Dokuz Eylül Üniversitesi Mühendislik Fakültesi Fen ve Mühendislik Dergisi
Dokuz Eylul University Faculty of Engineering Journal of Science and Engineering

Basılı/Printed ISSN: 1302-9304. Elektronik/Online ISSN: 2547-958X

Mobil Uyumlu Çoklu Dil Destekli Hibrit Şifreleme Algoritması

Mobile Compatible Multi-Language Supported Hybrid Encryption Algorithm

Ömer Can Eskicioğlu [1], Ali Hakan Işık[2]*

[1] Burdur Mehmet Akif Ersoy Üniversitesi, Mimarlık-Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Merkez-Burdur, Türkiye
[2] Burdur Mehmet Akif Ersoy Üniversitesi, Mimarlık-Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Merkez-Burdur, Türkiye
*Sorumlu Yazar / Corresponding Author **: ahakan@mehmetakif.edu.tr*

Geliş Tarihi / Received: 08.12.2021 *Araştırma Makalesi/Research Article*
Kabul Tarihi / Accepted: 27.05.2022 *DOI:10.21205/deufmd.2022247228*
Atıf şekli/ How to cite: ESKİCİOĞLU, Ö.C., IŞIK, A.H.(2022).Mobil Uyumlu Çoklu Dil Destekli Hibrit Şifreleme Algoritması. DEÜ FMD 24(72), 1007-1019.

Öz

Çalışmamız, günümüz şartlarına uygun simetrik tabanlı hibrit şifreleme algoritmasıdır. Temel amaç özgün tasarımla verilerimizin güvenliğini tahsis etmektir. Projemizdeki şifreleme algoritması 3 kademeli olarak tasarlanmıştır. Kademeli olarak şifreleme işleminde öncelikle statik belirlenmektedir. Belirlenen anahtarların yanına Arşimet sabiti ve 'belirtme sayısı' değerleri gelerek şifreleme işlemi gerçekleşmektedir. Dinamik olarak her şifreleme döngüsünde indis tekrar rastgele olacak şekilde değiştirilmektedir. Algoritma harf bazlı işlem yapmaktadır. Şifrelenen her harf için farklı indis ve belirtme sayısı fonksiyonu kullanılmıştır. Pi sayısından yararlanılarak harflere rastgele değer atama işlemleri gerçekleşmektedir. Rastgele atadığımız sayılardan oluşturduğumuz anlamlı verileri, Fibonacci dizisindeki elemanların indis sırasına göre doğrulama işlemi yapılmaktadır. Algoritmanın uygulanabilirliği bakımından çeşitli testlere tabii tutulmuştur. Yapılan bu testlerde 2KB veride %99,98, 10KB veride %99.996 ve 20KB veride %99.9962 doğruluk oranı elde edilmiştir. Oluşturulan harf havuzuna yeni eklemeler yapılabilmektedir. Harf havuzuna eklemeden sonra algoritmada herhangi bir tasarım değişikliği gerekmemektedir. Çalışmamız mobil platformlar ve çeşitli sistemler üzerinde sorunsuz olarak hizmet vermektedir. Şifreleme mekanizması kullanım açısından esnektir. Aynı giriş metni ile farklı sonuçlar elde edilmiş ve algoritmanın sağlıklı işleyişi kabul görmektedir.

Anahtar Kelimeler: *Şifreleme Algoritmaları, Simetrik Şifreleme, Çok Dil Destekli Hibrit Şifreleme, Mobil Uyumlu Şifreleme Algoritması*

Abstract

Our study is an symmetric based hybrid encryption algorithm suitable for today 's conditions. The main purpose is to allocate the security of our data with original design. The encryption algorithm in our project is designed in 3 stages. In the stages encryption process , the static values (secret keys) are determined first. Archimedes constant and 'number of specifications' values are displayed next to the specified keys and encryption is performed. Dynamically, the index is changed to be random again

at each encryption cycle. The algorithm performs letter based operations. For each encrypted letter, different index and number of functions are used. Using the Pi number, random value assignment operations are performed. The validation of meaningful data that we have generated from randomly assigned numbers is done according to the index order of the elements in the Fibonacci array. It has been subjected to various tests in terms of the applicability of the algorithm In the tests obtained, 99.98% accuracy in 2KB data, 99.996% in 10 KB data and 99.9962% in 20KB data were obtained. New additions can be made to the created letter pool. No design changes to the algorithm are required after insertion into the letter pool. Our work serves on mobile platforms and various systems without any problems. The encryption mechanism is flexible in use. Different results have been obtained with the same input text and the healthy functioning of the algorithm is accepted.

Keywords: *Encryption Algorithms, Symmetric Encryption, Multi-Language Supported Hybrid Encryption, Mobile Compatible Encryption Algorithm*

1. Giriş

İletişimde güvenlik, güncel ihtiyaçlarımız ve teknolojimiz doğrultusunda önemli bir hedeftir. Kullandığımız telefonlar, bilgisayarlar ve nesnelerin interneti (IoT) tabanlı birçok aygıt özgün güvenliğe muhtaçtır. Akıllı cihazların insanların yaşam ve hayat standartlarını yükseltmesi, kolaylaştırması kişinin ihtiyaçlarına veya alışkanlıklarına göre özelleşmesinin yolu mahremiyetin sürekli gözlenmesidir [1]. Bu gözlemlerin mahremiyet çerçevesinde korunması ve şifrelenmesi gerekmektedir.

Sistemdeki açıklardan yararlanmak isteyen bireylerin iletişim ve haberleşmemize engel olması veya değiştirmesi gibi olayların önüne geçebilmek için standart uygulamalardan farklı bir özgün çözüm üretmemiz gerekir. Çalışmamızın şifreleme tekniği, güvenliği ön plana çıkarmayı hedeflemiştir.

Bilgi güvenliği konusundan bahsedebilmemiz için öncelikle bilginin tanımını yapmamız gerekir. Bilgi, işlenmiş veridir. Son çıktıdır. Günümüz dünyasında veri yığınlarından anlamlı bilgiler çıkarmak çok değerli bir olaydır. Bu yazımızda bu değerli bilgileri şifreleme algoritmamız ile güvence altına alınacaktır.

Bilgi güvenliğinin sağlanması için bilgi varlığının korunması gerekir [2]. İletişim gerçekleşmeden önce yollanacak olan bilginin doğruluğu önemlidir. Kriptoloji bilimi sayesinde iletişim sırasında ki güvenlik tahsis edilebilir. Sağlanacak güvenlik 3. şahıslarca dinlenilen herhangi bir iletişim kanalında üst düzey korumayı hedeflemektedir. Kişisel mahremiyetin korunmasında, herhangi bir dijital dolandırıcılığa karşı güvenliğe, banka hesap bilgilerinin korunmasında, şirketlerin önemli verilerinin saklanmasında ve birçok internet kaynağında ki verilerin şifrelenmesine yardımcı olmaktadır.

Kriptografi bilimi, Bilgisayar bilimi ile Matematik bilimi arasındaki köprüdür. Dijital iletişim için matematiksel tekniklerden yararlanılır. Kriptografi biliminden hayatımızda, kimlik doğrulamalarında, sanal imzalarda, kredi kartlarında, telefon haberleşmelerinde ve birçok alanda yararlanılmaktadır. Güvenilirlik, kimlik doğrulama, veri bütünlüğü gibi bilgi güvenliği konularıyla [3] ilgili yapılan matematiksel çalışmalar kriptografinin önemli konularındandır.

