KSÜ Mühendislik Bilimleri Dergisi, 27(4), 2024
Araştırma Makalesi

KSU J Eng Sci, 27(4), 2024
Research Article

Kahramanmaras Sutcu Imam University
Journal of Engineering Sciences

Geliş Tarihi : 30.04.2024
Kabul Tarihi : 15.07.2024

Received Date : 30.04.2024
Accepted Date : 15.07.2024

KÖK ŞİFRE ALGORİTMA TASARIMI VE PERFORMANS ANALİZİ

ROOT PASSWORD ALGORITHM DESIGN AND PERFORMANCE ANALYSIS

Çağlar AKTÜRK[1*] (ORCID: 0009-0004-9850-1176)
Ahsen GÖKBOĞA[1] (ORCID: 0009-0007-6230-0630)
Zeynep YEKELER[1] (ORCID: 0009-0004-1702-3417)

[1] Milli Eğitim Bakanlığı, Şehit Osman Arslan Kız AİHL, Çorum, Türkiye

*Sorumlu Yazar / Corresponding Author: Çağlar AKTÜRK, cakturkmat@hotmail.com

ÖZET

Geçmişten günümüze kadar verilerin eksiksiz ve güvenli bir şekilde aktarılması sorun olmuştur. Şifreleyerek verileri aktarma yaygın olarak kullanılan bir yöntemdir. Farklı şifreleme algoritmaları geliştirilmiştir. Bu algoritmaların birbirlerine göre avantaj ve dezavantajları vardır. Kullanılan şifreleme yöntemlerinin genelde yabancı kaynaklı olduğu görülmektedir. Bu çalışmada hızlı ve veri bütünlüğünü koruyan, yerli ve özgün bir algoritma tasarlanması amaçlanmıştır. King (2010)'un "Matematik Sanatı" kitabındaki metinlerden yararlanılmıştır. Farklı boyutlardaki metinlerle algoritmanın şifreleme ve şifre çözme performansı incelenmiştir. Metinsel verileri şifrelemek için simetrik şifreleme yöntemi kullanılmıştır. Algoritma, irrasyonel sayıların rasgeleliğinden yararlanılarak tasarlanmıştır. Algoritmada ortak anahtar kullanılmaktadır. Algoritma Python ile uygulama haline getirilmiş ve UTF-8 karakter seti kullanılmıştır. Şifreli metinde harf frekans analizi yapılmıştır. Orijinal metin ile arasında dağılım olarak benzerlik olmadığı görülmüştür. Metinler orijinal hale getirildiğinde herhangi bir veri kaybı olmadığı tespit edilmiştir. Şifreleme ve çözme süresi ile metinlerin boyutları ölçülmüştür. Elde edilen sonuçlar yaygın olarak kullanılan TEA, XTEA, AES, DES, RSA ve RC5 şifreleme algoritmaları ile karşılaştırılmıştır.

Anahtar Kelimeler: Algoritma tasarımı, irrasyonel sayılar, performans analizi, şifreleme, şifre çözme

ABSTRACT

Complete and secure transfer of data has been a problem since the past. Transferring data by encryption is a widely used method. Different encryption algorithms have been developed. These algorithms have advantages and disadvantages compared to each other. It seems that encryption is generally of foreign origin. In this study, it was aimed to design a local and original algorithm that is fast and maintains data integrity. Texts in King's (2010) book "The Art of Mathematics" were used. The performance of the algorithm with texts of different sizes was examined. Symmetric encryption method was used to encrypt textual data. The algorithm is designed by taking advantage of the randomness of irrational numbers. A public key is used in the algorithm. The algorithm was implemented with Python and the UTF-8 character set was used. Letter frequency analysis was performed. It was seen that there was no similarity with the original text. It has been determined that there is no data loss when the texts are restored to their original form. The encryption and decryption time and the size of the texts were measured. The results obtained were compared with commonly used TEA, XTEA, AES, DES, RSA and RC5 encryption algorithms.

Keywords: Algorithm design, irrational numbers, performance analysis, encryption, decryption.

GİRİŞ

ToCite: AKTÜRK, Ç., GÖKBOĞA, A., & YEKELER, Z., (2024). KÖK ŞİFRE ALGORİTMA TASARIMI VE PERFORMANS ANALİZİ. *Kahramanmaraş Sütçü İmam Üniversitesi Mühendislik Bilimleri Dergisi*, 27(4), 1361-1374.

Teknolojinin hızlı bir şekilde gelişmesiyle elden yapılan birçok işlem sanal ortam üzerinden gerçekleştirilmeye başlanmıştır. Bu ortamlarda önemli bilgilerin ve verilerin paylaşılıyor oluşu güvenlik ihtiyacının önemini ortaya koymaktadır. Bilgilerin ve verilerin güvenli şekilde saklanması ve iletimi için günümüzde çoğu alanda kullanılan şifreleme yöntemlerinde güvenlik ve verimlilik gibi problemler ortaya çıkmıştır (İşçimen, 2023). İnternet kullanımının yaygınlaşması ile bilgilerin güvenliğinin sağlanmasının daha ciddi bir şekilde ele alınmasını gerektirmektedir, (Süküt, 2024). Bu sorunun çözülmesi için yapılan çok sayıdaki araştırmada bilginin güvenliği için gizlilik, bütünlük ve erişilebilirliğin sağlanmasının ve korunmasının insanlar açısından önemli olduğu açık bir şekilde görülmektedir (Topaloğlu vd., 2016). Bugünkü iletişim sistemleri verileri anlamlı olmayan cümleler haline getirip şifreleyerek alıcıya gönderilmesini, alıcının ise yapılan işlemin tam tersini yaparak asıl metne ulaşabilmesini sağlar (Yerlikaya, 2006). Hassanpour (2015), şifrelemeyi gizliliğin zayıf olduğu ortamlarda bilgiyi güvenli şekilde koruma ve bilginin anahtar olmadan okunmasını engelleme olarak ifade etmektedir. Bu şekilde bilgi kötü niyetli biri tarafından anlaşılmaz ve bilginin ele geçirilmesinin önüne geçilmeye çalışılır.

Şifreleme, insanların çok eski tarihlerden beri bilgilerini korumak amacıyla tercih ettiği bir yöntemdir. Fakat bilgi ve bilginin aktarım yöntemleri de zamanla değişime uğramıştır. Günümüz şartları her ne kadar daha hızlı ve büyük miktarda bilgi ulaşımına imkan sağlasa da bu durum ciddi bir güvenlik açığına ortam hazırlamıştır. Bu noktada siber güvenlik, bu açığın kapatılması ve bilgi güvenliğinin sağlanması alanında önemli bir role sahiptir (Üstün, 2022). Şifreleme ilk olarak Eski Mısırlıların anıtları üzerindeki yazılarda, daha sonrasında İbranilerin kutsal kitaplarında kullanılan kelimelerde görülmüştür (Soyalıç, 2005). Şifrelemenin tarihteki en bilinen örneklerinden biri, Julius Caesar'ın askerleri ve komutanlarıyla iletişim kurmak için kullandığı Sezar şifreleme yöntemidir (Stinson, 2002). Bu yöntemde veri, harflerin belirli ve sabit bir sayı kadar ötelenmesiyle şifrelenir. Anadolu'da geçmiş dönemlerde şifreleme ile haberleşmenin sağlandığı bazı olaylara rastlanmaktadır. Şifrelemenin kullanımının görüldüğü önemli olaylardan biri Kurtuluş Savaşı'nın dönüm noktalarından olan Büyük Taarruz'dur (Yeşilbaş, 2016). Bu savaşta askerlerin halk ile oldukça basit bir şifreleme yöntemi kullanarak haberleştikleri tespit edilmiştir.

Bilgi güvenliğinde verilerin gizli kalması, bütünlük içermesi ve doğrulanabilmesi gereken özelliklerdendir (Etem, 2022). Şifrelenen verilerin şifresi çözüldüğünde veri kaybı olmamalı, veri en yüksek düzeyde korunmalı, şifreli veri ile orijinal veri arasında kolay ilişki kurulamamalı, şifreleme işlemi basit şekilde gerçekleştirilmeli fakat şifre kolay çözülmemelidir (Yeşilbaş, 2016). Şifreleme yöntemlerinde doğal olarak güçlü ve zayıf taraflar bulunmaktadır. Şifrelenmek istenen verilere diğer kişilerin ulaşılması istenmediğinden, algoritma karmaşık hale getirilmeye çalışılmaktadır. Tercih edilecek şifreleme algoritması iyi incelenerek tercih edilmeli, hangi amaç doğrultusunda kullanılacağına göre karar verilmelidir. Şifreleme sisteminin güvenliği ne kadar iyi olursa olsun işlem hızının yavaş olması kullanım alanlarını kısıtlayacaktır. Bu nedenle, daha güvenli ve hızlı şifreleme algoritmalarının seçimine dikkat edilmelidir, (Şengel vd., 2020).

Tüm şifreleme ve şifre çözme işlemlerinde algoritma ve anahtar bulunmaktadır. Şifreleme ve şifre çözme işlemleri belirli kuralları olan algoritmalar ile yapılmaktadır. Algoritmalar matematiksel temele dayanarak oluşturulur. Nabiyev ve Zeka (2016), verilerin gizliliğini sağlamak için yerine koyma, yer değiştirme ve cebirsel yöntemler kullanıldığını ifade ederler. Yerine koymada metindeki harflerin olduğu aynı yere başka sayı ya da semboller konulur, yer değiştirmede metindeki harfler değiştirilmeden yerleri aynı şekilde değiştirilir. Cebirsel yöntemler ise matematiksel işlemler kullanılarak oluşturulan şifrelemelerdir.

