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.

```
run:
Rsa{p=114426475303399084397487382814541982983101848924200496814826659031313820799206059837925369005627318878129741178516538474960628758188061
q=146267629492016611838016663472081627737463572017267261126351325291938732053374856262788155238225330132839205002892532703924744266625851377311
N=167368892937549663989362803740781715610943002263369325593407833367724494115858746914185700471936026909182448347256942127655802934745077798
phi=167368892937549663989362803740781715610943002263369325593407833367724494115858746914185700471936026909182448347256942127655802934745077795
e=108872385657381487194915139493471017268942245904717151775613087416007135232347006439940542400592731599593923490403737776930661593068240500
d=124733096605664167028751403504589993572384843363842204510737062790323960647926808999206733567616823231938341053679440366868955802969976552
bitlength=1024,
r=java.util.Random@74a14482}
Şifrelenecek metni giriniz:
merhaba
Şifrelenecek string: merhaba
Stringin byte degeri: 109101114104979897
Şifrelenmiş byte: 11913110104611078341161084937-437934-101-10-13-1422785171016-59-56-421194137-483-111-75-712465-683182-16-120485994-31-9278-
Deşifrelenecek byte: 109101114104979897
Deşifrelenmiş string: merhaba
BUILD SUCCESSFUL (total time: 16 seconds)
```