BIL452 PROJE-3 RAPORU

Programımız projede istenenleri tamamı ile yapmaktadır. Program şu şekilde çalışıyor. Çalıştırılması gereken ilk dosya gönderici olmalıdır. Gönderici yani sunucu belirlediğimiz bir portu dinlemeye başlayacaktır. Alıcı yani istemci çalıştırılıp sunucunun IP adresini girdikten sonra belirlenen porttan sunucu ile iletişim kurmaya başlayacaktır.

Belirlediğimiz porttan göndericiye istek geldiğinde, istemci ile SSL el sıkışması yapacaktır. Eğer SSL el sıkışması başarısız olursa ekrana hata mesajı yazdırıp o istemci ile olan bağlantısını sonlandıracaktır. SSL el sıkışması başarılıysa önceden belirlemiş olduğumuz dosyanın adını ve kendisini istemciye yollayacak, her iki durumda da gönderici program gelebilecek yeni isteklere karşı portu dinlemeye devam edecektir.

Gönderici program, SSL el sıkışmasından sonra alıcının açık anahtarını (public key) ve sertifika tipini ekrana yazdıracaktır. Aynı şekilde alıcı program da, gönderici programda olduğu gibi, SSL el sıkışmasından sonra göndericinin açık anahtarını (public key) ve sertifika tipini ekrana yazdıracak ve dosya gönderim alım işlemlerine geçecektir.

Kullandığımız yöntemlere gelince her iki program tarafında da keystore yapısında hangi tip dosya (JKS) saklanacağı belirtiliyor ve keystore.jks dosyası bu keystore' a yükleniyor, akabinde bu jks' yi açmak için gerekli parola da yazılıyor. Ardından hangi sertifika tipi olacağı belirtilip keystore.jks içindeki entry' e parola girilerek ulaşılıyor.

İstemciden gelen jks dosyasının içerisindeki sertifikayı güvenilir olarak belirtmek için önce java yapısında bir keystore' a yükleniyor. Tanımlanan yapılar kullanılarak SSL socket initialize ediliyor. Ardından SSLServerSocket istemci için kimlik doğrulaması gerektirecek şekilde yapılandırılıyor.

Try bloğuna girildiğinde handshake kabul ediliyor. İstemciden gelen sertifika alınıyor ve içeriği görüntüleniyor. Daha sonraki kısımlarda ilk projede yaptığımız dosya gönderme ve alım işlemlerine (Dosya adı gönderimi, bytelara çevirilip bufferlardan iletimin sağlanması vs.) geçiliyor. Her iki programda da hata kontrolleri yapılıp implementasyon tamamlanıyor.

Gönderici program private_gönderici ve public_alıcı keylerine sahiptir.

(keystore & truststore2)

Alıcı program private_alıcı ve public_gönderici keylerine sahiptir.

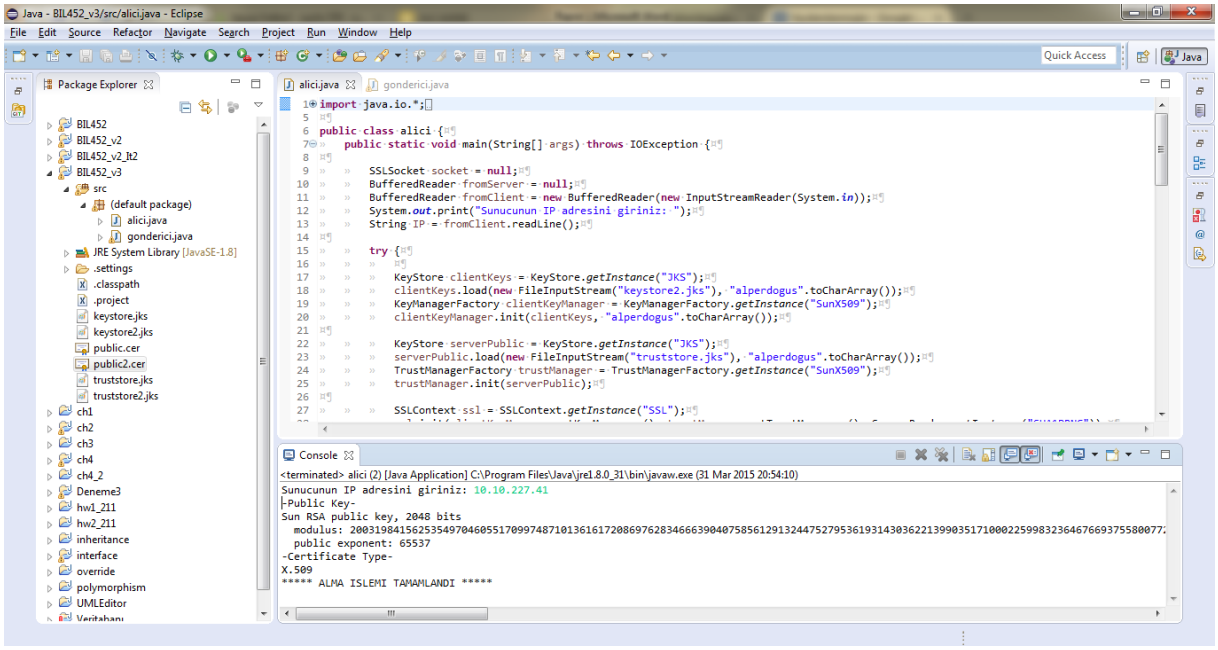
(keystore2 & truststore)

