T.C.
GEBZE TEKNİK ÜNİVERSİTESİ
MÜHENDİSLİK FAKÜLTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

ARAŞTIRMA ve PROGRAMLAMA

BİL 470 KRİPTOLOJİ VE BİLGİSAYAR GÜVENLİĞİ
DÖNEM PROJESİ RAPORU

ÖĞRENCİ
Şeyda Nur DEMİR
12 10 44 042

DERS ÖĞRETİM ÜYESİ
Prof. Dr. İbrahim SOĞUKPINAR

DERS ASİSTANI
-

KOCAELİ, 2021

1.AÇIKLAMA

1.1.Proje Bilgileri :

- Proje iki kısımdır, ilk kısım araştırma ve ikinci kısım programlamadır,
- Araştırma kısmı, PDF dosya formatında teslim edilecektir.
- Programlama kısmı, C dilinde yazılıp, kaynak kodları teslim edilecektir.
- Rapor, PDF dosya formatında proje ile birlikte teslim edilecektir.

1.2.Teslim Bilgileri :

- 8 Ocak 2021 tarihi Cuma günü saat 17:30'a kadar,
  Microsoft Teams (Ekipler) uygulaması üzerinden yüklenecektir.

1.3.Sunum Bilgileri :

- Sunum yapılmayacaktır.

2.PROJEDE İSTENENLER

2.1.Araştırma :

- OSI temel referans modelinin uygulama katmanında (katman 7), ağ katmanında (katman 3) ve taşıma katmanında (katman 4) kriptografik protokollerin uygulanmasının göreli avantajları ve dezavantajlarını araştırarak öneklerle karşılaştırmalı olarak açıklayın.

2.2.Programlama :

C veya phyton ile gerçekleştirilecek olan bu araçta şifreleme/deşifreleme ve özüt alma, dosya bütünlüğünün denetimi yöntemleri bizzat gerçeklenecek olup, arşiv/API kullanılmayacaktır. Gerçeklenenen programların kaynak kodları açıklamalı olarak verilecektir;

a) AES şifreleme algoritmasının gerçekleyiniz ve şifreleme/deşifrelemede test verileri ile birlikte kullanınız.

b) Gerçeklenen simetrik şifreleme algoritması kullanılarak CBC ve OFB modlarında çalışmayı gerçekleyip testlerini yapacak şekle getiriniz.

c) Herhangi bir doküman (.doc/.docx, .pdf, ppt, xls vs) üzerinde değişiklik yapılıp yapılmadığını ve yapanın kimliğini anlamak için, b şıkkındaki gerçeklemeyi özüt fonksiyonu olarak kullanarak özütünü alacak ve sadece işlem yapan kişinin bildiği bir anahtar ile şifreleyip dosyanın sonuna ekleyecek bir araç gerçekleştiriniz.

d) Dosyanın bütünlüğünün değişip değişmediğinin kontrolü için, c şıkkındaki işlemleri yaparak ilk üretilen özüt değer ile karşılaştıran doğrulama aracını gerçekleyerek örnek testleri gösteriniz.

3.BİRİNCİ KISIM : ARAŞTIRMA

Yapılanlar :

İstenen tüm araçlar gerçekleştirilmiştir.

