KRİPTOLOJİ' DE ASİMETRİK ŞİFRELEME YÖNTEMİYLE BİR UYGULAMA

Şeyma BEŞİR

LİSANS TEZİ

ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ

GAZİ ÜNİVERSİTESİ

TEKNOLOJİ FAKÜLTESİ

OCAK 2020

Şeyma BEŞİR tarafından hazırlanan **"KRİPTOLOJİ'DE ASİMETRİK ŞİFRELEME YÖNTEMİYLE BİR UYGULAMA"** adlı bu tezin Lisans tezi olarak uygun olduğunu onaylarım.

Doç. Dr. Hasan Hüseyin SAYAN …….....

Tez Danışmanı,

Bu çalışma, jürimiz tarafından oy birliği ile Elektrik Elektronik Mühendisliği Bölümünde Lisans tezi olarak kabul edilmiştir.

Prof. Dr. Çetin ELMAS …….…….....

Prof. Dr. Cemal YILMAZ …….....

Doç. Dr. Hasan Hüseyin SAYAN ….....……..

Bu tez, G.Ü. Teknoloji Fakültesi Elektrik Elektronik Mühendisliği'nce onanmıştır.

Prof. Dr. Murat YÜCEL ……

Elektrik Elektronik Mühendisliği Bölüm Başkanı

ETİK BEYAN

Gazi Üniversitesi Teknoloji Fakültesi Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum bilgi ve dokümanları akademik kurallar etik çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmamda özgün verilerim dışında kalan ve tezde yararlanılan eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu ve başka bir yerde sunmadığımı

Beyan ederim.

Şeyma Beşir

KRİPTOLOJİ'DE ASİMETRİK ŞİFRELEME YÖNTEMİYLE BİR UYGULAMA

(Lisans Tezi)

Şeyma BEŞİR

GAZİ ÜNİVERSİTESİ

TEKNOLOJİ FAKÜLTESİ

Ocak 2020

ÖZET

Teknolojinin gelişimi sonucunda dijital veri alışverişinin hızla ilerlemesi ve bilgisayarların yaygın kullanımı ile bilgi güvenliği, veri iletişiminde önemli bir konu haline gelmiştir. Kötü amaçlı yazılımlar, bilgi sızıntısı ve yetkisiz erişim gibi birçok güvenlik sorununun dikkate alınması gerekir. Bu sorunların çözümü, veriler için şifreleme ve deşifreleme yöntemlerini içeren kriptoloji bilimi ile sağlanmaktadır. Şifreleme algoritmaları, bilgi güvenliğinin sağlanmasında önemli bir rol oynamaktadır. Bu algoritmalar, veri gizliliğini artırmak amacıyla, şifrelenmiş bilginin yalnızca ilgili anahtara sahip olan kişiler tarafından çözülebilmesini sağlayan veya şifresi çözülebilen bilgilerin çözülemez hale getirildiği teknikler kullanır.

Bu tez çalışmasında; kriptolojinin tanımı ve gelişiminden bahsedilmiş, temel kriptoloji kavramları açıklanmıştır. Geçmişten bugüne kullanılan şifreleme yöntemleri açıklanmıştır. Kriptoloji' de asimetrik şifreleme yöntemiyle gerçekleştirilen uygulama tanıtılmıştır.

Anahtar Kelimeler: Kriptoloji, kriptografi, kriptoanaliz, asimetrik şifreleme yöntemleri

Sayfa Adedi : 32

Tez Yöneticisi : Doç. Dr. Hasan Hüseyin SAYAN

AN APPLICATION WITH THE METHOD OF ASYMMETRIC ENCRYPTION IN CRYTOLOGY

(Thesis)

Şeyma Beşir

GAZI UNIVERSITY

FACULTY OF TECHNOLOGY

January 2020

ABSTRACT

Information security; as a result of the development of technology, has become an important issue in data communication, with the speed of digital data exchange and widespread use of computers. Many security issues such as malwares, the leakage of information and unauthorized access should be taken into account. The solution of these problems is provided by science of cryptology, which includes encryption and decryption methods for the data. Encryption algorithms play an important role in providing information security. In order to increase privacy of data, these algorithms use techniques which enable an encrypted information to be decrypted only by persons having the relevant key, and which decryptable information can be rendered unsolvable.

In this thesis, the definition and development of cryptology is mentioned and basic concepts of cryptology are explained. The encryption methods used from the past to the present are explained. An application which get actualize with the asymmetric encryption method in cryptology has got introduced.

Key Words : Cryptology, Cryptography, Cryptoanalysis, The asymmetric encryption methods.

Page Number : 32

Advisor : Assoc. Prof. Dr. Hasan Hüseyin SAYAN

TEŞEKKÜR

Tezin hazırlanması sürecinde bana her türlü kolaylığı sağlayan, bilgi ve tecrübeleriyle beni destekleyen saygıdeğer hocam Doç. Dr. Hasan Hüseyin SAYAN' a, değerli tecrübelerinden yararlandığım Elektrik Elektronik Mühendisliği Bölümü'ndeki değerli öğretim üyelerine en içten dileklerimle teşekkür eder saygılarımı sunarım. Ayrıca çalışmalarım esnasında kendilerinden görmüş olduğum destek ve güvenden dolayı aileme teşekkürü bir borç bilirim.

İÇİNDEKİLER

Sayfa

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

RESİMLERİN LİSTESİ

Resim **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış bazı simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	**Açıklama**
C	RSA algoritmasındaki şifreli metin
d	RSA algoritmasında özel anahtar
e	RSA algoritmasında açık anahtar
M	RSA algoritmasındaki açık metin
n	RSA algoritmasında p ve q çarpımı (n=p*q)
p, q, g, h	DSA algoritmasında kullanılan parametreler
p,q	RSA algoritması için gerekli, asal ve birbirinden farklı sayılar
Φ	RSA algoritmasında gerekli fonksiyon (Φ = (p- 1). (q- 1))

Kısaltmalar	**Açıklama**
ABD	Amerika Birleşik Devletleri
AES	Advanced Encryption Standard-Gelişmiş Şifreleme Standardı
ASCII	American Standard Code for Information Interchange (Bilgi değişimi için Amerikan Standart kodu)
Base64	İkili verilerin ASCII karakterlerini kullanan ortamlarda iletilmesine ve saklanmasına sağlayan kodlama türü
DES	Data Encryption Standard-Veri Şifreleme Standardı
3DES	Üçlü Veri Şifreleme Standardı (Triple Data Encryption Standard)
DSA	(Digital Signature Algorithm)

ECC	(Elliptic Curve Cryptography- Eliptik Eğri Şifrelemesi)
IBM	International Business Machines
IEEE	Institute of Electrical and Electronics Engineers (Elektrik ve Elektronik Mühendisleri Enstitüsü)
NIST	(National Institute of Standards and Technology-Ulusal Teknoloji ve Standartları Enstitüsü)
NSA	ABD Ulusal Güvenlik Kurumu (National Security Agency)
ODTÜ	Ortadoğu Teknik Üniversitesi
RSA	Açık anahtar algoritması (Algoritmayı geliştiren R. Rivest, A. Shamir ve L. Adleman isimlerin baş harfler
UEKAE	(Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü)
XOR	Dış veya İşlemi (Exclusive OR)

1.GİRİŞ

Günümüzde iletişimin hızla gelişimi, internetin hayatımızın vazgeçilmezlerinden biri olmasına neden olmuştur. Bu gelişimle birlikte insanlar, internet aracılığıyla bilgi paylaşma yolunu tercih etmeye başlamışlardır [1,26].

İnternet kullanımının bu hızla yaygınlaşması, son yıllarda bir takım güvenlik sorunlarını da beraberinde getirmiştir. İnternet'in açık bir sistem olması ve üzerinde dolaşan verinin gasp edilmeye uygun olması, bu sorunların başlıca nedenleridir. İnternette alınan ve gönderilen veri paketlerinin halka açık birçok ağdan geçmesi, üçüncü şahıslar tarafından bu paketlere ulaşmayı mümkün kılmaktadır [2].

Bunun sonucunda, internet aracılığıyla yapılan bilgi alışverişleri esnasında, ağların dinlenmesi, gelen verilerin değiştirilmesi, başkasına ait bilgilere erişilmeye çalışılması, bir başkası gibi davranarak yanlış bilgi gönderilmeye çalışılması gibi önemli tehditler oluşmaya başlamıştır. Bütün bu tehditlerden korunmak amacıyla internet üzerindeki iletişimde güvenliğin sağlanması büyük önem kazanmıştır. Teknolojinin günlük yaşantımızda daha fazla yer almasıyla bu önem gittikçe artmaktadır [1].

Dijital ortamlarda metnin yanı sıra ses, resim ve diğer çoklu ortam bilgileri de giderek artmaktadır. Bu tür bilgilerin korunması sağlanmadıkça, internette güvenli bir şekilde iş yapmak veya gizli, şahsi yazışmalarda bulunmak asla mümkün olmayacaktır. Başkası tarafından dinlenme, bilginin değiştirilmesi, kimlik taklidi gibi tehditlerin ortadan kaldırılması ancak bilgi güvenliği ile sağlanmaktadır [2,3,26].

Bilginin yönetme yeteneğine sahip olması, toplumların birbirlerine üstünlük sağlayabilmek için ağır ve mekanik silahları kullanmak yerine 1990'lı yılların başlarında dünya literatürüne giren, siber savaş olarak da nitelendirilen Bilgi Savaşı'nı tercih etmeye başlamasına neden olmuştur. Bilgi güvenliğinde zafiyet yaşayan ülkeler, siber savaşın en etkili olduğu ülkelerdir. Gelecekte ve hatta şimdinin en büyük tehlikesi olan siber savaşla ilgili bu ülkelerde yeterli farkındalık oluşturulamaması bunun en büyük sebebidir. Dolayısıyla yeterli farkındalık sahibi olmayan ülkeler tarafından siber savaş, bir tehdit unsuru olarak algılanmamakta ve bilgi güvenliği için alınması gereken tedbirler önemsenmemektedir. Bu durumun aksine bilginin

korunması ve güvenliğinin sağlanması gün geçtikçe büyüyen bir hızla önem kazanmaktadır [4].

