|  |  |  |
| --- | --- | --- |
|  | **MARMARA ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ** |  |

**5G VE WIRELESS TEKNOLOJİLERİNDE KULLANILAN ŞİFRELEME ALGORİTMALARIN ANALİZİ**

BERKE SERTEL

**YÜKSEK LİSANS TEZİ** Mekatronik Mühendisliği Anabilim Dalı

**DANIŞMAN**

Dr. Öğr. Gör. Uğur Kesen

**EŞ-DANIŞMAN**

İSTANBUL, 2025

|  |  |  |
| --- | --- | --- |
|  | **MARMARA UNIVERSITY**  **INSTITUTE FOR GRADUATE STUDIES IN PURE AND APPLIED SCIENCES** |  |

**ANALYSIS OF THE ENCRYTION ALGORITHMS IN 5G AND WIRELESS TECHNOLOGIES**

BERKE SERTEL

**MASTER THESIS**

Department of Mechactronics Engineering

**Thesis Supervisor**

Dr. Öğr. Gör. Uğur Kesen

**Thesis CO- Supervisor**

ISTANBUL, 2025

|  |
| --- |
| **Kabul ve Onay Belgesi (Türkçe)**  **Metindeki mor yazıları kendi tezinize uygun şekilde değiştiriniz. Bu metin kutusu ve gereksiz sayfaları siliniz.** |

**MARMARA ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ**

Marmara Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Öğrencisi Berke Sertel’in “**5G ve Wireless Teknolojilerinde Şifreleme Algoritmalarının analizi**” başlıklı tez çalışması, 20 Haziran 2025 tarihinde savunulmuş ve jüri üyeleri tarafından başarılı bulunmuştur.

**Jüri Üyeleri**

Dr. Öğr. Gör. Uğur Kesen (Danışman)

Marmara Üniversitesi (İMZA)

Dr. Öğr. Gör. Hüseyin Yüce (Üye)

Marmara Üniversitesi (İMZA)

Dr. Öğr. Üyesi Adı SOYADI (Üye)

Marmara Üniversitesi (İMZA)

**ONAY**

Marmara Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulu’nun ………… tarih ve ………… sayılı kararı ile Berke Sertel’in Mekatronik Mühendisliği Programında Yüksek Lisans derecesi alması onanmıştır.

**Fen Bilimleri Enstitüsü Müdürü Prof. Dr. Bülent Ekici**

|  |
| --- |
| **Kabul ve Onay Belgesi (İngilizce)**  **Metindeki mor yazıları kendi tezinize uygun şekilde değiştiriniz. Bu metin kutusu ve gereksiz sayfaları siliniz.** |

**MARMARA UNIVERSITY INSTITUTE FOR GRADUATE STUDIES IN PURE AND APPLIED SCIENCES**

Berke Sertel, a Master of Science student of Marmara University Institute for Graduate Studies in Pure and Applied Sciences, defended his thesis entitled “**Analysis of encryption algorithms in 5G and Wireless Technologies**”, on June 20, 2025 and has been found to be satisfactory by the jury members.

**Jury Members**

Dr. Lect. Uğur Kesen (Advisor)

Marmara University (SIGN)

Dr. Lect. Hüseyin Yüce (Jury Member)

Marmara Üniversitesi (SIGN)

Assist.Prof. Adı SOYADI (Jury Member)

Marmara Üniversitesi (SIGN)

**APPROVAL**

Marmara University Institute for Graduate Studies in Pure and Applied Sciences Executive Committee approves that Berke Sertel be granted the degree of Master of Science in Department of Mechatronics, Mechatronics Program on May 31, 2011. (Resolution no: 12345).

**Director of the Institute Prof. Dr. Adı SOYADI**

**ÖNSÖZ**

Bu yüksek lisans tez çalışmam süresince benden desteklerini, yardımlarını, zamanını esirgemeyen tez danışman hocam Dr. Öğr. Gör. Uğur Kesen’e teşekkür ederim.

Konu hakkında bana her türlü desteği veren, sorduğun her soruda sonuna kadar bana açıklama yapan sevgili hocam Dr. Öğr. Gör. Hüseyin Yüce’ye teşekkür ederim.

Bana her daim destek olan ve yanımda olan babam Kemal Haldun Sertel, annem Fatma Kumsal Sertel ve kardeşim Kaya Sertel’e,

Tezi yazma sürecinde bana yardımcı olan, Huawei firmasındaki yöneticim, Serhat Gül’e,

Bana yardımlarını esirgemeyen değerli arkadaşım Mehmet Zeki Sildir ve Zeynep Güler’e,

Bu yüksek lisans tezini ortaya çıkarmamda bana katkısı olan herkese,

Ve son olarak tüm katılımcılara,

Teşekkürü borç bilirim.