- **Part1** klasörünün içerisindedir.
- Bu kısımda, OSI temel referans modelinin, uygulama katmanı, ağ katmanı ve taşıma katmanı üzerinde, kriptografik protokollerin uygulanmasının, göreli avantajları ve dezavantajları değerlendirilmiştir.
- **Öncelikle** konunun anlaşılması adına, bazı belirli terimler açıklanmıştır.
- **Ardından** araştırma hakkında genel bir görüş beyan edilmiş, ve ilgili yorumlar yapılmıştır.
- **Son olarak**, örnekler ile istenen bu üç katman kıyaslanmıştır.
- Araştırma hazırlanırken, **ders kayıtları** tekrar izlenmiştir, **ders kitabı** incelenmiştir, tarafımıza sağlanan **sunum dosyaları** incelenmiştir, bunlara ek **internet** üzerinden araştırma yapılmıştır, ve **literatür taraması** yapılmış.
- Faydalanılan kaynakların bağlantı adresleri araştırma sonunda verilmiştir.
- Bu araştırmanın bana en büyük faydası, **referans modelleri** hakkında daha kapsamlı bir görüş kazanmak, **kriptografik protokollerin** amaçlarını ve kullanım alanlarını öğrenmek, özelde ise **OSI katmanlarında kullanılan protokollerin örnekleri** hakkında bilgi sahibi olmak olmuştur.
- Araştırma, Part1 klasörü içerisinde "**docx**" uzantılı ve "**pdf**" uzantılı olmak üzere 2 formatta da teslim edilmiştir.

4.İKİNCİ KISIM : PROGRAMLAMA

Yapılanlar :

<u>İstenen tüm araçlar gerçekleştirilmiştir.</u>

- **Part2** klasörünün içerisindedir.
- Her araç, **Part2a**, **Part2b**, **Part2c** ve **Part2d** şeklinde, ayrı ayrı klasörlerde gerçekleştirilmiştir.
- Her klasör içerisinde, ekran görüntülerinin bulunduğu "**ScreenShots**" klasörleri bulunmaktadır. Bu klasörlerde her part için **5 ekran görüntüsü** bulunmaktadır.
- Kodlarımı dönem sonunda açık kaynak olarak paylaşacağım için, kodlamalarımda isimlendirmeler, daha çok kişiye katkı sağlayabilmesi amacı ile, **İngilizce** olarak yapılmıştır. Raporda ise kendimi daha iyi ifade edebilmem adına, **Türkçe** tercih edilmiştir.
- Bunlardan ilki, "**Content of File**" görüntüsüdür, burada dosya içeriğinin ilk hali bulunmaktadır.
- İkincisi, "**Execution**" görüntüsüdür, burada ödevin nasıl çalıştırılacağı gösterilmektedir.
- Üçüncüsü, "**Object and Execution Files**" görüntüsüdür, burada ödevin ilk "compile and link" işlemi, yani "derlenmesi" sonrası oluşan "object files" ve "execution file", yani "obje dosyaları" ve "çalıştırılabilir dosyalar"ının neler olduğu gösterilmektedir.
- Dördüncüsü, "**Output Files**" görüntüsüdür, burada ödevin çalıştırılması sonucu oluşan "çıktı dosyaları" yer almaktadır.
- Beşincisi, "**Make Clean**" görüntüsüdür, burada ise ödev klasörünün obje ve çalıştırılabilir dosyalarının temizlendiği, ancak çıktı dosyalarının durduğu, son hali görünmektedir.
- Her partın klasörünün içerisinde, ekran görüntülerinin bulunduğu klasör haricinde bulunan tüm dosyalar, istenenlerin gerçekleştirildiği araca ait dosyalardır. Kodlama kısmını "**C Programlama Dili**"nde gerçekleştirdiğim için, burada C'ye ait bazı dosyalar mevcuttur.
- Asıl aracın bulunduğu, "main fonksiyonu"nun yazıldığı dosyalar "**main.c**" dosyalarıdır.
- Main dosyası hariç, aracın gerçekleştirildiği C dosyaları da bulunmaktadır, bunlar "**header**" ve "**implementation**" dosyalarıdır, yani "**başlık**"ların bulunduğu dosyalar ve algoritmanın gerçeklendiği "**implementasyon**" dosyalarıdır
- Ödevin kolayca çalıştırılabilmesi için, her parta özel "**Makefile**" dosyası bulunmaktadır. Bu sayede, **terminal (uçbirim, linux ortamında komut çalıştırma sistemi)** açılıp aracın bulunduğu klasör içine gelindiğinde, sadece "**make all**" komutu ile, tüm kod derlenebilir, çalıştırılabilir dosyalar oluşturulabilir, ve sadece "**make clean**" komutu ile bunlar tekrar silinebilir.
- "**make all**" komutu yazılıp, kod derlendiğinde, ve çalıştırılabilir dosyalar oluştuğunda, aracı **test etmek için**, çalıştırılabilir dosyanın çalıştırılması gerekir. Tüm bu aşamalar, ekran görüntüleri klasöründe gösterilmiştir.
- Ödevde, gerçeklenenlerin açıkça görünmesi adına, araçlar "**txt**" uzantılı "**metin dosyaları**" üzerinde test edilmiştir, ayrıca oluşan ara dosyalar, geçici olanlar hariç, kaldırılmamıştır; dilenirse araçlar, farklı uzantılı dosya tiplerinde denenebilir, veya oluşan ara dosyalar kaldırılıp, sadece çıktı dosyaları alınabilir.
- Burada belirtilmelidir ki, **farklı veriler ile test edilmek istenirse**, kodun içeriğinin değiştirilmesi gerekir.
- Takip eden sayfalarda, her partta gerçekleştirilen **araç** tanıtılacaktır, girdi dosyalarının nasıl olması gerektiğinden, ve çıktı dosyalarının neler olacağından bahsedilecektir.