Keylerin oluşturulmasında aşağıdaki siteden fayda sağlanmıştır.

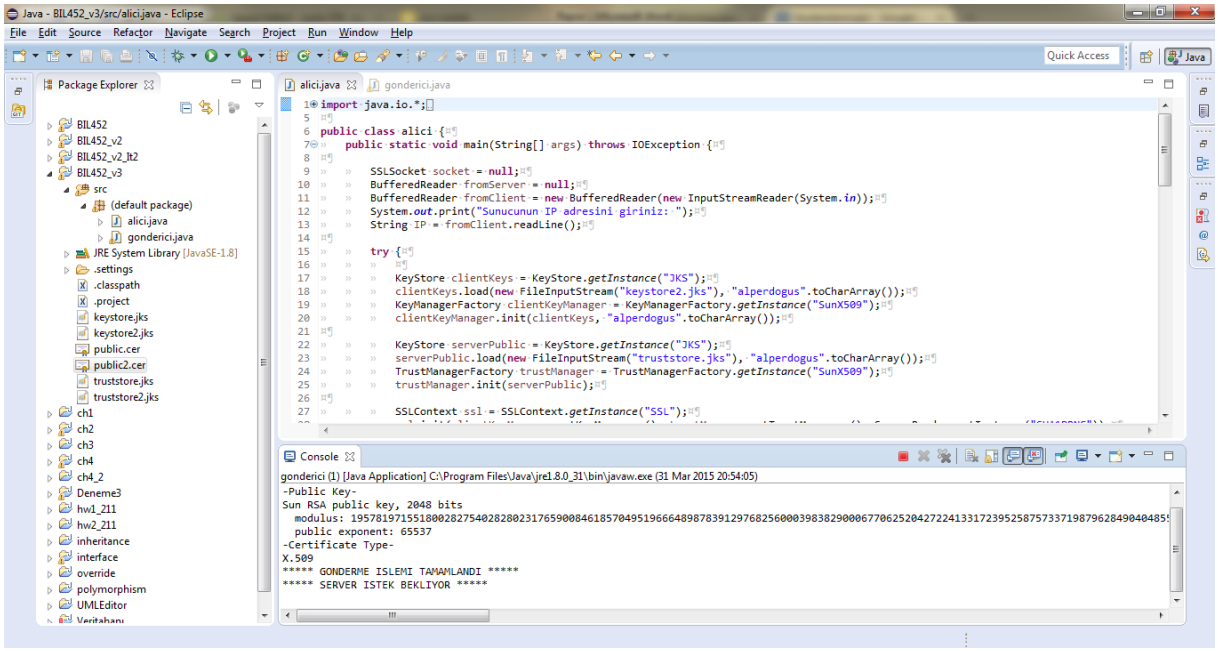
http://crishantha.com/wp/?p=445

Hata kontrolleri ve handshake başarısızlığı internet bağlantısının yavaşlığına (timeout), keylerin şifrelerinin eşleşmemesine ve portların uyuşmamasına vs. bağlı olarak çalışmaktadır.