**July, 2024**



İÇİNDEKİLER

Ön Söz**I**

İÇİNDEKİLER**II**

ÖZETIII

ABSTRACT**IV**

SEMBOLLER**V**

KISALTMALAR**VI**

ŞEKİL TABLOSU**VI**

TABLO LİSTESİ**VI**

1.GİRİŞ**1**

- 1.1 Şifreleme ve Deşifreleme2

- 1.2 Şifreleme Algoritmaları2

- 1.2.1 Asimetrik Şifreleme Algoritmaları2

- 1.2.2 Simetrik Şifreleme Algoritmaları2

- 1.2.3 Asimetrik/Simetrik Algoritmaların Avantajlarının/Dezavantajları2

1.2.4 5G ve Wireless Teknolojilerde amaca uygun olan algoritmalar2

- 1.3 Public/Private Key2

- 1.3.1 Public Key Encryption 2

- 1.3.2 Public/Private Key2

- 1.4 5G Teknolojisinin Gelişimi2

- 1.5 Wireless Teknolojisi Gelişimi2

- 1.6 Amaç ve Önem2

- 1.7 Literatür Araştırması5

- 1.7.1 Şifreleme Algoritmalarıyla ilgili yapılmış olan çalışmalar5

- 1.7.2 5G teknolojilerinde şifreleme algoritmalarıyla ilgili yapılmış olan çalışmalar5

- 1.7.3 Wireless ile ilgili şifreleme algoritmalarıyla ilgili yapılmış olan çalışmalar5

2- Materyal ve Yöntem5

- 2.1 Kullanılacak olan şifreleme algoritmaları5

- 2.2 Visual Studio IDE’si5

- 2.3 OpenSSL Kütüphanesi5

- 2.3.1 OpenSSL’in kurulumu5

- 2.3.2 OpenSSL kütüphanesinin IDE’ye entegre edilip test edilmesi5

- 2.4 C++ Programlama Dili5

- 2.4.1 C++ dilinin kullanım alanları5

- 2.4.2 Neden C++ dili kullanılıyor5

- 2.5 Git Bash5

3- Bulgular ve Tartışma5

- 3.1 OpenSSL kütüphanesindeki algoritmaların test edilmesi5

- 3.1.1 Performans açısından analiz edilmesi5

- 3.1.2 Güvenilirlik açısından analiz edilmesi5

- 3.1.3 Parametrelerin Fayda Optimizasyonuna göre değerlendirilmesi5

- 3.2 Elde edilen bulguların Grafiğe Dökülmesi5

4- Sonuç5

5- Referanslar5



IV

Tarih boyunca insanlar birbirlerine gizli verileri gönderirken özellikle 3.kişilerin ellerine geçmemesini hedeflenmiştir. Verilerin gizlenmesinde geçmişten günümüze çok sayıda farklı yöntem kullanılmıştır. Bunların en örneklerinden bir tanesi Almanların 2. Dünya savaşında kullanmış olduğu Enigma makinesidir. Bu makine verileri gönderirken o zamanın teknolojisiyle çözülmesi son derece zor bir algoritma ile verileri göndermekteydi. Bu örnek aynı zamanda haberleşirken veri şifreleme yönteminin önemli bir örneğidir. O zamandan günümüze şifreleme algoritmalarında ciddi anlamda bir gelişme göze çarpmaktadır. Bu tez çalışmasında da hayatımıza yeni yeni girmekte olan 5G ve Wireless teknolojilerde hangi algoritmaların kullanıma daha elverişli olduğunun analizi yapılmıştır.

**5G VE WİRELESS TEKNOLOJİLERİNDE KULLANILAN ŞİFRELEME ALGORİTMALARI**

**ÖZET**

Veri Şifreleme algoritmaları, herhangi verinin taşınırken veya bilgisayarda kayıtlıyken dışardan gelebilecek saldırılara karşı korunmasını sağlayan ve pek çok farklı çeşidi olan algoritmalardır. Bu algoritmaların, her ne kadar tehlikelerden korunmak için de kullanmak bazen bu saldırıların engellenmesi mümkün olamayabilir. Bu yüzden bu tezin önemli kısımlarından biri de olası saldırı durumlarında söz konusu algoritmaların güvenlik açısından ne oranda yeterli olduğunun analiz edilmesidir. Bu algoritmaların hepsi farklı yöntemleri kullanarak verilerimizin güvenliği sağlamaktadır ancak bu algoritmaların sanal fidye programları gibi kötü amaçlar için de kullanılabileceği unutulmamalıdır.

Veri şifreleme algoritmaları, OpenSSL 3.parti kütüphanesinin de hayatımıza girmesiyle beraber programlamada sıkça kullanılır bir hale gelmiş oldu. OpenSSL kütüphanesi, herhangi bir programa dilinin SL(Standard Library)'inde yer almadığından dolayı bu kütüphane kod yazmanın tek yolu bu kütüphanenin çalışılan IDE(Integrated Development Environment)'ye entegre edilmesidir. OpenSSL kütüphanesi sadece veri şifreleme algoritmalarını değil aynı zamanda da güvenlik veri taşımada son derece önemli bir yere sahip SSL ve TLS protokollerini de içermektedir. Bu kütüphanede mevcut olup bu yüksek lisans tezinde de kullanılacak olan algoritmalardan bazıları: AES, RSA, Chacha20, DSA, Camellia, Seed gibi algoritmalardır.

Bu algoritmalar, analiz edilirken iki parametre çok önemli yere sahip olacaktır. Bunlar güvenilirlik ve performans parametreleridir. Bir veri şifreleme algoritması değerlendirilirken bir özellik bakımından çok iyi ama diğeri açısından da en azından iyi olması gerekir. Bu tez kapsamından bu kriterler göz önünde bulundurularak bir analiz yapılmıştır. Elde edilen analiz sonuçlarından bir grafik elde edilip bir sonuca ulaşılacaktır.

