RSA ŞİFRELEME ALGORİTMASI VE ARİTMETİK MODÜL UYGULAMASI

Tarık YERLİKAYA[1]
Hakan GENÇOĞLU[2]
Mustafa Kadir EMİR[3]
Mustafa ÇANKAYA[4]
Ercan BULUŞ[5]

Özet

Sistemler arası bağlantılarda ya da herhangi iki nokta arasındaki haberleşmede verinin güvenli bir şekilde gittiğinden emin olmak gerekmektedir. Bunun sağlanması ise gönderilen verinin şifrelenmesi ile olur. Şifreleme, günümüzde dijital ortamda bir gereklilik haline gelmiştir. Bu çalışmada temel kriptografi terimlerinden bahsedilmiştir. Yaygın olarak kullanılan yöntemler incelenmiş ve çalışmanın amacına uygun olarak RSA şifreleme yöntemi seçilmiştir. Bir genel anahtarlı şifreleme tekniği olan RSA, çok büyük tamsayıları oluşturma ve bu sayıları işleminin zorluğu üzerine yapılandırılmıştır. Bu çalışmada, büyük sayılar ile çok uzun süren işlemler çeşitli metotlar kullanılarak kısa sürede sonuçlandırılmıştır. Anahtar oluşturma işlemi için büyük asal sayılar kullanılarak daha güvenli bir yapı oluşturularak çalışmaya yansıtılmıştır.

Anahtar Kelimeler: *Kriptografi, RSA,Uzatılmış Öklid Teoremi, Modüler Üs Alma*

[1] Trakya Üniversitesi, Bilgisayar Mühendisliği Bölümü, Edirne
[2] İstanbul Aydın Üniversitesi, Anadolu Bil Meslek Yüksek Okulu, İstanbul
[3] Trakya Üniversitesi, Bilgisayar Mühendisliği Bölümü, Edirne
[4] Trakya Üniversitesi, Bilgisayar Mühendisliği Bölümü, Edirne
[5] Namık Kemal Üniversitesi, Bilgisayar Mühendisliği, Tekirdağ

1.GİRİŞ

Günümüzde, teknolojinin gelişmesiyle birlikte bilgisayar ve internet hayatımızda büyük yer sahibi olmaya başlamıştır. Daha çok insanın online olduğundan beri internet üzerinden işlemler yapmak kaçınılmaz bir hal almıştır. Bunun yanı sıra banka işlemleri, ticari ilişkiler, devlet işlerinde, askeri işlerde, özel görüşmeler ve benzeri önemli işlevlerin sorunsuz yapılması için güvenlik ön planda tutulması gerekmektedir.

Güvenliği sağlamanın yolu da şifreleme ve kimlik denetiminden geçmektedir. Sistemler arası bağlantılarda ya da herhangi iki nokta arasındaki haberleşmede verinin güvenli bir şekilde gittiğinden emin olmak gerekir. Bunun sağlanması ise gönderilen verinin şifrelenmesi ile olur. Böylece açık haberleşme kanalları kullanılarak verinin güvenli bir şekilde ulaştırılması sağlanır. İletişimde, açık bir haberleşme kanalı kullanılıyorsa gizli tutulmak istenen bilginin yetkisiz bir kişi tarafından dinlenebileceği veya haberleşme kanalına girip (araya girme) veriyi bozabileceği ya da değiştirebileceği (yanlış verinin gönderilmesi) düşüncesi her zaman için önemli bir problem oluşturur.

Kriptoloji esas olarak iki bölüme ayrılır, kriptografi (şifreleme) ve kriptanaliz (şifre çözme). Gönderilmek istenen orijinal mesaj açık mesaj (plain text) ve bu mesajın şifrelenmiş hali şifreli mesaj (cipher text-cryptograph) olarak adlandırılır. Şifreleme, askeri ve diplomatik iletişimde güvenliği sağlamak için bin yıldır kullanılmaktadır. Ancak bugün artık özel sektörde de gereksinim duyulmaktadır. Sağlık hizmetleri, finansal işler gibi konularda bilgisayarlar arasındaki haberleşmede açık kanallar kullanılarak yapılmaktadır. Bu açık kanalların kullanılması sırasında yukarıda sayılan işlerin güvenli ve gizli bir şekilde yapılabilmesi için şifrelemeye gerek duyulmaktadır.

Şifreleme, günümüzde dijital ortamda bir gereklilik haline gelmiştir. Bu çalışmada temel kriptografi terimlerinden bahsedilmiş, yaygın olarak kullanılan yöntemler incelenmiş ve çalışmanın amacına uygun olarak RSA şifreleme yöntemi seçilmiştir. RSA, dijital ortamda verilerin güvenli bir şekilde saklanması ve transfer edilmesi amacıyla Rivest, Shamir ve Adleman tarafından yaratılmış bir şifreleme yöntemidir.

