**BİL 470 KRİPTOGRAFİ VE BİLGİSAYAR GÜVENLİĞİ ÖDEV**

**GÖKHAN HAS - 161044067**

**ARAŞTIRMA :**

Her protokol anlatılırken içerisinde avantaj ve dezavcantajlarına değinilmiştir. Değinilmeyen protokoller birbirleri ile karşılaştırma yapıldığı için özet bölümde bu özellikleri görülebilmektedir.

**KATMAN 7:**

Katman 7, OSI ağ modelindeki uygulama düzeyinde iletişim katmanıdır. Ağ oluşturmada, hizmetler arasındaki iletişim, fiziksel / donanım katmanından uygulama katmanına kadar uzanan çok sayıda katmanda gerçekleşir. 7. Katman, kullanıcıya en yakın iletişim katmanı için kısaltma olarak kullanılır. Katman 7 protokolleri arasında HTTPS, MIME ve SET gibi protokolleri bulunur.

**HTTPS:** Tarayıcılar ve sunucular arasındaki iletişimi saldırganlar tarafından engellenmeye ve kurcalanmaya karşı korur. Bu, günümüzün internet trafiğinin büyük çoğunluğu için gizlilik, bütünlük ve kimlik doğrulama sağlar. Adres çubuğunda bir kilit simgesi gösteren herhangi bir web sitesi HTTPS kullanıyor demektir. Bu sitelerde işler yaparken olmayan sitelere göre daha korunaklı olduğumuzu söyleyebiliriz.

**S/MIME:** Çok Amaçlı İnternet Posta Uzantısı (MIME), sınırlı e-posta yeteneklerini genişletmek için Bell Communications tarafından önerilen bir standarttır. MIME, gönderen tarafındaki ASCII olmayan verileri NVT 7 bitlik verilere dönüştürür ve istemci SMTP'ye iletir. Alıcı tarafındaki mesaj, orijinal verilere geri aktarılır. MIME kullanarak video ve ses verilerini gönderebilmemizin yanı sıra, onları 7 bit ASCII verilerinde de aktarır. Tek bir mesaj ile birden fazla eklenti gönderilebilir.

**SET:** Güvenli Elektronik İşlem veya SET, bir senaryoda kredi kartı kullanılarak yapılan elektronik işlemlerin güvenliğini ve bütünlüğünü sağlayan bir sistemdir. SET, ödemeyi mümkün kılan bir sistem değil, bu ödemelere uygulanan bir güvenlik protokolüdür. Kredi kartları ile internet üzerinden yapılan ödemeleri güvence altına almak için farklı şifreleme ve hashing teknikleri kullanır.

**Avantajlar ve Dezavantajlar Özet**

HTTPS, şifreleme ve koruma sağlar. Web sitesini korsanlardan korumaya yardımcı olur. S/MINE, HTTPS’in avantajlarına ek olarak kimlik doğrulamaya sahiptir. Çok daha fazla verimlidir. SET ise donanımdan bağımsız olarak kredi kartı bilgileri için güvenlik sağlar.

HTTPS, için SSL sertifikasına ihtiyaç vardır. Ek olarak maaliyet yükü oluşturur. Performans bakımından yetersizdir. Birkaç aracı hizmet veya güvenlik duvarı çerçevesi, HTTPS ile yerel ayarlara erişime izin vermeyebilir. S/MIME daha pahalıdır. Yalnızca e-posta servislerinde kullanılır. SET için ek olarak yazılım kurulması gerekir.

**KATMAN 3:**

3. Katman, ağ katmanı olan Açık Sistemler Ara Bağlantısı (OSI) Modelinin üçüncü katmanını ifade eder.

Katman 3, ortam erişim kontrolü ve akış kontrolünden ve Katman 1 işlemlerinin hata kontrolünden sorumlu olan Katman 2'nin (veri bağlantı katmanı) aksine, ara yönlendiriciler arasındaki tüm paket iletimlerinden sorumludur. Katman 3, ağ düğümleri arasında veri aktarımı için kullanılan ve sanal devreler (VC) olarak bilinen mantıksal yollar oluşturan ağın yönlendirme ve anahtarlama teknolojilerini sağlar. Katman 3'ün ana işlevleri, yönlendirme ve iletmenin yanı sıra ağ üzerinden çalışma, adresleme, paket sıralaması, tıkanıklık kontrolü ve daha fazla hata işlemeyi içerir. IPsec protokolü şifreleme de kullanılır.