Part2a :

Bu part için istenilenlerin tümü gerçekleştirilmiştir.

- Bu partta, verilen bir dosyanın, AES şifreleyici ile şifrelenmesi ve deşifrelenmesi istenilmiştir.
- Şifreleme ve deşifreleme işlemleri gerçekleştirilmiştir.
- Girdi olarak "**Plain_Text.txt**" isimli dosya alınır, bu dosya ödev ile birlikte teslim edilmiştir.
- **AES** şifreleme **128 bitlik blok**lar ile yapılmıştır, **anahtar uzunluğu** da **128 bit**tir, dolayısıyla **10 round** gerçekleştirilir. AES şifreleme ve deşifreleme fonksiyonları da implement edilmiştir, ancak örnek testler AES'in **default (varsayılan)** olarak kullandığı "**ECB**" modunda gerçekleştirilmiştir.
- Şifreleme ve deşifrelemede kullanılan **anahtar** :
  {0x0f, 0x15, 0x71, 0xc9, 0x47, 0xd9, 0xe8, 0x59, 0x0c, 0xb7, 0xad, 0xd6, 0xaf, 0x7f, 0x67, 0x98}
- Şifreleme için kullanılan **başlangıç vektörü** :
  {0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1}
- Deşifreleme için kullanılan **başlangıç vektörü** :
  {0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1}
- Bu kısımda yapılanlar, diğer tüm partlarda da direk olarak kullanılmıştır.
- Çıktı olarak şifrelenmiş "**Encrypted_Text_ECB.txt**" dosyası ve deşifrelenmiş "**Decrypted_Text_ECB.txt**" dosyası olmak üzere 2 dosya verir.

Part2b :

Bu part için istenilenlerin tümü gerçekleştirilmiştir.

- Bu partta, verilen bir dosyanın, AES şifreleyici ile, "**CBC**" ve "**OFB**" modlarında, şifrelenmesi ve deşifrelenmesi istenilmiştir.
- Şifreleme ve deşifreleme işlemleri bu modlarda gerçekleştirilmiştir.
- Girdi olarak "**Plain_Text.txt**" isimli dosya alınır, bu dosya ödev ile birlikte teslim edilmiştir.
- Bu kısımda yapılanlar, ilk partta gerçeklenenler direk olarak kullanılmıştır, buna "**CBC**" ve "**OFB**" modları eklenmiştir.
- Bu kısımda yapılanlar, diğer tüm partlarda da direk olarak kullanılmıştır.
- Çıktı olarak "**CBC**" modunda şifrelenmiş "**Encrypted_Text_CBC.txt**" dosyası ve deşifrelenmiş "**Decrypted_Text_CBC.txt**" dosyası, "**OFB**" modunda şifrelenmiş "**Encrypted_Text_OFB.txt**" dosyası ve deşifrelenmiş "**Decrypted_Text_OFB.txt**" dosyası olmak üzere 4 dosya verir.

