KRİPTOGRAFİ VE AĞ GÜVENLİĞİ TEKNİK RAPORU
AES – DES – RSA Kullanarak İstemci–Sunucu Şifreleme Sistemi Analizi

Öğrenci Bilgileri
- **Ad Soyad:** Hüseyin Bünyamin Gülme
- **Öğrenci No:** 439591
- **GitHub Deposu:** https://github.com/huseyingulme/Kriptoloji

1. Giriş ve Problemin Tanımı
Bilgi güvenliği, modern bilgisayar ağlarının en temel gereksinimlerinden biridir. Günümüzde bankacılık sistemleri, e-ticaret platformları, bulut tabanlı servisler ve IoT altyapıları büyük ölçüde istemci–sunucu mimarisi üzerinden çalışmaktadır. Bu mimaride istemci ile sunucu arasında sürekli olarak veri alışverişi gerçekleşmekte ve bu veriler çoğu zaman açık ağlar (internet gibi) üzerinden iletilmektedir.
Açık ağ ortamlarında gerçekleştirilen veri iletimi;
- **Pasif saldırılar** (dinleme, trafik analizi)
- **Aktif saldırılar** (veri değiştirme, paket enjeksiyonu)
- **Replay saldırıları**
- **Man-in-the-Middle (MITM)** saldırıları

gibi çok sayıda tehdit barındırmaktadır. Bu tehditlere karşı en temel savunma mekanizması kriptografidir.
Bu projede ele alınan temel problem şudur:
Bir istemci ile sunucu arasında, ağ üzerinde dinlenmeye açık bir ortamda, veriler nasıl güvenli biçimde iletilebilir?
Bu soruya cevap ararken, yalnızca "hangi algoritma daha güçlüdür?" yaklaşımı benimsenmemiş; aynı zamanda **hangi algoritma hangi amaç için uygundur**, **performans–güvenlik dengesi nasıl sağlanır** ve **ağ üzerindeki pratik etkiler nelerdir** gibi sorular da araştırılmıştır.

1.1. Çalışmanın Amacı ve Kapsamı
Bu çalışmanın temel amaçları aşağıdaki şekilde özetlenebilir:
- Simetrik ve asimetrik kriptografik algoritmaların çalışma prensiplerini uygulamalı olarak incelemek
- AES, DES ve RSA algoritmalarını gerçek bir istemci–sunucu haberleşmesi üzerinde karşılaştırmak
- Hibrit şifreleme yaklaşımının neden modern sistemlerde zorunlu hale geldiğini göstermek
- Şifrelenmiş ağ trafiğinin Wireshark gibi araçlarla nasıl göründüğünü analiz etmek
- Manuel kriptografik implementasyonlar aracılığıyla algoritmaların iç yapısını derinlemesine kavramak

Bu kapsamda proje, hem **kriptografi** hem de **ağ güvenliği** disiplinlerini birlikte ele alan bütüncül bir çalışma olarak tasarlanmıştır.

2. Sistem Mimarisi ve Tasarım Yaklaşımı
2.1. İstemci–Sunucu Modelinin Seçilme Gerekçesi
İstemci–sunucu mimarisi, gerçek dünyada kullanılan güvenli iletişim sistemlerinin büyük çoğunluğunun temelini oluşturmaktadır. HTTPS, FTPS, SSH gibi protokoller bu mimari üzerine kuruludur. Bu nedenle projede seçilen mimari, teorik bilgilerin pratik karşılığını görmek açısından özellikle tercih edilmiştir.
TCP protokolü, aşağıdaki nedenlerle kullanılmıştır:
- Paket sıralaması ve yeniden iletim mekanizmaları
- Güvenilir bağlantı yapısı

- Uygulama katmanında güvenliğin test edilmesine olanak tanıması

Bu sayede kriptografik güvenlik, alt katman güvenliğinden bağımsız olarak ele alınabilmiştir.

2.2. Katmanlı Mimari Yaklaşım

Sistem, aşağıdaki mantıksal katmanlara ayrılmıştır:

1. **Kullanıcı Arayüzü Katmanı (GUI)**
2. **Paketleme ve İletişim Katmanı**
3. **Kriptografik İşlem Katmanı**
4. **Kontrol ve Yönlendirme Katmanı (ProcessingManager)**

Bu katmanlı yapı sayesinde:

- Kodun bakımı kolaylaşmış
- Güvenlik açıklarının izole edilmesi mümkün hale gelmiş
- Her katmanın sorumluluğu net biçimde ayrılmıştır

Bu yaklaşım, yazılım güvenliğinde önerilen **separation of concerns** ilkesine uygundur.