Günlük yaşamımızın vazgeçilmezi olan elektronik cihazlar, internet bankacılığı, kablosuz ağlar, telefonlar, kredi/banka kartları gibi teknolojik uygulamalarda güvenliğin sağlanması önemlidir [4]. Güvenliği sağlamak için şifreleme teknikleri kullanılır ve bu şifreleme tekniklerinin performansını artırmak için çeşitli analizlere tabii tutulmuştur [5].

Saldırganlara karşı bilgi mesajların gizliliğini korumak için asimetrik veya simetrik şifreleme algoritmaları kullanılmaktadır [6]. Açık anahtarlı (asimetrik) şifreleme algoritmaları çözülmesi zor ve karmaşık matematiksel teoremler üzerine kurulmuş algoritmalardır [7]. Bilginin korunması ve güvenli şekilde taşınması önemli bir sorun haline gelmiştir [8]. Bilgi çağımızın en değerli hazinesidir. Bu hazineyi güvenli bir şekilde korumamız gerekmektedir. Bilgi güvenliğini sağlayacak şifreleme mekanizmasının güvenilir ve hızlı olması gerekmektedir. Güvenlik ihtiyaçları doğrultusunda çalışmamız çoklu dil desteğine

sahip hibrit bir yapıya sahip şifreleme mekanizmasıdır.

Şifreleme genellikle yüksek veri hızlarında yapılmalıdır, bu bazen kriptografik donanımın desteklenmesiyle karşılanır [9]. Algoritmamız

verimli ve performanslı çalışmaktadır. Çok büyük veri yığınları için donanım desteklenmesi düşünülebilir. Çalışmamızda gönderici ve alıcı arasındaki iletişimi deterministik bir karmaşıklık ilişkisi kullanılarak mesajın şifrelenmesi sağlamaktır. Literatürdeki çalışmalar incelendiğinde benzer çalışmaların olduğu anlaşılmaktadır. Bu çalışmalar;

Yerlikaya vd. şifreleme algoritmalarının sınıflandırılması yapılmıştır. Asimetrik ve simetrik şifreleme algoritmalarının özellikleri ve yapıları analiz edilmiştir. Bu algoritmaların avantajları ve dezavantajları üzerinde bilgiler verilmiştir. Yazarlar Diffie-Helman anahtar dağıtımını ve RSA algoritmasının işleyişini ve yapılarını incelemiştir [7].

Levi vd. açık anahtarlı sistemlerdeki yaşanılan sorun ve problemlere değinilmiştir. Açık anahtar sistemlerinin nasıl tasarlanacağı konusunda kriterler oluşturulmuştur. Kullanımda olan sertifika ve PKI sistemlerinin problemlerinden bahsedilmiştir. Yazarların geliştirdikleri e-posta sisteminin pratikte kullanılmakta olduğu özelliklerinden bahsedilmiştir [10].

Baykara vd. çalışmada günümüzün bilişim dünyasındaki güvenliğe dikkat çekilmiştir. Bilgi sistemleri ve bilgi güvenliğini sağlamak için günümüzde sıkça kullanılan güvenlik araçlarının işlevlerini ve özelliklerine bakılmıştır [2].

Rogaway vd. şifreleme algoritması SEAL 3.0'dan bahsedilmiştir. Şifreleme sırasında sahte verilerin işlemci üzerindeki maliyetine dikkat çekilmiştir. Yazarlar ayrıca Vernam şifrelemesine değinilmiştir [9].

Prajapat vd. Fibonacci Qmatrix kullanarak simetrik şifreleme algoritmalarında anahtar değişimi ile iletişim kanalı üzerinden bilgi aktarımından bahsedilmiştir. Bu yaklaşım ile hesaplama gücü ve süresini azalmaktadır. Yazarlar, bilgi güvenliği dünyasında önemli bir talebi karşılayabilecek bir yaklaşım önermektedir [11].

Özkaynak vd. kaotik sistemler yardımıyla yeni bir şifreleme yöntemi tasarlanması amaçlanmaktadır. İlgili çalışmada kaos tabanlı blok şifreleme algoritması 105 ortalama değer almıştır. Katı çığ kriteri 0.375 ile 0.601 arasında değişmektedir [12].

Wang vd. kaotik Tent haritası temelli dinamik S-Box'ları kullanarak bir simetrik blok şifreleme algoritması oluşturmuşlardır. Yazarlar çalışmada 104 ortalama değer almıştır. Katı çığ kriteri 0.485 ile 0.515 arasındadır [13].

Cocks vd. ortak anahtarlı kimlik tabanlı şifreleme sistemi önerilmiştir. Önerilen tasarımın güvenliğine ve karşılaşacağı problemler üzerinde çalışılmıştır [14].

Waters vd. tamamen güvenli verimli bir kimlik tabanlı şifreleme tasarımı sunulmaktadır. Yazarlar çalışmasında yaptıkları tasarımın güvenliğini Bilinear Diffie-Helman (BDH) sorununa indirgemektedir [15].

Lewko vd. çoklu yetkili özellik tabanlı şifreleme sistemi önerilmektedir. Sistemde bir taraf genel anahtarı oluşturur ve farklı kullanıcılara özniteliklerini yansıtan özel anahtarlar vermektedir. Sistemde en büyük teknik engellerden biri olan çarpışma riski, öznitelik tabanlı şifreleme sistemi tarafından, anahtar seçimi rastgele yapılarak çarpışma direnci oluşturulmuştur [16].

Bellare vd. anonimlik ve anahtarın gizliliği olarak adlandırılan yeni bir şifreleme düzeni güvenlik gereksinimi olduğunu ispatlamaktadırlar. Yazarlar bilinen şifreleme şemalarının anonimliklerini ve yapılan çeşitli saldırıların sonuçlarını araştırmaktadırlar. Çalışmada RSA-OAEP bahsedilmektedir. Bahsedilen bir doldurma şemasıdır ve sık sık RSA şifrelemesinde kullanılmaktadır [17].

Zengin [18] tarafından yapılan çalışmada DNA'dan esinlenerek yeni bir Genetik Şifreleme Algoritması (GEA) oluşturulmuştur. GEA ile Standart Şifreleme Algoritması (AES), Asimetrik Şifreleme Algoritması (RSA) ve Gelişmiş Şifreleme Algoritması (AES) detaylı olarak karşılaştırılmıştır.

Hamdi vd. kriptanalitik saldırılara karşı dirençli, yüksek hıza sahip ve kolay uygulanabilirliğine sahip bir şifreleme yöntemi önerilmiştir. Önerilen yönteme göre kaotik sistemler kullanarak blok ve akış şifrelerine dayalı basit ve verimli bir hibrit şifreleme algoritması oluşturulmuştur. Kaos tabanlı şifreleme yöntemi, yüksek düzeyde güvenlik sağlamaktadır. Değerlendirme ve analiz

sonucunda yüksek düzeyde kriptografik özelliklere sahip olduğu tespit edilmiştir [19].

