aurum

AURUM MÜHENDİSLİK SİSTEMLERİ VE MİMARLIK DERGİSİ
AURUM JOURNAL OF ENGINEERING SYSTEMS AND ARCHITECTURE

Cilt 5, Sayı 1 | Yaz 2021
Volume 5, No 1 | Summer 2021, 29-40

ARAŞTIRMA MAKALESİ / RESEARCH ARTICLE

RSA VE RC4 ALGORİTMALARININ PERFORMANS KARŞILAŞTIRMASI

Tuğçe YÜKSEL[1]
[1]Bilişim Güvenliği Teknolojisi Bölümü, İstanbul Gelişim Meslek Yüksekokulu,
Gelişim Üniversitesi, İstanbul, Turkey
tyuksel@gelisim.edu.tr, ORCID No: 0000-0002-1487-6041

Büşra ÖZGÜN[2]
[2]Bilgisayar Mühendisliği Bölümü, Lisansüstü Eğitim Enstitüsü,
İstanbul Aydın Üniversitesi, İstanbul, Turkey
ozgunbusra@gmail.com, ORCID No: 0000-0003-3213-9018

Geliş Tarihi/Received Date: 19.01.2021 Revizyon Tarihi/Revision Date: 28.05.2021
Kabul Tarihi/Accepted Date: 10.06.2021

Özet

Günümüzde bilgi teknolojileri sistemlerinin en önemli çalışma alanlarından biri güvenliktir. İletişim teknolojilerinin hızla gelişmesi, bilgi güvenliği sorunlarını da beraberinde getirmiştir. Sistemler arasındaki iletişimde veya herhangi iki nokta arasındaki bağlantıda verinin güvenli olarak gönderilmesi önem taşımaktadır. Bunun sağlanabilmesi için, uygun bir şifreleme tekniği kullanılarak verinin şifrelenmesi gerekir ve bu kriptoloji adı verilen bilim dalının konusudur. Verilerin güvenilir bir şekilde iletilmesi ve elde edilmesi için kriptoloji bilimi kullanılarak çeşitli anahtarlama, şifreleme ve şifre çözme algoritmaları geliştirilmiştir. Bu çalışmada, yaygın olarak kullanılan asimetrik şifreleme yöntemi olan RSA algoritması ile simetrik şifreleme yöntemi olan RC4 algoritmasının performansları karşılaştırılmıştır. Sonuç olarak RC4 algoritması kullanılarak, şifrelenmiş bir bilginin, deşifrelenmesinin RSA algoritmasına göre daha hızlı olduğu gösterilmiştir.

Anahtar Kelimeler: Şifreleme, Şifre Çözme, RSA, RC4.

PERFORMANCE COMPARISON OF RSA AND RC4 ALGORITHMS

Abstract

Today, one of the most important fields of study of information technology systems is security. The rapid development of communication technologies has brought information security problems. It is important to send data securely in the communication between systems or any connection between two points. In order to achieve this, data must be encrypted using an appropriate encryption technique and this is the subject of the science called cryptology. Various keying, encryption and decryption algorithms have been developed using the science of cryptology in order to transmit and retrieve data in a reliable manner. In this study, the performances of the RSA algorithm, which is a widely used asymmetric encryption method, and the RC4 algorithm, which is a symmetric encryption method, are compared. As a result, it has been shown that encrypted information is decrypted faster than RSA algorithm by using RC4 algorithm.

Keywords: Encryption, Decryption, RSA, RC4.

1. GİRİŞ

Güvenliği sağlamak amacıyla askeri ve diplomatik iletişimde uzun yıllardır kullanılan şifreleme yöntemine günümüzde de ihtiyaç duyulmaktadır. Açık bir haberleşme kanalı üzerinden iletişim sağlandığında bilginin yetkisiz bir kişi tarafından dinlenebileceği, veriyi bozabileceği veya değiştirebileceği riski önemli bir sorundur. Herhangi iki nokta arasındaki iletişimde veya sistemler arasındaki bağlantılarda verinin güvenli bir şekilde gönderilmesi büyük önem taşıdığından veri şifrelenerek açık haberleşme kanalları aracılığıyla ulaştırılır (Yerlikaya, Buluş ve Buluş, 2006a). Şifreleme, hassas bilgilerin güvenliğini garanti altına almanın başlıca araçlarından biridir.

Yunan kökenli krypto's (gizli) ve lo'gos (kelime) sözcüklerinin bir araya gelmesi ile oluşan ve iletişimde gizlilik bilimi olarak ifade edilen Kriptoloji, kriptografi (şifreleme) ve kriptoanaliz (şifre çözme) olmak üzere ikiye ayrılır (Singh ve Supriya, 2013).