Metnin şifrelenmesi ve şifresinin çözülebilmesi için anahtara da ihtiyaç duyulmaktadır. Anahtarların aynı olduğu durumlarda bu işlemler simetrik veya gizli anahtarlı şifreleme sistemleri olarak; anahtarlar farklı olduğunda ise asimetrik ya da açık anahtarlı sistemler olarak adlandırılır (Soyalıç, 2005). Simetrik anahtarlı şifreleme, gönderici ve alıcının bilgiyi hem şifrelemede hem de şifre çözmede ortak bir anahtar kullandıkları şifrelemedir. Simetrik şifreleme, bilgiyi şifreleme ve şifreli bilgiyi çözmede çok hızlı olmasından kaynaklı günümüzde yaygın kullanılmaktadır. Simetrik anahtarın kullanıldığı sistemler asimetrik anahtarın kullanıldığı sistemlerden daha kolay ve hızlıdır; fakat bilgilerin güvenliği açısından iki tarafın anahtarı değiştirme zorunluluğu bir dezavantajdır (Aghayev, 2017). Asimetrik şifreleme yöntemleri anahtarın paylaşımı açısından daha güvenlidir. Taraflar görüşmelerine gerek kalmadan kişisel anahtarlar oluşturabilir ve bilgilerini bu anahtarla şifreleyebilirler. Sadece simetrik yöntemlerin değil asimetrik şifreleme yöntemlerinin de dezavantajları bulunmaktadır. Asimetrik şifrelemeler çok büyük sayılar ve karmaşık cebirsel işlemlerle yapılır (Kodaz ve Botsalı, 2010). Bu durum şifrelerin çözülmesinin ciddi bir zaman ve iyi bir donanım gerektireceği anlamına gelmektedir.

Şifrelemede geleneksel olarak bilinen ve kaydırma şifreleme diye adlandırılan Sezar şifreleme çok tercih edilmemektedir. Polat (2022), kaydırma şifrelemede aynı sayıda öteleme yapıldığı için pek güvenilir bir yöntem olmadığını, bu nedenle şifre çözmenin çok uzun zaman almayacağını ifade etmiştir. Şifrelemede geleneksel yöntemlerin yanında bir de modern yöntemler vardır. Modern şifrelemenin tüm şifreleme ve şifre çözme algoritmalarında anahtar kullanılmaktadır (Üstün, 2022). Veriyi şifreleme ve şifre çözme bu anahtarla yapılmaktadır. Simetrik şifreleme yöntemlerinden Veri Şifreleme Standardı (Data Encryption Standard-DES) şifreleme algoritmasında veriler sabit uzunluktaki bloklara ayrılır ve anahtar yardımıyla her blok ayrı ayrı şifrelenir. Anahtarın uzunluğuna göre şifre çözme işlemi kolaylaşıp zorlaşmaktadır (Buhurcu, 2022). Simetrik şifreleme algoritmalarından biri de Gelişmiş Şifreleme Standardı'dır (Advanced Encryption Standard-AES). Blok şifreleme algoritması olan AES, güçlü ve hızlı bir şifreleme algoritmasıdır (Topaç, 2023). Bu algoritmanın dezavantajı basit bir matematiksel algoritma olmasına rağmen büyük bloklara sahip olduğu için fazla güç ve kaynak harcamasıdır (Kaya ve Türkoğlu, 2023). Küçük Şifreleme Algoritması (Tiny Encryption Algorithm-TEA) şifreleme algoritması blok şifrelemeyi kullanır. Diğer algoritmalara göre basit oluşu ve daha az satırdan oluşan algoritma yapısıyla dikkat çekmektedir (Günden, 2010). Genişletilmiş Küçük Şifreleme Algoritması (Extended Tiny Encryption Algorithm-XTEA) genişletilmiş TEA olarak adlandırılır ve TEA gibi aritmetik işlemleri kullanır (Ökdem ve Kırtay, 2018). Rivest Cipher 5 (RC5) şifreleme algoritması blok ve anahtar büyüklüğü, tur sayısı ile veriye bağlı değişken özelliği bakımından diğer algoritmalardan farklıdır (Polat, 2022). Asimetrik şifreleme algoritmalarından olan Rivest-Shamir-Adleman (RSA) günümüzde de kullanılmaktadır. RSA'da gönderilecek mesaj belirli aralıktaki pozitif tam sayı bloklarına dönüşümü yapılarak şifrelenir (Topaç, 2023). Günümüzde kullanımı oldukça yaygın olan bu şifreleme sistemlerinin çoğu yabancı kaynaklıdır. Bilgi güvenliğine ciddi bir tehdit oluşturacağından yerli sistemlerin tercih edilmesi oldukça önemlidir (Ülker, 2014).

Günümüzde algoritmaların güvenliği anahtarlar ile sağlanır. Şifreleme ve şifre çözme işlemlerinin tümünde anahtarlardan yararlanılır. Anahtar, gönderici ve alıcı tarafından önceden belirlenen ve başkalarının bilmediği özel verilerdir. Gönderici bu anahtarı kullanarak bilgiyi şifreler ve bir kanal üzerinden alıcıya gönderir; alıcı ise kendisine gelen bilgiyi yine anahtar yardımıyla çözerek asıl bilgiye ulaşılır (Soyalıç, 2005). Algoritmalarda anahtar kullanımının en önemli avantajı uygulamaya zorla giriş yapan herhangi birinin anahtarı bilmeden hiçbir işlem yapamaması ve bilgilerin bu şekilde güvende tutulabilmesidir (Günden, 2010). Gizli anahtarlı şifreleme ve şifre çözmede aynı anahtar kullanılmaktadır (Hassanpour, 2015). Açık anahtarlı şifrelemede ise tüm kullanıcıların hem şifreleme hem de şifreyi çözmede kullandığı açık ve gizli olan iki tür anahtarı vardır (Aghayev, 2017). Açık anahtarı herkes görebilir. Gizli anahtar ise sahibi dışında kimsenin bilmediği bir anahtardır. Şifreleme işlemleri tamamlandıktan sonra şifrelenen metin gizli bir anahtarla birlikte alıcıya güvenlik ve gizlilik ilkelerine uygun bir şekilde gönderilir (Özyılmaz, 2014).

Şifrelemede en önemli unsurlardan biri de anahtar değişiminin nasıl yapıldığıdır. Şifrelemede sürekli olarak aynı anahtar kullanılmamalı, kullanılan gizli anahtar belirli ve kısa periyotlarla değiştirilmelidir. Daha önceden birbiriyle tanışmayan kişiler arasında anahtar alışverişi yapılması güvenlik açığı ortaya çıkarabilir (Soyalıç, 2005). Diffie-Hellman anahtar değişimi algoritması şifreleme alanında bir dönüm noktası kabul edilebilir; çünkü bu zamana kadar önemli bir sorun teşkil eden anahtar değişiminde kişilerin yüz yüze görüşmesi gibi bir güvenlik açığı oluşturmadan çözüm getirmiştir (Ülker, 2014). Bu yöntem ile simetrik şifreleme algoritmasında kullanılan gizli anahtar belirli aralıklarla değiştirilebilir ve değişimdeki güvenlik sorunu ortadan kalkmış olur.

Güçsüz bir şifreleme algoritması beraberinde dezavantajdan başka hiçbir şey getirmeyecektir. Şifreleme algoritmaları sistemin hızı ve maliyeti gibi kriterler de göz önünde bulundurularak tasarlanmalıdır. Sistemin güvenliğini kanıtlamak için literatürde kabul görmüş bazı analizler kullanılmalıdır. Bunlardan biri de harf frekans analizidir (Etem, 2022). Şifrelemenin hangi dilde yazıldığı bilinirse frekans analizi yapmak daha kolay olmaktadır (Çimen vd., 2008). Bu yöntem bir dilin sahip olduğu belirli yapısal nitelikleri kullanarak şifre çözme işlemini gerçekleştirmeyi hedeflemektedir (Arda ve Buluş, 2003). Türkçede en çok kullanılan sesli harfler A, E, İ ve sessiz harfler ise N, R, L, K, D; en az kullanılan harfler ise C, Ö, P, F, J'dir (Dalkılıç ve Dalkılıç, 2002). Harf frekans analizinde metnin oluşturulduğu dilde en çok kullanılan harfler ile şifrelenmiş metinde en çok bulunan harflerin sıklığı belirlenmekte, en çok kullanılan harfler karşılıklı olarak eşleştirilip ve yerine koyulmaktadır (Buluş, 2006). Bu şekilde işlem tüm harflere uygulanılarak metin çözülmeye çalışılmaktadır. Frekans analizi en çok kullanılan harften en az kullanılana kadar eşleşmelerle yapıldığında şifre çözme işlemindeki başarı oranı artmaktadır (Çimen vd., 2008). Bu analiz aynı

zamanda şifreli metni çözmek için kullanılan bir saldırı yöntemidir. Algoritmaların da bu gibi saldırılara karşı güçlü olması gerekmektedir.
Bu çalışmanın amacı, gelişen teknoloji ile birlikte güvenlik ihtiyacına yönelik güvenli ve verimli bir şifreleme algoritması tasarlanması ve incelenmesidir. Çalışmada tasarlanan algoritma ile geleneksel ve günümüz şifreleme yöntemlerini ele alarak avantaj ve dezavantajlarını analiz etmektedir. Bilginin aktarımı ve siber güvenli açısından daha etkin stratejilerin geliştirilmesi açısından literatüre katkı sağlaması beklenmektedir.