Roma imparatoru Sezar'dan günümüze bilginin korunması amacıyla geliştirilen birçok teknik vardır. Bilginin güvenliğini sağlamak için birçok yol geliştirilmiş olsa da bilginin korunmasında en büyük yapı taşı bilginin gizlenmesi olmuştur. Bu bilim kriptoloji olarak adlandırılmıştır [5].

Kriptoloji, haberleşen iki ya da daha fazla tarafın güvenli olarak bilgi alışverişinde bulunmasını sağlayan, temelinde matematiksel zor problemler bulunan tekniklerin ve uygulamaların bütünüdür. Kriptoloji, bilgilerin şifrelenmesi ve şifrelenmiş bilgilerin çözümlenmesi için kullanılan metotlarla ilgilenir [6,3].

İnsanoğlunun gereksinim duyduğu en önemli ihtiyaçlardan biri güvenlik ihtiyacıdır. Bilgi iletiminin en hızlı ve en güvenli şekilde yapılması, günümüz yazılımlarının ve donanımlarının hedefi haline gelmiştir. Bu ihtiyacının giderilmesi şifreleme algoritmaları ile mümkün olmaktadır [7].

Bir bilginin değeri, bilgiyi elinde tutan kişi ya da kurumların yaşamsal faaliyetlerine olan etkisi tarafından belirlenir. Örneğin devletler açısından düşünüldüğünde bir ulusun güvenliği ve sürekliliği için, o ulusun elindeki milli istihbarat verilerini bilgiye dönüştürmesi ve elde ettiği bilgilerin güvenliğini en iyi şekilde sağlaması gerekmektedir. Bunu sağlayabilmek, potansiyel tehdit unsurlarının farkında olmakla mümkündür. Bilgi güvenliğini tehdit eden unsurlar; bilgide kayıplar (güvenlik ihlali), bilginin değiştirilmesi (bütünlük ihlali), başkası tarafından ele geçirilme (gizliliğin ihlali) gibi unsurlardır. Kriptoloji bilginin güvenliği, bütünlüğü ve gizliliği ile ilgilenir [4].

Günümüzde kullanılan şifreleme ve deşifreleme teknikleri; her türlü verinin iletiminde, bu verilerin saklanıp depolanmasında ve bu bilgilerin güvenliğinin sağlanmasında kullanılmaktadır. Bütün bunların arasında en çok kullanılan ve yaygın olan uygulamaların başında internette kullanılan bilgiler gelmektedir. Bu verilerin güvenli bir şekilde aktarılması ise şifreleme işlemlerinin görevidir [7].

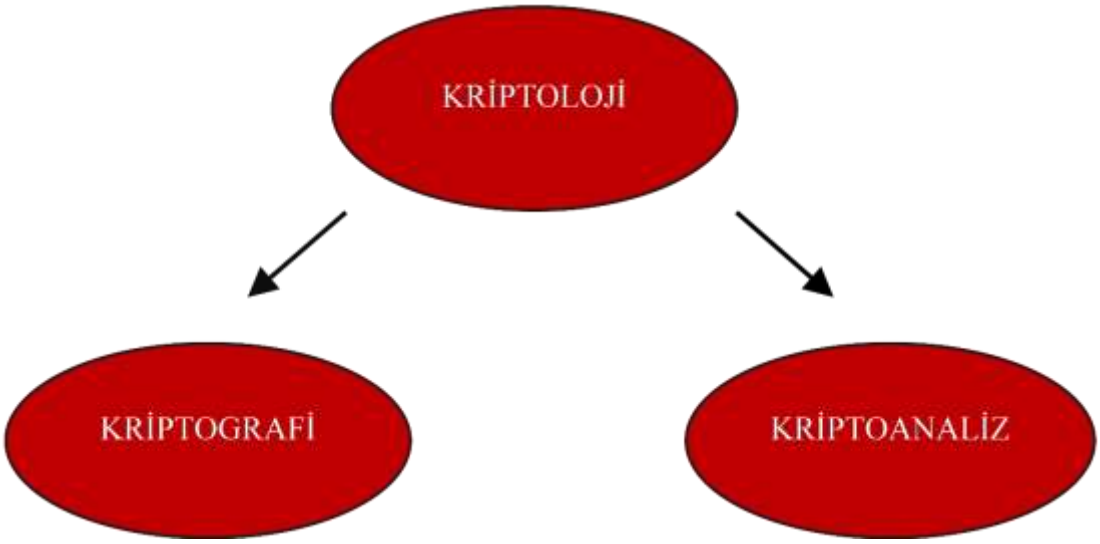
Kullandığımız kredi ve bankomat kartları, cep telefonları, internet vs. ile ilgili bilgilerin çeşitli yollarla ele geçirilebilme ihtimali vardır. Bu nedenle bu bilgilerin şifrelenmesi gerekir, yani gerçek bilgiler yerine bu bilgilerin değiştirilmiş formatını kullanmaya, tutmaya ve göndermeye ihtiyaç vardır. Kısacası, gizli haberleşme, kimlik doğrulama ve elektronik imza gibi uygulamalarda şifreleme kullanılmaktadır [1].

2.KRİPTOLOJİ

Kriptoloji terimi, Yunan dilinde ‘kryptos’ (saklı – gizli) ve ‘logos’ (sözcük) kelimelerinden türetilmiştir. Bu nedenle kriptoloji terimi, dilimizde ‘gizli sözcük’ olarak açıklanmıştır. Bu açıklamayla, kriptolojideki temel amacın, belirli sözcüklerin anlamını gizlemek, sözcüklerin güvenliğini sağlamak, gizliliğini korumak olduğu anlaşılmaktadır [8].

Kriptoloji, bilginin gizlenmesi ve tekrar ortaya çıkarılması ile ilgilenen matematiksel bir bilim dalıdır. Başka bir deyişle Kriptoloji, haberleşmede veri güvenliğini sağlayan kripto cihazlarının ve bu cihazlarda kullanılan algoritmaların güvenilirliğini araştıran, matematik bazlı elektrik ve elektronik mühendisliği, bilgisayar bilimleri, bilgisayar mühendisliği, istatistik ve fizik bölümlerini ilgilendiren disiplinler arası bir alandır [4,9].

Kriptoloji, kriptografi ve kriptoanaliz olmak üzere iki alt başlığa ayrılır.



Şekil 1.1. Kriptografi ve Kriptoanaliz

2.1.Kriptografi

Kriptografi, Yunan dilinde ‘krypto’ (saklı – gizli) ve ‘graphein’ (yazı) kelimelerinden türetilmiştir. Dolayısıyla kriptografi dilimizde ‘gizli yazı’ anlamındadır. Genel olarak çoğu kaynaklarda şifreleme olarak tanımlanmıştır. Kriptografi işlemi, veriyi anlamsız hale getirme, veri üzerinde meydana gelen herhangi bir değişimi engelleme ya da verinin yetkisiz kişiler tarafından kullanımını önleme amaçlı yapılmaktadır. Dolayısıyla kriptografi, verinin şifrelenmesi konusuyla ilgilenmiştir [8].

Kriptografi, verilerin gizliliğini, bütünlüğünü, güvenliğini sağlar. Bu işle meşgul olan kişilere kriptograf denir. Kriptografi yani şifreleme bilimi günümüzde güncel hayatın pek çok alanında kullanılmaktadır. Örneğin bankamatikler, rezervasyon sistemleri, e-posta iletileri, telefon bankacılığı, normal bankacılık işlemleri, cep telefonları, uydu sistemleri, füze sistemleri, savaş uçakları, sağlık sistemleri, mimari projeler, fatura sistemleri gibi daha pek çok alanda kullanılabilmektedir [4].

Bilginin gizliliğini sağlamak kriptografinin temel amacıdır. Bu amaçla kullanılan üç temel yöntem aşağıdaki gibidir:[4]

1. Yerine Koyma Yöntemleri

2. Yer Değiştirme Yöntemleri

3. Cebirsel Yöntemler

2.1.1 Yerine Koyma Yöntemleri (Substitution Methods)

Şifrelenecek metindeki harflerin yeri değiştirilmeden bu harfler yerine sayılar, semboller ya da farklı bir alfabeden alınan harfler kullanılarak şifreli metnin elde edildiği yöntemdir [4].

2.1.2 Yer değiştirme yöntemleri (Transposition Methods)

Şifrelenecek metindeki harflerin yerlerinin değiştirilmesiyle şifreli metin elde edilen, başka hiçbir harf, sembol ya da sayının kullanılmadığı yöntemdir. Sezar şifreleme algoritması, bu yöntem için verilebilecek en güzel örnektir [4].

2.1.3 Cebirsel yöntemler (Algebraic Methods)

Matematiksel bazı fonksiyonların kullanımı, yerine koyma ve yer değiştirme işlemlerinin karışımı gibi karmaşık yapıda olan işlemleri kapsayan yöntemlerdir [4].

Kriptografi; gizlilik, bütünlük, kimlik doğrulama, inkâr edememe gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemleri içermektedir [9].

2.1.4.Bilgi Güvenliği Kavramları

Bilgi güvenliği; teknoloji (yazılım ve donanım), insan, süreç, yöntem ve metodoloji gibi birçok kavramı kapsamakta ve bilişim dünyası için oldukça önemli görülmektedir. Ayrıca bilgi güvenliği, "Bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından ele geçirilmesini önlemek" olarak tanımlanır [10].