Viswanath vd. oluşturulan senaryoda büyük veri, veri depolama, veri hırsızlığı ve yetkisiz erişimle ilgili birçok zorlukla karşı karşıya kalmaktadır. Bu nedenden büyük verileri bulutta depolanmasını sağlayan bir şifreleme algoritması önerilmiştir. Önerilen yöntemde çerçeve, veri yükleme, dilimleme, indeksleme, şifreleme, dağıtım, şifre çözme, alma ve birleştirme işlemlerini içermektedir. Algoritma, 2630 KB/S şifreleme performansı elde etmiştir [20].

Abroshan [21] tarafından yapılan çalışmada performans üzerinde düşük bir etkiyle bulut bilişimde güvenliği artırmak için etkili bir kriptografi çözümü önerilmektedir. Önerilen bu çözüm, eliptik eğri tabanlı bir algoritma ile birlikte geliştirilmiş Blowfish algoritması kullanmaktadır. Blowfish verileri ve eliptik eğri algoritması anahtarını şifrelemektedir. Böylece verilerin güvenliği ve şifreleme performansı arttırılmaktadır. Ayrıca veri bütünlüğünü sağlamak için dijital imza tekniği kullanılmaktadır.

Koçak [22] tarafından yapılan çalışmada Kriptografi ile Steganografi tekniklerinden yararlanılarak hibrit bir yöntem önerilmiştir. RGB görüntülerde yeşil ve kırmızı kanallardaki en az 2 değerliğe sahip bitler değiştirilmiş ve gizlenmiştir.Görüntüde toplamda 4 bitte değişiklik yaparak şifrelenecek metin boyutu arttırılmıştır.

Doğan ve Çelik [23] tarafından yapılan çalışmada görüntü şifrelemesi için geleneksel kripto yöntemleriyle karma bir şifreleme metodu önerilmiştir. Yer değiştirme ve Afin kripto yöntemlerinin birlikte çalıştığı bir metot kullanılmıştır. Şifreli görüntüler zikzak ve 8'e 4 kod tarama modelleri kullanarak güçlendirilmiştir.

Şatır ve Kendirli [24] tarafından yapılan çalışmada web sayfalarının URL'lerini kullanan bir steganografik yöntem önerilmiştir. Yazarlar çalışmalarında güvenliği arttırmak için DES ve LZW kodlama algoritmaları kullanılmıştır. Yapılan analizler kapsamında sistemin kullanılabilir olduğu sonucuna varılmıştır.

Çavuşoğlu [25] tarafından yapılan çalışmada iki yeni kaotik sistem tasarlanmış ve analiz edilmiştir. Ayrıca geliştirilen kaotik sistemler için 2 yeni Rassal Sayı Üreteci tasarımları yapılmıştır. Yapılan tez çalışmasında blok şifreleme algoritmalarında kullanılan S-box üretim algoritması hazırlanmıştır. Literatürdeki çalışmalarda üretilen S-Box'lar ile karşılaştırılıp performans analizi yapılmıştır. Kaos tabanlı çalışan simetrik bir hibrit şifreleme algoritması CS-AES geliştirilmiştir. Geliştirilen tasarımlar ile literatür karşılaştırılmıştır.

Atar [26] vd. tarafından yapılan çalışmada Sıkıştırılmış Algılama (SA) ile veri boyutunun ve sensör sistemlerinin azaltılması için Dik Eşleştirme Arayış (DEA) algoritması kullanılmıştır. Şifreleme ve sıkıştırma işlemleri için SA-DEA ile Çift Rastgele Faz Şifreleme (DRPE) metotları birleştirilmiştir.

Anlaşılacağı üzere bilgi güvenliğinin sağlanması ve gerekli güven ortamının oluşturulması için çeşitli gereksinimler gereklidir. Araştırmacılar bu gereksinimleri en hızlı ve güvenli olarak sağlayabilmek için çeşitli çalışmalar yapmaktadır. Yapılan araştırmalar algoritmalar üzerindeki işlemlerden ve optimize süreçlerinden oluşabilecek problemlerden sıkça bahsetmektedir. İncelenen çalışmalardaki sonuçlara dayanarak şu tespitler ifade edilebilir:

- Yaşanılan problemler ve sorunlar ilgili sistemlerde maliyet ve zaman kaybına yol açmaktadır. Araştırmacılar tarafından sıkça bahsedilen konular arasındadır.

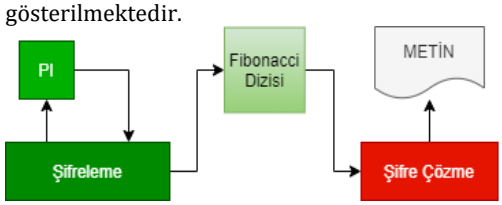
- Açık anahtarlı şifrelemenin kompleks ve işlem gücüne dayalı bir süreç olduğunu ve algoritmaların optimize edilmesinin önemine ilgili çalışmalarda dikkat çekilmek istenmektedir.

- Simetrik ve asimetrik algoritmaların güçlü ve zayıf olduğu durumlar üzerinde çalışmalar mevcuttur. Literatürde ayrıca algoritmalara yapılan ataklar üzerine çeşitli çalışmalarda vardır. Literatürde elde edilen bilgiler ile çalışmamdaki hibrit şifreleme tekniğinin özgün olarak yapılması ve istenilen ihtiyaçları karşılaması amaçlanmıştır. Araştırmacıların yaptıkları çalışmalardaki çeşitli sorunlar göz önüne alınarak yüksek başarımlı bir algoritma oluşturulmuştur. Oluşturulan bu algoritma simetrik şifreleme ile benzer özellikler barındırmasıyla ve modüler bir yapıda geliştirilebilir olmasıyla dikkat çekmektedir. Algoritmada dinamik şifreleme mekanizmasının olması gelebilecek saldırılar karşısında dirençli olmayı amaçlamaktadır.

2. Materyal ve Metot

Çalışmamızda gönderici ve alıcı arasındaki iletişim, şifreleme çeşitlerinden olan simetrik şifreleme tekniği kullanılarak gerçekleşir. Bu şifreleme algoritmasında asimetrik şifrelemenin aksine ortak bir tek anahtar vardır. Açık anahtarlı şifrelemede 2 çeşit anahtar mevcuttur. Genel Anahtar, orijinal verileri veya düz metni şifrelemek ve bir şifreli metin oluşturmak için kullanılır [27]. Özel Anahtar ise oluşturulan bu şifreli metni çözümlemek için oluşturulmuştur. Algoritmanın hibrit çalışmasının birden fazla nedeni vardır. Öncelikle ortak bir anahtarın yanı sıra simetrik algoritmalarda rastlanan "S-Box" a benzer bir yapı kullanılmaktadır. Algoritmanın kelime havuzunda bir eşleştirme yöntemi kullanılarak statik bir değer atama işlemi yapılmaktadır. Ayrıca bu statik değerlerin yanına harfe göre dinamik bir ataması da yapılmaktadır. Algoritma genel olarak simetrik şifreleme hiyerarşisine dayanmaktadır. Şekil 2'de ve Şekil 4'te bulunan tablo simetrik algoritmalardaki özellikler ile benzerdir.

Bilgi mesajımızın şifrelenmesi pi sayısının (Arşimet sabiti) karmaşıklığından ve Fibonacci dizisinin uyumundan faydalanılarak geliştirilmiş bir yöntemdir. Pi sayısı seçmemizin nedeni ise rakamlar belli bir düzene veya örüntüye göre gitmemektedir. Şimdiye kadar rastlantısal bir benzerlik bulunamamıştır. Bu bizim için büyük bir avantajdır. Çalışmanın genel yapısı Şekil 1'de gösterilmektedir.



