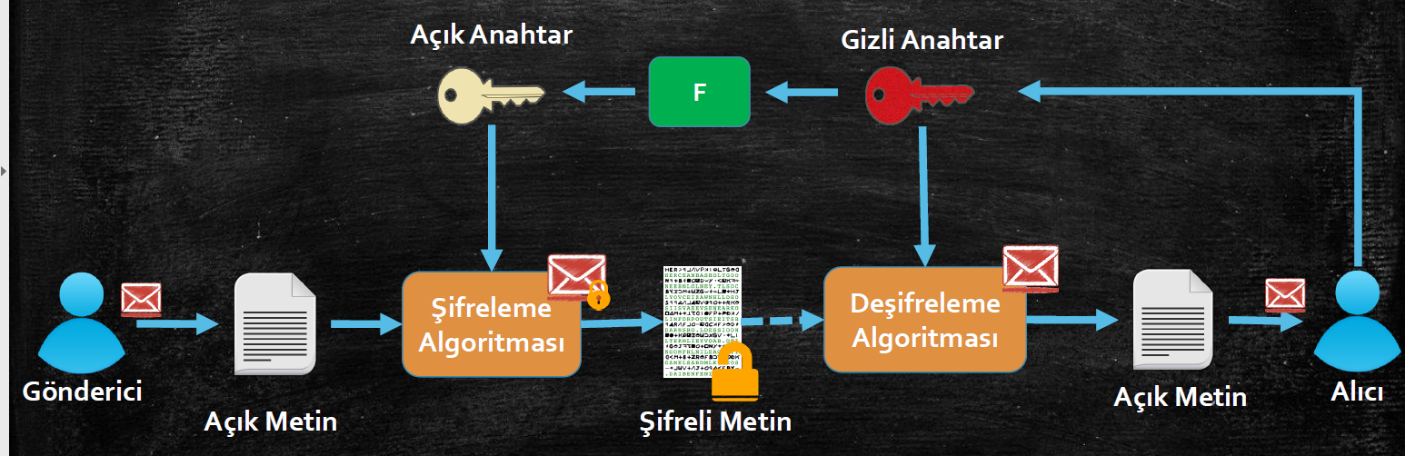
**AMAÇ :** Bu uygulamanın amacı kişiye asimetrik şifreleme algoritmalarının çalışma yapısını göstermektir.

**ÖNBİLGİ :**

Açıklama eklenecek.



RSA özel anahtar yapısı :

A.1.2 RSA private key syntax

An RSA private key should be represented with the ASN.1 type

RSAPrivateKey:

RSAPrivateKey ::= SEQUENCE {

version Version,

modulus INTEGER, -- n

publicExponent INTEGER, -- e

privateExponent INTEGER, -- d

prime1 INTEGER, -- p

prime2 INTEGER, -- q

exponent1 INTEGER, -- d mod (p-1)

exponent2 INTEGER, -- d mod (q-1)

coefficient INTEGER, -- (inverse of q) mod p

otherPrimeInfos OtherPrimeInfos OPTIONAL

}

**UYGULAMA :**

1. **Uygulama öncesi yapılacaklar :**

* sudo apt-get install openssl komutuyla şifreleme uygulamasını kurun.

1. **Uygulamanın Yapılışı:**
2. **openssl genrsa -out private\_key.pem 1024** komutunu kullanarak 1024 uzunluğunda özel anahtar oluşturun.
3. **cat private\_key.pem** komutuyla anahtarın içeriğini gözatın ve 1024 değerini değiştirerek yeni anahtarlar oluşturup farklarını gözlemleyin. Anahtar boyutunun en az kaç olacağını bulun?
4. **openssl rsa -in private\_key.pem -out public\_key.pem -outform PEM -pubout** komutunu kullanarak oluşturuduğunuz özel anahtardan açık anahtar oluşturun.
5. **cat public\_key.pem** komutuyla açık anaktarın içeriğini gözatın.
6. **openssl rsautl -encrypt -inkey public\_key.pem -pubin -in metin.txt -out sifreliMetin.dat** komutunu kullanarak açık anahtarla metin.txt dosyasını şifreleyin.
7. **openssl rsautl -decrypt -inkey private\_key.pem -in sifreliMetin.dat -out metin3.txt** komutunu kullanarak şifreli metni deşifre edin.
8. **openssl genrsa 32 -out private\_key.pem** ile gizli anahtar oluşturun.
9. **openssl rsa -text < private\_key.pem** ile asimetrik şifreleme için kullanılan asal sayıları ve modulusları bulun.
10. Daha büyük anahtar uzunlukları için aynı işlemi yapın ve asal sayıları bulun. Eğer değerleri görüntüleyemiyorsanız <https://lapo.it/asn1js/> adresindeki scripti kullanabilirsiniz.
11. Openssl ans1parse < private\_key.pem komutuyla asal sayıların ve modulus değerlerinin yapısnını gözlemleyin.
12. Bozuk private key sorusu.

**ANALİZ :**

**REFERANSLAR :**