Literatür Araştırması

Literatürde şifreleme ile ilgili birçok çalışma vardır. Sivan vd. (2023), Buhurcu (2022), Eskicioğlu ve Işık (2022), Topaloğlu vd. (2016) yeni bir şifreleme algoritma tasarımı yapmışlardır. Sivan vd. (2023), yaptıkları çalışmada verileri üç anahtar kullanarak ASCII kodu ile şifrelemiştir. Veriler yüksek hızda ve kayıpsız şekilde metin ve rakamlar olan her veri şifrelenmiştir. Yapılan testler sonucunda yüksek verilerde bile oldukça hızlı bir sonuç elde edildiği sonucuna ulaşmışlardır. Üç anahtar kullanılıyor olması şifrelemede güvenliği artırmasına rağmen anahtar yönetiminde karmaşıklık oluşturabilmektedir. Buhurcu (2022) çalışmasında, simetrik anahtarlı AES algoritması kullanarak güvenli bir iletişim modeli önermiştir. Gizli anahtar için asimetrik şifreleme algoritması olan RSA kullanmıştır. Mobil cihazlar için bir mesajlaşma uygulaması geliştirerek uygulamanın performansını incelemiştir. Uygulama yüksek güvenlik sağlamıştır. Her veri türünde etkili sonuç vermemektedir. Eskicioğlu ve Işık (2022), çalışmalarında hibrit bir şifreleme algoritması tasarlamışlardır. Üç kademeden oluşan algoritmada verilerin güvenliği sağlanmaya çalışılmıştır. Şifreleme durağan olarak belirlenen anahtarlar ve değişken indislerle gerçekleşmektedir. Algoritmada pi sayısı ile fibonacci dizisi kullanılmıştır. Algoritmanın mobil ortamlarda sorunsuz çalıştığı, uygulanabilirliği farklı yöntemlerle denendiği ve yüksek doğruluk sonuçları elde edildiği görülmüştür. Dinamik indis değişimi ve rasgele sayı ataması düşük performanslı cihazlarda kaynak tüketimin artırabilmektedir. Topaloğlu vd. (2016), çalışmalarında bilgi güvenliğini sağlamak için alfabetik yer değiştirme tekniğine dayanan özgün bir şifreleme algoritması geliştirmişlerdir. Algoritma tasarımında Sezar Şifreleme, Çoklu Alfabe ve Enigma tekniklerinden yararlanmışlardır. Bu algoritma ile metinler şifrelenerek güvenli şekilde saklanabilmekte ve gerektiğinde de şifresi çözülerek eski haline getirilmektedir.

Simetrik ve asimetrik şifreleme algoritmalarının incelenmesi ve karşılaştırması ile ilgili olarak Ülker (2014), Günden (2010), Kodaz ve Botsalı (2010), Buluş (2006) ve Yerlikaya (2006); şifreleme algoritmalarının performans analizi ile ilgili olarak Rameel ve Asif (2024), Kaya ve Türkoğlu (2023), Karagöz (2022), Ökdem ve Kırtay (2018) çalışmaları bulunmaktadır. Garipcan ve Erdem (2024) çalışmalarında rasgelelik kavramından bahsetmişlerdir. Rasgele sayı üreteçlerinin nasıl çalıştığını açıklamışlardır. Çalışmalarının etkinliğini ve güvenirliğini istatiksel testlerle incelemişlerdir.

Mevcut çalışma ve algoritmalarda farklı yöntemler kullanılmaktadır. Yerli algoritmalarla literatürde daha az karşılaştırıldığı görülmüştür. Bu çalışmanın yapılma nedeni verilerin saklanması ve aktarılmasının her zaman güncel bir konu olması ve yerli bir şifreleme algoritma tasarımına katkı sağlamak olmuştur. Bu çalışmada yeni ve özgün bir algoritma tasarlanmış, performans analizi yapılarak güncel algoritmalarla karşılaştırılmıştır. Kök Şifre algoritmasının diğer çalışmalardan farkı; algoritmada irrasyonel sayıların rasgeleleğinin kullanılmasıdır. Yapılan çalışmanın kriptoloji alanına katkı sağlaması düşünülmektedir.

YÖNTEM

Bu çalışmada, metinsel verilerin şifrelenip güvenli şekilde gönderilmesi ve eksiksiz şekilde şifrenin çözülmesi için simetrik şifreleme yöntemi kullanılmıştır. İrrasyonel sayıların rasgeleliğinden yararlanılarak özgün bir şifreleme ve şifre çözme algoritması tasarlanmıştır. Metinsel veriler şifrelenip metinsel veriler elde edilmiştir. Bu algoritma için sözde kodu Şekil 1'deki gibidir. Bu algoritma Python dilinde kodlanarak uygulama haline getirilmiştir.

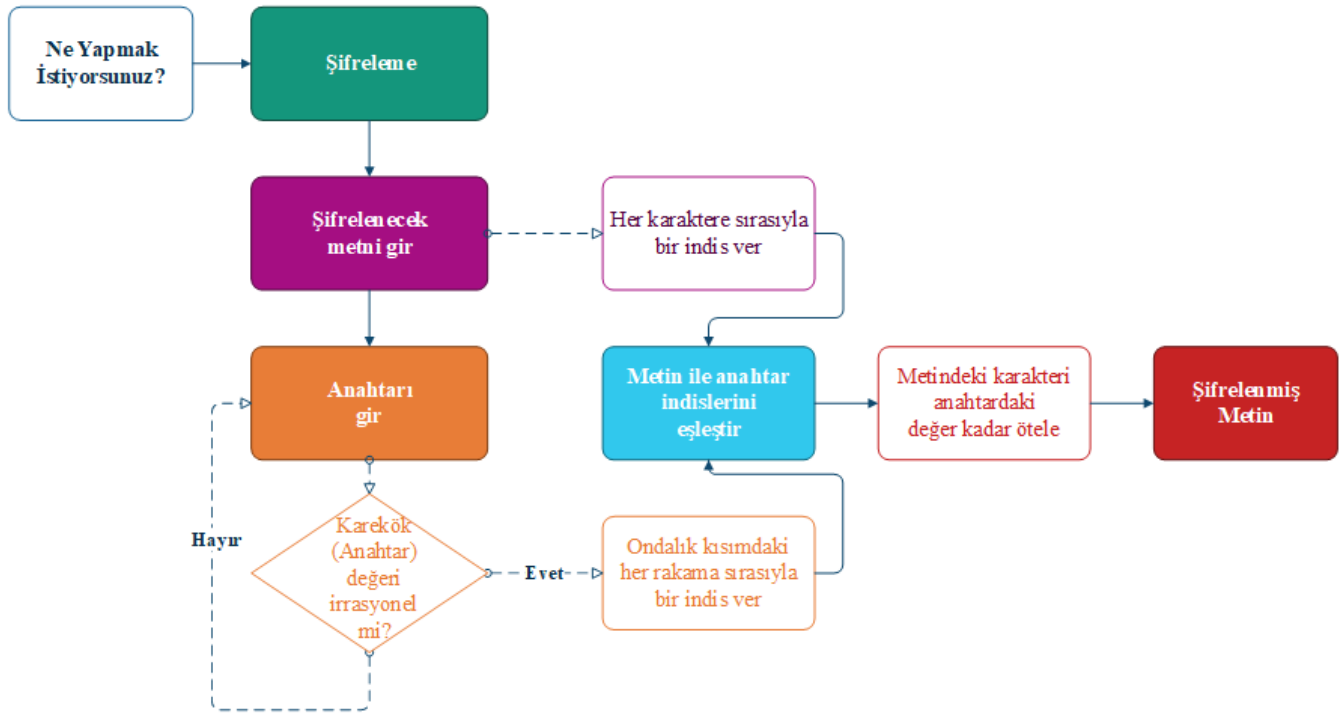
Programlamada Türkçe karakterleri de kapsadığı için UTF-8 karakter seti seçilmiştir. Algoritmanın şifreleme ve şifre çözme performansları incelenmiştir. Şifrelenen ve şifresi çözülen verinin boyutu (byte), şifreleme ve şifre çözme süreleri (milisaniye) program yardımıyla ölçülmüştür. Kök Şifre olarak adlandırdığımız algoritmanın performansının incelenmesinde King (2010)'un "Matematik Sanatı" kitabındaki metinlerden faydalanmıştır. Literatürde yaygın olarak kullanılan güncel şifreleme algoritmaları ile aynı boyuttaki metinler üzerindeki şifreleme ve şifre çözme performansları karşılaştırılmıştır.

```
1   Başla
2   Göster "Şifrelenecek metni gir:"
3   metin = Kullanıcı_Girdisi()
4   Göster "Şifreleme anahtarını gir:"
5   anahtar = Kullanıcı_Girdisi()
6   Eğer Karekök_Irrasyonel_Mi(anahtar) ise:
7       anahtar_rakamları = Ondalık_Rakamları_Al(Karekök(anahtar))
8       şifrelenmiş_metin = ""
9       For i = 0 to Uzunluk (metin) - 1:
10          öteleme_değeri = anahtar_rakamları [i % Uzunluk(anahtar_rakamları)]
11          şifrelenmiş_metin += Karakter_Ötele(metin[i], öteleme_değeri)
12      Göster "Şifrelenmiş Metin: " + şifrelenmiş_metin
13  Değilse:
14      Göster "Anahtar irrasyonel değil, lütfen başka bir anahtar girin."
15  Bitir
```