Şifreleme algoritması, düz metin üzerinde çeşitli yer değiştirmeler ve dönüşümler gerçekleştirir. Günümüzde kullanılan şifreleme algoritmaları, açık anahtarlı (asimetrik) ve gizli anahtarlı (simetrik) olarak sınıflandırılır.

Asimetrik şifreleme sistemleri üzerine ilk çalışma, Diffie ve Hellman tarafından 1976 yılında yapılmıştır. Daha sonra Rivest, Shamir ve Adleman RSA şifreleme yöntemini bulmuşlardır. RSA sisteminin güvenliği, büyük sayılarla yapılan matematiksel işlemlerin zorluğuna dayanmaktadır (Çakar ve Varol, 2007). RSA veri güvenliğini sağlamak için 1987 yılında Rivest tarafından simetrik bir şifreleme algoritması olan RC4 geliştirilmiştir (Singha ve Raina, 2011).

Nidhi Singhal ve S. Raina 2011 yılında yaptıkları bir çalışmada AES ve RC4 algoritmalarını karşılaştırmışlar ve deneyler sonucunda RC4'ün şifreleme ve şifre çözme için AES'den daha hızlı ve enerji açısından verimli olduğunu belirlemişlerdir (Singha ve Raina, 2011).

RSA algoritması kullanılarak ses verisi şifreleme ve şifre çözme işlemleri için uygulama geliştirilmiştir. Tushar Kanti Saha ve arkadaşları 2012 yılında yaptıkları bir çalışmada beş yüz Bangla konuşma dilini altı farklı hoparlörden kaydederek ve RIFF (.wav) dosya formatı olarak saklamışlardır. Ardından, geliştirdikleri program ile bu kelimelerin verilerini tamsayı veriler olarak çıkararak bir metin dosyasında saklamışlardır. Son olarak, geliştirdikleri program ile konuşma verilerini şifrelemişlerdir (Rahman, Saha ve Bhuiyan, 2012).

2013 yılında Shikha Kuchhal ve Ishank Kuchhal, veri güvenliğini sağlamak için Matlab araç kutusunda bulunan çeşitli araçlar yardımıyla RSA algoritmasını kullanarak metni şifrelemek ve şifre çözmek için bir program geliştirmişlerdir (Kuchhal ve Kuchhal, 2013).

Şifreleme ve şifre çözmeyi "Bir mesajın ağ ortamındaki davetsiz misafirlerden gelen anlamlarını gizlemenin en iyi yollarından biridir." olarak ifade eden Nentawe Goshwe, 2013 yılında yaptığı bir çalışmada, belirli bir ileti bloğu boyutuna sahip RSA algoritması kullanan bir ağ ortamında veri şifreleme ve şifre çözme için tasarlanmış bir yazılım geliştirmiştir. Bu yazılım ile veriler güvenli olmayan bir ağ ortamı vasıtasıyla bir bilgisayar terminalinden diğerine aktarılabilir (Goshwe, 2013).

Prerna Mahajan ve Abhishek Sachdeva 2013 yılında yaptıkları bir çalışmada AES, DES ve RSA şifreleme tekniklerinin performansını araştırmışlardır. Kullanılan metin dosyalarına ve deney sonuçlarına göre, AES algoritmasının en kısa süre şifreleme yaptığı ve RSA'nın en uzun şifreleme süresini tükettiği, AES algoritmasının DES ve RSA algoritmalarından çok daha iyi olduğu belirlemişlerdir (Mahaja ve Sachdeva, 2013).

Saranya ve arkadaşları yaptıkları bir çalışmada RSA algoritmasında üssün değerini analiz etmişlerdir. Üssün değeri yükseldikçe RSA algoritmasının güvenliğinin de yüksek olduğundan dolayı daha iyi bir güvenlik sağlamak için üstel değerin RSA algoritmasında uygulanmasını önermişlerdir (Saranya, Vinothini ve Vasumathi, 2014).

Kunal Gagneja ve John Singh 2015 yılında RSA algoritması üzerindeki güvenlik konularını araştırmışlar, RSA'nın matematiksel mimarisini temel alarak problemleri belirlemişlerdir. RSA algoritmasının, xor'un başlatılması ve karıştırılmasından ötürü AES, DES gibi diğer algoritmaların güvenlik avantajlarına sahip olduğunu ifade etmişler ve RSA yavaş çalışan bir algoritma olduğu için kaba kuvvet saldırısı yapmanın daha fazla zaman alacağını belirtmişlerdir (Gagneja ve Singh, 2015).

2017 yılında Tarık Yerlikaya ve Hakan Gençoğlu yaptıkları çalışmada, RSA algoritmasının mobil cihazlardaki performansını test etmişlerdir. RSA algoritması mobil cihazların sınırları dikkate alınarak optimize edilmiş ve algoritmanın hızlı çalışması sağlanmıştır (Yerlikaya ve Gençoğlu, 2017).