Şekil 1. Çalışmanın genel yapısı

Şifreleme işlemimizde ilk olarak bilgi mesajı istenir. Mesaj harflere bölünür. Her harf için 5 haneli bir yer ayrılmaktadır. Şekil 2'de belirtilen görselde 3 basamağı statik olarak, 4. ve 5. rakam ise dinamik olarak verilir.

İlk 3 Basamak :

111	112	121	122
a - e	ı - i	o - ö	u - ü
211	**212**	**221**	**222**
b - c - ç - d - f	g - ğ - h - j - k	l - m - n - p - r	s - ş - t - v - y - z

' ' : 000

ÜNSÜZ İSE İLK BASAMAK (2);

b , c , ç , d , f	g , ğ , h , j , k
1.satır 1.sütun	1.satır 2.sütun
l , m , n , p , r	s , ş , t , v , y
2.satır 1.sütun	2.satır 2.sütun

z (222)

" " (000)

ÜNLÜ İSE İLK BASAMAK (1);

a , e	ı , i	o , ö	u , ü
1.1	1.2	2.1	2.2

Şekil 2. Şifreleme mekanizmasında ilk 3 basamağın seçimi

İlk 3 haneyi statik olarak bir düzene göre değerleri verilmiştir. Sayımızın 4. hanesini yazarken pi sayısından referans alınmıştır. Şekil 3'te rastgele verilen bir numara üzerinde örnek yapılmaktadır.

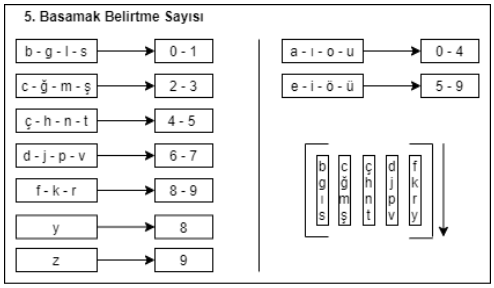
```
1.RASTGELE NUMARAMIZ : 4 OLSUN

PI SAYISI:

3,1,4,1,5,9,2,6,5,3,5,8,9,7,9,3,2,3,8,4,6,2,6,4,3,3,8,3,2,7,9,5,0,2
0-1-2-3-A-B-C-Ç-D-E-F-G-Ğ-H-I-İ-J-K-L-M-N-O-Ö-P-R-S-Ş-T-U-Ü-V-Y-Z

A : 1115(İlk 3 basamak statik bir mantığa göre 4. basamak rastgele
verildi)
```

Şekil 3. Pi Sabiti Üzerinden Rastgele Atılan İndis Örneği

Uygulaması yapılan bilgisayar programında pi sayısının ilk 1000 hanesi liste şeklinde tanımlanmaktadır. Program tanımlanan pi sayısının basamaklarını geçmemek şartıyla rastgele bir sayı üretip oluşturulan listeden denk gelen indisteki liste elemanını almaktadır. Alınan indis değerinden itibaren her alfabenin harfi bir sonraki indis değerine atanarak alfabedeki harflere denk gelen bir sayı dizisi çıkarılmıştır. Pi sayısına atanan rastgele sayı, başlangıç indisi olarak kabul edilir. Her seferinde 1 arttıracak şekilde alfabedeki harfler yazılır. Harf bazlı 5 basamaklı şifrelemenin 4 hanesini tamamlanmıştır.

Şekil 2' de görüldüğü gibi şifrelenmek istenen harfin, ilk 3 basamağı statik olarak tablodan alınmaktadır. 4. Basamak ise Şekil 3'te görüldüğü gibi pi sayısının elemanlarından oluşan listeden başlangıç indisinin konumuna göre alınmıştır.

Şifreleme mekanizmamızda istenilen 5. basamağı oluşturabilmemiz için ünsüz harflerden oluşan matrisin transpozu alınacaktır. Harfi şifreleyebilmek için son adım belirtme sayısı olarak tabir edeceğimiz, harfe özgü sayı atama işlemidir.



Şekil 4. Belirtme Sayısı Seçimi - Matris Transpozu

Belirtme sayısını bulabilmek için alfabenin ünlü ve ünsüz harfler olarak 2 gruba ayırma işlemi yapılmaktadır. Ayrılan gruplar ise tekrar 4'e bölünmektedir. Yukarıda bahsedilen ilk 3 basamak, kural dahilinde verilmektedir. Ancak Arşimet sabitinde harflere denk gelen sayı 4'lü harf gruplarında tekrar ederse, harfler arasında çakışma tespiti kanısına ulaşılabilir. Bu sorunun önüne geçebilmek için belirtme sayısı kullanılmıştır.

Bilgisayardan rastgele atılan rakamların arasına oluşturulan 5 haneyi yerleştirme işlemleri tamamlanmıştır. Gönderilen kişide ki özel anahtar rastgele atadığımız değerler arasındaki 5 haneyi bulmasına yardımcı olacaktır.

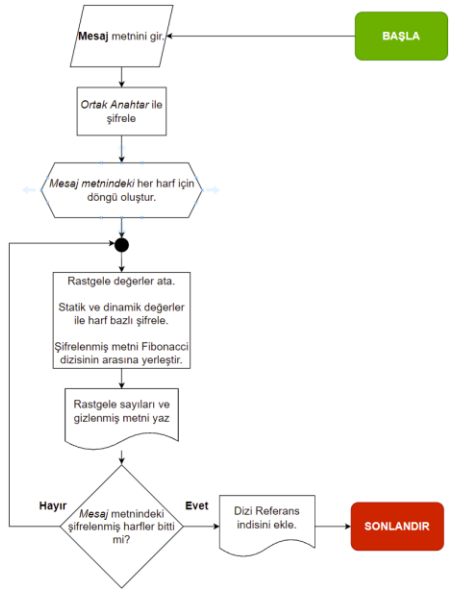
Harflerin tek tek 5 hane olarak şifrelenmesi ve Fibonacci dizisine arasına yerleştirilmesi ile kısmi olarak şifrelenme tamamlanmaktadır. Harfler Fibonacci dizisinin *n-2* ve *n-1*. terimlerinden sonra 5 basamak yazılır ve ondan sonra *n-2* ve *n-1* toplamı *n* olarak yazılmaktadır. Şifreli yapı (1)' de gösterilmektedir.

$$(n-2)(n-1)(4\ hane)(Belirtme\ S.)(n) \qquad (1)$$

n : Fibonacci dizisindeki ilk atanan başlangıç indisi

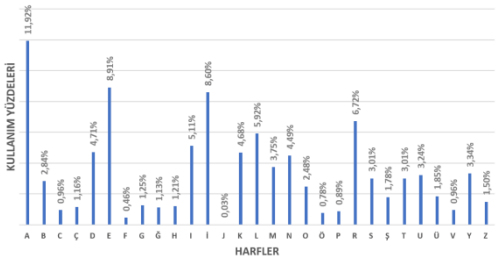
Bu yöntemle harf için şifreleme işlemi tamamlanır. Ancak rastgele sayıların arasında harflerin belli bir düzene göre yazılması sakıncalıdır. Bu riskten dolayı tekrar pi sayısından rastgele atama yapılmaktadır. Şifrelenmiş metinde harfler arasındaki uzaklıklarda rastgele olmaktadır. Son olarak ise şifrelenmiş metinin sonuna, ilk başta rastgele atadığımız pi sayısının indisi yazılmakta ve referansı belli edilmektedir. Şekil 5'te algoritmanın akış diyagramı gösterilmektedir.