3. Veri Paketleme Stratejisi ve Güvenlik Etkileri

3.1. Metadata Kullanımının Önemi

Sadece verinin şifrelenmesi, güvenli iletişim için yeterli değildir. Alıcı tarafın:

- Hangi algoritmanın kullanıldığını
- Hangi anahtar ile çözümleme yapılacağını
- Paketin geçerli olup olmadığını

bilmesi gerekir. Bu nedenle DataPacket yapısı, **metadata destekli** olarak tasarlanmıştır.
Timestamp alanı özellikle dikkat çekicidir. Bu alan sayesinde:

- Aynı paketin tekrar gönderilmesi tespit edilebilmekte
- Replay saldırıları için temel bir savunma sağlanmaktadır

Gerçek dünyada TLS protokollerinde kullanılan **nonce** ve **sequence number** mekanizmaları ile benzer bir mantık izlenmiştir.

3.2. JSON Paketleme Modunun Akademik Katkısı

JSON tabanlı paketleme modu, doğrudan güvenliği artırmasa da **analiz edilebilirliği** ciddi ölçüde artırmıştır. Bu sayede:

- Şifreli veri ile kontrol bilgileri net biçimde ayrılmış
- Ağ analiz araçlarında paket içeriği daha anlaşılır hale gelmiştir
- Öğrenci açısından kriptografik süreçlerin gözlemlenmesi kolaylaşmıştır

Bu özellik, projeyi salt bir kodlama çalışması olmaktan çıkarıp, deneysel bir güvenlik analizine dönüştürmüştür.

4. Kriptografik Algoritmaların Derinlemesine İncelenmesi

4.1. AES'in Modern Kriptografideki Rolü

AES, günümüzde güvenli veri şifrelemenin fiili standardı haline gelmiştir. Bunun temel nedenleri:

- Güçlü matematiksel altyapı
- Donanım hızlandırma desteği (AES-NI)
- Uzun anahtar seçenekleri (128/192/256 bit)

Manuel implementasyon sürecinde özellikle şu noktalar dikkat çekmiştir:

- AES'in byte tabanlı çalışması
- Lineer ve lineer olmayan dönüşümlerin dengesi
- Difüzyon ve konfizyon prensiplerinin başarılı uygulanması

Bu durum, AES'in neden DES'in yerini aldığını açıkça göstermektedir.

4.2. DES'in Eğitsel Değeri ve Güvenlik Açıkları

DES algoritması, kriptografi tarihinde önemli bir yere sahiptir ancak günümüz standartlarına göre yetersizdir. Projede yapılan denemeler, kısa anahtar uzunluğunun saldırgan açısından nasıl bir avantaj sağladığını somut biçimde ortaya koymuştur.

DES'in projeye dahil edilmesi sayesinde:

- Feistel ağ yapısı detaylı biçimde incelenmiş
- Simetrik şifreleme algoritmalarının evrimi anlaşılmış
- "Güvenli görünen" bir algoritmanın zamanla nasıl zayıflayabileceği görülmüştür

Bu durum, kriptografide **zaman faktörünün** ne kadar kritik olduğunu göstermektedir.

4.3. RSA ve Asimetrik Kriptografinin Sınırları

RSA, anahtar dağıtımı ve kimlik doğrulama için vazgeçilmezdir; ancak veri şifreleme için uygun değildir. Projede yapılan ağ analizleri, RSA'nın büyük anahtar boyutlarının ağ üzerinde ciddi bir yük oluşturduğunu açıkça ortaya koymuştur.

Bu gözlem, teorik olarak bilinen bir gerçeğin pratikte doğrulanmasını sağlamıştır:
RSA güvenlidir, ancak pahalıdır.