Ayşe Beşkirli ve arkadaşları tarafından 2019 yılında yapılan bir çalışmada, RSA algoritmasının şifrelemedeki etkisi incelenmiştir. Algoritmanın diğer algoritmalar ile bir arada kullanılması sonucu oluşacak yeni algoritmanın daha hızlı ve güvenilir olacağı ifade edilmiştir (Beşkirli, Özdemir ve Beşkirli, 2019).

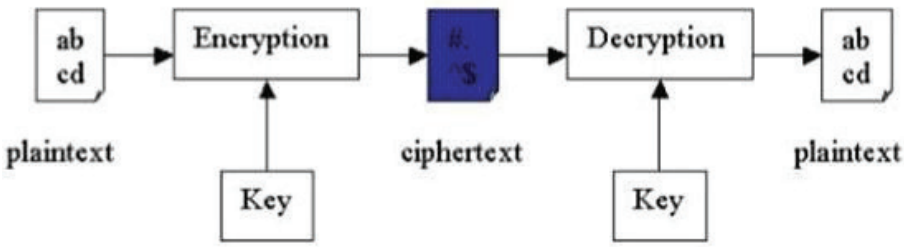
2020 yılında yapılan bir çalışmada, tıbbi verilerin büyük tekrarının ve yüksek hassasiyetinin özelliklerini hedefleyerek, Huffman sıkıştırması ve RC4'e dayalı güvenli bir veri depolama algoritması sunulmuştur. Geliştirilen algoritmanın sadece RC4 şifreleme verimliliğini korumakla kalmadığı, aynı zamanda şifreli metin verilerinin miktarını azalttığı ve anahtar akışının rastlantısallığını, gizliliğini ve güvenliğini de geliştirdiği belirtilmiştir (Zhang, Liu ve Ni, 2020).

Riguang Lin ve Sheng Li 2021 yılındaki çalışmalarında, RSA algoritmasına dayalı yeni bir görüntü şifreleme şeması önermişlerdir. Deneysel sonuçlar, araştırmada önerilen görüntü şifreleme şemasının etkili olduğunu ve güçlü anti-saldırı ve anahtar duyarlılığına sahip olduğunu kanıtlamıştır (Lin ve Li, 2021).

Bu çalışmada şifreleme yöntemlerinden bahsedilmiş, simetrik şifreleme yöntemi olan RC4 algoritması ile asimetrik şifreleme yöntemi olan RSA algoritmasının performansları karşılaştırılmıştır.

2. SİMETRİK ŞİFRELEME ALGORİTMALARI

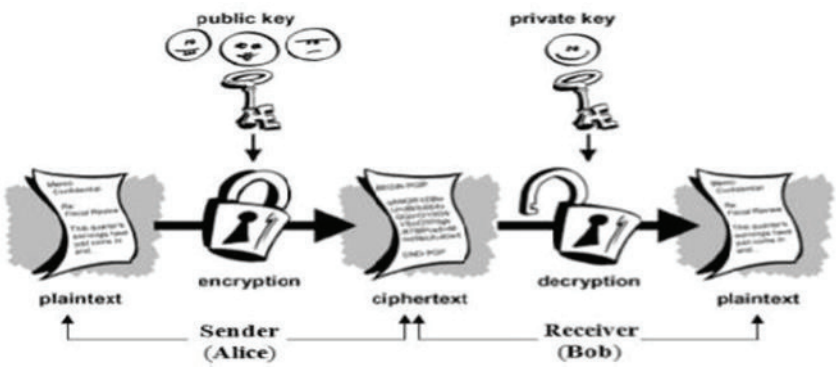
Şifreleme ve şifre çözme için tek bir gizli anahtar kullanılan simetrik şifreleme algoritmalarında, Şekil 1'de görüldüğü gibi şifrelenen metinle birlikte gizli anahtar da alıcıya gönderilir. Şifreleme ve çözme işlemlerinde çok hızlı olduklarından dolayı günümüzde yaygın olarak kullanılan simetrik şifreleme algoritmalarının güvenli anahtar dağıtımı zorluğu bulunmaktadır (Yerlikaya, Buluş ve Buluş, 2006a). DES, 3DES, AES, RC4, Blowfish yaygın olarak kullanılan simetrik şifreleme algoritmalarıdır.