Şekil 1. Kök Şifre Algoritmasının Sözde Kodu

Şifreleme Algoritması

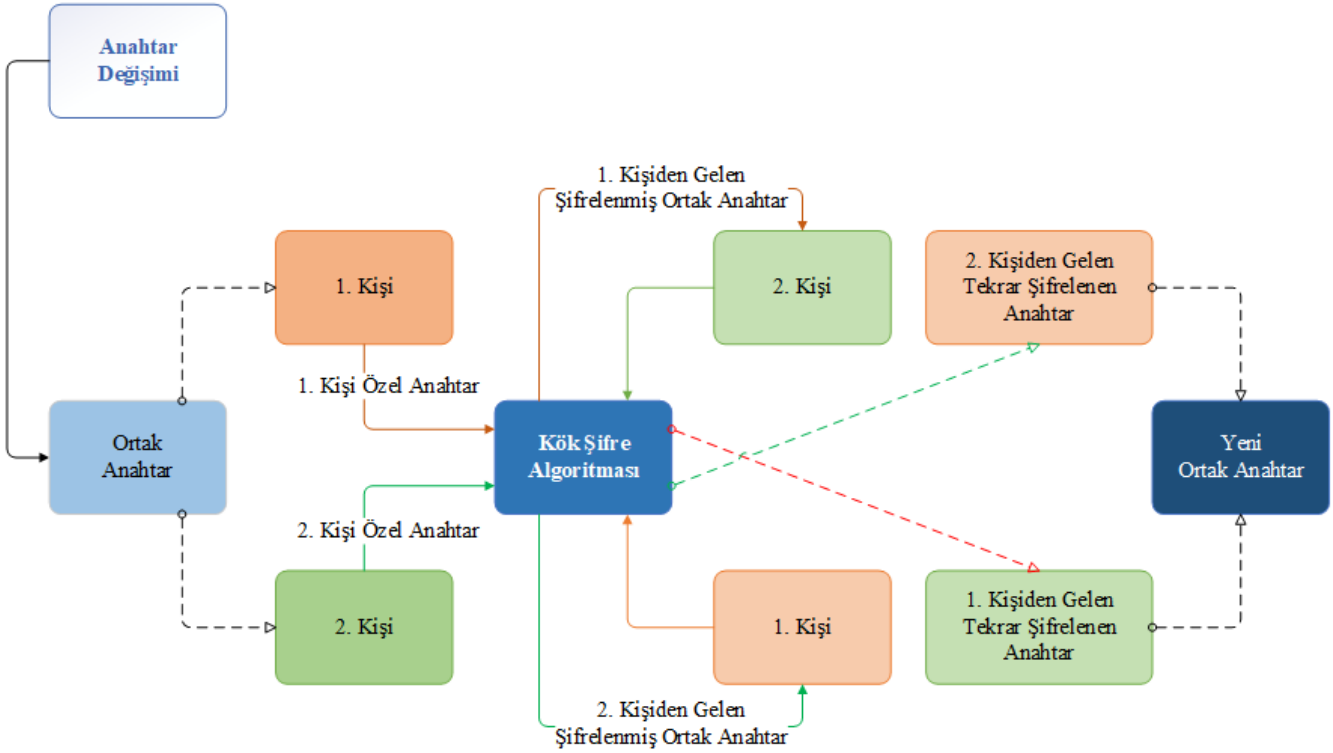
Şifreleme iki kısımdan oluşmaktadır. İlk kısımda şifreleme anahtarı uygun şekilde seçilmekte; ikinci kısımda metindeki harf, rakam ve boşluk gibi karakterler anahtar ile eşleştirilip şifrelenmektedir. Metnin şifrelenmesi ve şifrenin çözülmesi için ortak bir anahtar kullanılmaktadır. Anahtar için seçilen sayının karekök değeri bulunmaktadır. Bu değerin ondalık kısmındaki her rakama bir indis atanmaktadır. Şifrelenmek istenen metindeki her karaktere de birer indis atanmakta ve bu karakterler aynı indisli anahtar değeri ile eşleştirilmektedir. Daha sonra her karakter eşleşmedeki anahtar değeri kadar ötelenmektedir. Bu şekilde her karaktere karşılık yeni bir karakter tanımlanmaktadır. Şifreleme algoritması Şekil 2'de gösterilmiştir. Şifreleme yapılan anahtar ile şifre çözme işlemi yapılmaktadır, aksi takdirde metin eski haline getirilememektedir.



Şekil 2. Şifreleme Algoritması

Anahtar Seçimi

Şifreleme algoritması irrasyonel sayıların ondalık kısmındaki rakamların düzensiz sıralanmasından faydalanılarak oluşturulmuştur. Thomas vd., (2014) irrasyonel sayıları, ondalık açılımları tekrarlı olmayan ve rasyonel olmayan reel sayılar olarak tanımlamıştır. İrrasyonel sayıların ondalık kısmındaki rakamlar düzenli değil rasgele şekilde gelmektedir. Bunun sonucunda hangi karaktere ne kadar öteleme yapılacağı belli değildir. Anahtar seçiminde irrasyonel sayılar olması istenmektedir. Eğer karekökten çıkabilen rasyonel bir sayı anahtar olarak girilecek olursa program uyarı vererek farklı bir değerin girilmesini istemektedir. Sıfır rakamı ile eşleşen karaktere öteleme yapmamaktadır. Her anahtar değişiminde farklı ötelemelerle yeni şifrelenmiş metinler ortaya çıkmaktadır. Şifre çözme sürecinde ise şifreleme algoritması ters şekilde çalışmaktadır.



Şekil 3. Anahtar Değişimi

Anahtar Değişimi

Anahtar güvenlik açısından ya da istenildiği zaman değiştirilebilmektedir. Anahtar değişimi de aynı şifreleme algoritması ile yapılmaktadır. Şekil 3'te anahtar değişim algoritması gösterilmektedir. Asimetrik şifreleme yöntemlerinde olduğu gibi ortak anahtarın yanı sıra anahtar değişiminde kullanmak için herkesin kendine özgü bir özel anahtarı vardır. Ortak anahtar şifreleme ve şifre çözme için, özel anahtar da anahtar değişiminde gereklidir. Ortak anahtar iki kişi tarafından karşılıklı olarak bilinse de özel anahtarı sadece kişiler bilmektedir. En son kullanılan ortak anahtar kişilerin kendine özel anahtarları ile şifrelenip birbirine gönderilir. Gelen şifreli mesaj tekrar kişiye özel anahtarla şifrelendiğinde aynı anda iki tarafta da ortak bir karakter oluşmaktadır. Programda karaktere karşılık gelen sayı değeri anahtar olarak kabul edilmekte, bir sonraki anahtar değişimine kadar güvenli şekilde kullanılmaktadır.

BULGULAR

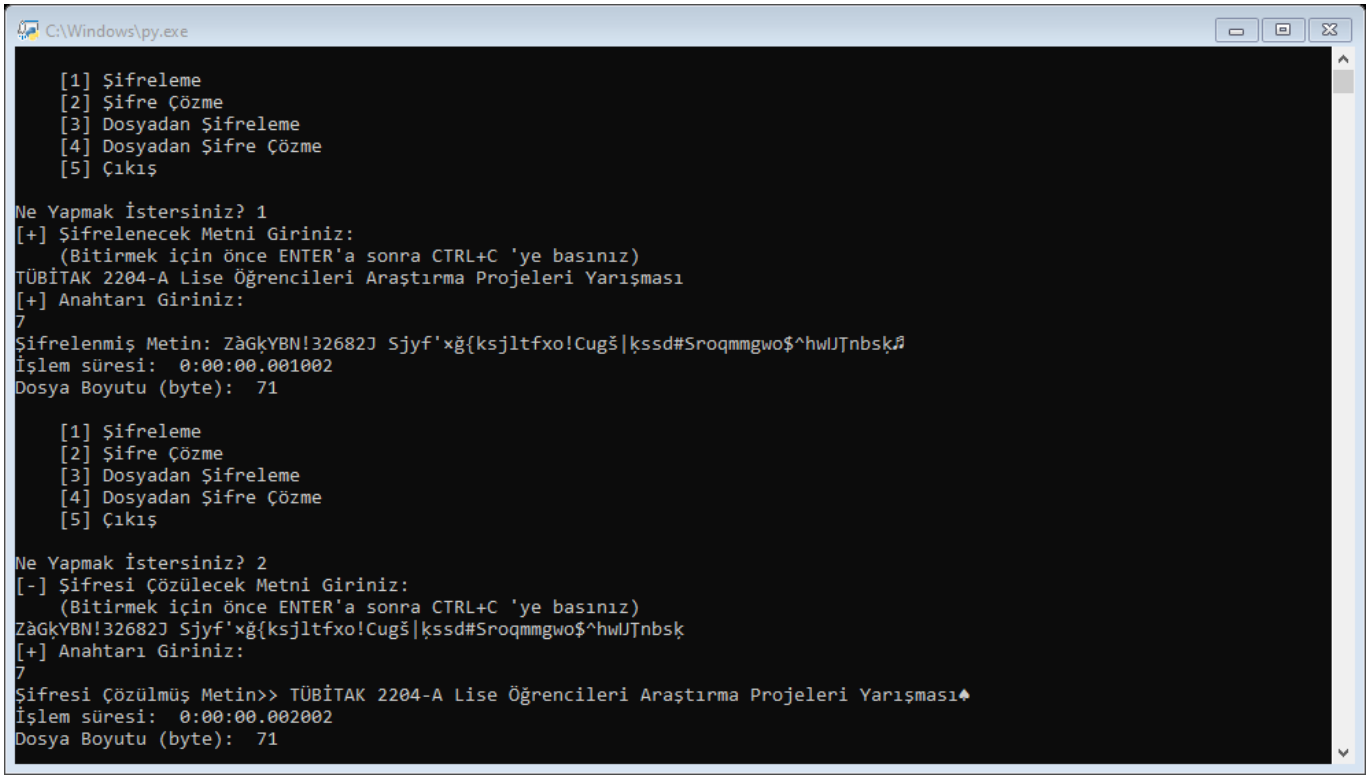
Bu kısımda farklı dosya boyutundaki metinlerin şifreleme ve şifre çözme süreleri ile elde edilen verilerin boyutları gösterilmiştir. Programda süreler milisaniye (ms) ve dosya boyutları byte (B) ile gösterilmektedir. Dosya boyutlarında kilobyte (KB) dönüşümü yapılarak incelenmeye başlanmıştır (1KB = 1024B). Bu işlemler AMD A4-5000 APU Radeon, HD 1.50 GHz İşlemci, 4.00 GB RAM donanıma sahip bilgisayarda yapılmıştır.

Metin Şifreleme ve Şifre Çözme Bulguları

Kök Şifre algoritmasının uygulaması "TÜBİTAK 2204-A Lise Öğrencileri Araştırma Projeleri Yarışması" metni üzerinde gösterilsin. Şifreleme için öncelikle uygun bir anahtar seçimi yapılır. Burada anahtar olarak karekök değeri

irrasyonel sayı olan "7" sayısı alınsın. Karekök sayısının değeri 2,6457513… şeklindedir. Anahtarın ondalık kısmında yer alan 6457513… rakamları örnek metindeki her karakter ile eşleştirilir ve anahtardaki her bir rakam değeri kadar ötelenir. "T" karakteri 6, "Ü" karakteri 4, "B" karakteri 5, … kadar ötelenmektedir. UTF-8 karakter setinde öteleme sonucu "T" karakteri "Z", "Ü" karakteri "à", "B" karakteri "G", … karakterlerine dönüşerek örnek metin "ZàGķYBN!32682J Sjyf'×ğ{ksjltfxo!Cugš|ķssd#Sroqmmgwo$^hwIJŢnbsķ" olarak şifrelenir.

