keys-code1
Step 1: Generate the RSA modulus (N)
We need to two generate numbers, then we need to create the prime numbers for this process. They are method of creating prime numbers:

- Miller-Rabin code (Library)
- Fermat code (Library)

The initial procedure begins with selection of two prime numbers namely p and q, and then calculating their product N:

$$N = p * q$$

Step 2: Derived Number (e)
Consider number e as a derived number which should be greater than 1 and less than multiplication of (p-1) and (q-1).

$$1 < e < (p-1) * (q-1)$$

Step 3: Public Key (e)
Choose "e" and e must be prime. We can try to use prime numbers test again.
Step 4: Private Key (d)
Private Key d is calculated from the numbers p, q and e. The mathematical relationship between the numbers is as follows:

$$d * e = 1 mod(n)$$

- Extended Euclidean Algorithm (Library)

Encryption-code2
We need to plaint text and we create the new plain text by using ASCII.

- ASCII code (Library)

Every letter in original text converted by using ASCII and we define the "P". By the way, P means that plain text and C means that cipher text.

$$C = P^e mod((p-1) * (q-1))$$

Decryption-code3
Considering receiver C has the private key d, the result modulus will be calculated as:

$$P = C^d mod((p-1)*(q-1))$$

Basic RSA attacks-code4 and code 5

- If chooses the small "e"

  $$P < N^{1/e}$$

  We can just take the e-th root and reach the plain text.

- If secret massages send to many receivers by using same e and different d. These encrypted by Chinese Remainder Thm.(Library)