Şekil 1: Simetrik Şifreleme (Preetha ve Nithya, 2013)

3. ASİMETRİK ŞİFRELEME ALGORİTMALARI

Açık anahtarlı şifreleme/deşifreleme algoritmaları, şifreleme için bir anahtar, deşifreleme için ise bu anahtarla ilişkisi olan başka ikinci bir anahtar kullanarak güvenliği sağlar. Gizli anahtarların dağıtılması açık anahtarlı şifrelemenin amaçlarından biridir. Kullanılan algoritma ve anahtar uzunluğu işlemlerin hızını belirler. Yavaş çalışmalarına rağmen, anahtar dağıtım kolaylığı, kriptoalaniz direnci gibi avantajlarından dolayı açık anahtar tabanlı algoritmalar tercih edilmektedir (Çakar ve Varol, 2007). Diffie-Hellman, RSA, DSA, El Gamal asimetrik şifreleme algoritmalarındandır. Şekil 2'de asimetrik şifreleme işlemi yer almaktadır.



Şekil 2: Asimetrik Şifreleme (Rahman, Saha ve Bhuiyan, 2012)

4. MATERYAL VE METOD

4.1 RSA Algoritması

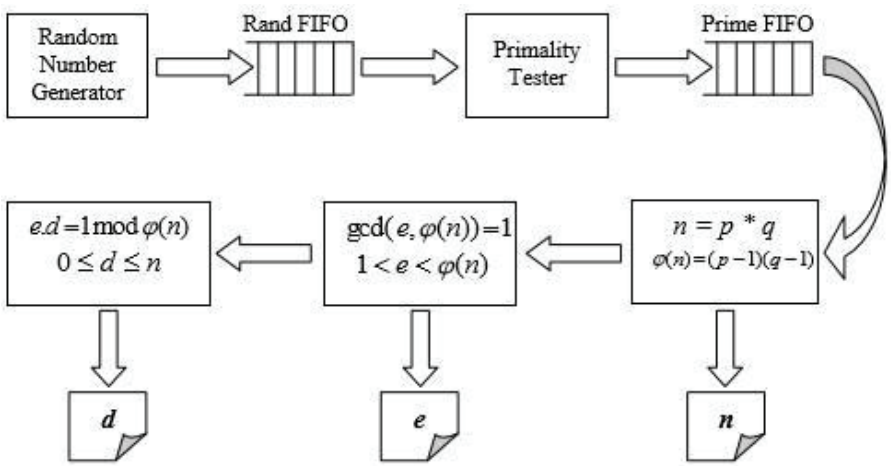
Ron Rives, Adi Shamir ve Leonard Aldeman tarafından 1976 yılında geliştirilen RSA algoritması açık anahtarlı şifreleme yöntemlerinden biridir. Şifreleme yöntemi adını bu üç kişinin soy isimlerinin baş harflerinden almaktadır (Yerlikaya ve diğerleri, 2011).

Simetrik şifrelemede kullanılan tek anahtar yönteminin yerine, açık (public key) ve gizli (private key) olarak iki anahtar kullanılır. Bir kişinin karşı tarafa şifreli mesaj iletebilmesi için o tarafın açık anahtarına ihtiyacı varken, mesajı alan tarafın da mesajı okuyabilmesi için gizli bir anahtara ihtiyacı vardır.

RSA algoritması, gizlilik ve dijital imza sağlamak amacıyla kullanılabilir. Özellikle kullanıcısı fazla olan sistemlerde verinin güvenli olarak paylaşılmasına ve sayısal imza ile kimlik doğrulamasına imkân sağlamaktadır. Kullanılacak anahtarın sayısal büyüklüğü, sistemin güvenilirliğinin ve hızının yüksek olması için önemlidir. Güvenilirlik derecesi, şifrelemede kullanılan asal sayıların büyüklüğü ile orantılıdır. RSA şifreleme sistemin ortaya çıkmasıyla, günümüzde asimetrik şifreleme algoritmaları daha yaygın olarak kullanılmaya başlamıştır (Yerlikaya ve diğerleri, 2006b).

RSA algoritması anahtar üretimi, şifreleme ve şifre çözme olmak üzere üç adımdan oluşur. Anahtar üretim adımları Şekil 3'te yer almaktadır.

- P ve Q gibi rastgele iki büyük asal sayı seçilir.
- Seçilen iki asal sayının çarpımı hesaplanarak N değerinde tutulur. (N = P.Q)
- Totient fonksiyonu hesaplanır. Totient değeri seçilen iki asal sayının bir eksiklerinin çarpımıdır. φ(n) = (p-1)(q-1).
- Totient fonksiyonu değeri (φ(n)) ile aralarında asal olan ve 1<e<φ(n) şartını sağlayan rastgele bir e sayısı seçilir.
- e*d ≡ 1 mod (φ(n)) ve 1<d<φ(n) koşulunu sağlayan bir d sayısı hesaplanır. Genel anahtar (n,e); özel anahtar d elde edilmiş olur (Bodur, Kara ve Zavrak, 2015).