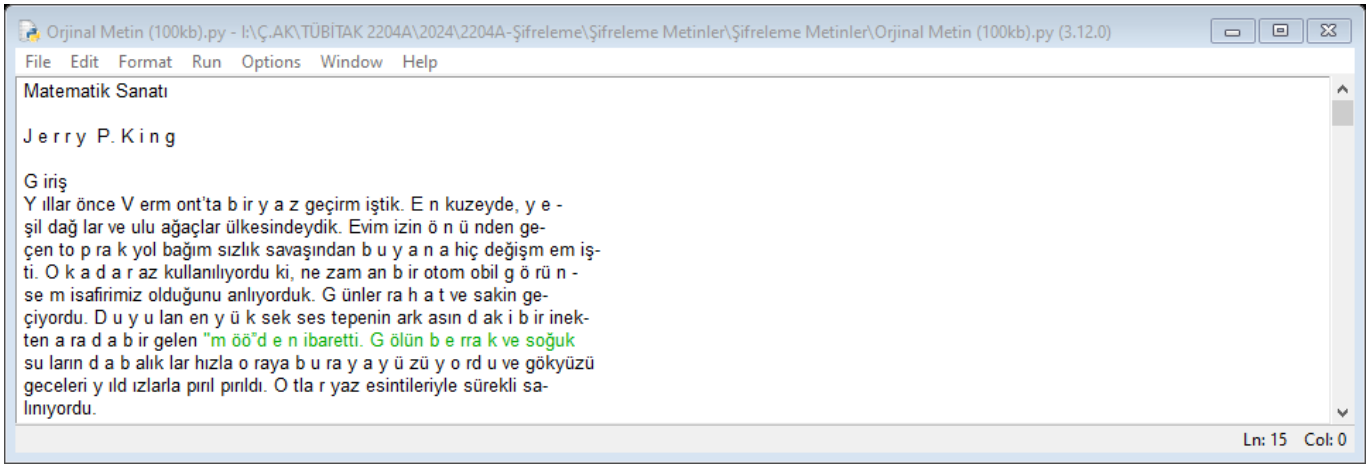
Yapılan işlemler tersten yapılarak şifreli metin orijinal hale gelmektedir. Örnek metnin "7" anahtarı ile şifrelenmesi ve şifrenin çözülmesi Şekil 4'te verilmiştir. Şifrelenen metnin şifresi çözüldükten sonra orijinal metinle aynı olduğu görülmüştür.



Şekil 4. Şifreleme ve Şifre Çözme Uygulaması

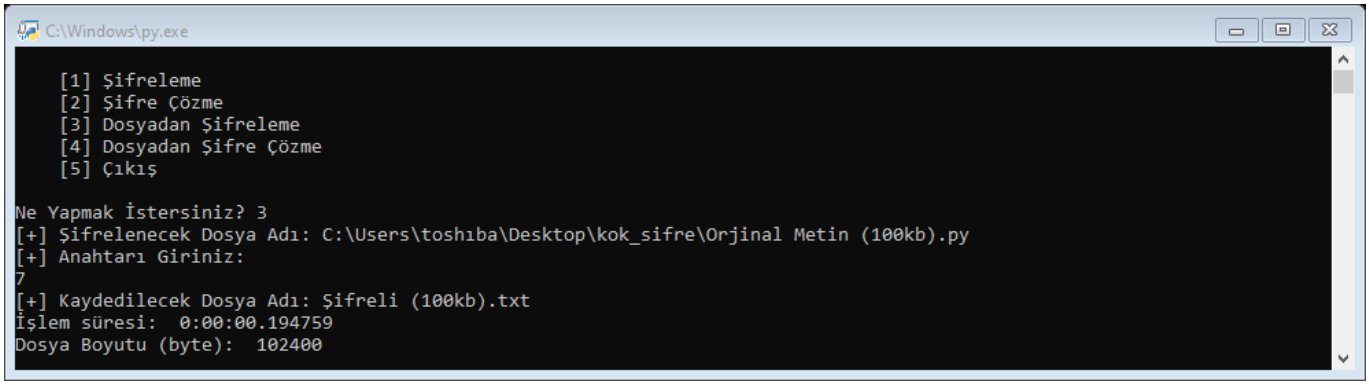
Metin Dosyası Şifreleme ve Şifre Çözme Bulguları

Algoritmanın performansının incelenmesinde King (2010)'un "Matematik Sanatı" kitabından faydalanmıştır. Boyutu yüksek olan metinsel veriler dosya olarak şifrelenmekte ve şifresi çözülebilmektedir.

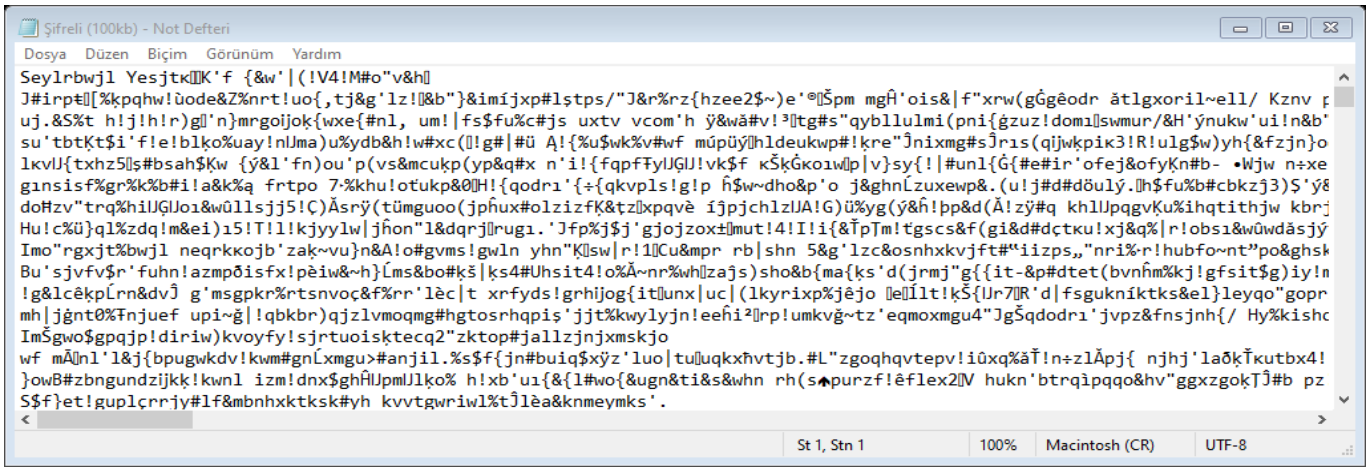


Şekil 5. 100KB'lık Orijinal Metin

Kitaptaki metinler 100 KB, 200 KB, 300 KB, 400 KB ve 500 KB olarak bölümlere ayrılmış ve Şekil 5'deki gibi .py uzantılı şekilde metinsel dosya haline getirilmiştir. Şifreleme yapılması için Kök Şifre uygulamasına yüklenmiş ve şifreleme anahtarı "7" olarak seçilmiştir. Şekil 6'da 100 KB'lik dosyanın şifreleme uygulamasındaki şifreleme süresi ve dosya boyutu gösterilmektedir. Şifrelenen metin Şekil 7'deki gibi .txt dosyası olarak kaydedilmiştir.

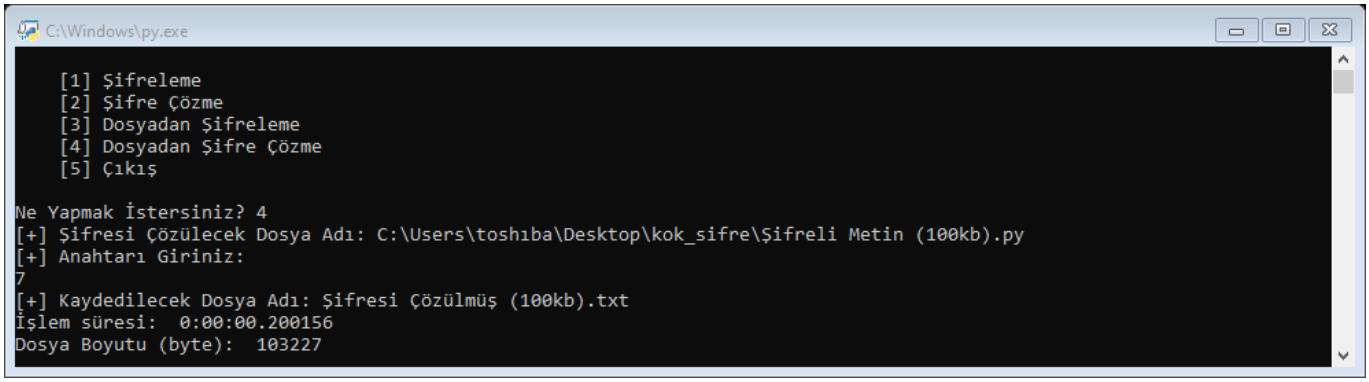


Şekil 6. Kök Şifre ile 100KB'lık Metin Dosyasını Şifreleme

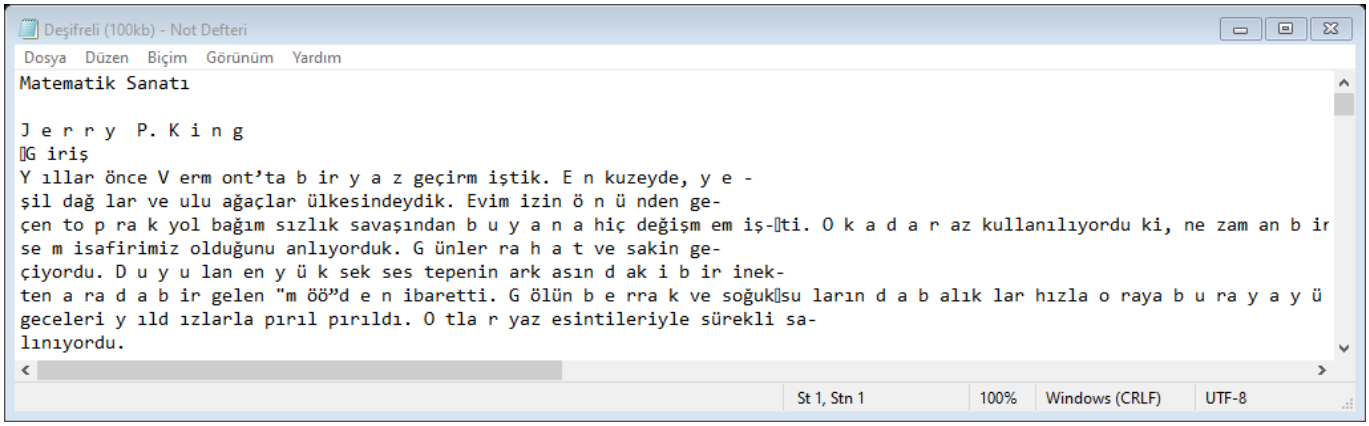


Şekil 7. 100KB'lık Şifrelenmiş Metin

Şekil 8'deki gibi .py uzantılı şekilde şifreli metin Kök Şifre uygulamasına yüklenmiştir. Aynı anahtar ile şifresi çözülmüştür. Şifresi çözülen metin Şekil 9'deki gibi .txt uzantılı olarak gösterilmiştir.