Son indiste referansın belli edilmesi, şifreli metne sahip olan herkesin metni tamamını anlama fırsatı vermemektedir. Oluşturulan şifreli metinden sadece harf sayısı kadar indis değeri kadar bilgi edinecektir. Ancak şifrelenmemiş metnin uzunluğu bilinmediğinden dolayı ve şifreli metinden harflere denk gelecek indislerin yerini net bulunmadığından dolayı eldeki veri bir anlam ifade etmeyecektir. Algoritma katmanlı mimariye sahiptir. Tüm şifreleme katmanlarını elde eden bir şifreli metin sahibi şifreli metni çözebilmektedir.



Şekil 5. Algoritmanın Akış Diyagramı

Şekil 6'da alfabemizde en sık kullanılan harfler gösterilmektedir. Harflerin kullanım yüzdelerine göre şifreli metinde sayıların denk gelme sıklığı incelendiğinde bağlantı veya benzerlik kurulamadığı gözlemlenmektedir.

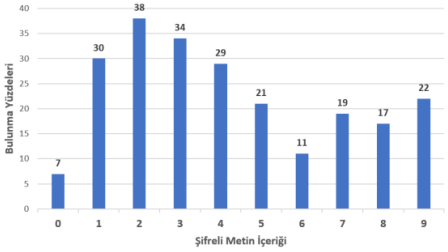


Şekil 6. Türkçede Sık Kullanılan Harfler

Örneğin mesaj metnimizi "kriptoloji" olarak girildiği zaman değişken uzunlukta şifreli metinler üretilmiştir. Şifreli metin örneği;

42502917777479722891442128823353352378911442216823343892134112065538793739574934463522116855756213422294554895750645913211219034362764314423322180377631453352481321121933428987999572915865418144233212263779942099348914411205233 21

Şifreli metinimizin sayılarının frekans analizi sonucunda Şekil 7'deki grafik elde edilmektedir.



Şekil 7. Kriptoloji Kelimesinin Şifreli Metinde Frekans Analizi

Frekans analizi kapsamında Türkçede kullanılan en sık harfleri eşleştirmek yada bir çıkarım yapmak için şifreli metindeki tekli sayılar uygun değildir. Şifreli metinde ikili, üçlü hatta dörtlü kombinasyonlara bakmak gerekmektedir. Ancak şifreleme işleminde şifreli harflerin arasına rastgele uzunlukta ve farklı sayılardan oluşan kaotik bir ortam sağlanmıştır. Şekil 2'de görüldüğü üzere oluşturduğumuz kodlama yapısıyla en fazla kullanılan sayıların 1 ve 2 olduğu anlaşılmıştır. Ancak bir çıkarım yapmak söz konusu değildir. Çünkü 1 ve 2 sayısı tüm harflerde sürekli olarak kullanılmaktadır.

Statik değerler tablosu, pi listesinin başlangıç indisi, belirtme sayısı değeri ve fibonacci serisine göre şifreleme yapıldığını bilen bir şifreli metin sahibi şifreyi çözebilmektedir. Ancak çözme süresi şifreli metnin uzunluğuna göre değişkenlik gösterip, birden fazla kriptanaliz yöntemini paralel olarak kullanması gerekmektedir. Her şifreli metinde tüm argümanlar değişeceği için elinde geniş bir şifreli metin havuzu da olması gerekmektedir.

Şifreli metni çözebilmek için öncelikle fibonacci dizisindeki indisler şifreli metin üzerinde aranmaktadır. Arama işlemi, fibonacci dizisinde ardışık iki sayıya göre öncelikli arama yapmaktadır. Ayrıca şifreli metnin son indisini bir değişkende kaydedilmektedir. Bulunan ardışık indisler toplanır ve 5 hane sonrasındaki sayıya eşitliği kontrol edilir. Yapılan kontrol sonucunda eşleşen numaralar potansiyel şifreli harf taşımaktadır. Harfin konumunun bulunabilmesi için öncelikli olarak statik değerler tablosundan ilk 3 indis kontrol edilmektedir. Daha sonra pi sayısındaki değer ve sırayla belirtme sayısına bakılmaktadır. Bu 5 değer ile harfimizin kesin olarak yeri saptanılmaktadır. Böylece şifre çözme işlemi kademeli olarak ve yüksek doğruluk ile bulunabilmektedir.

3. Bulgular

Asimetrik şifreleme algoritmalarında yapılan işlemler (şifreleme, kimlik doğrulama, şifre çözme) simetrik algoritmalara göre daha yavaş süreçlerdir. Kullanılan şifreleme mekanizması, şifrelenen mesajın uzunluğu ve uygulamanın çalıştığı platform, işlemlerin hızını belirleyen faktörlerdendir [10].

Şifreleme algoritması çeşitli yazılım dillerinde yazılıp, performans/başarım karşılaştırılması değinilmiştir. Algoritmanın hesaplama karmaşıklığını ve avantajlarını netleştirmek için ayrıntılı bir teorik/uygulama analizi yapılmıştır [28]. Algoritmanın uygulama programı hazırlanıp arama/zaman tepki süreleri optimal bir performans sağlamaktadır [29].

Oluşturulan şifreli yapı sağına ve soluna gelecek rastgele uzunlukta ve rastgele verilen numaralar ile karmaşıklığı arttırılmaya çalışılmıştır. Ancak rastgele sayılar yan yana dizilerek oluşturulan şifreli yapıya benzer sonuç çıkarabilmektedir. Ortalama 0.005 hata payı ile çok düşük olasılıkta olan bu durum, genel metni etkilemeyecek kadar küçük olduğu için dikkate alınmamaktadır. Ancak şifrelenecek metnin doğruluğunu şifre çözme performansında düşürebileceği için performans sonuçlarında yer verilmektedir.

3.1. Şifreleme performansı

Tablo 1'de görüldüğü üzere algoritmanın şifreleme performansı, şifrelenmek istenen harf ve şifrelenme süresi ile ölçülmüştür. Şifrelenecek harf sayısı arttığı için kullandığımız şifreleme algoritması her seferinde yeni değerler istemek zorundadır. Her isteme durumunda yazılım yeni değer verecektir. Bu durum harf sayısı ile geçen zaman arasındaki benzerliği açıklamaktadır. Bu orantı beklenen bir durumdur. Daha büyük metin boyutlarının hesaplama süresi ve işlem gücünde artışa neden olduğu ispatlanmıştır [11].

