Assignment6

Pablic Key cryltogralhy

we will ase RSA for this assignment.

How RSA works: example

we have vector which comlutes q and s Prime

$a : qs$

Totient of a $\varphi(a) = (q-1)(s-1)$

$e = 65537$

$d = e^{-1} \bmod \varphi(a) \longrightarrow de = \bmod \varphi(a)$

So the encryption of some measeage n

$E(m) = m^{e} \bmod n$

$D(E(m)) = (E(m))^{d} \bmod n$

My task:

① generate keys (Pablic, Private)

② encrylt files

③ decrylt files

* In this assignment we are going to read integers with

large sizes. In order to do this, we will need to include and use libraries. The library that we are going to use is GMP.