Şekil 8. Kök Şifre ile 100KB'lık Metin Dosyasının Şifresini Çözme



Şekil 9. 100KB'lık Şifresi Çözülmüş Metin

Şifreleme ve Şifre Çözme Süresi Bulguları

Kök Şifre uygulamasına metin dosyası olarak yüklenen verilerin şifreleme ve şifre çözme çıktıları için farklı zamanlarda 10 ölçüm yapılmıştır. Ölçümlerde oluşan süreler milisaniye olarak Tablo 1'de gösterilmiştir. Algoritmanın performansının değerlendirilmesinde kullanmak için ölçümlerin ortalaması alınmıştır.

Tablo 1. Şifreleme ve Şifre Çözme Ölçüm Süreleri

Ölçümler	Şifreleme Süresi (ms)					Şifre Çözme Süresi (ms)				
	100KB	**200KB**	**300KB**	**400KB**	**500KB**	**100KB**	**200KB**	**300KB**	**400KB**	**500KB**
1. Ölçüm	203	390	562	765	968	203	390	578	765	968
2. Ölçüm	187	374	562	765	968	203	390	578	765	984
3. Ölçüm	203	375	578	765	953	203	406	562	781	984
4. Ölçüm	187	390	562	781	953	203	390	593	796	953
5. Ölçüm	187	390	593	781	953	187	390	578	781	953
6. Ölçüm	203	390	578	765	953	203	406	593	781	953
7. Ölçüm	187	390	578	781	953	187	390	578	765	984
8. Ölçüm	203	374	562	765	953	187	390	562	812	953
9. Ölçüm	203	390	578	781	953	187	390	593	796	953
10. Ölçüm	187	390	562	781	953	187	390	578	765	953
ORTALAMA	**195**	**385,3**	**571,5**	**773**	**956**	**195**	**393,2**	**579,3**	**780,7**	**963,8**

Yapılan ölçümler sonucunda ortaya çıkan şifreleme ve şifre çözme ortalama süreleri Tablo 2'de gösterilmiştir. Şifreleme işleminin şifre çözmeden daha kısa sürdüğü tespit edilmiştir. 100 KB'lik metin dosyasının şifreleme ve şifre çözme süreleri ortalamasının aynı çıktığı; 200 KB, 300 KB, 400 KB ve 500 KB'lik metin dosyalarında yapılan şifreleme ve şifre çözme işlemlerindeki süre farkı birbirine çok yakın olduğu belirlenmiştir.

Tablo 2. Kök Şifre Şifreleme ve Şifre Çözme Ortalama Süreleri

Dosya Boyutları	Şifreleme Süresi (ms)	Şifre Çözme Süresi (ms)	Toplam Süre (ms)	Aradaki Süre Farkı (ms)
100 KB	195	195	390	0
200 KB	385,3	393,2	778,5	7,9
300 KB	571,5	579,3	1150,8	7,8
400 KB	773	780,7	1553,7	7,7
500 KB	956	963,8	1919,8	7,8

Şifreleme ve Şifre Çözme Dosya Boyut Bulguları

Kök Şifre ile yapılan şifreleme ve şifre çözme işlemi sonucu oluşan dosyaların boyutları kilobyte (KB) olarak Tablo 3'te gösterilmiştir. Dosya boyutları her ölçümde aynı çıkmıştır. Şifrelenip şifresi çözüldükten sonra orijinal metinde herhangi bir veri kaybının olmadığı tespit edilmiştir. Şifresi çözülen dosyala boyutunun orijinal metin daha fazla olduğu görülmüştür.

Tablo 3. Şifreleme ve Şifre Çözme Dosya Boyutları

Dosya Boyutları	Şifreli Dosya Boyutu (KB)	Şifresi Çözülmüş Dosya Boyutu (KB)	Şifresi Çözülmüş ve Şifreli Dosya Farkı	Şifresi Çözülmüş ve Orijinal Dosya Farkı
100 KB	100,80	101,30	0,50	1,30
200 KB	201,63	202,69	1,06	2,69
300 KB	302,24	304,06	1,82	4,06
400 KB	403,00	405,39	2,39	5,39
500 KB	503,70	506,75	3,05	6,75

Harf Frekans Analizi Bulguları

Örnek olarak Şekil 4'teki gibi şifrelenen "TÜBİTAK 2204-A Lise Öğrencileri Araştırma Projeleri Yarışması" metninin harf frekans analizi Tablo 4'te gösterilmiştir. Büyük-küçük harfleri farklı veri olarak saymamak için tüm metin küçük karaktere dönüştürülerek harf frekans analizi yapılmıştır. Ayrıca analize sadece harfler alınmış, rakam ya da boşluk gibi karakterler tabloda yer almamıştır. Bu analize göre sesli harflerden en çok A, İ, E ve I; sessiz harflerden en çok R, T ve L'nin bu metinde yer aldığı görülmüştür.

Tablo 4. Orijinal Metnin Harf Frekans Analizi

Harf	a	r	i	e	t	l	ı	s	ş	m	ü	b	k	ö	ğ	n	c	p	o	j	y
f	7	7	5	5	3	3	3	2	2	2	1	1	1	1	1	1	1	1	1	1	1

"ZàGķYBN!32682J Sjyf'×ğ{ksjltfxo!Cugš|ķssd#Sroqmmgwo$^hwIJŢnbsķ" şeklinde oluşan şifreli metnin harf frekans analizi Tablo 5'te gösterilmiştir. Bu analizde sesli harflerden en çok O; sessiz harflerden S, G, K ve J'nin bu metinde yer aldığı görülmüştür. Şifreli olarak ortaya çıkan karakterle metin eşleştirildiğinde aynı şifreli harflerin farklı orijinal harfleri temsil ettiği görülmüştür. Şifreli metinde Türkçe'ye özgü harflerin dışında UTF-8 karakter yapısının zengin içeriği sayesinde evrensel sembollerin de olduğu görülmüştür.

Tablo 5. Şifreli Metnin Harf Frekans Analizi

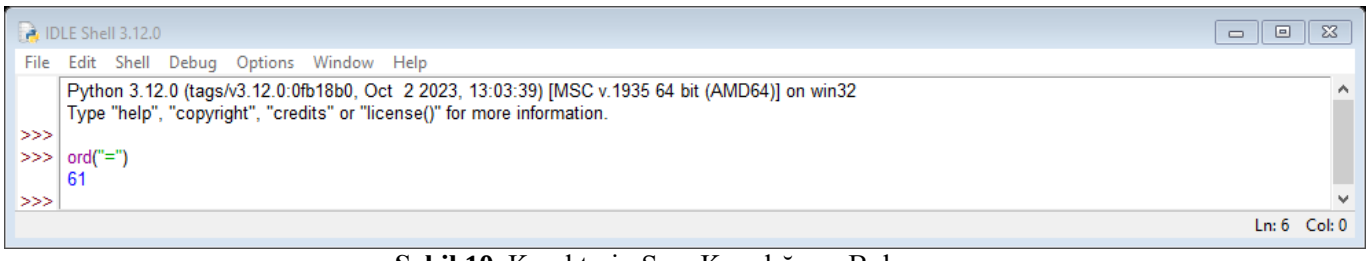
Harf	s	g	ķ	j	o	y	b	n	f	m	w	z	à	ğ	k	l	t	x	c	u	š	d	r	q	h	ij	ţ
f	6	3	3	3	3	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Anahtar Değişimi Bulguları

Şifreleme algoritmasında güvenliğin sağlanması için hem ortak hem bireysel anahtar kullanılmaktadır. Güvenlik açısından da ortak anahtarların değiştirilmesi gerekmektedir. Şekil 3'teki anahtar değişimi için "7" ortak anahtarın değişimi örnek üzerinden gösterilsin. Ortak anahtar her iki kişi tarafından bilinmektedir. Fakat özel anahtarlar kişiye özeldir ve kişiden başkası bilmemektedir.

1. kişinin kişisel anahtarı "5" ve 2. Kişinin kişisel anahtarı "6" olsun. Ortak anahtar 1. kişinin özel anahtarı ile Kök Şifre algoritması ile şifrelenip "9" elde edilir ve 2. kişiye gönderilir. Daha sonra 2. kişi gelen şifreli metni kendi özel anahtarı ile aynı algoritma ile tekrar şifreler. Bunun sonucunda şifreli karakter "=" olarak bulunur.

Aynı şekilde "7" ortak anahtarı 2. kişinin özel anahtarı, şifreleme algoritması ile şifrelenip ";" elde edilir ve 1. kişiye gönderilir. 1. kişi de 2. kişiden gelen şifreli metni kendi özel anahtarı ile tekrar şifreleyip "=" aynı şifreli karaktere ulaşır. Anahtarda sayı kullanılacağı için Şekil 10'daki gibi "=" karakterinin sayı karşılığı bulunur. Bu şekilde ortak anahtarın her iki tarafta da "61" olarak güncellendiği ve değiştirildiği görülmüştür.