Şekil 3: RSA Anahtar Üretimi İçin Sistem Mimarisi (Rahman, Saha ve Bhuiyan, 2012)

Genel ve özel anahtarlar elde edildikten sonra mesaj genel anahtar ile şifrelenerek karşı tarafa gönderilir. Şifrelenecek verinin sayısal karşılığının e'ninci kuvveti alınarak mod n deki karşılığı bulunur ve şifreli metin elde edilir (Mert ve Şeker, 2014).

$c = m^e \bmod n$ (1)

Genel anahtarla şifrelenen bir metin özel anahtar ile açılabildiğinden dolayı yine aynı şekilde, şifreli metnin sayısal karşılığının d'ninci kuvveti alınarak mod n deki karşılığı bulunur ve orijinal metin elde edilir (Mert ve Şeker, 2014).

$m = c^d \bmod n$ (2)

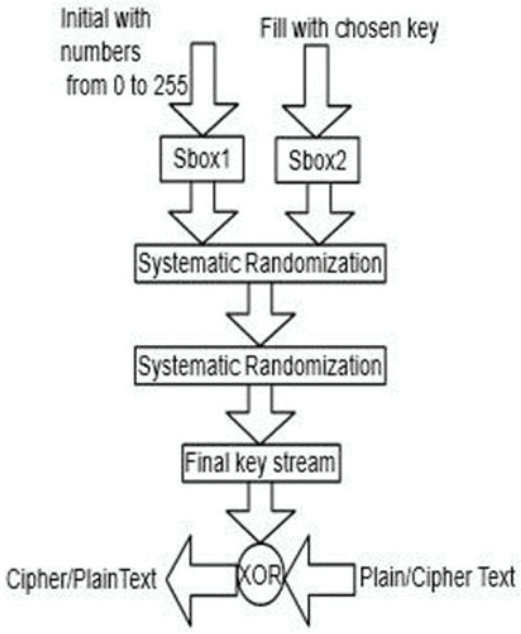
4.2 RC4 Algoritması

Popüler bir akış şifresi olan ve "Rivest Cipher 4" olarak anılan RC4, 1987'de Ron Rivest tarafından tasarlanmıştır (Guo, Feng ve Fu, 2021). Aynı algoritma hem şifreleme hem de şifre çözme için kullanılır, çünkü veri akışı üretilen anahtar diziyle sadece XOR işlemi yapılır. Anahtar akışı, kullanılan düz metinden tamamen bağımsızdır. 256 bit bir durum tablosu başlatmak için 1 - 256 bit arasında değişen uzunlukta bir anahtar kullanır. Durum tablosu daha sonra sözde rastgele bitlerin üretilmesi ve daha sonra şifreli metin elde etmek üzere düz metinle XOR yapılan bir sahte rastgele akış üretmek için kullanılır. Bu algoritma, rastgele bir permütasyonun kullanımına dayanır (Mousa ve Hamad, 2006).

RC4 algoritması başlatma ve işlem olmak üzere iki aşamadan oluşur. Başlangıç aşamasında 256 bitlik durum tablosu S, bir tohum olarak K tuşunu kullanarak doldurulur. Durum tablosu kurulduktan sonra, veri şifrelendiği için düzenli bir şekilde değiştirilmeye devam eder (Rahman, Saha ve Bhuiyan, 2012).

RC4 şifreleme algoritması için adımlar Şekil 4'teki gibidir.

1. Şifrelenecek veriler ve seçilen anahtar alınır.
2. İki adet string dizi oluşturulur.
3. 0'dan 255'e kadar sayı içeren bir dizi başlatılır.
4. Seçilen anahtar ile diğer dizi doldurulur.
5. Anahtar dizisine bağlı olarak ilk dizi rastgele oluşturulur.
6. Son anahtar akışını oluşturmak için kendi içindeki ilk dizi rastgele oluşturulur.
7. Şifreli metni elde etmek için XOR son anahtar akışı veri ile şifrelenir (Rahman, Saha ve Bhuiyan, 2012).

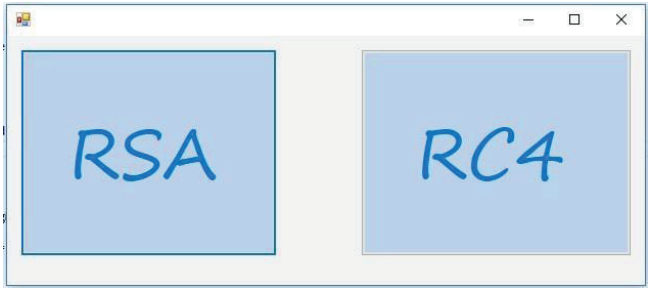


Şekil 4: RC4 Şifreleme Algoritması (Rahman, Saha ve Bhuiyan, 2012)

Değişken anahtar uzunluğuna sahip olan RC4 algoritması basit, hızlı ve açıklaması kolaydır. Hem yazılım hem de donanımda verimli bir şekilde uygulanabilir. SSL protokolünü kullanarak güvenli web sitelerine giden ve güvenli web sitelerinden gelen trafik şifrelemesinde olduğu gibi güvenli iletişim için de kullanılır (Bodur, Kara ve Zavrak, 2015).