Bu yüksek lisans tezi temelde 3 adımdan oluşmaktadır. İlk olarak OpenSSL kütüphanesindeki şifreleme algoritmaları kullanılarak algoritmalara ilişkin sınıflar oluşturulacaktır. Oluşturulan sınıflar için çeşitli test case durumları oluşturularak farklı durumlar için algoritmaların nasıl çalıştıkları test edilecektir. Elde edilen test sonuçlarına bağlı olarak farklı durumlar için farklı grafikler elde edilerek bir sonuca varılacaktır.

Throughout history, people have aimed to send secret data to each other without it falling into the hands of third parties. Various methods have been used to hide data from the past to the present. One of the most notable examples is the Enigma machine used by the Germans during World War II. This machine transmitted data using an algorithm that was extremely difficult to decipher with the technology of that time. This example also represents a significant case of data encryption methods in communication. Since then, there has been a remarkable development in encryption algorithms. This thesis analyzes which algorithms are more suitable for use in the emerging 5G and wireless technologies.

Data encryption algorithms are used to protect data from external attacks while being transmitted or stored on computers, and there are many different types of these algorithms. Although these algorithms are used to protect against threats, sometimes it may not be possible to prevent such attacks. Therefore, one of the important aspects of this thesis is to analyze the security sufficiency of these algorithms in case of potential attacks. These algorithms ensure the security of our data using different methods, but it should not be forgotten that they can also be used for malicious purposes, such as ransomware programs.

With the introduction of the OpenSSL third-party library, data encryption algorithms have become frequently used in programming. Since the OpenSSL library is not included in the standard library of any programming language, the only way to write code using this library is to integrate it into the IDE (Integrated Development Environment) being used. The OpenSSL library not only includes data encryption algorithms but also the SSL and TLS protocols, which are extremely important for secure data transmission. Some of the algorithms available in this library and used in this master's thesis include AES, RSA, ChaCha20, DSA, Camellia, and SEED.

While analyzing these algorithms, two parameters will be of utmost importance: reliability and performance. When evaluating a data encryption algorithm, it should perform very well in one aspect and at least good in the other. In this thesis, an analysis is conducted considering these criteria. A graph will be generated based on the analysis results, leading to a conclusion.

This master's thesis fundamentally consists of three steps. First, classes related to the algorithms will be created using the encryption algorithms in the OpenSSL library. Various test cases will be generated for the created classes to test how the algorithms perform in different scenarios. Based on the test results obtained, different graphs will be produced for different scenarios, leading to a conclusion.

**ANALYSIS OF THE ENCRYPTION ALGORITHMS IN 5G AND WIRELESS TECHNOLOGIES**

**ABSTRACT**

**YENİLİK BEYANI/**



**SEMBOLLER/SYMBOLS**

**E :** Public Key

**D :** Private Key

**T :** Totient

**N :** Aktif kural sayısı

**S :** Kanal kesit alanı (m2)

**t :** Zaman (s)

**T :** Sıcaklık (°C)

** :** Hava hızı (m/s)

**wi :** Üyelik fonksiyonunun maksimum seviyeye ulaştığı değer

**8 :** Hız hata toleransı

**A(x) :** x’in A bulanık kümesindeki değeri

**KISALTMALAR/ABBREVIATIONS**

**AES :** Advanced Encryption Standards(Türkçeleri eklenecek)

**CT :** Cipher Text

**DES :** Data Encryption Algorithm

**DH :** Diffie Helman

**DSA :** Digital Signature Algorithm

**FTP :** File Transfer Protocol

**PT :** Plain Text

**RC4 :** Rivest Encryption

**RSA :** Rivest-Shamir-Adleman

**SSL :** Secure Sockets Layers

**TLS :** Transfer Layer Protocol

**ŞEKİL**

xi

**TABLO LİSTESİ/LIST OF TABLES**

xiii

**Tez Şablonu**

1

**Bölümlerin genel düzeni aşağıdaki gibi olmalıdır.  
Bu metin kutusu ye gereksiz metinleri siliniz.**

# 1. GİRİŞ/INTRODUCTION

## Kriptografi, güvenli iletişim verilerin korunmasını sağlayan bilim dalıdır. Kriptografi kelimesi aslında Antik Yunanca ‘da gizli anlamına gelen "kriptos" ve yazı anlamına gelen "graphi" kelimelerinden gelmektedir. Bu bilim dalının hayatımıza girişiyle birlikte veri şifreleme de hayatımıza girmiş oldu. Veri şifreleme geçmişte günümüze pek çok farklı alanda kullanılmıştır çünkü tarih boyunca insan birbirleriyle haberleşirken verilerin gizli tutulmasına önem vermiştir. Kısacası veri şifreleme Alan Turing'in bilgisayarı icat etmesiyle hayatımıza girmemiştir aslında haberleşmede gizliliğin önemli olduğu her yerde veri şifreleme teknikleri kullanılmıştır. Kriptoloji aslında bir matematik bilimidir ve genelde sayılar teorisi üstüne kurulmuştur.

## Tarihte ilk kriptolog, yaklaşık olarak milattan önce 20.yüzyılda Mısırda yaşamış olan bir katiptir. Bu kâtip efendisinin hayatının yazarken hiyeroglifleri şifrelenmiş bir şekilde oluşturmuştur. Ayrıca yazılan bazı hiyeroglifler o zamana kadar daha önce hiç kullanılmamıştı. Her ne kadar kriptografi bu şekilde ortaya çıksa da Milattan önce 1000 yılına kadar çok da bir ilerleme kaydedememiştir. Dünyanın farklı farklı yerlerinde bağlantısız bir şekilde en temel biçimde kullanılmıştı ancak medeniyetlerin yıkılışıyla ileriki adımlara geçilememişti.