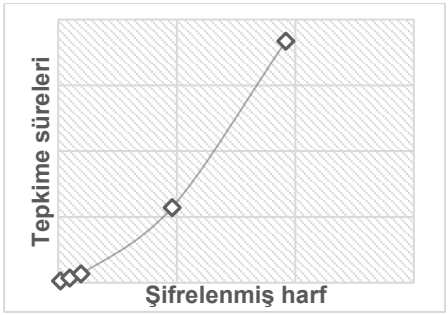
Günümüzde sıklıkla kullanılan şifreleme algoritmaları ile karşılaştırıldığında özgün değeri ve başarımı yüksek bir yapı önümüze gelmektedir. Aktif olarak kullanılan algoritmalardan performans, başarım ve işlem hacmi bakımından bir eksikliği bulunmayan özgün bir model oluşturulmuştur. Şekil 9.'da belirtilen şifreleme algoritmaları ile karşılaştırıldığında büyük veriler için şifreleme hızı kullandığımız sistemden dolayı daha fazla olduğu gözlemlenmiştir. Bu durumun nedeni ise şifreli metin uzunluğundan kaynaklanmaktadır. Ancak şifreleme algoritmalarıyla güvenilirlik bakımından karşılaştırılabilecek kapasiteye sahiptir. Şekil 8'de algoritmanın şifreleme performansının tepki süresi ve şifreli sayı arasındaki ilişkiyi göstermektedir.

Yüksek boyutlu girdi metinlerine göre hız bakımından diğer DES, TEA ve XTEA ile karşılaştırılabilmektedir. Düşük veri boyutlarında tüm algoritmalarda yakın sonuçlar elde edilmektedir.

Tablolardaki veriler ile çalışmamızdaki veriler farklı yazılım ve donanımlarda test edilmiştir. Algoritmamız daha güçlü donanımlarda ve verimli yazılımlar ile benzer sonuçlar vermesi düşünülmektedir.

Tablo 1. Mesaj uzunluğuna göre şifreleme performansı

100 Bayt		500 Bayt		1KB		5KB		10KB	
Şifreli Harf	Tepki Süresi (ms)	Şifreli Harf	Tepki Süresi (ms)	Şifreli Harf	Tepki Süresi (ms)	Şifreli Harf	Tepki Süresi (ms)	Şifreli Harf	Tepki Süresi (ms)
2002	12	9547	35	19118	65	96080	584	191713	1846
1955	12	9646	40	19339	67	96169	557	191774	1782
2004	14	9592	36	19158	68	95807	569	192184	1877
1974	13	9616	36	19161	65	96391	582	191990	1844
1988	12	9657	34	18998	63	96098	559	192029	1860
1896	12	9583	39	19263	67	95669	598	192108	1805
1967	13	9512	36	19208	65	96204	598	191866	1794
1932	13	9687	36	19227	68	95328	524	192275	1861
1964,75	**12,6**	**9605**	**36,5**	**19184**	**66**	**95968,2**	**571,4**	**191992,4**	**1834**



Şekil 8. Şifreleme Performansı

Oluşturulan hibrit yöntem ile şifreli metnin uzunluğu diğer algoritmalara göre fazladır. Bu fazlalık şifreli metnin oluşturulmasında yoğun işlem hacmine ve daha deterministik bir yapı olmasından kaynaklanmaktadır.

Açık anahtarlı sistemler, açık anahtarın uzunluğuna ve gücüne göre çıktı metnin çözme performansını değiştirmektedir. Genellikle bu sistemlerde anahtar büyüklüğü, karmaşıklık ile doğru orantılıdır.

Örneğin; Tablo 2'de görüldüğü üzere açık anahtarlı şifreleme algoritmalarından RSA'daki anahtar uzunluğu ve Eliptik eğri şifreleme de EEŞ gibi parametreler değişiklik gösterebilir. Gösterilen değişiklikler neticesinde anahtara göre şifreleme hacmi ve karmaşıklığı değişebildiği görülmektedir. Algoritmamızda yukarıda bahsedilen anahtar büyüklükleri ve karmaşıklık durumunda kaynaklanan hız düşüşü gibi performans kaybı yaşamamaktadır. Çalışmamızda hibrit anahtar olarak belirtebileceğimiz yapı sayesinde anahtarın boyutunu istenildiği kadar artırılsa bile şifreli metnin çözme performansı değişmediği gözlemlenmiştir.

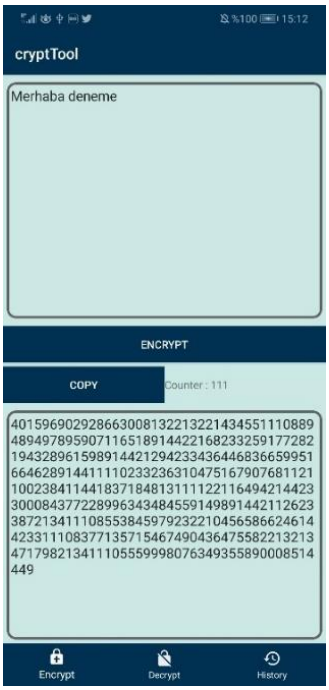
ŞİFRELEME	TEA	XTEA	AES	DES	RSA	RC5
100 KB	13148	14069	550	15786	5360	803
200 KB	68592	71650	2792	90345	32364	4740
300 KB	192907	185324	8969	239743	84167	16569
400 KB	489996	366183	19526	468525	180224	31239
500 KB	625274	625373	36363	820021	299300	53713

Şekil 9. Algoritmaların Şifreleme Süreleri [30]

Tablo 2. Şifreli Metin Uzunlukları [31]

RSA	Süre(ms)	EEŞ	Süre(ms)
512 bit	2.2	-	-
1024	10.3	160	7.2
2048	59.6	224	10.0
4096	390.5	-	-
-	-	384	30.8

Kapalı anahtarlı şifrelemede belirtilen algoritmalarda ki gibi S-Box tablosuna benzer bir yapı kullanılmıştır. Ancak hibrit yöntem kapalı anahtarlı şifreleme özelliklerinin tamamını taşımamaktadır. Çalışma kapsamında önerilen yöntemde şifreleme ve şifre çözme işlemi yapabilen bir mobil uygulamanın Şekil 10'de görüntüsü verilmektedir.

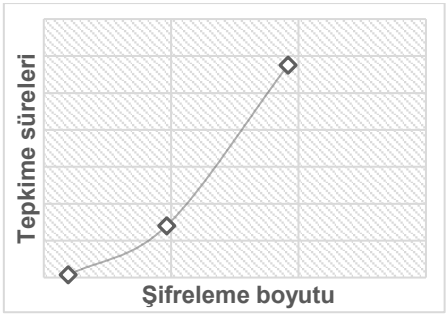


Şekil 10. Mobil platformda şifreleme programı

3.2. Şifre çözme performansı

Tablo 3'de şifreli metnin uzunluğuna göre çözme performansı gösterilmiştir. Veri boyutlarına bakıldığında açık metnin 19 katı olacak şekilde şifreli metin üretilmiştir. Başarımı çok yüksek olarak sonuçlar bulunmuştur. Hata payı göze alınamayacak derecede küçüktür. Oluşan bu şifreli metindeki karmaşıklık ve rastgelelik algoritmanın dayanıklılığını artırdığı söylenebilir.

Bulunan şifre çözme performans verileri beklenilen değerleri vermektedir. Algoritmadaki şifreli metnin uzunluğu, çözen sistemdeki işlem gereksinimi ve tepkime süresinin artışına neden olmaktadır.



Şekil *11*. Şifre çözme performansı

Şekil 11'da şifre çözme performansı gösterilmektedir. Tablolar ve grafikler sonucunda mesajımızın uzunluğu, şifreli metin uzunluğu ve işlem süresinde doğru orantı tespit edilmiştir. Çalışmamızda açık metindeki harf sayısı artırıldığında, başarımın yükseldiği gözlemlenmektedir. Başarım oranları son derece yüksektir. Şekil 12'de mobil uygulamada şifre çözme işlemi yapılmaktadır.

