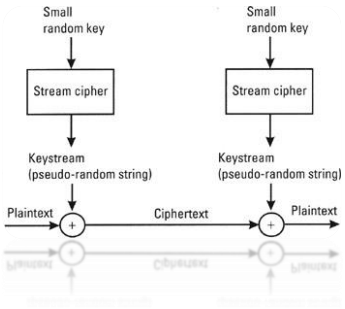
AMAÇ : Bu uygulamanın amacı kişiye simetrik kripto sistemler ve dizi tabanlı şifreleme algoritmalarının genel çalışma yapısını göstermek ve kişinin bu prensiplere dayalı şifreleme /deşifreleme uygulamaları oluşturabilmesine katkıda bulunmaktır.

ÖNBİLGİ :

Simetrik Kripto Sistemler : Simetrik kripto sistemler aynı yada benzer anahtar çiftlerini kullanarak şifreleme ve deşifreleme işlemlerini yapan kriptolama yapılardır. Simetrik kripto sistemlerde şifreleme algoritması ve deşifreleme algoritması birbirinin tersi şeklindedir. Simetrik şifreleme dizi şifreleme ve blok şifreleme algoritmalarını kullanarak yapılır.

Dizi tabanlı Şifreleme Algoritmaları: Dizi tabanlı şifreleme algoritmalarında şifrelenecek metindeki (plaintext) her bir basamak anahtar dizisindeki her bir basamağa denk gelecek şekilde şifreleme yapılır. Bu tip şifreleme işleminde algoritmanın girdisi yalnızca anahtardır. Algoritma anahtardan rastgele bir diziye çok benzeyen kayan anahtar dizisi üretir. Daha sonra kayan anahtar dizisinin elemanlarıyla düz metinin elamanları birebir şifrelenir.



UYGULAMA :

A. Uygulama öncesi yapılacaklar :

Anahtar_dizisi_üret (gizli_anahtar, kayan_anahtar_dizisi_boyu) → kayan_anahtar_dizisi

Gizli anahtar ve bu anahtar kullanılarak oluşturulacak şifreleyici kayan anahtar dizisinin boyutunu parametre olarak alan ve verilen parametrelere göre rastgele kayan dizi anahtar dizisi üreten bir fonksiyon dizayn edip, istediğiniz programlama dilinde kodlayın.

B. Uygulamanın Yapılışı:

Uygulama 1'de oluşturduğumuz şifreleme/deşifreleme algoritmasında anahtar olarak bu uygulama kapsamında oluşturduğumuz kayan anahtar dizisini kullanın. Sonuçları değerlendirin.

ANALİZ :

- Tasarladığınız kayan anahtar dizisi üretme fonksiyonunu açıklayın, diğer tasarımlara göre güçlü ve zayıf yönlerini sıralayın.
- Dizi tabanlı şifreleme algoritmasının şifreleme/deşifreleme sisteminiz üzerindeki etkisi açıklayın.
- Gizli anahtarın boyutunun tasarladığınız sistem üzerindeki etkisi gözleyin ve gözlemlerinizi sıralayın.