Feride ÇOLAK 385951

Rabia YILMAZ 385914

**RSA Algoritması**

* 1024 bitlik iki asal sayı seçildi.
* Bit sayı düştükçe şifrelenecek metnin karakter sayısı da düştüğü için büyük bir değer seçildi.
* r değeri random değer atıyor.
* n değeri p\*q’dur
* phi değeri T(n) olarak bildiğimiz (p-1)\*(q-1) değeridir.
* d değeri e’nin phi’ye göre modudur.
* e değeri phi ile aralarında asal bir sayıdır.
* Proje çalıştırıldığında p, q, phi, e, n ve d değerleri gösterilir.
* Projede console ekranında bir girdi beklenir.
* alınan mesaj teststring değerine atılır.
* Şifrele fonksiyonuna teststring değeri gönderilir.
* şifrele fonksiyonunda teststring adındaki string tipinde bir veridir.
* Ekrana şifrelenecek metin gösterilir.
* Bu metin bytesToString fonksiyonundan byte’a yani ASCII değerine dönüştürülür.
* Kript fonksiyonu byte çevrilen stringi alır ve bu dizinin elemanlarının her birinin e üssü alınır.
* bu değerde n ye göre mod alınır. böylelikle rsa gerçekleşmiş olur.
* Dekript metoduna da bu şifrelenmiş dizi gönderilir.
* Her değer için d üssü alınır. Daha sonra mod n alınır.
* Geriye dönen değer şifrelenmesini istediğimiz mesajın harflerinin ascii değerleridir.
* Ascii değerlerde Stringe çevrilir. Ekrana basılır.