Günümüzde haberleşmenin güvenilir bir şekilde yapılması ve bununla birlikte bilgi güvenliğinin sağlaması adına aşağıda belirtilen beş temel emniyet unsuru öne çıkmaktadır [8].

a) Gizlilik

b) Bütünlük

c) İnkar Edilemezlik

d) Kimlik Doğrulama

e) Haberleşmenin Sürekliliği

2.1.4.1. Gizlilik

Gizlilik, haberleşmede iletilen bilginin gizli kalmasıdır. Böylece bilgiye sadece erişim yetkisi verilmiş kişilerce erişilebilmektedir. Haberleşmede gizlilik şifreleme algoritmalarıyla sağlanmaktadır [8].

Gönderilmesi istenen bilgilerin şifreleme algoritmalarıyla şifrelenerek gönderilmesi, haberleşmenin gizliliğini sağlayarak verileri izinsiz erişimlere karşı korur.

2.1.4.2. Bütünlük

Taşınan bilginin içeriğinin haberleşirken değiştirilememesidir. Özetleme algoritmaları bu amaçla kullanılır [8].

Haberleşmede veri bütünlüğü için gönderilen mesajın özeti alınır. Alınan özet, mesajla birlikte karşı tarafa gönderilir. Karşı taraf alınan mesajın özetini çıkartır. Kendisine gönderilmiş özetle, çıkartılan özeti karşılaştırır. Karşılaştırma sonucunda eşitlik sağlanırsa mesajın değiştirilmediği anlaşılır. Eşitlik sağlanamamış ise mesajın değiştirildiği ortaya çıkar ve bu mesajın güvenilir olmadığı anlaşılır[8].

2.1.4.3. İnkâr Edilemezlik

Genel olarak yapılan herhangi bir işlemin yapıldığının inkâr edilememesinin sağlanması olarak tanımlanabilir.

Haberleşmede tarafların birbirinden gelen mesajları aldığını veya gönderdiğini doğrulaması veya bunu inkâr edememesi gerekir. Bunun sağlanması için mesajı gönderen ve alan kişilerin kayıtları güvenilir bir ortamda saklanmalıdır[8].

2.1.4.4. Kimlik Doğrulama

Kısaca bir haberleşmede, emniyet amacıyla alıcı ve gönderici tarafların birbirlerinin kimliklerini denetlemesi olarak tanımlanabilir.

Bu işlem, bilgiyi gönderen kişinin kimliğinden emin olma işlemidir. Kimlik tanımlama, kişinin kimliğinin bir sisteme tanıtılmasıyla başlar. Böylece, sistem tarafından kişinin kimliğinin tespiti sağlanır. Kimlik doğrulama ise sisteme giriş yapan kişinin iddia ettiği kimliği taşıyıp taşımadığının kontrol edildiği bir mekanizmadır[8].

2.1.4.5. Haberleşmenin Sürekliliği

Haberleşmenin hiç kesintiye uğramadan yapılmasıdır. Süreklilik, yetkili kullanıcıların bilgiye ve ilgili kaynaklara erişebileceklerini garanti etme durumudur [8].

2.2. Kriptoanaliz

Kriptoanaliz, Yunan dilinde ‘krypto’ (saklı – gizli) ve ‘analyein’ (çözme) kelimelerinden oluşturulmuştur. Bu yönüyle kriptoanaliz, saklı bilginin ya da şifrelenmiş verinin çözülmesi anlamına gelmektedir. En genel manada deşifreleme işlemi olarak tanımlanmaktadır. Ayrıca kriptoanaliz (deşifreleme), şifreleme tekniklerinin ve sistemlerinin kırılması olasılıklarıyla ve veri güvenliği konularında yoğunlaşmaktadır [8].

Başka bir deyişle kriptoanaliz, kriptografların şifreli hale getirdiği metinlerin analizi ve şifrelerin çözümü ile ilgilenen kriptoloji alt bilim dalıdır. Bu işi yapan kişilere kriptoanalist denir [4].

2.3. Kriptolojinin Amacı

Günümüzde şifreleme, bilgisayar ağları ve haberleşme sistemlerinde, birçok farklı veri koruma problemlerinin çözümünde en etkin ve yaygın bir yöntem olarak kullanılmaktadır [8].

Bu açıdan şifrelemenin en önemli üç temel amacı şunlardır [8]:

- Veri güvenliğinin sağlanması,
- Mesaj kaynağının ve bilginin doğruluğunun tespiti,
- Kullanıcının gerçek isminin saklanması olarak açıklanmaktadır.

2.4. Kriptolojinin Gelişimi

Şifre bilimi, şifre yazma ve çözmede 1940–1944 yılları arasında 2. Dünya Savaşında önemli ölçüde ilerleme kaydetmiştir. Temel olarak, şifre çözümün amacı, kullanılan şifrenin açıklarından ve şifrelenen metin hakkındaki bilgilerden yola çıkarak bütün anahtarları deneme zahmetinden kurtulmaktır. Nazilerin 1940–1944 savaşında kullandıkları ünlü Enigma şifreleme cihazının, bugünün sağlam şifreleme algoritmalarında kullanılan 116 bitlik bir anahtar uzunluğuna sahip olduğu bilinmektedir. Buna rağmen, savaş döneminde şifre bilimiyle uğraşan, bilgisayar biliminin öncüsü İngiliz Alan Turing, Enigma şifresinin yapısal zayıflıklarını

kullanarak, Colossus isimli ilk tüplü bilgisayar yardımıyla Nazilerin iletişimlerini açığa çıkarmayı başarmıştır.[1]

1970'lere kadar sadece askeri ve resmî kurumların kullandığı kriptografik yöntemler, 1976 yılında Diffie ve Hellman'ın önerdiği "Açık Anahtarlı Sistemler" kavramıyla bir devrim geçirmiştir. 1976 yılına kadar var olan şifre sistemlerinin güvenilirlikleri anahtarın gizliliğine dayanmaktaydı. Gizli anahtarlı sistemler olarak adlandıracağımız bu sistemlerde, şifreleme ve şifre çözme işlemi için önceden belirlenen anahtarlar kullanılmakta ve şifre sistemlerinin de bu şekilde olabileceği düşünülmekteydi. Ancak, açık anahtarlı sistemlerin keşfiyle aynı anahtarın hem alıcı hem de gönderici tarafından bilinmeden de güvenli haberleşmenin sağlanabileceği ortaya çıkmıştır. Ayrıca, açık anahtarlı sistemler gizliliğin yanı sıra veri bütünlüğü, kimlik kanıtlama ve inkâr edememe konularına da çözüm getirerek birçok yeni uygulamaları da beraberinde getirmiştir [9].

Ülkemizde şifreleme bilimi alanındaki çalışmalara, 1995 yılında TÜBİTAK bünyesinde UEKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü) biriminin kurulmasıyla başlanmıştır. Daha sonra ODTÜ'de Kriptografi Bölümü açılmıştır. Ülkemiz, bu alandaki çalışmalarına her ne kadar diğer ülkelerden daha sonra başlamış olsa da yapılan çalışmalarla önemli bir yer edinmeyi başarmıştır. Günümüzde ise şifreleme işlemlerinin özel veya devlet kurumları olmak üzere hemen her alanda kullanıldığı görülmektedir [10].

Günümüzde kriptoloji şifrelemeden ve şifre çözmeden daha fazlasını içerir. Kimlik denetimi de artık gizlilik kadar önemlidir. Herhangi bir iletiye adımızı ekleyip ağ üzerinden gönderdiğimiz zaman kimliğimizi ispatlamak için elektronik yöntemlere ihtiyaç duyarız. Kriptolojinin buna sunduğu çözüm sayısal imzadır [1].

3. KRİPTOLOJİ YÖNTEMLERİ

Zamanla teknolojinin gelişmesi, tarih boyunca kriptolojide meydana gelen değişim ve gelişmelerden dolayı, kriptoloji yöntemleri ikiye ayrılmaktadır.

Bunlar;

- Klasik Şifreleme Yöntemleri [8]
- Modern Şifreleme Yöntemleri [8]

3.1. Klasik Şifreleme Yöntemleri

Geçmişte sadece askeri ve bazı ileri akademik alanlarda kullanılan klasik şifreleme yöntemleri, algoritması gizli olan şifreleme yöntemlerini kapsamaktadır ve genellikle basit işlemlerle hesaplanabilecek algoritmalardan oluşmaktadır. İlk klasik yöntemlerden biri olarak Enigma İkinci Dünya Savaşı döneminde kullanılmıştır. Sezar, Vigenére, Vernam, Playfair, Hill sistemleri klasik yöntemlerden bazılarıdır [3].

3.1.1. Sezar Şifreleme (Caesar Cipher)

İlk klasik şifreleme tekniklerinden biridir. Gaius Julius Caesar, gönderdiği mesajların düşmanlar tarafından ele geçirilmesi tehlikesine karşın mesajlarında düşmanların anlayamayacağı bir şifreleme tekniği kullanmıştır. Zaman içerisinde bu yöntem, Sezar şifreleme yöntemi olarak anılmıştır. Bu yöntem öteleme şifrelemesi olarak da bilinmektedir.

Sezar şifreleme çok basit bir algoritmaya sahiptir. Bu yöntemde bir anahtar sayı belirlenir. Kelimelerdeki her bir harf, belirlenen anahtar sayı kadar ötelenerek anlaşılması zor yeni kelimeler oluşturulur.

Örneğin; şifrelenecek mesaj “kitap” ve anahtar sayı 3 olarak alınırsa şifreli mesaj olarak “nlvçş” elde edilir.

3.1.2. Enigma

2. Dünya Savaşı sırasında Nazi Almanyası tarafından gizlenmek istenen ve önemli olan mesajların şifrelenmesi ve tekrar çözülmesi amacı ile kullanılan şifre makinesidir. Enigma makinesi, ticari olarak 1920’li yılların başında kullanılmaya başlanmıştır [11].