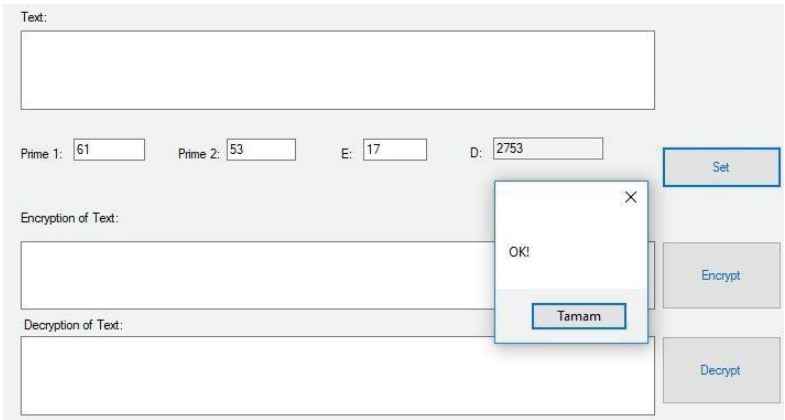
5. ARAŞTIRMA BULGULARI

Bu çalışmada RSA ve RC4 şifreleme algoritmalarının metin dosyalarını şifreleme ve şifre çözme sürelerini karşılaştırmak için Visual Studio C# ortamında bir uygulama geliştirilmiştir. Uygulama ilk açıldığında Şekil 5 'te görüldüğü gibi kullanıcıya hangi algoritmaları kullanacağına dair iki bölüm sunar. Birinci bölüm RSA algoritması ile ikinci bölüm ise RC4 algoritması ile şifreleme ve deşifreleme işlemlerini gerçekleştirmektedir.



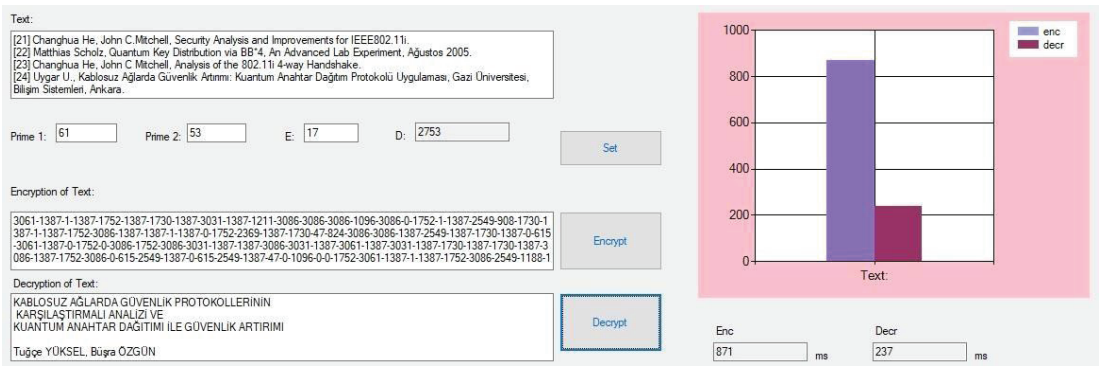
Şekil 5: RSA - RC4 Uygulaması İlk Ekran

RSA ekranı açıldığında iki büyük asal sayı değeri girip, RSA algoritması anahtar üretim aşamasında belirtilen şartı sağlayan bir e değeri veriyoruz. Şekil 6'da görüldüğü gibi "Set" butonuna tıkladığımızda program hem d değerini (gizli anahtar) buluyor hem de girdiğimiz sayıların asal sayı olup olmadığını kontrol ediyor.



