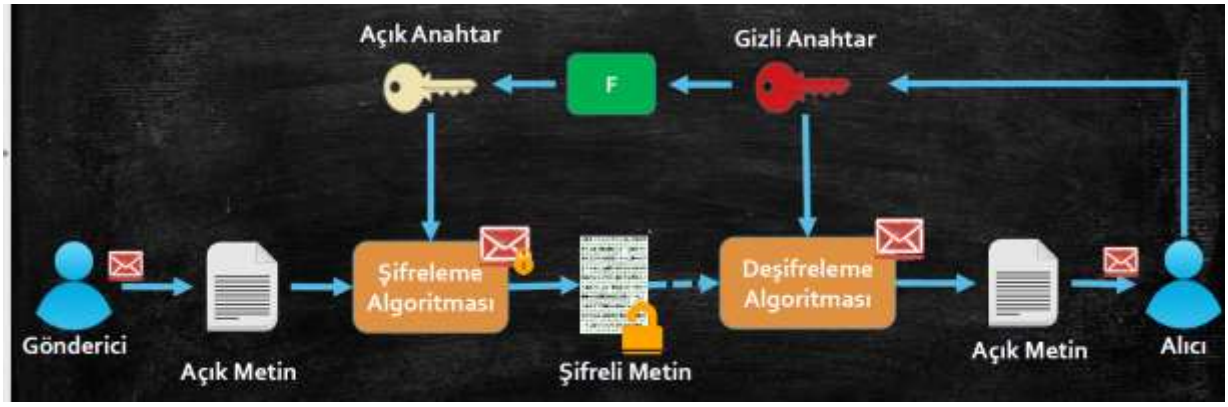
AMAÇ : Bu uygulamanın amacı kişiye asimetrik şifreleme algoritmalarının çalışma yapısını göstermektir.

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 :

A. <u>Uygulama öncesi yapılacaklar :</u>

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

B. <u>Uygulamanın Yapılışı:</u>

a. **openssl genrsa -out private_key.pem 1024** komutunu kullanarak 1024 uzunluğunda özel anahtar oluşturun.

b. **cat private_key.pem** komutuyla anahtarın içeriğini gözatın ve 1024 değerini değiştirerek yeni anahtarlar oluşturup farklarını gözlemleyin. Anahtar boyutunun en az kaç olacağını bulun?

c. **openssl rsa -in private_key.pem -out public_key.pem -outform PEM -pubout** komutunu kullanarak oluşturuduğunuz özel anahtardan açık anahtar oluşturun.

d. **cat public_key.pem** komutuyla açık anaktarın içeriğini gözatın.

e. **openssl rsautl -encrypt -inkey public_key.pem -pubin -in metin.txt -out sifreliMetin.dat** komutunu kullanarak açık anahtarla metin.txt dosyasını şifreleyin.

f. **openssl rsautl -decrypt -inkey private_key.pem -in sifreliMetin.dat -out metin3.txt** komutunu kullanarak şifreli metni deşifre edin.

g. **openssl genrsa 32 -out private_key.pem** ile gizli anahtar oluşturun.

h. **openssl rsa -text < private_key.pem** ile asimetrik şifreleme için kullanılan asal sayıları ve modulusları bulun.

i. Daha büyük anahtar uzunlukları için aynı işlemi yapın ve asal sayıları bulun. Eğer değerleri görüntüleyemiyorsanız https://lapo.it/asn1js/ adresindeki scripti kullanabilirsiniz.

j. Openssl ans1parse < private_key.pem komutuyla asal sayıların ve modulus değerlerinin yapısnını gözlemleyin.

k. Bozuk private key sorusu.

ANALİZ :

REFERANSLAR :