5. Hibrit Şifreleme Modelinin Stratejik Önemi

Hibrit şifreleme yaklaşımı, bu projenin en kritik kazanımlarından biridir. Bu yapı sayesinde:

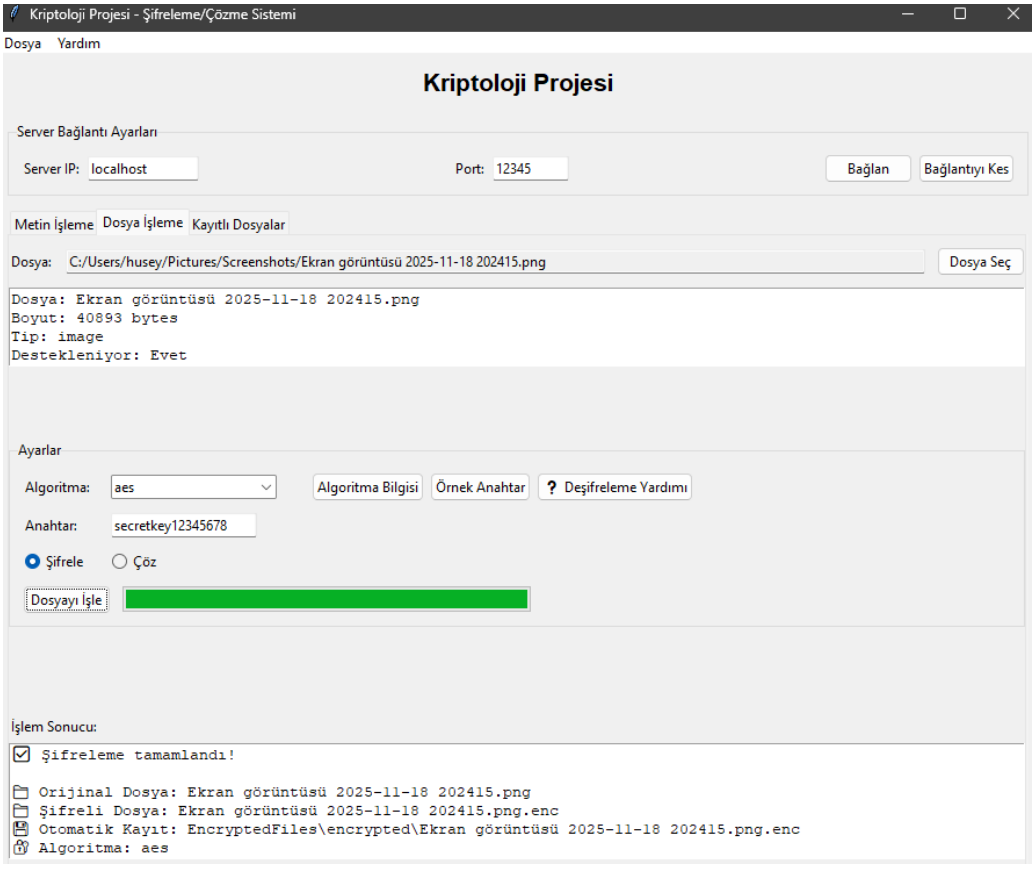
- Asimetrik kriptografinin güvenli anahtar paylaşımı avantajı
- Simetrik kriptografinin yüksek performansı

bir araya getirilmiştir.

Bu yaklaşım, modern TLS protokollerinde kullanılan:

- RSA + AES
- ECDHE + AES

kombinasyonlarının mantığını birebir yansıtmaktadır.