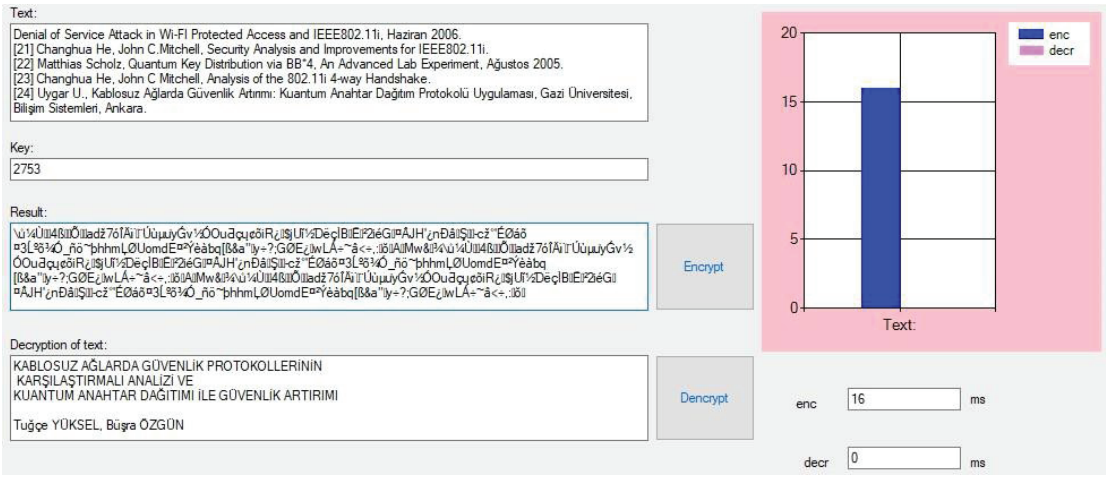
Şekil 6: RSA Anahtar Üretim Aşaması

Genel ve özel anahtarları belirledikten sonra Şekil 7'de görüldüğü gibi şifrelenecek olan metin "Text" alanına girilir. "Encryption" butonuna basıldığında şifreli metin, "Decryption" butonu ile de şifreli metin çözülerek orijinal metin elde edilir ve şifreleme/deşifreleme için geçen süre ekranda gösterilir.



Şekil 7: RSA Şifreleme ve Şifre Çözme Aşaması

RC4 ekranında şifrelenecek metin "Text" alanına girilir ve bir anahtar belirlenir. "Encryption" seçeneği ile şifreli metin elde edilir. Şifreli metni orijinal halini görmek için "Decryption" seçeneği seçilir. Şekil 8'de RC4 ile şifreleme ve deşifreleme işlemi yer almaktadır.



Şekil 8: RC4 Şifreleme ve Şifre Çözme İşlemi

Bu çalışmanın amacı RSA ve RC4 algoritmalarının performanslarını karşılaştırmak olduğu için her iki algoritma için farklı boyutlarda metin verileri girilerek deneyler artırılmıştır. Sonuçlar Tablo 1 ve Tablo 2' de yer almaktadır.

Tablo 1. RSA ve RC4 Şifreleme Süreleri

Dosya Boyutu	RSA(ms)	RC4(ms)
10 KB	3.5	2.1
100 KB	17.4	14.6
500 KB	51.6	46.8
1 MB	101.2	95.2
10 MB	1084.0	964.4
100 MB	10255.4	9022.4
500 MB	48616.2	45206.0
1 GB	92356.2	88314.2

Tablo 2. RSA ve RC4 Deşifreleme Süreleri

Dosya Boyutu	RSA(ms)	RC4(ms)
10 KB	2.9	1.5
100 KB	16.5	14.9
500 KB	52.8	51.2
1 MB	104.3	97.3
10 MB	996.0	892.6
100 MB	9892.5	8214.1
500 MB	44763.0	43402.0
1 GB	90124.2	82674.0

6. SONUÇ

Bilgisayarların yaygın olarak kullanılması ve bilgisayar ağlarının gelişmesi, bilgiye erişim kolaylaştırırken, güvenlik sorunları ortaya çıkarmıştır. Bilginin korunması ve güvenli bir şekilde iletilmesi büyük önem taşımaktadır.

Şifreleme işlemi, verileri belli bir algoritmaya göre yer değiştirme yaparak veya matematiksel işlemleri kullanarak karmaşık hale getirir. Kullanılan yöntemler incelendiğinde bu işlemler için geliştirilmiş çeşitli şifreleme algoritmaları bulunmaktadır. Simetrik şifreleme algoritmaları tek ve gizli bir anahtarla şifreleme ve deşifreleme işlemlerini geçekleştirirken; asimetrik şifreleme algoritmaları ile gönderen ve alıcı taraflar ortak bir gizli anahtar oluşturup, bu anahtarı kullanarak verilerini şifreleyebilirler.

Bu çalışmada simetrik ve asimetrik şifreleme yöntemleri hakkında genel bilgiler verilmiş, RSA ve RC4 şifreleme algoritmalarının şifreleme ve şifre çözme performanslarını karşılaştırılmıştır. Bir uygulama geliştirilerek farklı boyutlardaki metin verileri ile deneyler yapılmış, sonuçlar tablo halinde gösterilmiştir. Elde edilen sonuçlar, RC4 şifreleme yönteminin RSA 'ya göre daha hızlı olduğunu göstermektedir.