**IPsec:** Veri kimlik doğrulaması, bütünlük ve gizlilik sağlayan IP ağı üzerindeki 2 iletişim noktası arasında bir İnternet Mühendisliği Görev Gücü (IETF) standart protokol paketidir. Aynı zamanda şifrelenmiş, şifresi çözülmüş ve kimliği doğrulanmış paketleri tanımlar. Güvenli anahtar değişimi ve anahtar yönetimi için gereken protokoller burada tanımlanmıştır. Uygulama katmanı verilerini şifrelemek, genel internet üzerinden yönlendirme verileri gönderen yönlendiriciler için güvenlik sağlamak, şifreleme olmadan kimlik doğrulama sağlamak için, verilerin bilinen bir gönderenden geldiğini doğrulamak gibi ve Sanal Özel Ağ (VPN) bağlantısında olduğu gibi, iki uç nokta arasında tüm verilerin şifrelenmiş olduğu IPsec tünellemesini kullanarak devreler kurarak ağ verilerini korumak için kullanılır.

**Avantajlar ve Dezavantajlar Özet**

IPSec, uygulamalarla ilgili değildir, bu nedenle, IPSec VPN istemcileri tüm IP katmanı protokollerini destekler. IPSec, taşıma katmanına uygulanır ve uygulamalar için şeffaftır. IPSec bir yönlendiriciye veya güvenlik duvarına yüklendiğinde, kullanıcı veya sunucu sistemindeki yazılım ayarlarını değiştirmenize gerek yoktur. Terminal sisteminde IPSec gerçekleştirilse bile, üst katman yazılımı etkilenmez. IPSec VPN, yüksek güvenlik performansına sahiptir. IPSec protokolü ağ katmanında çalıştığı için, yalnızca tüm ağ kanalları değil, aynı zamanda kullanıcılar tüm kurumsal kaynaklara eriştiklerinde, aynı özel hat üzerinden kurumsal ağa doğrudan bağlı oldukları gibi şifrelenir. IPSec, iletilen kanalın yalnızca küçük bir bölümünü şifrelemekle kalmaz, aynı zamanda tüm kanalları da şifreler. Ek olarak, IPSec VPN ayrıca IPSec istemci yazılımının ve erişim cihazlarının uzaktan erişim istemcilerine uygun şekilde yüklenmesini ve yapılandırılmasını gerektirir; bu, erişim belirli erişim cihazları, yazılım istemcileri, kullanıcı kimlik doğrulama mekanizmaları ve önceden tanımlanmış güvenlik kuralları tarafından kısıtlandığı için güvenlik düzeyini büyük ölçüde artırır. .

IPSec VPN, istemci yazılımı gerektirir. IPSec VPN'de, müşteri sisteminin TCP / IP yığınını değiştirmek veya eklemek için her istemciye özel istemci yazılımı yüklemeniz gerekir. Çoğu sistemde bu, diğer sistem yazılımlarıyla uyumluluk sorunları riskine yol açabilir. Şu anda, IPSec protokolünün uyumluluğu için tutarlı bir standart yoktur. Neredeyse tüm IPSec istemci yazılımları özeldir ve başkalarıyla uyumlu olamaz.

**KATMAN 4:**

OSI Modeli, Katman 4, uç sistemler veya ana bilgisayarlar arasında şeffaf veri aktarımı sağlar ve uçtan uca hata kurtarma ve akış kontrolünden sorumludur. Tam veri aktarımı sağlar.

**TLS:** Taşıma Katmanı Menkul Kıymetleri (TLS), taşıma katmanında güvenlik sağlamak için tasarlanmıştır. TLS, Güvenli Hizmet Katmanı (SSL) adı verilen bir güvenlik protokolünden türetilmiştir. TLS, hiçbir üçüncü tarafın herhangi bir mesajı dinlememesini veya değiştirmemesini sağlar. SSL / TLS sürümü hangi şifre paketleri, kullanmak istediği sıkıştırma yöntemini ifade eder.