Şekil 10. Karakterin Sayı Karşılığının Bulunması

Farklı Çalışmalara Dair Bulgular

Simetrik ve asimetrik şifreleme algoritmaları ile ilgili olarak yapılan performans analizi çalışmaları vardır. Değişik boyutlardaki metinlerin şifrelenmesinde Ökdem ve Kırtay (2018) TEA, XTEA, AES, DES, RSA ve RC5; Kaya ve Türkoğlu (2023) AES ve RSA algoritmaların performans analizlerini yapmışlardır. Çalışmalardan elde edilen sonuçlar Tablo 6'da milisaniye ve Tablo 7'de saniye olarak gösterilmiştir.

Tablo 6. Şifreleme Algoritmalarının Şifreleme ve Çözme Süreleri (Ökdem ve Kırtay, 2018)

ŞİFRELEME	TEA	XTEA	AES	DES	RSA	RC5
100 KB	13148	14069	550	15786	5360	803
200 KB	68592	71650	2792	90345	32364	4740
300 KB	192907	185324	8969	239743	84167	16569
400 KB	489996	366183	19526	468525	180224	31239
500 KB	625274	625373	36363	820021	299300	53713

ÇÖZME	TEA	XTEA	AES	DES	RSA	RC5
100 KB	31	29	509	12208	5546	826
200 KB	62	59	3694	89249	32066	4676
300 KB	95	91	9357	244583	84880	17044
400 KB	163	173	20198	471627	171995	33597
500 KB	222	207	36937	885027	290633	57051

Tablo 7. Şifreleme Algoritmalarının Şifreleme ve Çözme Süreleri (Kaya ve Türkoğlu, 2023)

BOYUT	ALGORİTMA	SÜRE	
		Şifreleme	Çözme
100 KB	AES	0.12	0.5
	RSA	1.8	1.2

Metinsel verileri şifreleme sonucu Ökdem ve Kırtay (2018)'ın algoritmaları karşılaştırmasından elde ettikleri veri boyutları Tablo 8'de gösterilmiştir.

Tablo 8. Şifreli Metin Boyutları (Ökdem ve Kırtay, 2018)

VERİ BOYUTU	100 KB	200 KB	300 KB	400 KB	500 KB
TEA	604	1208	1812	2416	3020
XTEA	596	1192	1788	2382	2978
AES	150	300	449	600	749
DES	147	294	441	588	734
RSA	138	275	412	549	686
RC5	149	298	446	595	743

SONUÇ, TARTIŞMA ve ÖNERİLER

Bu çalışmada, irrasyonel sayıların rasgeleliğinden yararlanılarak özgün bir şifreleme ve şifre çözme algoritması tasarlanmıştır. Oluşturulan Kök Şifre uygulamasıyla 5 farklı boyuttaki metinsel dosyanın şifreleme ve şifre çözme süreci ile tasarımın performansı incelenmiştir. Metinsel veriler şifrelenerek metinsel veriler elde edilmiştir. Şifreleme sonucu oluşan metnin orijinal metinle benzerliğini incelemek için harf frekans analizi yapılmıştır.
Simetrik şifreleme algoritmaları, bilgiyi şifreleme ve şifreli bilgiyi çözmede çok hızlı olmasından dolayı günümüzde yaygın kullanılmaktadır (Özyılmaz, 2014). Şifreleme ve şifre çözmede asimetrik şifreleme yöntemi yerine simetrik şifreleme yönteminin tercih edilmesinin performans açısından daha yararlı olacağı yönünde Karagöz (2022) bir çalışma ortaya koymuştur. Kaya ve Türkoğlu (2023), tek anahtar kullanıldığı için simetrik şifreleme algoritmalarının yüksek boyuttaki verileri daha hızlı şekilde şifrelediğini ifade etmişlerdir. Bu nedenle Kök Şifre algoritmasının tasarımında simetrik şifreleme algoritması tercih edilmiştir. Ayrıca; Polat (2022), aynı sayıda öteleme yapılarak oluşturulan şifrelemenin güvenilir bir yöntem olmadığından ve şifre çözmenin kolay yapılacağından bahsetmektedir. Bu çalışmada şifreleme algoritması irrasyonel sayılardan yararlanılarak rasgele öteleme ile oluşturulmuştur. Rasgelelik unsuru, şifreleme algoritmasının güvenirliğini artırmada kritik bir rol oynamaktadır (Garipcan ve Erdem, 2024). Tasarlanan algoritma bu anlamda kaydırma şifrelemeden daha güvenilir bir yapıdadır.

Kök Şifre algoritmasının şifreleme süresi TEA, XTEA, AES, DES, RSA ve RC5 şifreleme algoritmalarından daha kısa sürmekte midir?
Algoritmanın performansı incelenirken metin dosyalarının şifreleme ve şifre çözme sürelerine bakılmıştır. Tablo 2'de

de gösterildiği gibi 100 KB'lik metin 195 ms, 200 KB'lik metin 385 ms, 300 KB'lik metin 571 ms, 400 KB'lik metin 773 ms ve 500 KB'lik metin 956 ms gibi ortalama sürelerde şifrelemeyi gerçekleştirmiştir. Eskicioğlu ve Işık (2022), metin dosyasının boyutlarındaki artışın şifreleme ve şifreyi çözme süresinde artışa neden olduğunu ifade etmişlerdir. Benzer şekilde bu çalışmada dosya boyutu arttıkça şifreleme süresi artmıştır.

Ökdem ve Kırtay (2018), simetrik ve asimetrik şifreleme algoritmalarının performans analizlerini yapmışlardır. Tablo 6'da görüldüğü gibi şifreleme süresinde AES'in en başarılı olduğunu tespit etmişlerdir. Yaptığımız çalışmadan elde edilen şifreleme süreleri ile Ökdem ve Kırtay'ın (2018) elde ettikleri sonuçlar karşılaştırılmıştır. Kök Şifre algoritmasının şifreleme süre performansının TEA, XTEA, AES, DES, RSA ve RC5 algoritmalarından daha iyi olduğu tespit edilmiştir. Kaya ve Türkoğlu'nun (2023) yaptıkları çalışmada AES ve RSA algoritmalarına ait şifreleme süreleri Tablo 7'de gösterilmiştir. Kök Şifre algoritması ile karşılaştırıldığında Kök Şifre algoritmasının şifreleme performansının RSA'dan daha iyi olduğu sonucu da elde edilmiştir. AES algoritmasının şifreleme süresi açısından Kök Şifre algoritmasından daha başarılı olduğu görülmüştür. Kök Şifre algoritması metinleri TEA, XTEA, DES, RSA ve RC5 şifreleme algoritmalarından daha kısa sürede şifrelemektedir.

Kök Şifre algoritmasının şifre çözme süresi TEA, XTEA, AES, DES, RSA ve RC5 şifreleme algoritmalarından daha kısa sürmekte midir?

Şifre çözme süreleri açısından algoritmaya bakıldığında Tablo 2'deki gibi 100 KB'lik metin 195 ms, 200 KB'lik metin 393 ms, 300 KB'lik metin 579 ms, 400 KB'lik metin 780 ms ve 500 KB'lik metin 963 ms gibi ortalama sürelerde şifreli metnin çözüldüğü tespit edilmiştir. Şifre çözmede kullanılan metin dosyasının boyutu arttıkça sürenin de arttığı görülmüştür. Ökdem ve Kırtay (2018), yaptıkları çalışmada metinlerin şifre çözme süreleri açısından TEA ve XTEA'nın en iyi performansa sahip olduğunu Tablo 6'daki gibi ifade etmişlerdir. Elde edilen süreler arası karşılaştırma yapıldığında Kök Şifre algoritmasının şifre çözme süresi açısından AES, DES, RSA ve RC5 algoritmalarından daha başarılı olduğu; TEA ve XTEA algoritmalarından daha başarısız olduğu söylenebilir.

Rameel ve Asif (2024) çalışmalarında güvenlik ve hız olarak AES'i başarılı bulurken DES'i başarısız bulmuştur. Ayrıca RSA'yı güvenli bir seçenek olmasına rağmen işlem süresinin uzun olduğunu ifade etmişlerdir. Kaya ve Türkoğlu'nun (2023) şifreli metni çözme sürelerine ait sonuçlar Tablo 7'de gösterilmiştir. Buradan elde edilen sonuçlar karşılaştırıldığında; Kök Şifre algoritmasının şifre çözme performansının AES ve RSA algoritmalarından daha iyi olduğu tespit edilmiştir. Kök Şifre algoritması şifreli metinleri AES, DES, RSA ve RC5 şifreleme algoritmalarından daha kısa sürede çözmektedir.

Kök Şifre algoritmasının şifrelemede dosya boyutu TEA, XTEA, AES, DES, RSA ve RC5 şifreleme algoritmalarından daha düşük müdür?

Şifreleme sonucu oluşan dosya boyutunun orijinal metinden daha büyük olduğu Tablo 3'te gösterildiği şekilde tespit edilmiştir. Kök Şifre ile şifreli metin çözüldükten sonra boyutunda artış meydana gelmiştir. Bu artışın nedeni kullanılan programın uzun boşluklar arasına [] sembolünü koymasından kaynaklanmaktadır. Şifrelenmiş verilerin boyutları ile ilgili olarak Ökdem ve Kırtay (2018) orijinal metin şifrelendiğinde dosya boyutunun AES, DES, RSA ve RC5'te %150; TEA ve XTEA'da %600 kata ulaştığını Tablo 8'deki gibi ifade etmektedir. Kök Şifre algoritmasında elde edilen artış oranı ise %0,5'tir. Bu haliyle diğer algoritmalara göre şifreleme sonunda daha az yer kaplamaktadır. Şifreli ve şifresi çözülmüş metin arasında herhangi bir boyut farkının olmadığı sonucuna ulaşan çalışmalar da vardır. Sivan vd., (2023) oluşturdukları şifreleme algoritmasında şifrelenen metin ile düz metnin aynı boyutta olduğu sonucuna ulaşmışlardır.

Kök Şifre algoritması harf frekans analizine karşı güçlü müdür?