7. KAYNAKLAR

Beşkirli, A., D. Özdemir ve M. Beşkirli. 2019. Şifreleme Yöntemleri ve RSA Algoritması Üzerine Bir İnceleme. Avrupa Bilim ve Teknoloji Dergisi Özel Sayı, S. 284-291.

Bodur, H., R. Kara ve S. Zavrak. 2015. RSA Şifreleme Algoritmasını Kullanarak SMS İle Güvenli Şifreleme Yöntemi. XVII. Akademik Bilişim Konferansı (AB 2015), Anadolu Üniversitesi, Eskişehir.

Çakar, H. ve A. Varol. 2007. Bilgi Güvenliği ve RSA Şifreleme Algoritmasının İncelenmesi. Ulusal Teknik Eğitim, Mühendislik ve Eğitim Bilimleri Genç Araştırmacılar Sempozyumu, Kocaeli Üniversitesi Bildiriler Kitabı, S.1411-1412.

Gagneja, K. ve K.J. Singh. 2015. A Survey and Analysis of Security Issues on RSA Algorithm. Research Journal of Applied Sciences, Engineering and Technology, 11(8), 847-853.

Goshwe, N.Y. 2013. Data Encryption and Decryption Using RSA Algorithm in a Network Environment. International Journal of Computer Science and Network Security, 13(7), 9-13.

Guo, T., Y. Feng ve Y. Fu. 2021. A New Form of Initialization Vectors in the FMS Attack of RC4 in WEP. Proceedings of the 10th International Conference of Information and Communication Technology, vol. 183, 456-461.

Kuchhal, S. ve I. Kuchhal. 2013. Data Security Using RSA Algorithm In Matlab. International Journal of Innovative Research & Development, 2(7), 479-483.

Lin, R. ve S. Li. 2021. An Image Encryption Scheme Based on Lorenz Hyperchaotic System and RSA Algorithm. Security and Communication Networks, vol. 2021, doi:10.1155/2021/5586959

Mahaja, P. ve A. Sachdeva. 2013. A Study of Encryption Algorithms AES, DES and RSA for Security. Global Journal of Computer Science and Technology Network, Web & Security, 13(15),14-22.

Mert, C. ve Ş. Şeker. 2014. RSA Şifreleme Sistemine Karşı Yeni Bir Çarpanlara Ayırma Saldırısı. Erzincan Üniversitesi Fen Bilimleri Enstitüsü Dergisi. 7(1), 108.

Mousa, A. ve A. Hamad. 2006. Evaluation of the RC4 Algorithm for Data Encryption. International Journal of Computer Science & Applications, 3(2), 49-50.

Preetha, M. ve M. Nithya. 2013. A Study and Performance Analysis of RSA Algorithm. International Journal of Computer Science and Mobile Computing, ISSN:2148-2683. 2(6), 128.

Rahman, M., T.K. Saha ve A. Bhuiyan. 2012. Implementation of RSA Algorithm for Speech Data Encryption and Decryption. International Journal of Computer Science and Network Security, 12(3), 74-82.

Saranya, Vinothini ve Vasumathi. 2014. A Study on RSA Algorithm for Cryptography. International Journal of Computer Science and Information Technologies, 5 (4), 5708-5709.

Singh, G. ve K. Supriya. 2013. A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. International Journal of Computer Applications, 67(19), 33.

Singhal, N. ve J.P.S. Raina. 2011. Comparative Analysis of AES and RC4 Algorithms for Better Utilization. International Journal of Computer Trends and Technology, ISSN: 2231-280. S. 177.

Yerlikaya, T., E. Buluş ve N. Buluş. 2006. Asimetrik Şifreleme Algoritmalarında Anahtar Değişim Sistemleri. 8. Akademik Bilişim Konferansları, Pamukkale Üniversitesi, Denizli.

Yerlikaya, T., E. Buluş ve N. Buluş. 2006. Kripto Algoritmalarının Gelişimi ve Önemi. 8. Akademik Bilişim Konferansları, Pamukkale Üniversitesi, Denizli.

Yerlikaya, T. ve H. Gençoğlu. 2017. Mobil Cihazlarda RSA Algoritmasının Performans Optimizasyonu. Trakya University Journal of Engineering Sciences, ISSN 2147–0308. 18(1), 43-52.

Yerlikaya, T., H. Gençoğlu, M. Emir, M. Çankaya ve E. Buluş. 2011. RSA Şifreleme Algoritması ve Aritmetik Modül Uygulaması. İstanbul Aydın Üniversitesi Dergisi, 3 (9) , 95- 104.

Zhang, J., H. Liu ve L. Ni. 2020. A Secure Energy-Saving Communication and Encrypted Storage Model Based on RC4 for EHR. IEEE Access, vol. 8, 38995-39012, doi: 10.1109/ACCESS.2020.2975208