Şekil 12. Mobil Platformda Şifre Çözme Programı

Yüksek veri boyutlarında şifre çözme süresinin diğer boyutlara göre daha çok gecikmesi beklenmekte olan bir durumdur.

Tablo 1. Mesaj Uzunluğuna Göre Şifre Çözme

1.8KB - 2KB Şifreli Harf			9KB – 10KB Şifreli Harf			19KB – 20KB Şifreli Harf		
Tepki Süresi (ms)	**Şifreli Harfler**	**Başarım**	**Tepki Süresi (ms)**	**Şifreli Harfler**	**Başarım**	**Tepki Süresi (ms)**	**Şifreli Harfler**	**Başarım**
141	1961	99,998	2802	9716	100	11321	19044	99,995
123	1868	100	2873	9648	99,994	11756	19255	99,997
158	1936	100	2753	9548	99,996	11548	19240	99,994
128	1907	99,9	2771	9682	100	11326	19171	99,994
132	1922	100	2742	9503	99,990	11355	19129	99,998
145	1887	99.9	2856	9663	99,992	11867	19186	99,992
136	1916	99,991	2792	9586	99,996	11562	18864	100
152	1874	99,992	2812	9709	100	11241	19386	100
Ort:	**Ort:**	**Ort:**	**Ort:**	**Ort:**	**Ort:**	**Ort:**	**Ort:**	**Ort:**
139	1909	99,98	2800	9632	99,996	11,497	19159	99,9962

Veri kaynağımız artarsa çözme süresi de artacaktır. Şifreleme ve şifre çözme işlemlerinde İntel i5 -5200U 2.20GHz işlemci 8GB RAM ve 2GB 920M ekran kartı donanımlarına sahip bir bilgisayarda sonuçlar ölçülmüştür. Daha iyi donanımlarda algoritmanın tepki süresi daha da düşmesi ön görülmektedir. Algoritmanın şifreleme ve şifre çözme performansı masaüstü ortamda C# dilinde yazılmış bir masaüstü programında ölçülmektedir. Şifreleme ve şifre çözme süreçlerini timer nesneleri arasına alarak elde edilen sonuçlar paylaşılmaktadır.

Mobil donanım için Android Studio geliştirme ortamı ile Java dilinde yazılmıştır. Mobil donanımda metin şifreleme ve şifre çözme fonksiyonları tasarlanmıştır. Şifrelenen ve çözülen metinler SQLite' ta oluşturulan bir tabloya kaydedilmektedir. Masaüstü programın performansına göre daha düşük performans göstereceği ön görülmektedir.

4. Tartışma ve Sonuç

Kriptoloji biliminin günlük yaşantımızdaki kullanım alanları sadece e-devlet veya elektronik posta ile sınırlı değildir. Bu bilim hayatımızda sürekli olarak kullandığımız internet trafiğinin önemli bir kısmının kontrolünü ve güvenliğini elinde tutmaktadır. Kredi kartı çiplerinden kimlik numaramıza kadar uzanan bu bilimin çalışma alanı vardır.

Sürekli olarak büyüyen internet ağı beraberinde devasa boyutlarda verilerde getirmektedir. Verilerin önemli bir kısmı mahremiyet gerektiren ve şifrelenmesi gereken bilgilerdir. Bu devasa bilgi yığınlarındaki önemli bilgileri hızlı bir şekilde şifreleyip ve şifre çözen bir yapı gerekmektedir.

Çalışmamızın şifreleme dünyasında alışılmadık bir yöntemle oluşturulmuş hibrit bir algoritmadır. Algoritmanın gerek performansı ve tanımlı olan metin havuzundaki esneklik sayesinde geniş bir kullanıcı kitlesi hedeflemektedir. Genel olarak sistem kapalı anahtarlı şifreleme üzerine kurulmuştur.

Kapalı anahtarlı sistemimiz dil havuzu bakımından zenginleşebilmektedir. Bu zenginleşmeyi sağlamak için algoritma tasarımında bir değişiklik yapmamız gerekmemektedir. Şifreleme algoritması modüler bir yapıya sahiptir.

Yapılan şifreleme algoritması statik ve dinamik veriler üzerinde işlem yapmaktadır. Genel olarak Kapalı Anahtarlı Şifreleme üzerine çalışmaktadır. Ortak bir anahtara sahiptir. Bu durumun yanı sıra çeşitli statik olarak oluşturulan şifreli metinler ile algoritmaya güçlendirmek hedeflenmiştir.

Bulgularımız ışığında algoritma yüksek verim elde etmiştir. Mobil ve masaüstü platformlarında

çalıştırılıp test edilmiştir. Performans aralığı kabul edilebilir durumdadır. Hızı kısa metinler için idealdir.

Çalışmada, Arşimet sabiti ve Fibonacci dizisini kullanılarak 3 katmanlı bir şifreleme işlemi gerçekleştirilmiştir. Modüler bir yapıya sahip olduğundan dolayı bu katmanlar artırılabilmektedir. Katman sayısı şifrelemede önemli bir güce sahiptir. Şifreli metnin ayıklamasında her bir katman süzgeç görevi görmektedir. Şifrelenen veri çok düşük hata payı ile bu süzgeçlerden geçip şifre çözme işlemi tamamlanmaktadır.

Algoritmamız kapalı anahtarlı şifrelemenin özelliklerine sahip harf havuzuna göre kodlanmış bir modüler yöntemdir. Bu nedenden dolayı uçtan uca şifreleme yapacak olan uygulamalar için cazip bir çözüm olarak görülmektedir. Metinsel içerikler, ses, görüntü ve video dosyaları üzerinde şifreleme yapılabilir. Genel bir sunucu üzerinden istemciler arasındaki iletişim şifreli olarak sağlanabilir. Böylece konuşma kanalına 3. şahıslar erişebilse dahi gönderilmek istenen metni göremeyecektir.

Algoritmamız ileriki çalışmalar için veri tabanı dosyalarının şifrelenmesinde ve dinamik parola oluşturma programlarında kullanılabilmektedir. RFID, RF sinyallerini ve ağda paylaşılan uygulamalar arasındaki iletişimde önerdiğimiz yöntem uyarlanarak şifrelenebilir. Bilgisayar, tablet ve telefonlarda şifrelemek istediğimiz uygulama, fotoğraf, ses ve metinsel içeriklerde algoritmamız bir çözüm olarak görülebilir.

Algoritmamız yapısal anlamda da iyileştirilebilir. Çalışmadaki statik verilerin tamamı dinamik olarak Arşimet sabitinden atama yapılarak indis numaraları ile çalışabilir. Böylece frekans analizi gibi kripto analiz yöntemlerinin şifreli metnimizi bulması zorlaştırılabilir. Metnin tamamının dinamik yapısı kaba kuvvet saldırılarının önüne geçebilir. Çalışmada ayrıca 3 kademeli olan şifreleme yapısı değiştirilebilir. Katman sayısı yükseltilerek karmaşıklık artırılabilir. Böylelikle şifreleme seviyesi daha yüksek düzeye çıkabilir. Ancak şifre çözme performansında düşüşler gözlenebilir.