## Ancak daha sonralarında (M.Ö. 6. yüzyıl) askeri istihbarat son derece önemli hale geldiğinden olsa gerek gelişimi hızlandı. O zamanda bu zamana istihbarat çok gelişti ve bununla beraber de kriptografi de bambaşka bir noktaya geldi. Bu yüksek lisans tezinin temeli de 5G ve Wireless teknolojilerinde kullanılmakta olan veya ilerde kullanılması muhtemel olan kriptografik algoritmaların güvenlik ve performans açısından analizi içermektedir.

Yapılan değerlendirmeler sonucunda algoritmalara ait farklı veriler farklı grafiklere dökülerek analiz edilecektir. Bu değerlendirmeler yapılırken algoritmaların private/public key kullanması ve algoritmaların verileri şifrelerken nasıl bir yol izleyeceği gibi konulara değinilecektir. Bu durumlar incelenirken günümüzde son derece popüler bir programlama dili olan C++ programlama dili kullanılacaktır. C++ 'ın yanı sıra veri güvenliğinde son derece önemli bir yere sahip olan OpenSSL 3.parti kütüphanesi de bu tez hayata geçirilirken kullanılmıştır. OpenSSL kütüphanesinin belli başlı elemanları verilerin güvenli taşınmasında kullanılan SSL/TLS protokolleri ve veriler taşınırken kimsenin eline geçmemesini için verilerin şifrelenmesini sağlayan veri taşıma protokolleridir. Bu protokollere ek olarak bu kütüphane veri şifreleme algoritmalarını da içerisinde barındırmaktadır.

* 1. **Şifreleme ve Deşifreleme**

Geçmişten günümüze veri korunumu son derece önemli olmuştur. Veri korunmasında en popüler yöntemlerden biri de veri şifrelemedir. Günümüzde Wireless, Bulut teknolojileri çok yaygın bir şekilde kullanılması sadece faydalı görünse de aslında pek tehlikeyi de beraberinde getirmiştir. Özellikle bu tarz veri taşınması gereken alanlarda şifreleme veri korunumunda son derece önemli bir yere sahiptir. Şifrelemenin hayatımıza girmesiyle birlikte veriler daha güvenilir bir şekilde taşınır hale gelmiştir. [1]

Veri Şifreleme ile ilgili yapılan ilk tez çalışmalarından bir tanesi 1945 yılında Claude Shannon tarafından yazılmış olan “A Mathematical Theory of Cryptography” isimli çalışmada şifreleme ve bilgi teorisinin temellerini atan bu çalışma, kriptografinin bilimsel bir disiplin olarak gelişmesini sağlayacaktır.[2]

Bu çalışmadan sonra matematiksel şifreleme teorisinin temellerini atan, 1976 yılında, Whitfield Diffie ve Martin Hellman tarafından yazılmış olan “New Directions in Cryptograhy” isimli makale ile birlikte kriptografinin bilimsel bir disiplin olarak gelişmesi sağlanmıştır.[3]

Akabinde 1977 yılında yazılmış olan, Açık anahtar kriptografi konseptini ilk defa ortaya atan, soyadlarıyla RSA algoritmasına da adını veren, Ronald Rivest, Adi Shamir ve Leonard Adleman tarafından yazılmış olan, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems” çalışmasıyla birlikte, kriptografinin geleceği şekillenmiştir. [4]

Veri şifreleme kullanıcılara ait özel verilerin bir yerden bir başka yere taşınırken dışardan gelebilecek saldırılara karşı alınmış olan bilgi koruma önlemidir. Günümüzde son derece sık kullanılan bir veri koruma yöntemidir. Şifreleme pek çok farklı araç için yapılabilir ancak bu yüksek lisans tez kapsamında bizim dikkate alacağımız kısım yazıların ve dosyaların şifrelenmesi ve deşifrelenmesini temel alarak ortaya konulacaktır.

Şifrelemenin en bilinen tiplerinden bir tanesi basit şifrelemedir. Bu tarz şifrelemelerde bir veri tüm kullanıcılara aynı şifreleme algoritmasını kullanarak gönderilmektedir.

### Bu yöntem şüphesiz ki güvenlik açısından son derece tehlikeli bir yöntemdir. Bu sebeple mümkün mertebe veri şifreleme algoritmalarının değişiklik göstermesi tercih edilmelidir.

### Basit şifrelemeden daha üstün olan bir yöntem ise anahtara dayalı şifreleme (Key Based Encryption(KYB)) yöntemidir. Bu tip şifrelemede rastgele üretilen anahtarlar kullanılarak yapılan şifrelemeye verilen isimdir. Bu anahtarlar algoritmaların tipine bağlı olarak public veya private key olabilir. Bir yazı şifrelenirken kullanılacak en basit yöntem anahtar kullanılarak yapılan şifrelemedir. Tahmin edebileceğimiz gibi anahtar karmaşıklığı arttıkça algoritmanın güvenliği de doğru oranlığı olarak artmaktadır. Günümüzde basit şifreleme yerine KYB tipi şifreleme tercih edilmektedir. Anahtara dayalı şifreleme yönteminde genelde makine tarafından rastgele üretilmiş son derece karmaşık ve ancak matematiksel yollar kullanılarak bulunabilecek anahtarlarla yapılan şifrelemelerdir. Bu tarz anahtarları temel alarak yapılan şifrelemelere şifreleme algoritmaları bölümünde değinilecektir.