Sunucu, her ikisi tarafından desteklenen en yüksek SSL / TLS sürümünün ne olduğunu kontrol eder, istemcilerden birinden bir şifre seti seçer (birini destekliyorsa) ve isteğe bağlı olarak bir sıkıştırma yöntemi seçer. Bundan sonra temel kurulum yapılır, sunucu sertifikasını sağlar. Bu sertifika ya istemcinin kendisi ya da istemcinin güvendiği bir tarafça güvenilmelidir. Sertifikayı doğruladıktan ve bu sunucunun gerçekten iddia ettiği kişi olduğundan emin olduktan sonra (ortadaki bir adam değil), bir anahtar takas edilir. Bu bir genel anahtar, "PreMasterSecret" olabilir veya şifre paketine bağlı olarak hiçbir şey olmayabilir. Artık hem sunucu hem de istemci simetrik şifreleme için anahtarı hesaplayabilir. El sıkışma tamamlandı ve iki ana bilgisayar güvenli bir şekilde iletişim kurabilir. Bitirerek bir bağlantıyı kapatmak için. TCP bağlantısı her iki taraf da bağlantının uygun olmayan şekilde sonlandırıldığını bilecektir. Bağlantı bundan dolayı tehlikeye atılamaz, sadece kesilir.

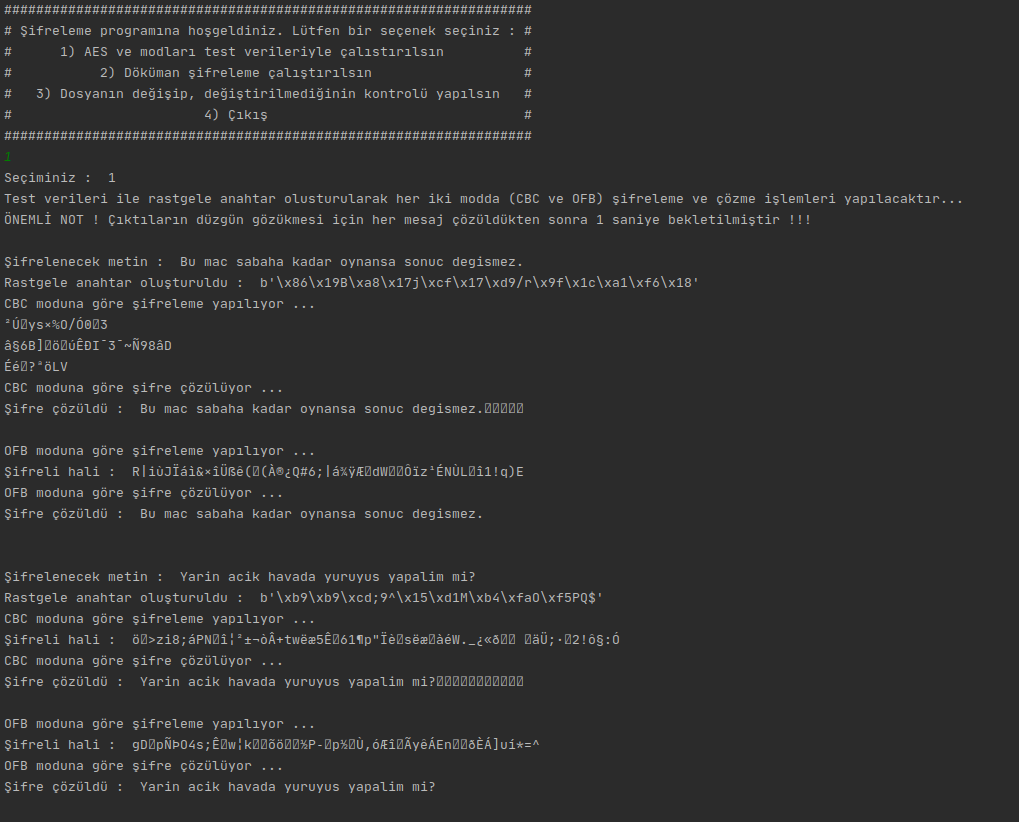
**Avantajlar ve Dezavantajlar Özet**

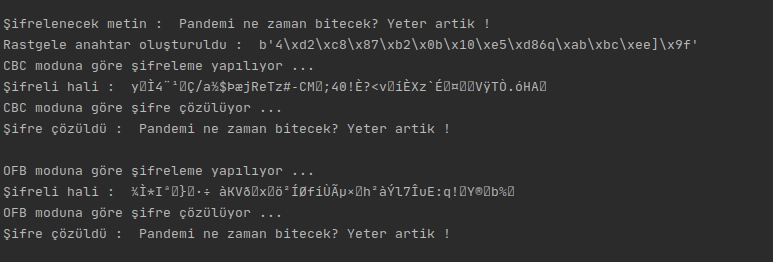
TLS / SSL, şifreleme kullanarak iletilen verilerin güvenliğini sağlamaya yardımcı olabilir. TLS / SSL, Microsoft Internet Explorer dahil çoğu web tarayıcısında ve çoğu işletim sistemi ve web sunucusunda çalışır. TLS / SSL, güvenli oturum sırasında kullanılan kimlik doğrulama mekanizması, şifreleme algoritmaları ve karma algoritma için işlemler sağlar. Windows server 2003 işletim sistemlerinde birçok uygulama TLS / SSL geçici olarak. Uygulama katmanının altında TLS / SSL uyguladığımız için, işlemlerinin çoğu istemci tarafından tamamen görünmezdir.

