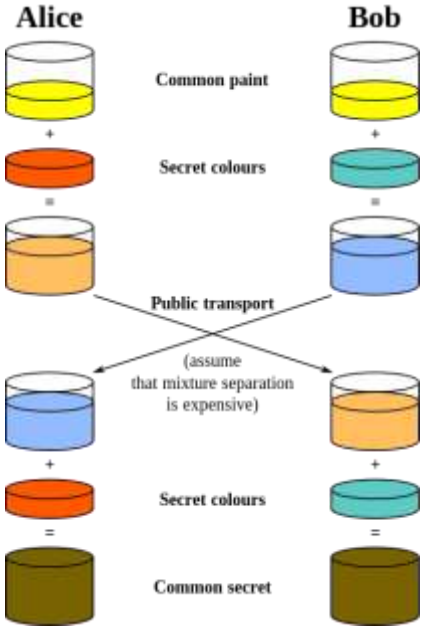
AMAÇ : Bu uygulamanın amacı kişiye açık anahtar altyapısı kullanarak anahtar değişim protokolünün genel yapısını gösterme ve kişiye basit şekilde Diffie Hellman algoritmasını kullanarak anahtar değişim yapacak bir sistem oluşturmasında katkıda bulunmaktır.

ÖNBİLGİ :

Diffie Hellman Açık Anahtar Dağıtım Şeması : İlk açık anahtar dağıtım tip PKDS idi ve Diffie & Helman tarafından yayınlandı. Bu bir açık anahtar dağıtım şemasıdır ve herhangi bir keyfi mesajı değiştirmek için kullanılamaz. Algoritmanın temeli sonlu bir alanda (Galois) ya bir asal sayının tamsayı modülü veya polinomsal alan üzerinde üstselleştirilmesine dayanır. Algoritmanın güvenliği bu alanlardaki logaritmik hesaplamanın güçlülüğüne dayanır.

Diffie Hellman Anahtar Değişim Protokolünün Çalışma Şeması:



- Güvensiz bir iletişim kanalı üzerinden anahtar değiştirmek isteyen A ve B olsun.

Bunlar;

- Büyük bir asal sayı seçerler p.
- a bir mod primitif elamanıdır.
- A'nın f gibi bir gizli sayısı vardır. (f<p)
- B'nin g gibi bir gizli sayısı vardır. (g<p)
- A açıklayacağı x'i hesaplar. X= a.power(f) mod p
- B açıklayacağı Y'yi hesaplar. Y=a.power(g) mod p
- Sonra anahtarlar aşağıdaki şekilde hesaplanır.
- Ortak gizli anahtar; K = a.power(f*g) mod p
- B'nin hesaplayabildiği K = X.power(f) mod p
- A'nın hesaplayabildiği K = Y.power(g) mod p

UYGULAMA :

A. Uygulama öncesi yapılacaklar :

Diffie & Helmann anahtar dağıtım şemasının genel çalışma şemasını incelenmesi gerekmektedir.

Cryptool (https://www.cryptool.org/en/) adresinden cryptool uygulaması indirilip kurulması gerekmektedir.

B. Uygulamanın Yapılışı:

a) Diffie_Hellman_anahtar_dağıtım_algoritması(yaklaşık_p_değeri) → Void

Diffie & hellman anahtar dağıtım şemasını kullanarak A ve B kullanıcılarının hesapladığı ve ortak olarak kullanılan anahtarları oluşturacak bir fonksiyon tasarlayıp kodlayınız?

b) Cryptool uygulamasında Diffie-Hellman Key Exchange simülasyonunu çalıştırıp sonuçları gözlemleyin.

c) Cryptool uygulamasında Diffie-Hellman Key Exchange on Network simülasyonunu çalıştırıp sonuçları gözlemleyin.

ANALİZ :

- Yaklaşık p sayısının büyüklük ve küçüklüğünü tartışınız, varsa eşik değerini belirtiniz.

- Kaç çeşit ayrık logaritma problemi vardır tartışın.