### Yazı şifreleme yapılırken temelde 3 temel eleman göze çarpmaktadır. Bunlar:

### 1-) Anahtar (Key)

### 2-) Şifrelenmemiş/Deşifrelenmiş Yazı (Plain Text)

### 3-) Şifrelenmiş Yazı (Cipher Text)

### **1.2 Şifreleme Algoritmaları**

Bu yüksek lisans tez çalışması kapsamında OpenSSL kütüphanesinde bulunan algoritmalardan bazıları kullanılacaktır. Kullanılacak olan algoritmalar özellikle 5G ve Wireless teknolojilerinde sıkça tercih edilen algoritmalar olmasına dikkat edilmiştir. Örneğin OpenSSL kütüphanesinde bulunan DES, AES, RSA, DH, RC4 gibi algoritmalar 5G ve Wireless teknolojilerde son derece sık kullanılan veri şifreleme algoritmalarından bazılarıdır. Bu algoritmaların çalışma prensipleri ve kategori analizleri bölüm 1.2.1 ve bölüm 1.2.2'de yapılacaktır. Şifreleme algoritmaları temelde asimetrik ve simetrik algoritma olmak üzere ikiye ayrılır.

Simetrik algoritmada hem şifreleme hem de deşifreleme aynı anahtar kullanılarak yapılır. Ancak asimetrik algoritmalarda şifrelemede farklı anahtar deşifrelemede farklı anahtar kullanılmaktadır. Her ne kadar asimetrik algoritmalar çoğunlukla daha güvenlidir denilse de bu durum her zaman böyle değildir. Çünkü güvenlik seviyesinin etkileyen bir başka kavram da şifreleme algoritmasının kullanacağı anahtarın uzunluğudur. Anahtarların uzunlukları ve karmaşıklıkları arttıkça dolaylı olarak algoritmanın güvenliği de artmaktadır. Anahtar uzunlukları veri şifreleme algoritmalarına bağlı olarak değişmektedir.

### **1.2.1 Simetrik Şifreleme Algoritmaları**

Daha öncesinde değindiğim gibi simetrik şifreleme algoritmalarında tek bir anahtar(key) kullanılmaktadır.

Simetrik şifreleme algoritmalarıyla ilgili ülkemizde çalışmalardan bir tanesi Fatih Özkaynak tarafından 2013 yılında yazılan “Kaos tabanlı simetrik şifreleme tasarım ve analizi” isimli doktora tezi çalışmasıdır.[5]

Başka bir çalışma ise Çağdaş Gül tarafından 2022 yılında yazılan “Spn Yapıdaki simetrik şifreleme algoritmalarının tasarımı, güvenliği ve performans analizleri” isimli yüksek lisans tezidir.[6]

2020 yılında ise, Mohammed N. Alenezi, Haneen Alabdulrazzaq and Nada Q. Mohammed tarafından yazılan olan “Symmetric Encryption Algorithms: Review and Evaluation study” isimli makale ile simetrik algoritmaların analizleri yapılmıştır.[7]

Bu anahtar hem şifrelemede hem de deşifrelemede kullandığında buna simetrik şifreleme algoritması adı verilir. Aşağıdaki şekil 1.1’de bununla ilgili bir örnek gösterilmiştir. Örnekte "hello" yazısı için şifreleme şifreleme ve deşifreleme yapılırsa anahtar 3 olarak alındığı takdirde hem şifreleme hem de deşifreleme bir anahtar kullanılarak yapılacaktır.

A close-up of a computer code

Description automatically generated

**Şekil 1.1 –** Simetrik Şifreleme ve Deşifreleme

Burada anahtar(key) 3 olduğundan dolayı sırasıyla tüm karakterler 3 adım ilerideki karakterlere dönüşerek şifreleme işlemini gerçekleştirecektir. Örneğin burada sırasıyla h harfi 3 alfabede ileri giderek k, e harfi 3 adım ileri giderek h, l harfleri 3 adım giderek o harfi ve son olarak o harfi 3 adım ileri giderek r harfine dönüşmüştür. Bunun yapılması sırasında karakterlerin alfabede ilerleme durumları aşağıdaki Şekil 1.2’de gösterilmiştir.

A yellow and black text

Description automatically generated

**Şekil 1.2 –** Simetrik Şifrelemede Alfabe

Deşifreleme sırasında da durum tam tersidir. Şifrelemenmiş durumdaki harfler sırasıyla alfabede geri gelerek deşifreleme işlemini gerçekleştirirler. Aşağıdaki şekildeki alfabede örneğin 'h' harfi için ne kadar ileri gidileceği gösterilmiştir. Buna göre 3 adım ilerideki k harfi elde edilecektir. Ancak anahtar 5 olsaydı bu durumda 5 adım ileri gidilerek buradaki harf olan 'm' harfi elde edilecekti. Simetrik algoritmalar arasında en popüler olanları: DES, RC4, 3DES, AES, Seed, Camellia ve Chacha20 algoritmalarıdır. Bu algoritmaların çoğu bu yüksek lisans tezi kapsamında C++ kodunda OpenSSL kütüphanesinin desteğiyle test edilmiştir. Günümüzde diğerlerine göre daha az kullanılan olan DES algoritmasıdır. Popülerliği en yüksek olanlardan biri ise şüphesiz ki AES (Advanced Encryption Standards) algoritmasıdır. Bu yüksek lisans tezi kapsamında başta AES algoritması olmak üzere belirtilen tüm algoritmaların performans ve verimlilik açısından analizleri yapılacaktır.