Stratejik planların uygulanmasında kullanılan şifreleme ve deşifreleme teknikleri veya algoritmaları, buluşlar, şifre çözücü makineler bilgisayar biliminin gelişmesinde önemli derecede etkili olmuştur denilebilir [10].

3.1.3. Vigenére Şifreleme (Vigenére Cipher)

Günümüzde yaygın olarak kullanılmayan geri dönüşümü kolay olan bir şifreleme türüdür. Aynı zamanda Vigenére şifrelemesinde birden fazla alfabe kullanılmaktadır. Şifreleme için bir anahtar seçilmektedir ve bu anahtara göre her harf farklı bir alfabeye göre şifrelenmektedir [5].

Alfabenin seçimine anahtar kelimeye göre karar verilir. Anahtar kelimenin farklı seçilmesi, şifrelenmemiş metinde aynı kelimeler için farklı şifreli metinler oluşmasını sağlar. Vigenére şifreleme için alfabedeki harflerin yer aldığı bir tablo kullanılır. Bu tablo şifreleme ve şifre çözme eylemlerinde sabit olarak kullanılır [3].

Geleneksel olarak, Vigenére şifresi, Vigenére tablosunu kullanarak alfabetik metinleri şifrelemek için geliştirilmiştir. Ancak son zamanlarda yapılan birçok çalışma, görüntü şifrelemesi için Vigenére`nin şifreleme yöntemini kullanmıştır [5].

3.1.4. Vernam Şifreleme (Vernam Cipher)

1917 yılında Amerika'da bir şirkette çalışan Gilbert Vernam adındaki mühendis, yeni bir şifreleme tekniği geliştirdi. Vernam şifresiyle beraber, matematiğin kriptografide sistematik olarak kullanılmaya başlandığı görülmektedir [10].

Bu yöntem Vigenére yöntemine benzemektedir. Farkı ikili sayı sistemine yer vermesi ve şifrelenmemiş metnin XOR (exclusive-or) işlemine tabi tutulmasıdır. Veri rastgele belirlenmiş ve kendisini tekrarlatmayan anahtarlar vasıtasıyla şifrelenir. Şifreleme işleminde ikili sistemde kodlanmış ASCII tablosu kullanılır. Rastgele belirlenen anahtar dizisinin her bir karakterine karşılık gelen ASCII koduna, şifrelenmemiş metinin her bir karakterinin ASCII kodu eklenerek (XOR) yeni şifreli karakter dizisi elde edilir [3].

3.1.5. Hill Şifreleme (Hill Cipher)

Leste S. Hill tarafından tasarlanan “Hill Şifresi” çok alfabeli şifreleme sistemlerine başka bir örnek olup çok alfabeli şifreleri daha pratik hale getirmesi bakımından oldukça önemlidir. Hill şifresi, tamamen lineer cebire dayandığı için kriptanalizi biraz teoriktir. Ancak yeterli düz metin ve onun karşılığı olan şifreli metin ele geçirildiği taktirde lineer cebir kullanılarak anahtar matris kolayca hesaplanabilir [10].

Bu yöntem, şifrelenmemiş metni bitişik ve aynı uzunluktaki bloklara bölerek şifreleyen ve bu şifreli blokları şifreli metin çıktısı olarak gruplara ayıran bir blok şifreleme algoritmasıdır. Hill şifrelemede şifreleme anahtarı olarak bir katsayılar matrisi (K) kullanılır. Katsayılar matrisinin elamanları ile şifrelenmemiş metindeki karakterlerin sayısal karşılıklarından oluşturulan matrisin elamanları çarpılır [3].

3.1.6. Playfair Şifreleme (Playfair Cipher)

Bu yöntem yerine koyma yönteminin bir türüdür. 5X5’lik matris düzeni ile şifreleme işlemini gerçekleştirir [3].

Playfair şifreleme algoritmasında, öncelikle bir anahtar belirlenir. Belirlenen anahtar 5X5’lik matrisin ilk hücresinden başlayarak yerleştirilir. Matriste geri kalan boş hücrelere, kullanılan alfabedeki harfler sırayla yerleştirilir. Alfabenin harf sayısı 25’i geçiyorsa çok kullanılmayan harflerin dışarıda bırakılması tercih edilir. Bu şekilde oluşturulan matris herhangi bir metni şifrelemek için kullanılır. Daha sonra şifrelenecek metin harf çiftleri şeklinde parçalanır.

Şifreli metnin oluşturulması için üç farklı durum değerlendirilir. Birinci durum harf çiftinin aynı satır veya sütunda bulunmadığı durumdur. Bu durumda bir harf çifti matris üzerinde aynı satır ve sütunda bulunmayıp bir dikdörtgen oluşturuyorsa, bu dikdörtgenin diğer köşelerinde bulunan harfler, önceki harf çiftinin yerine koyulur. İkincisi; harf çiftinin aynı satırda yer aldığı durumdur. Bu durumda her bir harf bir hücre sağa ötelenir. Üçüncüsü, harf çiftinin aynı sütunda yer aldığı durumdur. Bu durumda ise her bir harf bir hücre aşağı ötelenir. Bu işlemlerin her bir harf çiftine uygulanmasıyla şifrelenmiş metin oluşturulur [3].

Klasik şifreleme yöntemlerinin modern şifreleme yöntemlerine göre dezavantajları şu şekilde sıralanabilir: [8]

- Modern şifreleme yöntemlerine göre çok zayıf kalmaktadır.
- Kriptoanalizleri yapılmış olduğundan geçerliliği kalmamıştır. [8]
- Açık anahtar dağıtım problemi vardır. Verinin güvenliğini sağlamak için ciddi boyutta anahtarlar kullanılmaktır [8].
- Klasik şifreleme, sadece askeri işlemlerde ve ileri akademik kurumlarda kullanılmıştır [8].

3.2.Modern Şifreleme Yöntemleri

Modern şifreleme yöntemlerinin klasik şifreleme yöntemlerine göre üstün olduğu özellikler aşağıdaki maddelerde yer almaktadır.

- Kriptolojinin temellerini standartlaştırmıştır [8].
- Asimetrik şifreleme yöntemi keşfedilmiştir.
- Güvenlik tanımlamalarının biçimlendirilmesi sağlanmıştır [8].
- Bilgisayar ve internetin gelişmesine paralel ilerlemeler yapılmıştır [8].
- Kriptolojik yasaklamalara serbestlikler getirilmiştir [8].

Şifrelenmiş bir mesajın güvenliği kadar şifrelerken kullanılan yöntemlerin gizliliği de bir o kadar önemlidir [12]. Şifreleme sırasında açık mesaj şifreleme anahtarıyla şifrelenir. Açık mesaj ile şifrelenmiş mesaj arasındaki geçişler şifreleme algoritmasına ve anahtar bilgisine bağlıdır [8].

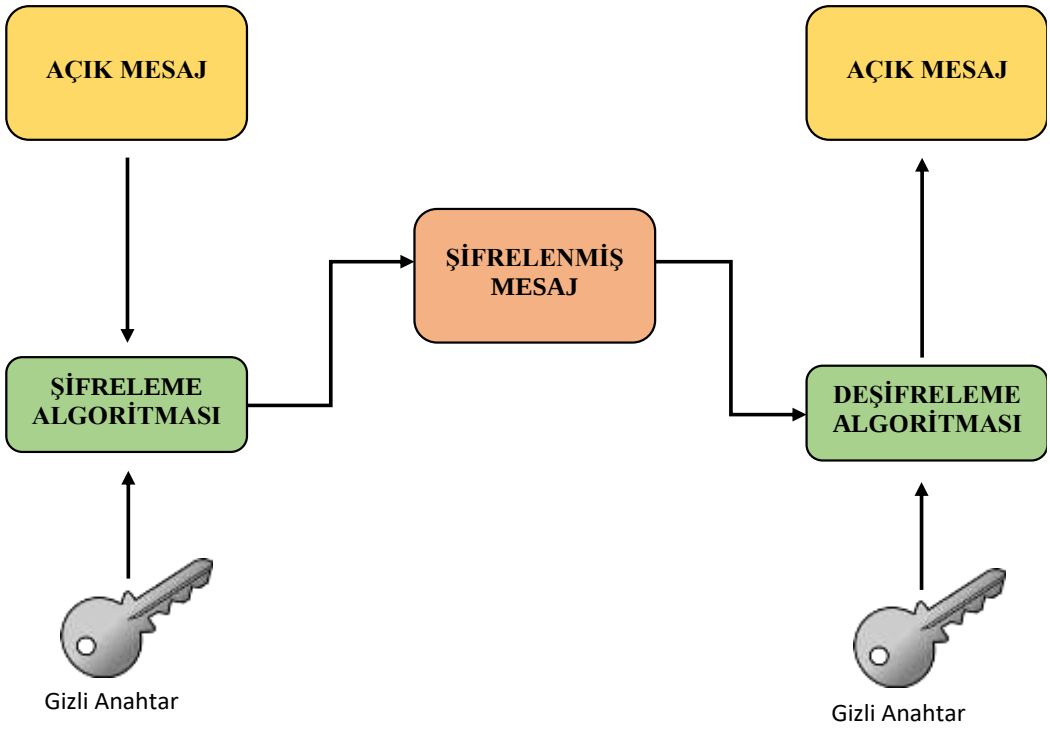
Modern şifreleme yöntemleri, şifreleme anahtarının işlevine göre temel olarak iki başlık altında açıklanabilir. Bunlar simetrik şifreleme yöntemi ve asimetrik şifreleme yöntemidir.

3.2.1. Simetrik Şifreleme (Gizli Anahtar) Yöntemi

En basit haliyle bir verinin şifrelendiği anahtar tarafından çözülebildiği şifreleme yöntemi olarak tanımlanabilir.