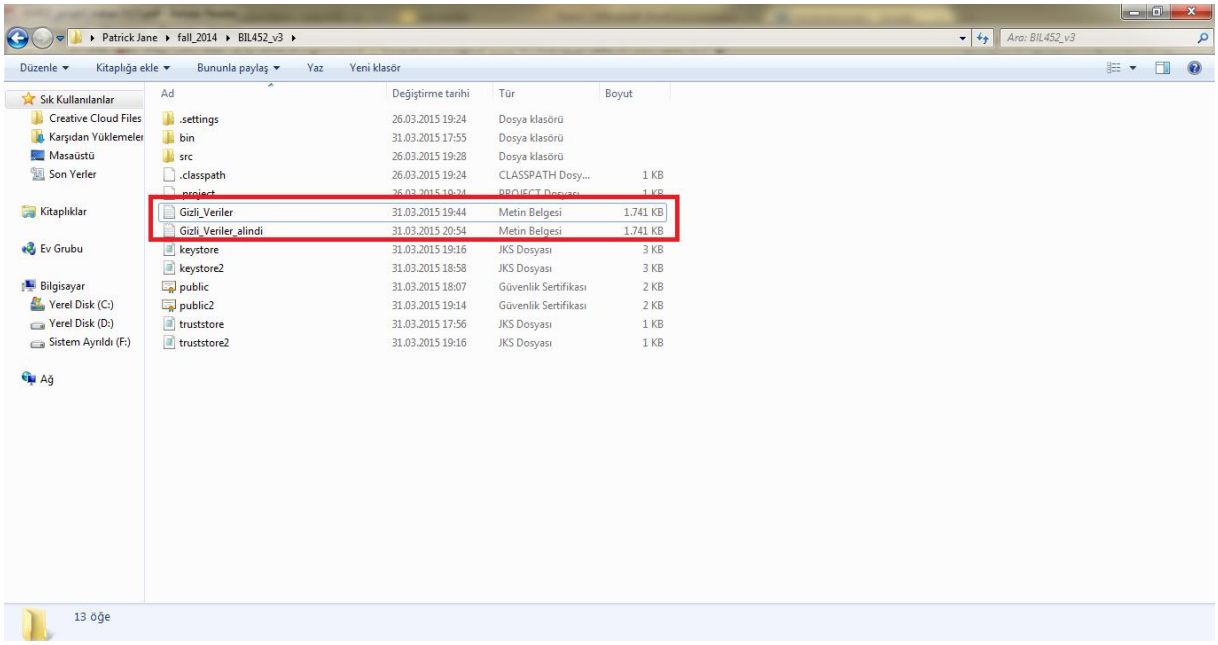
Alıcı program tarafından konsol görüntüsü:



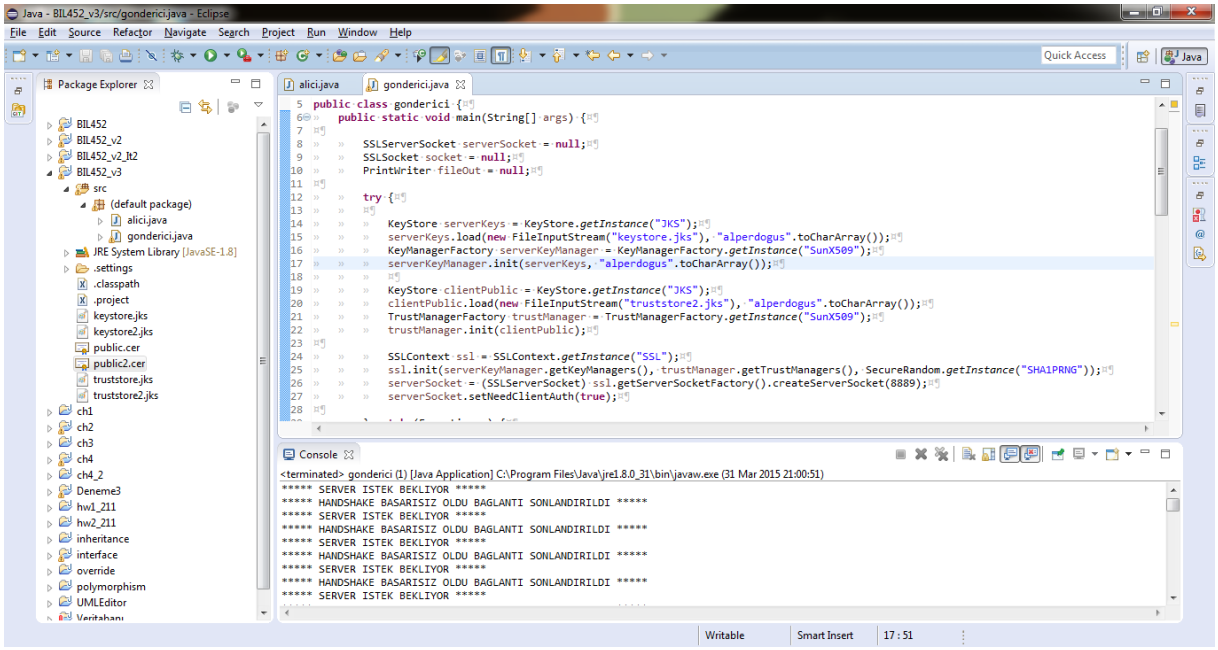
Gönderici program tarafından konsol görüntüsü:



Dosyanın başarıyla alındığının ekran görüntüsü:



Handshake' in başarısız olduğu senaryoda konsol ekran görüntüsü:



Alper Taday - 101101020

Berk Doğuş Eryetkin - 101101050