### **1.2.2 Asimetrik Şifreleme Algoritmaları (Özel karakter-büyük harfler-noktalama işaretlerinde şifreleme de eklenecek)**

Asimetrik algoritmalarda daha öncesinde bahsettiğimiz gibi şifreleme için farklı, deşifreleme için farklı bir anahtar kullanılır.

Asimetrik algoritmalarla ilgili yapılan önemli çalışmalardan bir tanesi Burak Baysan tarafından yazılan “sayısal veri ve deliller için küp tabanlı çok boyutlu asimetrik şifreleme yöntemi” isimli yüksek lisans tezidir. Bu çalışmada asimetrik algoritmalara farklı yaklaşım getirilmiştir.[8]

Bu konuda ülkemizde yapılan bir diğer önemli yüksek lisans tezi ise Mohammad Rahiq Baigzad tarafından 2021 senesinde yazılmış olan “RSA Yönteminde güvenlik açığı ve güçlendirilmiş RSA yöntemlerinin incelenmesi ile önerilen bir hibrit şifreleme modelinin ağ güvenliği açısından değerlendirilmesi” isimli tezdir. Bu tez, ağ güvenliği alanında RSA algoritmasının değerlendirmesini içermektedir.[9]

Bir başka önemli çalışma ise Shahzadi Farah, M. Younas Javed, Azra Shamim ve Tabassam Nawaz tarafından yazılmış olan “An experimental study on Performance Evaluation of Asymmetric encryption algorithms” isimli makaledir. Bu makalede asimetrik algoritmaların performans analizine değinilmiştir.[10]

Örneğin simetrik algoritmada verdiğimiz örneği asimetrik algoritma için verecek olursak, bir "hello" yazısını ele alalım. Burada şifreleme kullanılan anahtar 5 olarak belirlenmiştir. Ancak deşifreleme için farklı bir anahtar belirlenmiştir ve bu anahtar değeri de 21 olacaktır. Bu örnek ile ilgili şekil aşağıdaki gibidir.

A close-up of a computer code

Description automatically generated

**Şekil 1.3 –** Asimetrik Şifreleme ve Deşifreleme

Burada deşifreleme anahtarının 21 sebebi aslında alfabede şifreleme için ileri deşifreleme için ise geri gidilmesi yerine ileri gidilmeye devam edilerek ilk baştaki harf elde edilecektir. Aşağıdaki şekilde bulunan alfabede nasıl ilk karaktere ulaşıldığı gösterilmiştir.

A black and yellow text with purple arrow

Description automatically generated

**Şekil 1.4**

Simetrik algoritmalardan bazıları: DSA, RSA, DH, ECDSA, ECDH algoritmalarıdır. Bu algoritmaların çoğu bu yüksek lisans tezi kapsamında C++ kodunda OpenSSL kütüphanesinin desteğiyle test edilmiştir.

**1.2.3 Asimetrik/Simetrik Algoritmaların Avantajlarının/Dezavantajları**

Asimetrik ve simetrik algoritmalar hakkında yapılan ilk çalışmalardan biri olan ve 1979 yılında, Gustavus J. Simmons tarafından yazılan “Symmetric and Asymmetric Encryption” isimli makaledir. Bu makalede sismetik ve asimetrik şifreleme incelenmiştir.[11]

Ülkemizde ise bu alanda 2016 yılında Ünal Çavuşoğlu tarafından yazılmış olan “Kaos tabanlı hibrit simetrik ve asimetrik şifreleme algoritmalarının tasarımı ve uygulaması” isimli doktora tez çalışmasıdır.[12]

Ardından Burcu Sönmez tarafından yazılmış olan “Simetrik ve asimetrik şifreleme algoritmalarına yan kanal saldırıları uygulanması ve anormallik tespiti” isimli yüksek lisans tez çalışmadır.[13]

Asimetrik algoritmalar yavaş çalışmasına karşın simetrik algoritmalara kıyasla daha güçlü olduklarından daha güvenli bir şifreleme yapılmasına imkân sağlarlar. Güçlü olmasının sebebi de temelde daha karmaşık ve uzun anahtarlar kullanmasından kaynaklanmaktadır bu da şüphesiz CPU kullanımını arttırmaktadır. Simetrik algoritmalarda ise deşifreleme için bir private key kullanılacağı için bu anahtarların paylaşılması gibi zorunluluk söz konusu değildir. Bu da bu algoritmaların daha güvenlikli bir şekilde çalışmasına imkân sağlamaktadır. Duruma bağlı seçilebilirlik açısından daha küçük verilerin taşınmasında özellikle verim kritik yerlerde tercih edilebilir. Verimin çok da önemli olmadığı alanlarda biraz daha büyük verilerin de taşınmasında kullanılabilir. Güvenliğin verimden çok daha önemli olduğu ayrıca bellek açısından bir problem yaşamayacağımız alanlar için büyük verilerin taşınmasında da kullanılabilir. Kısaca asimetrik algoritmalar simetriğe göre daha güvenilirdir ancak simetrik algoritmalara göre verimsizlerdir.