Simetrik anahtarlamada genel olarak basit şifreleme algoritmaları kullanılmaktadır. Bu durum veri şifreleme için matematiksel açıdan daha az problem çıkaran bir yaklaşımdır ve çok kullanılan bir yöntemdir [1,2].

Simetrik şifreleme yönteminde şifreleme ve şifre çözme işlemleri için tek bir gizli anahtar kullanılmaktadır. Bu şekilde şifrelenmiş veri ağdan geçerken bir başkası tarafından elde edilip okunabilmesi için kişinin anahtara sahip olması gerekir [1,2,32,28].



Şekil 3.1. Simetrik şifreleme (gizli anahtar) yöntemi

Simetrik Şifreleme Yöntemlerinin Avantajları:

- Diğer şifreleme algoritmalarına kıyasla daha hızlı çalışır.
- Özel donanımla birlikte kullanılabilir [8,7].
- Bit sayısı düşük olduğundan dolayı anahtarın boyu nispeten daha küçüktür [7].

Simetrik Şifreleme Yöntemlerinin Dezavantajları:

- Anahtarların güvenli bir şekilde dağıtımı zordur [8,7].
- Kapasitesi sınırlıdır [8,7].
- Bütünlük ve kimlik doğrulama hizmetlerini güvenli bir şekilde gerçekleştirmek zordur [8,7].

3.2.1.1.Simetrik Şifreleme Algoritmaları

Simetrik şifreleme algoritmaları; dizi (akış) ve blok şifreleme algoritmaları olmak üzere ikiye çeşittir [7]. Bunlardan blok şifreleme, orijinal metni veya şifreli metni bloklara bölerek şifreleme ve deşifreleme işlemini yapar. Akış şifrelemede ise bir bit veya byte üzerinde şifreleme ve deşifreleme işlemleri yapılır [8].

Çok fazla sayıda simetrik şifreleme algoritması olmakla birlikte başlıca simetrik şifreleme algoritmaları şunlardır: [12]

- DES (Data Encryption Standard)
- 3DES (Triple Data Encryption Standard)
- AES (Advanced Encryption Standard)
- Blowfish

3.2.1.1.1. DES (Data Encryption Standart – Veri Şifreleme Standardı) Algortiması

Amerika Birleşik Devletleri tarafından kullanılan simetrik bir şifreleme algoritmasıdır. 1960'ların sonunda IBM'de çalışan Horst Feistel adlı bir araştırmacı başkanlığındaki bir grup Lucifer adı verilen bir şifreleme sistemi geliştirmiştir. 1973 yılında ABD standartlar enstitüsü NIST (National Institute of Standards and Technology) sivil kullanım için bir standart saptamak amacıyla firmaları davet eder ve yapılan incelemeler sonucu amaca en yakın çözüm olarak Lucifer bulunmuştur. 128 bitlik bir şifre anahtarına sahip Lucifer üzerinde çalışan ABD Güvenlik Teşkilatı (NSA) uzmanları tarafından bazı düzenlemeler yapılarak anahtar uzunluğu 56 bit'e indirilmiştir. Bu yeni algoritma 1977 yılında DES (Data Encryption Standard) olarak yayınlanmış ve kısa bir zamanda başta finans endüstrisi olmak üzere birçok alanda standart olarak kullanılmıştır. DES aynı zamanda, sabit diskte veri saklamak gibi tek kullanıcılı şifreleme amaçlı da kullanılabilir [1,22].

DES algoritması blok şifreleme mantığına göre çalışır. Dolayısıyla gönderilecek olan açık metin, metin boyutu sabit olan bloklara ayırılır. Oluşturulan bloklar 64 bit uzunluğuna sahiptir ve bir anahtar yardımıyla birbirinden bağımsız olarak şifrelenir. Anahtar uzunluğu 56 bittir ve anahtar ne kadar uzunsa şifreyi çözmekte o kadar zor olacaktır. Şifrelenmiş metnin tekrar açabilmesi için şifrelemedeki aynı işlem, yine ayrılmış olan bloklar üzerinden bağımsız olarak tekrar edilir [5,1,7].

3.2.1.1.2. Üçlü Veri Şifreleme Tekniği (3DES)

3DES algoritması, DES algoritmasının arka arkaya üç kez çalıştırılması ile elde edilmiştir. 3DES, DES' e göre üç kat fazla işlem yapar ve bundan dolayı 3 kat daha yavaş çalışır fakat DES algoritmasına göre daha güvenlidir. 3DES iki ayrı anahtar kullanarak üçlü şifreleme yapmaktadır. Brute Force (Kaba Kuvvet) saldırılarına karşı yeterli olmasından dolayı üç yerine iki anahtar kullanılır. 3DES algoritması DES algoritmasına göre 2 kat daha fazla güvenlik sağlamaktadır ki bu da 112 bitlik bir anahtara karşılık gelmektedir. Ve bu güvenlik bütün şifreleme işlemi boyunca da orantılı olarak artmaktadır [8,7].

3DES'te en önemli konu, üç adet anahtar bloğunun veya üçünden ikisinin aynı olmasından kaçınmaktır. Eğer anahtarlar aynı olursa işlem DES işleminden farksız olacaktır. DES' ten farksız olursa günümüz şartlarıyla kısa sürede şifrenin kırılması söz konusudur [8].

Genellikle, finans sektöründe (bankacılık), önemli güvenlik faaliyetlerinde ve internet üzerinden yapılan alışverişlerde (e-ödeme) kullanılmaktadır [7].

Avantajları:

- Şifrelenmiş bilgi tekrar çözülebildiğinden iki yönlü çalışabilmektedir. İki yönlü çalışmasından dolayı veriler rahat bir şekilde saklanabilir ve dilediğinde tekrar çağırılarak data tekrar çözülebilir [7].
- Kullanılan cihazların (bilgisayarın) eksikliklerini giderir [7].

Dezavantajları:

- Kullanılan anahtar sistemin güvenliğini oluşturur. Kullanılan anahtar ne kadar zayıfsa, şifrenin kırılması o kadar kolaydır [7].
- Günümüz teknolojisinde kullanılan daha gelişmiş AES algoritmasına nazaran 6 kat ağır işler [7].

3.2.1.1.3. AES (Advanced Encryption Standard – Gelişmiş Şifreleme Standardı) Algoritması

AES, Rijndael Joan Daemen ve Vincent Rijmen tarafından geliştirilen, simetrik bir blok şifreleme algoritmasıdır. AES algoritması, verilerin 128, 192 ve 256 bitlik anahtar boyutunu desteklemektedir ve dört temel işlem bloğuna bölünebilen 128 bit veri uzunluğuna izin vermektedir. Bloklar, 128-bitlik bir eşit blok boyutuna sahiptir fakat herhangi bir bit artışında güvenlik kuvveti artışını gösteren 128, 192, 256-bit'lik anahtar boyutları vardır [5].

AES'te 128 bit anahtarla 10 döngüde şifreleme yapılır. 192 ve 256 bit anahtarlarla sırasıyla 12 ve 14 döngüde şifreleme işlemi gerçekleşir. AES'in döngü sayısı anahtar genişliğine göre değişkenlik gösterir [8].

AES, kullandığı anahtar boyutuna göre tanımlanır. Bunlar; “AES-128”, “AES-192”, “AES256” gibi adlandırılır [8].

3.2.1.1.4.Blowfish

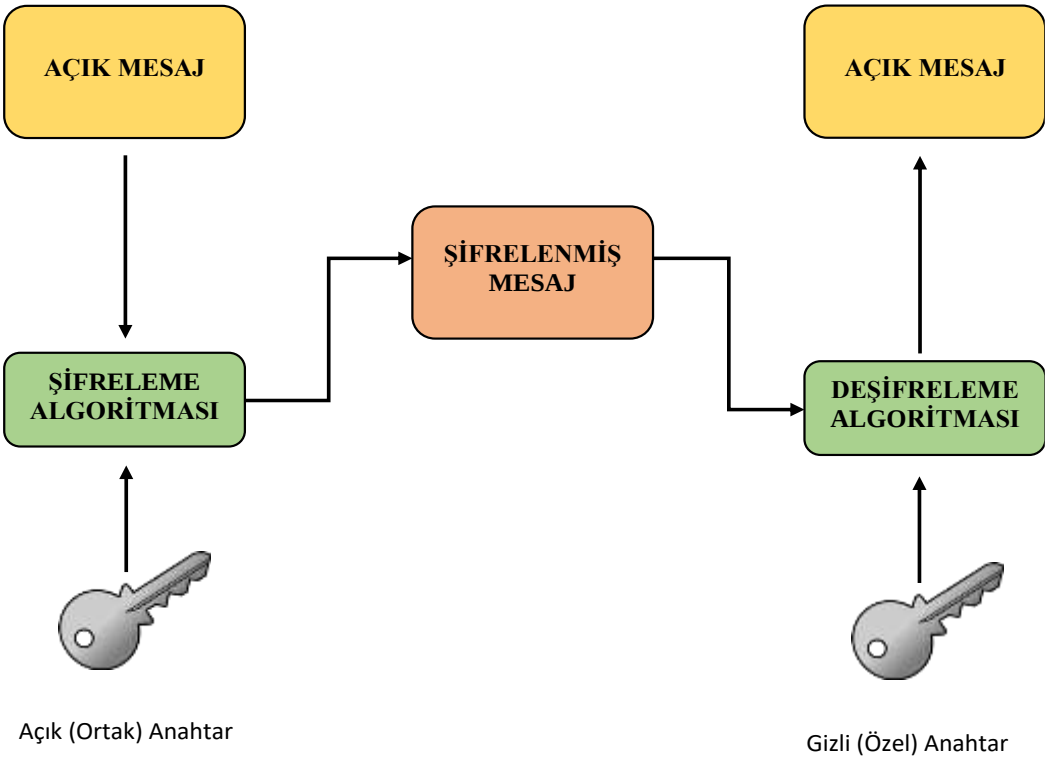
Blowfish algoritması, dünyanın önde gelen kriptologlarından Bruce Schneier tarafından,1993 yılında tasarlanmış ve kamuya açık hale getirilmiştir [13,22].