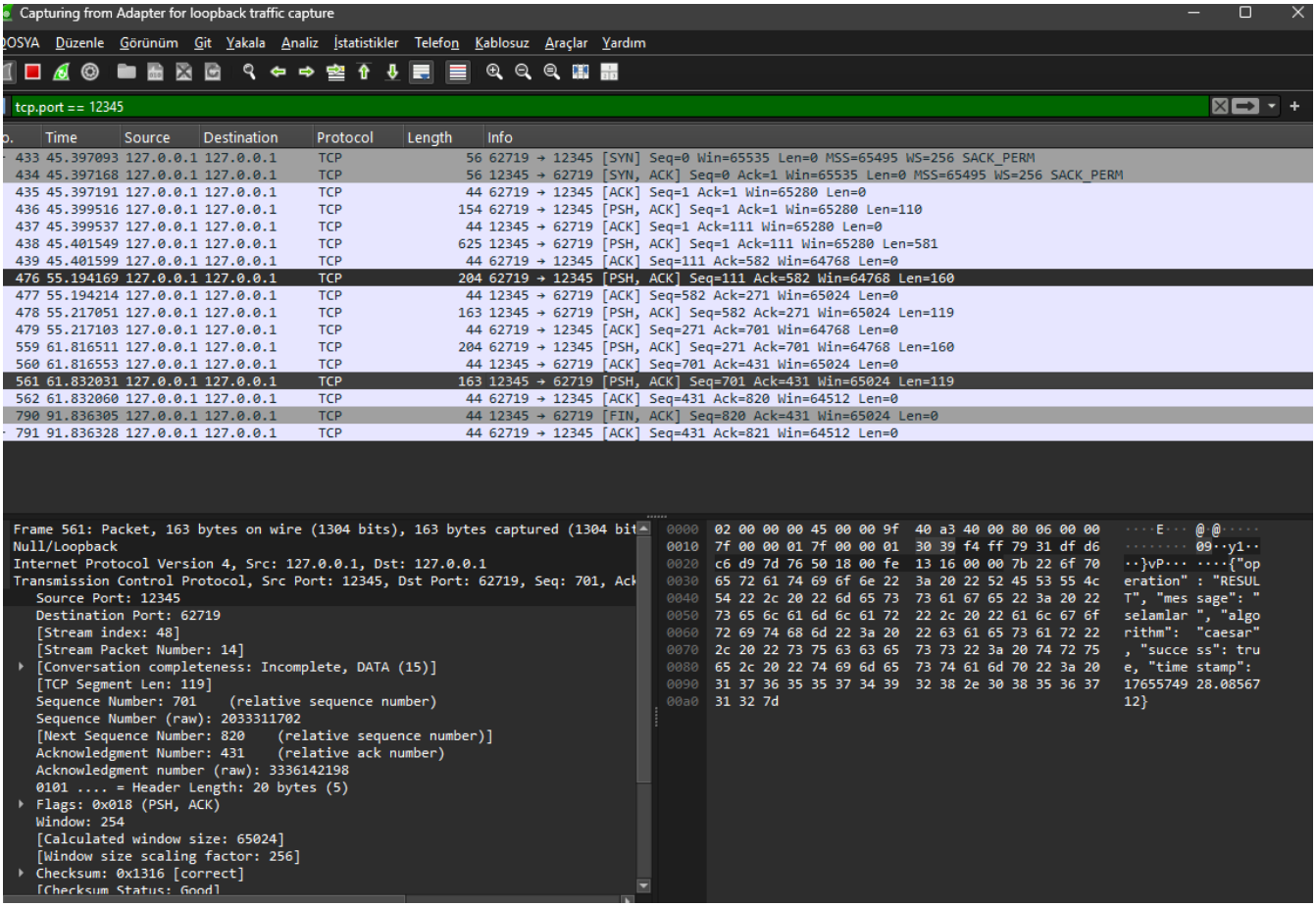


6. Wireshark Analizi ve Ağ Güvenliği Açısından Değerlendirme

Wireshark üzerinden yapılan incelemeler, kriptografinin ağ seviyesindeki etkilerini somutlaştırmıştır:

- Düz metin verinin tamamen gizlendiği
- Saldırganın yalnızca anlamsız byte dizileri görebildiği
- Paket boyutlarının kullanılan algoritmaya göre ciddi biçimde değiştiği

Bu analiz, “şifreleme yapılınca her şey güvenlidir” algısının yanlış olduğunu da göstermiştir. Yanlış algoritma seçimi, ağ performansını doğrudan olumsuz etkileyebilmektedir.



7. Genel Değerlendirme ve Öğrenilen Dersler

Bu proje sürecinde elde edilen en önemli kazanımlar şunlardır:

- Kriptografi yalnızca matematik değil, aynı zamanda sistem tasarımıdır
- Güvenlik, tek bir algoritma ile değil, bütüncül bir mimari ile sağlanır
- Manuel implementasyonlar, algoritmaların gerçek doğasını anlamak için vazgeçilmezdir
- Ağ trafiği analiz edilmeden yapılan güvenlik iddiaları eksik kalır

8. Sonuç

Bu çalışma, güvenli istemci–sunucu haberleşmesinin yalnızca güçlü algoritmalarla değil; **doğru mimari**, **hibrit şifreleme**, **paketleme stratejileri** ve **ağ seviyesi analizlerle** mümkün olduğunu göstermiştir. Proje, teorik kriptografi bilgisini pratik ağ güvenliği uygulamalarıyla birleştiren kapsamlı ve öğretici bir çalışma olarak tamamlanmıştır.