AMAÇ : Bu uygulamanın amacı kişiye simetrik şifreleme algoritmalarının çalışma yapısını kavratmaktır.

ÖNBİLGİ :

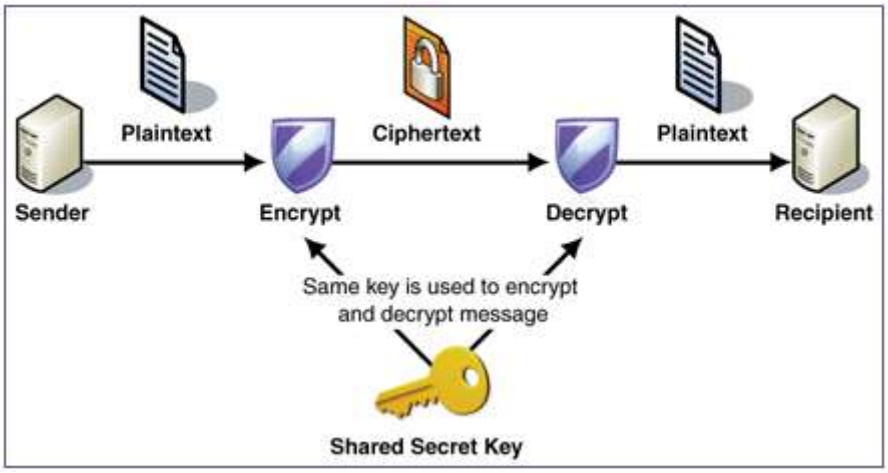
Gizli anahtar ile şifreleme ve deşifreleme yapılır. Anahtar gizliliği önemli. İşlemler tersinirdir ve aynı anahtar kullanılır. Anahtar dağıtım problemini beraberinde getiriyor; güvenli bir haberleşme kanalı veya güvenilir bir kurye yoluyla anahtar ulaşımı sağlanmalı. Anahtar gizliliğine dayandığından sıklıkla yeni anahtar üretimi gerekli. DES, 3DES, BLOWFISH, IDEA, CAST128, AES, RC5 yaygın algoritmalar.

Dönüşüm işlemi tersine çevrilebilirdir. Bu nedenle; Algoritmanın gizlenmesi gerekir. Ancak; Sadece şifreleyici ve şifre çözünün bilece bir anahtarın olması algoritma gizliliğini ortadan kaldırır.

Simetrik Şifreleme İçin iki şeye İhtiyaç vardır.

- Güçlü şifreleme algoritması
- Sadece gönderici ve alıcı tarafından bilinen gizli anahtar

Şifreleme algoritmasının bilindiğini var saydığımızda. İki tarafa arasında gizli anahtarın paylaşılması problemdir. Bu nedenle anahtar dağıtımı için güvenli bir yapı oluşturmalıyız.



UYGULAMA :

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

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

B. <u>Uygulamanın Yapılışı:</u>

a) openssl enc -aes-256-cbc -in metin.txt -out sifreliMetin.dat komutunu kullanarak metin.txt dosyasını AES şifrelem algoritması kullanarak şifreleyin.

a. -enc : Şifrele
b. -aes-256-cbc : Kullanılacak şifreleme algoritması
c. -in : Şifrelenecek dosya
d. -out : Dosyanın şifrelendikten sonraki adı.

b) **openssl enc -aes-256-cbc -d -in sifreliMetin.dat > metin2.txt** komutunu kullanarak şifreli metni deşifre edin.

   a. -d : Deşifre et

c) **diff metin.txt metin2.txt** komutlarıyla iki dosya arasında fark olup olmadığını kontrol edin.

d) 1 ve 2 numaralı işlemleri DES algoritmasını kullanarak gerçekleştirin.

e) aes-256-cbc ifadesindeki 256 ve cbc kavramlarını tartışın.

ANALİZ :

REFERANSLAR :