Blowfish, DES’in eksik kalmaya başlamasından sonra onun yerini alması amacıyla tasarlanan, 64-bit öbek büyüklüğüne ve 32 bit'ten 448 bit'e kadar anahtar uzunluğuna sahip bir simetrik şifreleme algoritmasıdır. Yüksek şifreleme ve e-posta gibi rutin kullanıcı uygulamaları konusundaki etkinliğiyle başarılı bir algoritma olarak değerlendirilmektedir. Blowfish kullanımını artıran en önemli özelliklerinden birisi yapıldığı zamanda kullanılmakta olan şifreleme algoritmaları lisanslı ve paralı satılmasına rağmen, Blowfish’in tamamen ücretsiz olmasıdır. Blowfish piyasada kullanılan en hızlı öbek şifreleyicilerdendir ve içerdiği karmaşık anahtar çizelgesi şifrenin kırılmasını zorlaştırmıştır [14,15,22].

3.2.2. Asimetrik Şifreleme (Açık Anahtar) Yöntemi

Asimetrik şifreleme yöntemlerinde, şifreleme için kullanılan anahtar ile şifre çözme için kullanılan anahtar birbirinden farklıdır. Mesaj şifrelenirken kullanılan anahtar, mesaj çözülerken kullanılamaz [2,12].

Bu yöntemde her kullanıcının iki adet anahtarı mevcuttur. Bu anahtarlardan birisi sadece kendisinin bildiği ve güvenli bir şekilde saklanması gereken gizli anahtar, diğeri ise herkesin kullanabilmesi için dağıtılan açık anahtardır. Anahtar çiftlerini üreten algoritmaların matematiksel özelliklerinden dolayı açık-özel anahtar çiftleri her kişi için farklıdır, diğer bir deyişle her kullanıcının açık-özel anahtar çifti yalnızca o kullanıcıya özeldir. Mesaj gönderen kişi, mesajını karşı tarafın açık anahtarıyla şifreleyerek gönderir. Bu mesaj ancak alıcının gizli anahtarıyla tekrar deşifre edilebilir [6,2,1].



Şekil 3.2. Asimetrik şifreleme (açık anahtar) yöntemi

Asimetrik Şifreleme Yöntemlerinin Avantajları: [7]

- Şifrelerin kırılması nispeten daha zordur.
- Kimlik doğrulama, bütünlük ve gizlilik ilkelerini gerçekleştirmek için güveli bir yoldur [7].
- Kullanılacak olan anahtarı kullanıcı kendisi belirleyebilir.
- Şifreleme için kullanılan ortak (açık) karşılıklı aktarılması gerekli değildir, [7].
- Deşifreleme için kullanılan özel (gizli) anahtar internetteki bir sunucu tarafından dağıtılabilir [7].
- Şifrelemede iki anahtar kullanıldığı için sayısal imza ile inkâr edilemezliği sağlar [7].

Asimetrik Şifreleme Yöntemlerinin Dezavantajları:

- Bu yöntemde güvenliğin sağlanabilmesi için çok büyük asal sayılar kullanılmaktadır. Bu da zaman açısından çok büyük problemleri beraberinde getirmektedir [2].
- Asimetrik şifreleme yöntemleri, simetrik şifreleme yöntemlerine göre çok daha yavaştır [2].
- Ayrıca asimetrik şifreleme yöntemlerinde çok büyük sayılar kullanmasından dolayı donanımsal yapılara uyum sağlaması zorlaşmaktadır. [2].
- Anahtarlar uzun olduğundan bit sayıları da uzundur [7].

3.2.2.1. Asimetrik Şifreleme (Açık Anahtar) Algoritmaları

Bu algoritmalara açık anahtar algoritmaları denmesinin sebebi şifre anahtarının genel kullanıma açık olmasıdır. Bir yabancı bir iletiyi şifrelemek için şifreleme anahtarını kullanabilir, ancak sadece ilgili şifre çözüm anahtarına sahip bir kişi iletinin şifresini çözebilir. Bu sistemde, şifre anahtarına genellikle açık anahtar adı verilmektedir. Şifre çözüm anahtarı da genellikle özel anahtar olarak adlandırılmaktadır [2].

Başlıca asimetrik şifreleme algoritmaları aşağıdaki gibidir: [7]

1. Diffie Helman
2. RSA (Ronald L.Rivest, Adi Shamir ve Leonard Adleman)
3. DSA (Digital Signature Algorithm)
4. ECC (Elliptic Curve Cryptography- Eliptik Eğri Şifrelemesi)

3.2.2.1.1. Diffie-Helman

İnsanlığa ilk duyurulan asimetrik (açık anahtar) şifreleme algoritmasıdır.1976 yılında Witfield Diffie ve Martin Hellman tarafından bulunmuş ve "New Directions in Cryptography" isimli makalelerinde yayımlanmıştır [16,17].

Açıklanacak olursa, bilgi alışverişinin gerçekleşeceği kanal aracılığıyla, alıcı ve verici taraflar arasında iletişimin güvenli olarak sağlanması amacıyla ortak bir anahtar belirlenmesini sağlayan protokoldür. Bu algoritma Diffie-Helman anahtar değişimi olarak da adlandırılır ve yalnızca ortak gizli anahtarın belirlenmesinde kullanılmaktadır.

Bilgi alışverişinde bulunacak tarafların, kullanacakları ortak anahtarı, birbirlerine güvenli bir şekilde iletilebilmesi algoritmanın ana hedefidir. Bu ortak anahtar aracılığıyla taraflar arasında şifreli mesaj paylaşımı sağlanabilmektedir. Diffie–Hellman algoritmasıyla simetrik şifreleme algoritmalarının gizli anahtarı koruma ve dağıtım sorunu önemli derecede çözülmüştür.

3.2.2.1.2. RSA (Ronald L.Rivest, Adi Shamir ve Leonard Adleman)

Diffie ve Hellman tarafından bulunan kamuya açık anahtarlı şifreleme yönetimini kullanan Ronald Rivest, Adi Shamir ve Leonard Adleman, kendi isimlerinin ilk harflerinden oluşan RSA algoritmasıyla çığır açmışlardır [1,3].

RSA, günümüzde en çok kullanılan açık anahtar algoritmasıdır. Ayrıca en çok test edilen algoritmalardan biridir. RSA hem bilgi şifrelemede hem de dijital imza sistemlerinde kullanılabilmektedir [1].

RSA algoritmasının en büyük dezavantajı, asimetrik bir şifreleme algoritması olması ve büyük sayılarla işlem yapması nedeniyle yavaş olmasıdır.

Çeşitli problemlere uygulanmaya başlanan RSA algoritması, birçok gerçek dünya problemlerinde ve mühendislik alanında kullanılmaktadır. Özellikle son yıllarda RSA algoritması ile ilgili çok sayıda çalışma bulunmaktadır [18].

RSA algoritmasının güvenliği kullanılan anahtarların uzunluğuna bağlıdır. Anahtarların yeterince uzun olması algoritmayı daha güvenli hale getirir. Kullanılan anahtarların uzunlukları algoritmanın kullanılacağı alana göre değişebilmektedir.

RSA algoritması, anahtar oluşturma, şifreleme ve deşifreleme olmak üzere üç aşamadan oluşmaktadır.

3.2.2.1.2.1. Anahtar Oluşturma

RSA şifreleme algoritması açık (ortak) ve gizli(özel) olmak üzere iki anahtar kullanır. Şifreleme işlemi herkes tarafından bilinen açık anahtar ile yapılır. Deşifreleme işlemi, sadece alıcı tarafından bilinen gizli anahtar kullanılarak yapılır. Böylece şifreli mesaja sadece gizli anahtar sahibi erişim sağlayabilir.

RSA algoritmasının anahtar oluşturma adımları aşağıdaki gibidir:

- Birbirinden farklı ve asal olmak şartıyla rastgele p ve q sayıları seçilir [36].
- n= p*q değeri hesaplanır [18,1,16,19,14].
- $\Phi(n) = (p-1)*(q-1)$ değeri hesaplanır [18,1,16,19,14,4].
- $1< e <\Phi(n)$ aralığında ve EBOB $(\Phi(n), e) = 1$ olmak şartıyla rastgele bir e sayısı üretilir [18,1,16,14].
- $1 < d < \Phi(n)$ aralığında ve $e*d= 1 \pmod{\Phi(n)}$ şartını sağlayan d sayısı üretilir [18,1,16,14].
- (n ,e) şifreleme işleminde kullanılmak için oluşturulan açık anahtardır.
- (n ,d) deşifreleme işleminde kullanılmak için oluşturulan gizli anahtardır.

3.2.2.1.2.2. Şifreleme

RSA algoritmasının şifreleme adımları aşağıdaki gibidir:

C ve M tamsayı olmak üzere;

- Açık anahtar olan (n, e) bilgiyi gönderecek olan kişi tarafından elde edilir.
- Açık metin $M \in [0, n-1]$ aralığında olmak şartıyla bir tamsayıya dönüştürülür [18].
- Şifreli metin $C \equiv M^e \pmod{n}$ şeklinde hesaplanır [18,1,4].
- Bilgiyi gönderecek olan kişi C şifreli metnini bilgiyi alacak olan kişiye gönderir.

3.2.2.1.2.3. Deşifreleme

Şifre çözmek için oluşturulan gizli anahtar (d) kullanılarak $M \equiv C^d \pmod{}$ eşitliğinin sağlanması sonucunda açık metin elde edilir [18,1,4].