Part2c :

Bu part için istenilenlerin tümü gerçekleştirilmiştir.

- Bu partta, verilen bir dosyanın, AES şifreleyicinin CBC modunda şifrelenmesinin kullanılarak, bir dosyanın **özütünün alınması** istenmiştir, alınan özütün yine AES ile şifrelenerek, orijinal dosyanın sonuna yazılması, yani **imzalanması** istenmiştir.
- Girdi olarak "**Plain_Text.txt**" isimli dosya alınır, bu dosya ödev ile birlikte teslim edilmiştir.
- Bu kısımda yapılanlar, ilk iki partta gerçeklenenler direk olarak kullanılmıştır, buna özüt fonksiyonun alındığı "**hash**" kodu ve özütün şifrelenip dosya sonuna eklendiği "**sign**" kodları eklenmiştir.
- **Özüt alma işlemi**, AES şifreleyicinin CBC modunda, anahtarsız kullanılması, başlangıç vektörünün "Sıfır Vektörü" olarak verilmesi, ve 128 bitlik son bloğun alınması ile, gerçekleştirilmiştir.
- **İmzalama işlemi,** alınan özütün, AES şifreleyici ile CBC modunda şifrelenip, dosyanın sonuna eklenmesi ile gerçekleştirilmiştir.
- Bu kısımda yapılanlar, diğer partta da direk olarak kullanılmıştır.
- Çıktı olarak AES şifreleyicinin CBC modunda çalıştırılması sonucu alınan özüt "**Hash_of_File.txt**" dosyası ve özütün şifreli hali ile imzalanmış "**Signed_Text.txt**" dosyası olmak üzere 2 dosya verir.

Part2d :

Bu part için istenilenlerin tümü gerçekleştirilmiştir.

- Bu partta, verilen bir imzalı dosyanın, iletilmesi sırasında, değiştirilip değiştirilmediğini kontrol eden bir **doğrulama aracı** istenmiştir.
- Girdi olarak "**Plain_Text.txt**" isimli dosya alınır, bu dosya ödev ile birlikte teslim edilmiştir.
- Bu kısımda yapılanlar, ilk üç partta gerçeklenenler direk olarak kullanılmıştır, buna dosyanın değiştirilip değiştirilmediğini kontrol eden "**auth**" doğrulama aracı eklenmiştir.
- **Doğrulama işlemi** için, **ilk olarak** alınan imzalı dosyanın, imza kısmının deşifrelenmesi ile taşınan özüt değeri elde edilir, **ikinci olarak** alınan imzalı dosyanın, imza kısmı hariç orijinal kısmının özüt değeri alınır, **son olarak** taşınan dosyanın imzasından elde edilen özüt değer ile dosyanın içeriğinden alınan özüt değer kıyaslanır, eğer özüt değerler aynı ise dosyanın değiştirilmediği **doğrulanır**, farklı özüt değerlerle karşılaşmış isek, dosyanın aynı kaldığı **doğrulanamaz**, dosya saldırıya uğramış olabilir, ve verilerimiz risk altındadır demektir.
- Çıktı olarak özütün alındığı "**Hash_of_File.txt**" dosyası ve imzalamanın yapıldığı "**Signed_Text.txt**" dosyası olmak üzere standart 2 dosya verir, ayrıca doğrulama sonucunu komut satırı ekranında bir uyarı ile gösterir.

RAPOR SONU

SON DEĞİŞİKLİK : 08.01.2021 15:30

ÖĞRENCİ
Şeyda Nur DEMİR
12 10 44 042

DERS ÖĞRETİM ÜYESİ
Prof. Dr. İbrahim SOĞUKPINAR

DERS ASİSTANI
-

KOCAELİ, 2021