Kaynakça

[1] Turak, Y. 2015. Nesnelerin interneti ve güvenliği http://www.yigitturak.com/wp-content/uploads/IoTGuvenligi.pdf (Erişim Tarihi: 04.12.2021).

[2] Baykara M., Daş R., Karadoğan İ. 2013. Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi. 1st International Symposium on Digital Forensics and Security, 20-21 Mayıs, Elazığ, 231–239.

[3] Fındık O. 2004. Şifrelemede Kaotik Sistemin Kullanılması. Selçuk Üniversitesi, Bilgisayar Mühendisliği Bölümü, Yüksek lisans Tezi, Konya.

[4] Akleylek S., Murat Yıldırım H., Tok Z. Y. 2011. Kriptoloji Ve Uygulama Alanları: Açık Anahtar Altyapısı Ve Kayıtlı Elektronik Posta. Akademik Bilişim, 2-4 Şubat, Malatya, 713–718.

[5] Pakshwar R., Trivedi V. K., Richhariya V. 2013. A Survey On Different Image Encryption And Decryption Techniques, International Journal of Computer Science and Information Technologies, Cilt. 4, s. 113-116.

[6] Yıldırım K., Demiray H. E. 2013. Simetrik Ve Asimetrik Şifreleme Yöntemlerine Metotlar: Çırpılmış Ve Birleşik AKM-VKM, Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, Cilt. 23, s. 539–548.

[7] Yerlikaya T., Buluş E., Buluş N. 2006. Asimetrik Şifreleme Algoritmalarında Anahtar Değişim Sistemleri. Akademik Bilişim, 9-11 Şubat, Denizli.

[8] Yerlikaya T., Buluş E., Buluş N. 2006. Kripto Algorıtmalarının Gelişimi Ve Önemi. Akademik Bilişim, 9-11 Şubat, Denizli.

[9] Rogaway P., Coppersmith D. 1993. A Software-Optimized Encryption Algorithm. International Workshop on Fast Software Encryption, 9-11 Aralık, Cambridge, 56-63.

[10] Levi A., Mahmut Ö. 2002. Açık Anahtar Tabanlı Şifreleme Neden Zordur?. Akademik Bilişim, 6-8 Şubat, Karabük, 6–8.

[11] Prajapat S., Jain A., Singh Thakur R. 2012. A Novel Approach For Information Security With Automatic Variable Key Using Fibonacci Q-Matrix, International Journal of Computer and Communication Technology, Cilt. 3, s. 54-57.

[12] Özkaynak F., Özer A. B., Yavuz S. 2011. Kaos Tabanlı Yeni Bir Blok Şifreleme Algoritması, IV. Ağ ve Bilgi Güvenliği Sempozyumu, 25-26 Kasım, Ankara, 108.

[13] Wang Y., Wong K. W., Liao X., Xiang T. 2009. A Block Cipher With Dynamic S-Boxes Based On Tent Map, Communications In Nonlinear Science and Numerical Simulation, Cilt. 14, s. 3089–3099. DOI: 10.1016/J.CNSNS.2008.12.005

[14] Cocks C. 2001. An Identity Based Encryption Scheme Based On Quadratic Residues. IMA International Conference On Cryptography And Coding, 17-19 Aralık, Cirencester, 360–363.

[15] Waters B. 2005. Efficient Identity-Based Encryption Without Random Oracles. Annual International Conference on the Theory and Applications of Cryptographic Techniques, 22-26 Mayıs, Aarhus, 114–127.

[16] Lewko A., Waters B., 2011. Decentralizing Attribute-Based Encryption. Annual International Conference on the Theory and Applications of Cryptographic Techniques, 15-19 Mayıs, Tallinn, 568–588.

[17] Bellare M., Boldyreva A., Desai A., Pointcheval D. 2001. Key-Privacy In Public-Key Encryption. International Conference on the Theory and Application of Cryptology and Information Security, 9-13 Aralık, Gold Coast, 566–582.

[18] Zengin, Mustafa. 2021. Genetik Kod Yöntemi İle Kriptoloji Uygulamasi. Karabük Üniversitesi, Bilgisayar Mühendisliği Bölümü, Yüksek lisans Tezi, Karabük.
[19] Hamdi, M., Miri, J., Moalla, B. (2021). Hybrid encryption algorithm (HEA) based on chaotic system. Soft Computing, Cilt. 25, s. 1847-1858.
[20] Viswanath, G., & Krishna, P. V. (2021). Hybrid encryption framework for securing big data storage in multi-cloud environment. Evolutionary Intelligence, Cilt. 14, s. 691-698.
[21] Abroshan, H. (2021). A hybrid encryption solution to improve cloud computing security using symmetric and asymmetric cryptography algorithms. International Journal of Advanced Computer Science and Applications, Cilt. 12.
[22] Koçak, C. 2015. Kriptografi Ve Stenografi Yöntemlerini Birlikte Kullanarak Yüksek Güvenlikli Veri Gizleme. Erciyes Üniversitesi Fen Bilimleri Enstitüsü Fen Bilimleri Dergisi, Cilt. 31, s. 115-123.
[23] Doğan, N., Çelik, H. 2021. Tarama Modeli Kullanan Karma Bir Görüntü Şifreleme Yöntemi. Politeknik Dergisi, Cilt. 1.
[24] Şatir, E., Kendirli, O. 2013. A Hybrid Steganographic Approach Via Web Adresses. İleri Teknoloji Bilimleri Dergisi, Cilt. 2, s. 53-60.
[25] Çavuşoğlu, Ü. 2016. Kaos Tabanlı Hibrit Simetrik Ve Asimetrik Şifreleme Algoritmaları Tasarımı Ve Uygulaması. Sakarya Üniversitesi, Bilgisayar ve Bilişim Sİstemleri Mühendisliği Bölümü, Doktora Tezi, Sakarya.
[26] Atar, E., Ersoy, O. K., Özyılmaz, L. 2017. Dik Eşleştirme Arayış Yöntemi Ile Hibrit Veri Sıkıştırma Ve Optiksel Kriptografi. Journal of the Faculty of Engineering and Architecture of Gazi University, Cilt. 32, s. 139-147.
[27] Akanksha M. 2012. An ASCII Value Based Data Encryption Algorithm And Its Comparison With Other Symmetric Data Encryption Algorithms, International Journal on Computer Science and Engineering, Cilt. 4, s. 1650.
[28] Yang Y.-G., Xia J., Jia X., Zhang H. 2013. Novel Image Encryption/Decryption Based On Quantum Fourier Transform and Double Phase Encoding. Quantum Information Processing, Cilt. 12, s. 3477–3493. DOI: 10.1007/s11128-013-0612-y
[29] Schneier B. 1993. Description Of A New Variable-Length Key, 64-Bit Block Cipher (Blowfish). International Workshop on Fast Software Encryption, 9-11 Aralık, Cambridge, 191–204.
[30] Ökdem S., Kirtay M. 2018. Kablosuz Ağlarda Şifreleme Algoritmalarının Performans Analizi. ISAS 2018 1st International Symposium on Innovative Approaches in Scientific Studies, 11-13 Nisan, Antalya, 461–464.
[31] Akben S. B., Subaşı A. 2005. RSA Ve Eliptik Eğri Algoritmasının Performans Karşılaştırması. KSÜ Fen ve Mühendislik Dergisi, Cilt. 8, s. 35–40.