3.2.2.1.3. DSA (Digital Signature Algorithm)

DSA, NIST (National Institute of Standards and Technology) tarafından sayısal imza standardı olarak yayınlanmıştır. ABD tarafından kullanılan dijital doğrulama standartlarının bir parçasıdır. DSA, RSA gibi oldukça yaygın kullanılan açık anahtarlı bir şifreleme algoritması olmasına rağmen, RSA 'dan farklı olarak sadece imzalamada kullanılabilir, şifrelemede kullanılamaz [1].

DSA algoritması şu şekilde çalışır: [1]

- p, bit uzunluğu 512 ve 1024 arasında olan bir asal sayı,
- q, bit uzunluğu 160 olan ve $p-1$ sayısını bölen bir asal sayı,
- g, $p-1$'den küçük herhangi bir h sayısı için $g \equiv h(p-1) / q \ (mod\ p)$ eşitliğini sağlayan 1'den farklı herhangi bir sayı olmak üzere p, q ve g sayıları uygun yöntemler kullanılarak bulunur [1].

3.2.2.1.4.ECC (Elliptic Curve Cryptography- Eliptik Eğri Şifrelemesi)

Eliptik Eğri Kriptografisi (ECC), 1985 yılında Victor Miller ve Neil Koblitz tarafından açık anahtar şifrelemesini uygulamak için alternatif bir mekanizma olarak keşfedildi. ECC, sonlu alanlar üzerindeki eliptik eğrilerin cebirsel yapısına dayanan asimetrik(açık) anahtar kriptografisinin teknik bir yoludur [19].

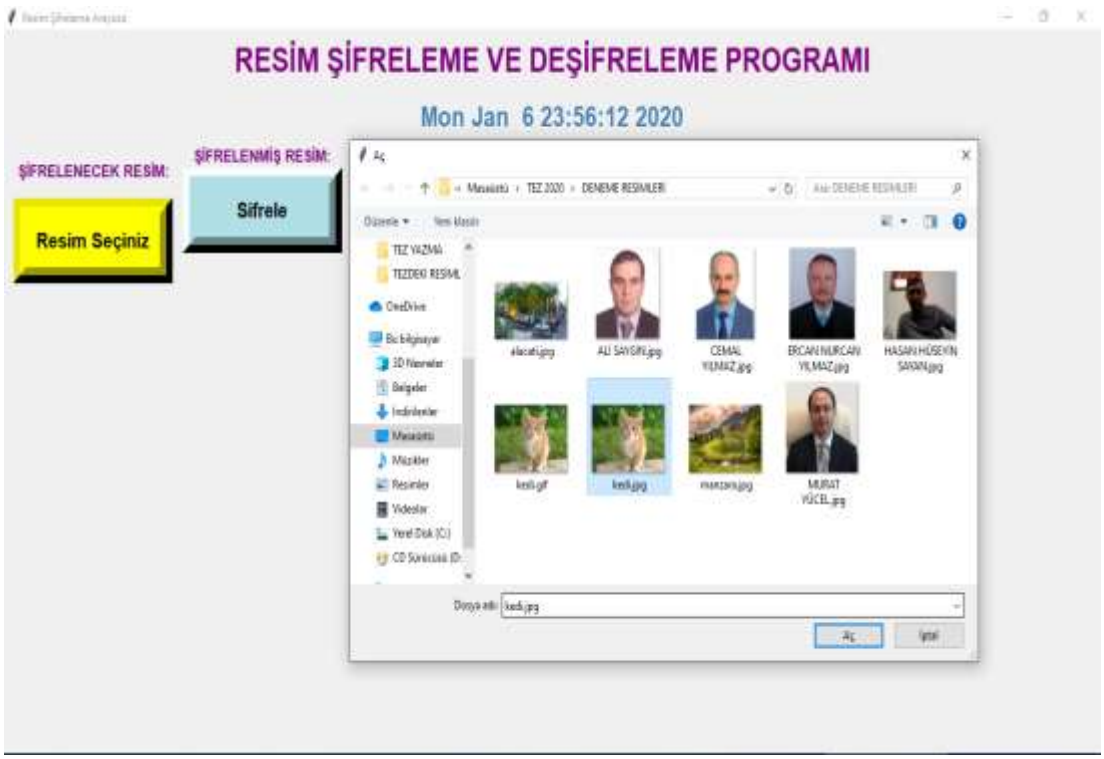
Algoritmada açık anahtar, karmaşık cebirsel ve geometrik denklemler kullanılarak üretilir. ECC, şifreleme işlemi için açık anahtar kullanırken, şifre çözme için özel anahtar kullanır. ECC, bilgi işlem gücünü ve pil kaynağı tüketimini azaltmak buna bağlı olarak da performansı artırmak üzere tasarlanmıştır. Bundan dolayı ECC, mobil cihaz uygulamaları için daha hızlı, verimli ve güvenli bir model sağlamıştır [17].

4. ÖRNEK UYGULAMA: RESİM ŞİFRELEME VE DEŞİFRELEME

Bu çalışmada asimetrik şifreleme (açık anahtar) yöntemi kullanılarak, resim aktarımının güvenli gerçekleştirilebilmesi için PYTHON programlama dilinde örnek bir uygulama geliştirilmiştir.

4.1. Örnek uygulama python kullanıcı arayüzü

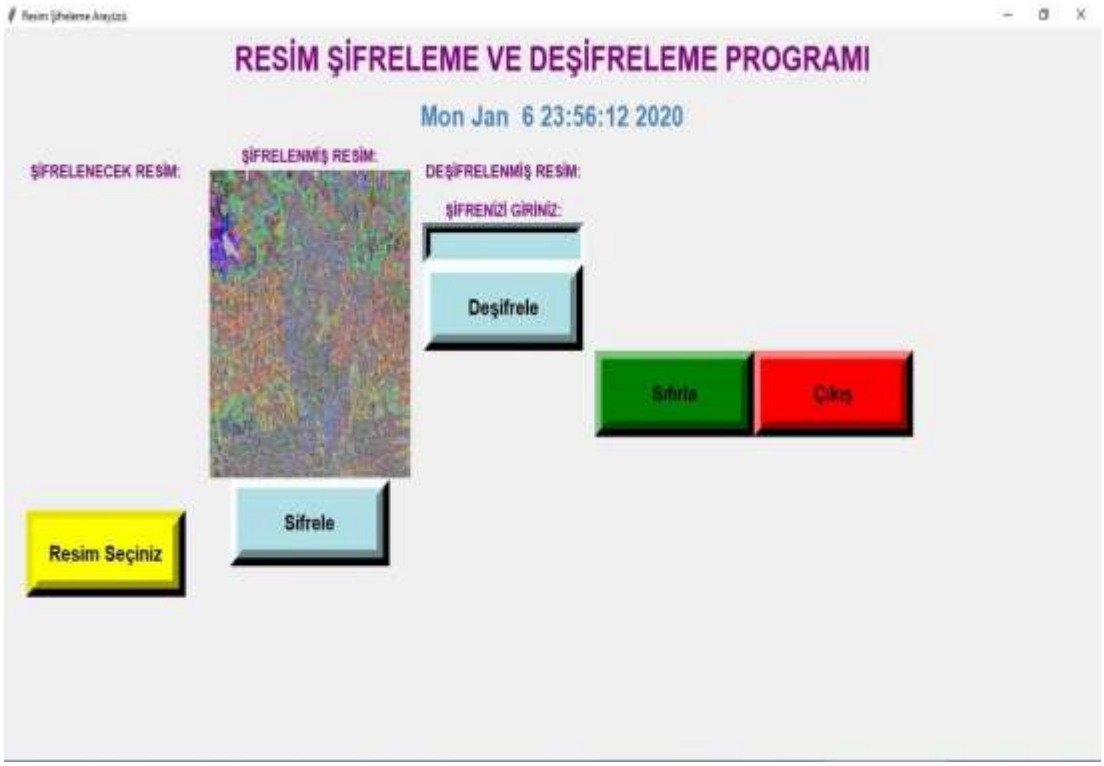
Uygulama çalıştırıldığında kullanıcının ilk olarak şifrelemek istediği resmi, uygulamada bulunan resim seçiniz butonuna basıldığında açılan resim yükleme penceresinden seçerek uygulamaya yüklemesi gerekmektedir.



Resim 4.2. Örnek uygulama resim yükleme penceresi

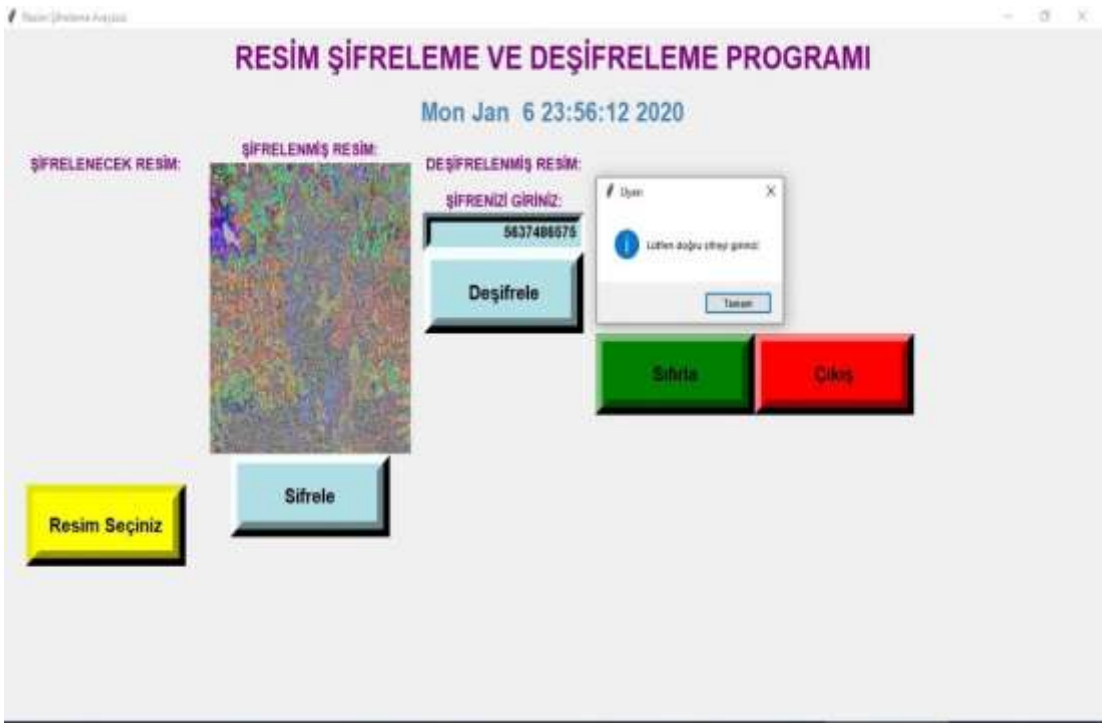
Resim 4.3. Örnek olarak şifrelenecek resim

Kullanıcı, arayüzde bulunan şifrele butonuna bastığında resim şifreleme işlemi gerçekleşir ve şifrelenen resim arayüzde görüntülenir .Şifrelenmiş resim daha sonra kullanılabilmesi için kullanıcının resim seçtiği dizine kaydolur.