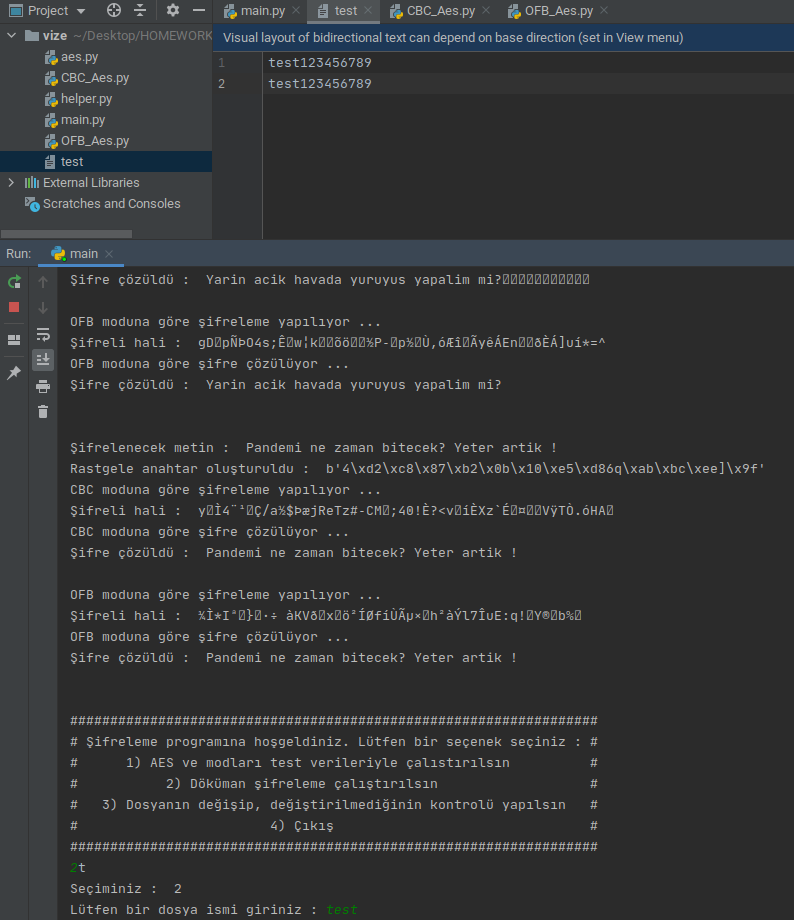
Diğer birçok güvenli şifreleme yöntemiyle karşılaştırıldığında TLS daha yüksek gecikme sağlar. TLS kullanıldığında, sitenin trafiğine ek gecikme eklenecektir. TLS'nin genel olarak güvenli olduğu düşünülse de, TLS'nin bazı sürümleri hâlâ Ortadaki Saldırılara karşı savunmasızdır. Bunun yanı sıra SLOTH, POODLE ve DROWN gibi diğer siber saldırı türlerinin de duyarlı olduğu bulunmuştur. TLS'nin en son sürümleri birçok platformu desteklese de, yalnızca birkaç platformu destekleyebilen TLS 1.3 gibi bazı sürümler vardır. Popüler İşletim sistemi sağlayıcısı Microsoft, uygulama sürecinde zorluklarla karşılaşmaktadır. Bir TLS sertifikası uygulamak ücretsiz değildir, bazı maliyetler vardır. Bununla birlikte, TLS endüstrisindeki rekabet nedeniyle, TLS sertifikasının maliyeti büyük ölçüde azaltıldı. Ödenmesi gereken miktar, alan adlarının ve alt alan adlarının sayısına bağlıdır. Bunun dışında kimlik doğrulamasına da bağlı olabilir. Ağ mimarisindeki karmaşıklık, TLS sertifikasının bir başka önemli dezavantajıdır. Bu durumda otomatik olarak ağ topolojisi de karmaşık hale gelebilir ve bu da daha fazla yük devretmeye yol açabilir. Bunun üstesinden gelmek için uygun bir ağ uzmanı işe alınmalıdır.