Türkçede sesli A, E ve İ ile sessiz N, R, L, K ve D en çok kullanılan harflerdir (Dalkılıç ve Dalkılıç, 2002). Şifreleme örneği olarak kullanılan "TÜBİTAK 2204-A Lise Öğrencileri Araştırma Projeleri Yarışması" metninde sesli harflerden en çok A, İ, E ve I; sessiz harflerden R, T ve L'nin yer aldığı görülmüştür. Türkçe'de çok kullanılan harflerle benzerlik göstermektedir. Şifreleme algoritması şifre çözme saldırılarına karşı gerekli direnci göstermelidir (Etem, 2022). Metnin şifresini çözmede kullanılan saldırı yöntemlerinden biri olan harf frekans analizine karşı algoritma güçlü olmalıdır. Şifreli metnin harf frekans analizine bakıldığında sesli harflerden en çok O; sessiz harflerden S, G, K ve J'nin şifreli metinde yer aldığı görülmüştür. Orijinal metindeki aynı harflerin farklı karakterle şifrelendiği görülmektedir. Şifreli metinde aynı karakterler de orijinal metindeki farklı harfleri temsil ettiği

görülmüştür. Orijinal metin ile şifreli metin arasında bu anlamda benzerlik olmadığı tespit edilmiştir. Bu haliyle harf frekans analizi saldırısına karşı algoritmasının güçlü olduğu görülmektedir.

Kök Şifre algoritmasının şifreleme ve şifre çözmede veri kaybı var mıdır?

Verilerin güvenliği için gizlilik ve bütünlüğün sağlanmasının öneminden Topaloğlu vd., (2016) bahsetmektedir. Kök Şifre algoritması ile metinler şifrelenmiş, şifrelenen metinler orijinal haline getirilerek incelenmiştir. Şifrelenen metnin Kök Şifre algoritması ile şifresi çözüldükten sonra eksiksiz ve başarılı bir şekilde eski haline getirildiği tespit edilmiştir. Orijinal metne ait herhangi bir eksikliğin ve veri kaybının olmadığı, verilerin bütünlüğünü koruduğu belirlenmiştir.

Bu çalışmada anahtar olarak kareköklü sayılar kullanılmıştır. Farklı kök dereceleri ile anahtarlar elde edilebilir. Sadece köklü sayılar değil farklı irrasyonel sayılar kullanılabilir. Şifrelemede rasgele pozitif yönlü öteleme yapılmıştır; negatif yönlü öteleme tercih edilebilir. Bu çalışmada sadece metin dosyaları incelenmiştir; ses ve resim gibi farklı dosya türleri şifrelenip algoritmanın performansına bakılabilir. Harf frekans analizi için daha farklı uzunluktaki metinler incelenebilir. Kök Şifre uygulamasına ara yüz eklenebilir. Daha farklı donanıma sahip bilgisayarda algoritmanın performansı incelenebilir.

KAYNAKLAR

Aghayev, M. (2017). *Kriptoloji ve veri şifreleme teknikleri üzerine* (Yüksek Lisans Tezi). Ege Üniversitesi, Fen Bilimleri Enstitüsü, İzmir.

Arda, D. ve Buluş, E. (2003). Türk Alfabesi ve Yapısal Özellikleri Kullanılarak Tek Alfabeli Yerine Koymada Şifreleme ve Kriptanaliz. *20. Türkiye Bilişim Kurultayı*, İstanbul.

Buhurcu, H. (2022). *Kriptoloji ve steganografiyle güvenli iletişim sistemi tasarımı* (Yüksek Lisans Tezi). Selçuk Üniversitesi, Fen Bilimleri Enstitüsü, Konya.

Buluş, H. N. (2006). *Temel şifreleme algoritmaları ve kriptanalizlerinin incelenmesi* (Yüksek Lisans Tezi). Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne.

Çimen, C., Akleylek, S. ve Akyıldız, E. (2008). *Şifrelerin matematiği: kriptografi*. ODTÜ.

Dalkılıç, M. E. ve Dalkılıç, G. (2002). On the cryptographic patterns and frequencies in Turkish language. In *International Conference on Advances in Information Systems* (pp. 144-153). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-36077-8_14

Eskicioğlu, Ö. C. ve Işık, A. H. (2022). Mobil Uyumlu Çoklu Dil Destekli Hibrit Şifreleme Algoritması. *Dokuz Eylül Üniversitesi Mühendislik Fakültesi Fen ve Mühendislik Dergisi*, *24*(72), 1007-1019. https://doi.org/10.21205/deufmd.2022247228

Etem, T. (2022). *Kriptografi-Bilgi güvenliği için rastgele sayı üreteci geliştirilmesi* (Doktora Tezi). Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elazığ.

Garipcan, A. M. ve Erdem, E. (2024). Kriptografide Rasgelelik Kavramı ve Gerçek Rasgele Sayı Üreteçlerinin Test Metodolojisi. *Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi*, *15*(1), 61-75. https://doi.org/10.24012/dumf.1384343

Günden, Ü. (2010). *Şifreleme algoritmalarının performans analizi* (Yüksek Lisans Tezi). Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, Sakarya.

Hassanpour, A. A. (2015). *Asal sayıların şifreleme teorisindeki uygulamaları* (Yüksek Lisans Tezi). Atatürk Üniversitesi, Fen Bilimleri Enstitüsü, Erzurum.

İşçimen, N. (2023). *Asimetrik Şifreleme Algoritmasının Kullanılmasıyla Veri Güvenliğinin Sağlanması* (Doktora Tezi). Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Edirne.

Karagöz, F. (2022). *Bulut veri güvenliğinde şifreleme yöntemlerinin performans değerlendirmesi* (Yüksek Lisans Tezi). Necmettin Erbakan Üniversitesi, Fen Bilimleri Enstitüsü, Konya.

Kaya, A. ve Türkoğlu, İ. (2023). Simetrik ve Asimetrik Şifreleme Algoritmalarının Performans Karşılaştırılması. *Fırat Üniversitesi Mühendislik Bilimleri Dergisi*, *35*(2), 891-900.

https://doi.org/10.35234/fumbd.1296228

King, J. P. (2010). Matematik sanatı (19. baskı). Ankara: TÜBİTAK Popüler Bilim Kitapları.

Kodaz, H. ve Botsalı, F. M. (2010). Simetrik ve asimetrik şifreleme algoritmalarının karşılaştırılması. *Selçuk University Journal of Engineering Sciences*, *9*(1), 10-23.

Nabiyev, V. V. ve Zeka, Y. (2016). İnsan-bilgisayar etkileşimi. *Seçkin Yayıncılık, Sözkesen Matbaacılık: Ankara*, 2-55.

Ökdem, S., ve Kırtay, M. (2018). Kablosuz ağlarda şifreleme algoritmalarının performans analizi. In *ISAS 2018 1st International Symposium on Innovative Approaches in Scientific Studies* (pp. 11-13). http://hdl.handle.net/20.500.11787/4916

Özyılmaz, Ç. (2014). *Kriptolojiye giriş* (Yüksek Lisans Tezi). Karabük Üniversitesi, Fen Bilimleri Enstitüsü, Karabük.

Polat, F. (2022). *Kriptoloji bilimi ve anahtar dağıtım şemaları* (Yüksek Lisans Tezi). İbrahim Çeçen Üniversitesi, Lisansüstü Eğitim Enstitüsü, Ağrı.

Rameel, M., & Asif, Z. (2024). Fortifying Information Security: A Comparative Analysis of AES, DES, 3DES, RSA, and Blowfish Algorithm. EasyChair Preprint no. 13536. *Communications*, *2*, 5. https://easychair.org/publications/preprint/Kjbz

Sivan, İ., Selman, H., Akhter, A. F. M. ve Cevat, A. (2023). Veritabanı Güvenliğini Sağlamak için Yeni Bir Veri Şifreleme Algoritması. *Acta Infologica*, *7*(1), 1-16. http://dx.doi.org/10.26650/acin.1134979

Soyalıç, S. (2005). K*riptografik hash fonksiyonları ve uygulamaları* (Yüksek Lisans Tezi). Erciyes Üniversitesi, Fen Bilimleri Enstitüsü, Kayseri.

Stinson, D. R. (2002). *Classical Cryptograph, Cryptography Theory and Practice*, Ed: Rosen, K. H., Chapman ve Hall / CRC, New York, 2: 1-20.

Süküt, F. (2024). Arşivcilik ve Belge Yönetimi Faaliyetlerinde Blokzincir Teknolojisi: Bilgi Güvenliği Bağlamında Bir Değerlendirme. *Library Archive and Museum Research Journal*, *5*(1), 1-35. https://doi.org/10.59116/lamre.1357399

Şengel, Ö., Aydın, M. A., & Sertbaş, A. (2020). Determining the cryptography algorithm and model for mobile payment systems. *Acta Infologica*, *4*(1), 21-33.

Thomas, G. B., Weir, M. D., Hass, J. R., ve Bayram, M. (2014). *Thomas Calculus*. Pearson.

Topaç, Ç. (2023). *Mobil haberleşmede şifreleme algoritmaları ile güvenli kısa mesaj servisi uygulaması* (Yüksek Lisans Tezi). Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Edirne.

Topaloğlu, N., Calp, M. H. ve Türk, B. (2016). Bilgi güvenliği kapsamında yeni bir veri şifreleme algoritması tasarımı ve gerçekleştirilmesi. *Bilişim Teknolojileri Dergisi*, *9*(3), 291. https://doi.org/10.17671/btd.36875

Ülker, Ü. (2014). *Klasik teknikler kullanılarak bir kriptografi algoritması geliştirilmesi ve des algoritması ile performans analizlerinin karşılaştırılması* (Yüksek Lisans Tezi). Gazi Üniversitesi, Bilişim Enstitüsü, Ankara.

Üstün, M. (2022). F*ark denklemleri kullanılarak tasarlanan şifreleme algoritmasının güvenlik analizi* (Yüksek Lisans Tezi). Necmettin Erbakan Üniversitesi, Fen Bilimleri Enstitüsü, Konya.

Yerlikaya, T. (2006). *Yeni şifreleme algoritmalarının analizi* (Doktora Tezi). Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Edirne.

Yeşilbaş, E. (2016). *Cebirsel kriptoloji yöntemleri ve bazı uygulamaları* (Yüksek Lisans Tezi). Recep Tayyip Erdoğan Üniversitesi, Fen Bilimleri Enstitüsü, Rize.