Resim 4.4.Örnek olarak şifrelenmiş resim

Uygulamada asimetrik (açık anahtar) şifreleme yöntemlerinden biri olan RSA algoritması kullanılarak resim şifreleme ve deşifreleme işlemi gerçekleştirilmiştir. Geliştirilen yazılım, program her çalıştığında farklı gizli ve açık anahtarların üretilmesini sağlar. Resim şifreleme işlemi, RSA algoritmasının anahtar üretme aşamasında bulunan denklem yardımıyla üretilen, açık anahtar (n,e) ile sağlanır.Şifrelenen resim, kullanıcının şifrelenecek resmi seçtiği dizine kaydolur. Böylece bu uygulama ile kullanıcının seçtiği herhangi bir resmin, üçüncü şahıslar tarafından anlaşılmaması amacıyla şifrelenmesi sağlanmaktadır.



Resim 4.5. Örnek olarak şifrelenmiş resim ve hatalı şifre uyarı mesajı

Deşifreleme işleminin gerçekleşebilmesi için kullanıcının, arayüzde belirtilen alana kendisine ait şifresini girmesi ve deşifrele butonuna basması gerekmektedir. Bu aşamada RSA algoritmasıyla üretilen gizli anahtar (n,d) yardımıyla kullanıcı şifrelenmiş resmi deşifreleyebilmektedir. Geliştirilen yazılım, kullanıcının girdiği gizli şifreyi denetlemekte olup, kullanıcı tarafından yanlış şifre girildiği takdirde uygulama uyarı mesajı vermektedir.

Resim 4.6. Örnek olarak deşifrelenmiş resim

Gizli şifre kullanıcı tarafından doğru girildiği takdirde deşifreleme işlemi gerçekleşmektedir. Deşifrelenen resim arayüzde görüntülenmekte ve kullanıcının şifrelenecek resmi seçtiği dizine kaydolmaktadır.

SONUÇ VE ÖNERİLER

Şifreleme, bilgiyi matematiksel işlemleri kullanarak veya bilgiyi belli bir algoritmaya göre yer değiştirme işlemi yaparak karmaşık hale getirerek gerçekleştirilir. Bu işlemleri gerçekleştirerek bilgi güvenliğini sağlayan farklı şifreleme algoritmaları bulunmaktadır. Bu tez çalışmasında bahsedilen algoritmalar açıklanmıştır. Uygulamada kullanılan, asimetrik şifreleme yöntemlerinden biri olan RSA şifreleme algoritması, matematiksel işlemleri kullanarak şifreleme yapmaktadır. Dolayısıyla güvenlidir ve kullanımı çok yaygındır.

Kullanılan algoritmaların, ne kadar güvenli olursa olsun gelecekte çözülme tehlikesiyle karşı karşıya olduğu unutulmamalıdır. Dolayısıyla çözülme olasılığı çok daha düşük, güçlü, güvenilir, hızlı ve her alanda kullanılabilecek yeni şifreleme ve deşifreleme algoritmalarının geliştirilmesi gereklidir. Günümüz teknolojisi, yeni algoritmaların geliştirilebilmesi için oldukça gelişmiştir. Bununla birlikte farklı matematiksel işlemlerin kullanılmasıyla algoritmalara güç kazandırılabilir.

KAYNAKÇA

[1] HASSANPOUR, A. A. (2015). *ASAL SAYILARIN ŞİFRELEME TEORİSİNDEKİ UYGULAMALARI.* Erzurum.

[2] KODAZ, H., & BOTSALI, F. M. (2010). SİMETRİK VE ASİMETRİK ŞİFRELEME ALGORİTMALARININ KARŞILAŞTIRILMASI. *Teknik-Online Dergi*.

[3] OBAİD, Z., SABONCHİ, A., & AKAY, B. (2016). *KLASİK KRİPTOLOJİ YÖNTEMLERİNİN KARŞILAŞTIRILMASI.* Kayseri.

[4] COŞKUN, A., & ÜLKER, Ü. (2013). Ulusal Bilgi Güvenliğine Yönelik Bir Kriptografi Algoritması Geliştirilmesi ve Harf Frekans Analizine Karşı Güvenirlik Tespiti. *BİLİŞİM TEKNOLOJİLERİ DERGİSİ, CİLT: 6, SAYI: 2*, 31-39.

[5] ATALAY, N. S., DOĞAN, Ş., TUNCER, T., & AKBAL, E. (2019). İmge Şifreleme Yöntem ve Algoritmaları. *DÜMF Mühendislik Dergisi 10:3 (2019)*, 815-831.

[6] KIRIMLI, M., & ERDEM, O. A. (tarih yok). AÇIK ANAHTAR KRİPTOGRAFİSİ İLE SAYISAL İMZA TASARIMI VE UYGULAMASI.

[7] ŞAHİN, F. (2015). Modern Blok Şifreleme Algoritmaları. *İstanbul Aydın Üniversitesi Dergisi 26*, 23-40.

[8] BAYAR, E. (2012). *MODERN KRİPTOSİSTEMLERLE ŞİFRELEMENİN MODELLENMESİ İLE VERİ GÜVENLİĞİNİN SAĞLANMASI.* İstanbul.

[9] Akleylek, S., Yıldırım, H., & Yüce Tok, Z. (2 - 4 Şubat 2011). Kriptoloji ve Uygulama Alanları: Açık Anahtar Altyapısı ve Kayıtlı Elektronik Posta. *Akademik Bilişim'11 - XIII. Akademik Bilişim Konferansı Bildirileri*, (s. 713-718). İnönü Üniversitesi, Malatya.

[10] TOPALOĞLU, N., CALP, M. H., & TÜRK, B. (EYLÜL 2016). Bilgi Güvenliği Kapsamında Yeni Bir Veri Şifreleme Algoritması Tasarımı ve Gerçekleştirilmesi. *BİLİŞİM TEKNOLOJİLERİ DERGİSİ, CİLT: 9, SAYI: 3*, 291-301.

[11] Kamali, S. H., Shakerian , R., Hedayati , M., & Rahmani, M. (2010). A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption. *International Conference on Electronics and Information Engineering (ICEIE 2010)* (s. 141-145). Kyoto, Japan: IEEE.

[12] YILMAZ, M., & BALLI, S. (2016). VERİ ŞİFRELEME ALGORİTMALARININ KULLANIMI İÇİN AKILLI BİR SEÇİM SİSTEMİ GELİŞTİRİLMESİ. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:2, No:2*, 18-28.

[13] Panda, M. (2016). Performance Analysis of Encryption Algorithms for Security. *Signal Processing, Communication, Power and Embedded System (SCOPES).* India: IEEE.

[14] https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/şifreleme-yöntemleri

[15] Taki El-Deen, A. E., El-Badawy, E.-S. A., & Gobran, S. N. (2014). Digital Image Encryption Based on RSA Algorithm. *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 1, Ver. IV (Jan. 2014)*, PP 69-73 .

[16] Yerlikaya, T., Buluş, E., & Buluş, N. (tarih yok). ASİMETRİK ŞİFRELEME ALGORİTMALARINDA ANAHTAR DEĞİŞİM SİSTEMLERİ.

[17] Yassein, M. B., Aljawarneh , S., Qawasmeh, E., Mardini, W., & Khamayseh , Y. (2017). Comprehensive Study of Symmetric Key and Asymmetric Key Encryption Algorithms. *ICET*. Antalya,Turkey: IEEE.

[18] Beşkirli, A., Özdemir, D., & Beşkirli, M. (Ekim 2019). Şifreleme Yöntemleri ve RSA Algoritması Üzerine Bir İnceleme. *Avrupa Bilim ve Teknoloji Dergisi,Özel Sayı*, 284-291.

[19] Chaouch , A., Bouallegue, B., & Bouraoui , O. (2016). Software Application for Simulation-Based AES, RSA and Elliptic-Curve Algorithms. *2nd International Conference on Advanced Technologies for Signal and Image Processing - ATSIP'2016* . Monastir, Tunisia : IEEE.

ÖZGEÇMİŞ

Kişisel Bilgiler

Ad,Soyad : Şeyma BEŞİR

Uyruğu : T.C.

Doğum tarihi ve yeri : 03.02.1998 Samsun

Medeni hali : Bekar

Telefon : 0 (505 487 98 34)

e-mail : seymabesir@hotmail.com

Eğitim Derece	**Eğitim Birimi**	**Mezuniyet tarihi**
Lise	Trabzon Yomra Fen Lisesi	2016

Yabancı Dil

İngilizce