**PROGRAMLAMA PROJESİ**

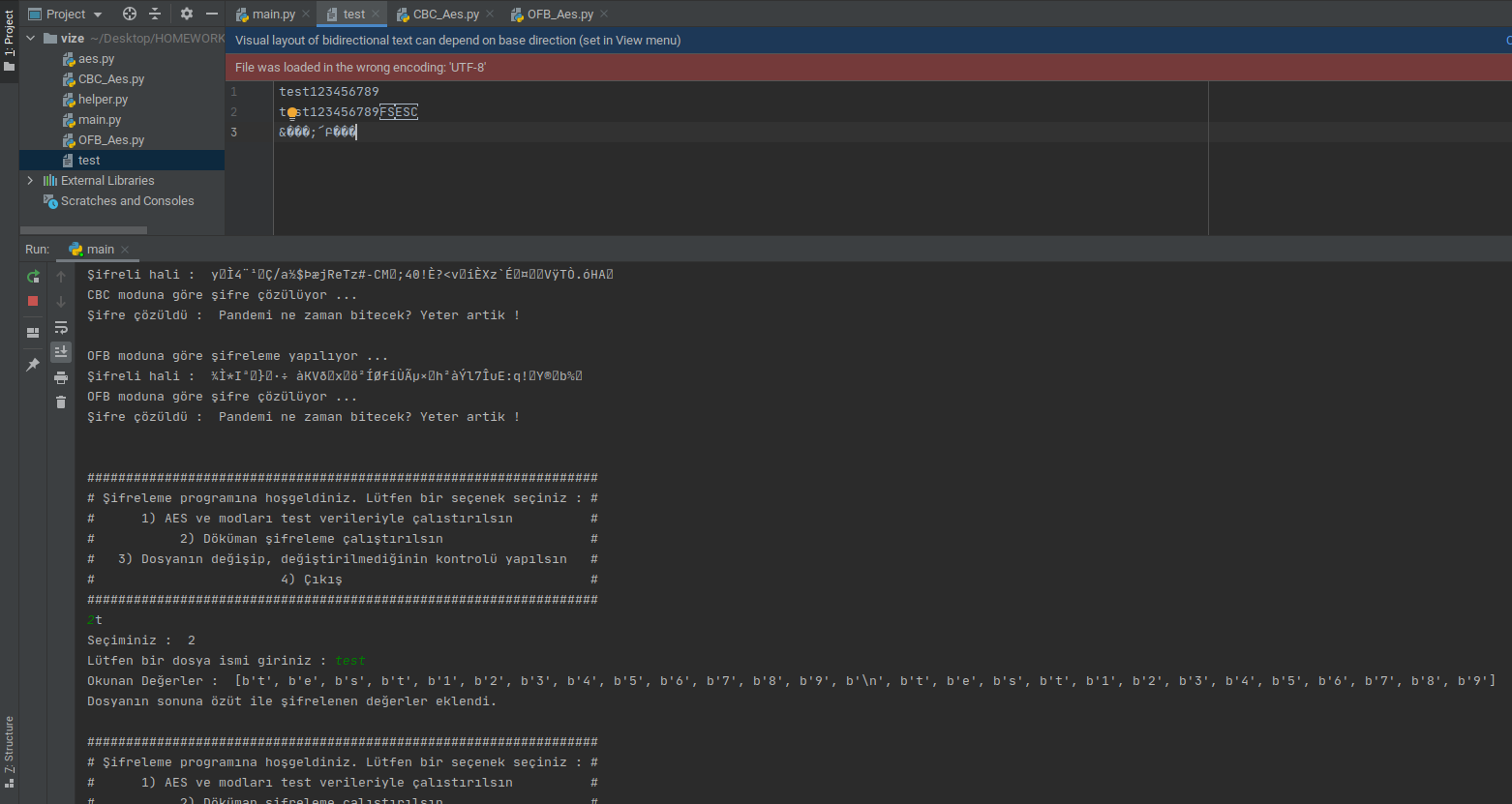
Kaynak kodlarındaki main.py dosyası python3 komutu ile çalıştırıldığında bir menü ekrana gelir. Kullanıcı 1,2,3 veya 4 seçeneklerinden birini seçer. İlk seçenek seçildiğinde kodda bulunan test verileriyle AES, CBC ve OFB moduna göre şifreleme, şifre çözme işlemleri yapılır ve kullanıcıya aşağıdaki gibi bilgilendirme mesajları basılır.