**1.2.4 5G ve Wireless Teknolojilerde amaca uygun olan algoritmalar**

Wireless teknolojinin ardından son yıllarda hayatımıza giren 5G teknolojisiyle birlikte, bu alanda bilgi güvenliği önemli bir hale geldi. Bundan dolayı veriler tanışınırken güvenlik amaçlı şifreleme algoritmalarının da önemi arttı.

5G ve Wireless konusunda, ülkemizde yapılan önemli çalışmalaradan biri, Samira Suleymanova tarafından yapılmış olan “5G teknolojisi için düşük gürültülü yükselteç tasarımı” isimli yüksek lisans tez çalışmasıdır. Ancak bu tezin veri şifreleme algoritmalarıyla bir alakası yoktur.[14]

5G alanında şfirelemede ise yurtdışında yapılan önemli çalışmalardan bir tanesi, Kosei Sakamoto, Fukang Liu, Yuto Nakano, Shinsaku Kiyomoto ve Takanori Isobe tarafından, 2021 yılında yazılan “Rocca: An efficient AES based Encryption Scheme for Beyond 5G” isimli makaledir.[15]

Bunun ardından 2022 yılında Khalid Fadhil, Kayhan Zrar Ghafoor ve Halgurd S.Maghdid tarafından yazılmış olan “Analysis of Encryption Algorithms Proposed for Data Security” isimli makaledir. [16]

2.Materyal ve Yöntem

Bu yüksek lisans tez çalışması kapsamında kodun yazılmasında Microsoft Visual Studio IDE (Kısaltmalar kısmına eklenecek)’si kullanılacaktır. Bu IDE windows apilerini barındırması ve sağladığı kod yazım kolaylıkları göz önünde bulundurulduğunda seçilebilir olarak son derece uygundur. Visual Studio IDE'si ile birlikte 3.parti OpenSSL kütüphanesine yer verilecektir. OpenSSL kütüphanesi güvenli veri tanışmasında kullanılan TLS ve SSL veri taşıma protokollerinin yanı sıra bu tezin temelini oluşturan veri şifreleme algoritmalarını da barındıran bir 3.parti kütüphanedir. OpenSSL kütüphanesindeki bazı başlıca algoritmalar: AES, DH, RSA ve benzeri algoritmalardır. OpenSSL standart kütüphaneye ait olmadığından, IDE'ye entegre edilmesi bir mecburiyettir.

Bu araçların yanı sıra günümüzde son derece popüler bir programlama dili olan C++ programlama dili kullanılacaktır. C++ dilinin sürekli C++ standart komitesi tarafında gelişir durumda olması, programlama dillerinin temeli olan C dilini temel alarak ortaya çıkar bir dil olması şüphesiz ki seçile bilirliğini arttırmaktadır. C++ dili aynı zamanda C dilinin üzerine koyarak gittiğinden dolayı son derece gelişmiş modern araçlara sahip bir programlama dilidir. Buna ek olarak C++ dili optimizasyon anlamında son derece gelişmiş olduğundan özellikle verimin kritik olduğu alanlarda son derece kullanışlı bir programlama dili olma özelliği gösterir. Günümüzde, başta savunma sanayi olmak üzere gömülü sistemlerin olduğu pek çok sektörde kullanılmaktadır.

**2.1 Kullanılacak olan Şifreleme algoritmaları**

Yapılan çalışmada OpenSSL kütüphanesinde de bulunan veri şifreleme algoritmalarına yer verilmiştir. Tezin bu bölümünde kullanılan şifreleme algoritmalarının nasıl çalıştığı hakkında bilgi verilmiştir.

**2.1.1 AES Şifreleme Algoritması**

AES algoritması, 2001 yılında ABD Ulusal Standart ve Teknoloji Enstitüsü(NIST) tarafından bulunan veri şifrelemede sıkça kullanılan simetrik bir şifreleme algoritmasıdır. Sadece public key kullanmasına karşın güvenilir simetrik algoritmalardan biridir. Özellikle de DES algoritmasının kırılmasıyla birlikte bu algoritmanın bulunmasının yolu açılmıştır. Bu algoritma DES algoritmasına göre daha güvenilir olduğundan tercih edilmektedir. Günümüzde DES algoritması çok kullanılmaktadır bunun en önemli nedeni ise AES algoritmasına kıyasla yaklaşık olarak 6 kat daha hızlı çalışmaktadır. Buna göre veri güvenliğinin çok da önemli olmadığı hızın yani performansın önemli olduğu yerlerde DES algoritması tercih edilirken, performanstan çok veri güvenliğinin önemli olduğu alanlarda ise AES algoritması daha yaygın bir şekilde kullanılmaktadır. Bu algoritmada private key uzunlukları değişiklik gösterebilir. Örneğin 128 bit, 192 bit veya 256 bitlik private key ile bu algoritma kullanılabilir. Şüphesiz anahtar uzunluğu arttıkça algoritmanın çözülmesi de zorlaşmakla birlikte üretim aşaması dolasıyla verimi de düşmektedir. AES algoritmasında yazı şifrelenirken sırasıyla aşağıdaki adımlar aşağıdaki gibidir:

**2.1.2 DH Şifreleme Algoritması**

**2.1.3 RSA Şifreleme Algoritması**

**2.1.4 Seed Şifreleme Algoritması**

**2.1.5 Camellia Şifreleme Algoritması**

**2.1.6 DSA Şifreleme Algoritması**

- 2.1 Kullanılacak olan şifreleme algoritmaları5

- 2.2 Visual Studio IDE’si5

- 2.3 OpenSSL Kütüphanesi5

- 2.3.1 OpenSSL’in kurulumu5

- 2.3.2 OpenSSL kütüphanesinin IDE’ye entegre edilip test edilmesi5

- 2.4 C++ Programlama Dili5

- 2.4.1 C++ dilinin kullanım alanları5

- 2.4.2 Neden C++ dili kullanılıyor5

- 2.5 Git Bash5



**Şekil 1.1.** Fen Bilimleri Enstitüsü logosudur.

**Tablo 1.1.** Tablo düzeni örneğidir.

|  |  |  |  |
| --- | --- | --- | --- |
| Parametre | Numune 1 | Numune 2 | Numune 3 |
| pH | 7,2 | 8,1 | 6,8 |
| Sıcaklık (oC) | 22 | 21 | 23 |
| Klor (mg/L) | 1,23 | 1,66 | 2,56 |

**KAYNAKLAR/REFERENCES**

3

**Çeşitli örnekler aşağıda verilmiştir**

**Makale:**

Yazar soyadı, yazar adının baş harfi., (yayın yılı). Makale Adı. Derginin Adı, cilt numarası (varsa parantez içinde sayısı), sayfa numaraları.

*Orn.*

Ercan, S. (1974) Cost Minimizing Single Sampling Plans with AIQL and AOQL Constaints. Management Science, Theory Series, 20, 1112-1122.

Hellinga, C., Schellen, A.A.J.C., Mulder, J.W., van Loosdrecht, M.C.M., Heijnen, J.J. (1998) The SHARON process: An innovative method for nitrogen removal from ammonium-rich waste water. Water Science and Technology, 37(9), 135-142.

Liu, J.X., Liang, Z. (2008) Landfill leachate treatment with a novel process: Anaerobic ammonium oxidation (Anammox) combined with soil infiltration system. Journal of Hazardous Materials, 151(1), 202-212.

**Bildiri:**

Yazar soyadı, yazar adının baş harfi., (yayın yılı). Bildiri Adı. Bilimsel Toplantının Adı, bilimsel toplantının düzenlendiği tarih ve şehir.

*Orn.*

Acar, M.H., Yılmaz, P. (1997) Effect of Tetramethylthiuramdisulfide on the Cationic Polymerization of Cylohexeneoxide. The 2nd International Conference on Advanced Polymers via Macromolecular Engineering, 2-14 August, Orlando, Florida, USA.

**Kitap:**

Yazar soyadı, yazar adının baş harfi., (yayın yılı). Kitabın Adı, cilt numarası (var ise) ve kaçıncı baskı olduğu, Yayınevi, Yayımlandığı şehir.

*Orn.*

Bowersock, T.L., Park, K., Kosswig, K. (1997) Vaccines and Other Immunological Products, Encyclopedia of Pharmaceutical Technology, 1st Edition., Swarbrick, J., Boylan, J.C. Editors.; Marcel Dekker, Inc., New York, USA.

Çetmeli, E., Çakıroğlu, A., Uludağ, E. (1976) Yapı Statiği II, İ.T.Ü İnşaat Fakültesi Matbaası, İstanbul, Türkiye.

**Tezler:**

4

Gümüş, F.U. (1998) Endosulfan’ın Kalıntı Analizlerine Uygun Yeni Yöntemlerin Geliştirilmesi. Doktora Tezi*,* Marmara Üniversitesi Fen Bilimleri Enstitüsü, İstanbul, Türkiye, 77-79.

Nelson, M.R. (1988) Constraints on the Seismic Velocity Structure of the Crust and Upper Mantle Beneath the Eastern Tien Shan, Central Asia. PhD Thesis, MIT, Cambridge, MA, USA, 54-60.

**Patent ye Standardlar**

Sisaky, A., Golab, F., Myer, B. (1989) Rust resistant Potatoes. UK Patent 2 394 783, Jan 23.

TS-40561 (1985) Çelik Yapıların Plastik Teoriye Göre Hesap Kuralları. Türk Standartlar Enstitüsü*,* Ankara, Türkiye.

**Raporlar**

McCafirey, R., Abers, G. (1988) SYN3 : A program for Inversion of Teleseismic Body Wave Forms on Microcomputers. Air Force Geophysics Laboratory Technical Report, AFGL-TR-88-0099, Hanscomb Air Force Base, MA.

**Elektronik Yayınlar**

Svoboda, K. P. (2004) Herbs, Spices, and Condiments. *Encyclopedia of Plant and Crop Science* (2004) 559-563, <http://www.dekker.com/sdek/abstract> (17.09.2007).

T.C. Ölçme, Seçme ve Yerleştirme Merkezi, Aday İşlemleri Sistemi, <http://ais.osym.gov.tr/,> 07 Mart 2012.

**Kişisel Görüşmeler**

Özçelik, N. (2001) Kişisel Görüşme. Çanakkale Seramik Fbr. A.Ş.

**ÖZGEÇMİŞ**