****

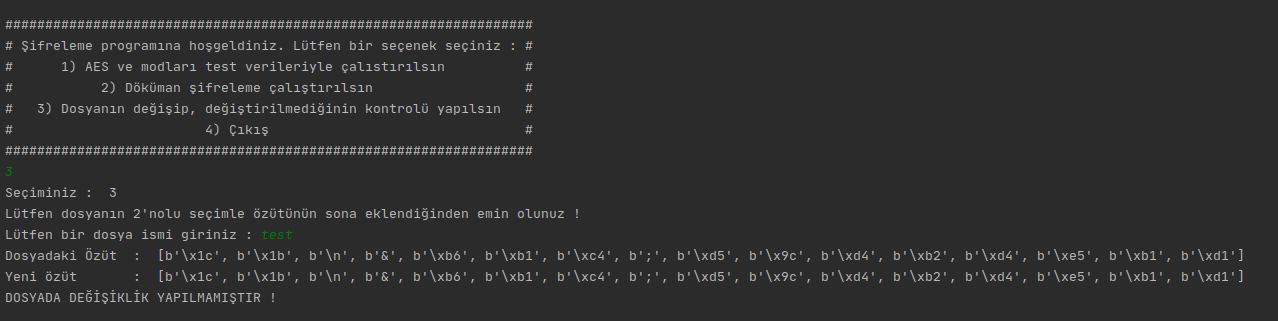
****



Daha sonra 2 nolu seçenek basıldığında dosya ismi girilmesi gerekmektedir. Burada aynı dizinde bulunan test isimli dosya girilmiştir. Sonuç bir aşağıdaki ekran görüntüsündedir. Eğer ekran görüntüsü okunmuyorsa ekran görüntüleri adlı klasörden detaylıca bakılabilir.



Daha sonra dosyada değişiklik yapılmadan 2 nolu seçenek tekrardan çalıştırılır. Dosyada değişiklik yapılmadığında aşağıdaki gibi mesaj ekrana basılmaktadır.



test adlı dosyada bir değişiklik yapılmış daha sonra tekrardan 3 nolu seçenek çalıştırıldığında aşağıdaki gibi dosya değişmiştir mesajı ekrana basılmatadır.