2. RSA ŞİFRELEME ALGORİTMASI

İlk defa 1977 yılında Ron Rivest, Adi Shamir ve Leonard Adleman tarafından oluşturulan RSA algoritması geliştiricilerinin soy isimlerinin ilk harfleriyle anılmaktadır.

Bir genel anahtarlı şifreleme tekniği olan RSA, çok büyük tamsayıları oluşturma ve bu sayıları işleminin zorluğu üzerine düşünülmüştür. Anahtar oluşturma işlemi için asal sayılar kullanılarak daha güvenli bir yapı oluşturulmuştur. Anahtar oluşturma algoritması şu şekildedir:

• P ve Q gibi çok büyük iki asal sayı seçilir.

• Bu iki asal sayının çarpımı N = P.Q ve bu bir eksiklerinin φ(N)=(P-1)(Q-1) hesaplanır.

• 1'den büyük φ(N)'den küçük φ(N) ile aralarında asal bir E tamsayısı seçilir.

• Seçilen E tamsayısının mod φ(N)'de tersi alınır, sonuç D gibi bir tamsayıdır.

• E ve N tamsayıları genel anahtarı, D ve N tamsayıları ise özel anahtarı oluşturur.

Genel ve özel anahtarları oluşturduktan sonra gönderilmek istenen bilgi genel anahtar ile şifrelenir. Şifreleme işlemi şu şekilde yapılmaktadır:

Şifrelenecek bilginin sayısal karşılığının E'ninci kuvveti alınır ve bunun mod N deki karşılığı şifrelenmiş metni oluşturmaktadır. Genel anahtar ile şifrelenmiş bir metin ancak özel anahtar ile açılabilir. Bu yüzden şifrelenmiş metin, yine aynı yolla, şifrelenmiş metnin sayısal karşılığının D'ninci kuvveti alınır ve bunun mod N deki karşılığı orijinal metni oluşturur.

Bu algoritmada iki asal sayının çarpımını kullanarak anahtar oluşturulmasının sebebi, iki asal sayının çarpımını asal çarpanlarına ayırmak asal olmayan sayıları ayırmaktan daha zorlu olmasıdır.

Formül işleme koyulduğunda en çok zaman alan süreç, üst alma ve mod bulma işlemleridir. Süreci hızlandırmak için E değerinin küçük ya da hesaplanması kolay bir değer seçilebilir. Bu da yukarıda bahsettiğimiz gibi değerin küçüklüğü ve tekrarlı kullanılması güvenliği azaltmaktadır.

Fakat bu durumu engelleyecek metotlar da mevcuttur. Bu çalışmada uzatılmış Öklid algoritması ve modüler üs alma metotları kullanarak, büyük sayılarla kısa sürede işlem yaparak şifrelenme yapılmaktadır.

3. UZATILMIŞ ÖKLİD ALGORİTMASI

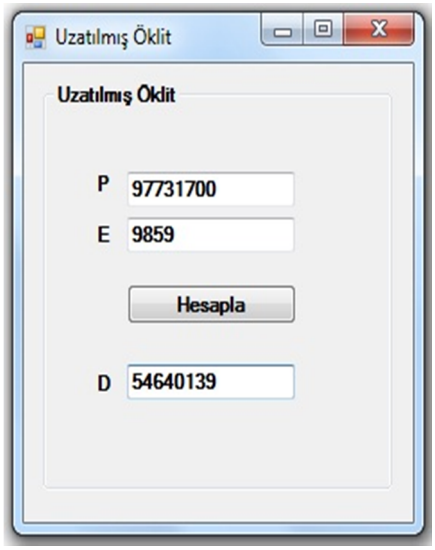
Uygulanan metodun amacı belirli bir tabana göre verilen sayının hızlı yani kısa sürede tersini bulmaktır. Basitçe DE=1 Mod P denklemini bilinen bir E ve P sayısı için çözmektedir.

Başka bir ifadeyle bir sayının bir modda hangi sayıyla çarpılınca 1 sonucunu verdiğini bulmaktır.

Buna göre algoritmada tersi alınacak olan sayı E ve taban değeri olan P biliniyor olacak ancak D sayısı aranacaktır. Bu sayı aşağıdaki şekilde ifade edilmektedir.

E^{-1} =D Mod p
E*D=1 Mod p

Aşağıda C# dilindeki program modülünde mod yani (N= P * Q) değeri P kısmına, açık anahtarımız ise E kısmına yazıldığında, program değerleri işleyince D yani gizli anahtar hızlı bir şekilde bulunmuş olmaktadır.



Şekil 1-Uzatılmış Öklid Modülü

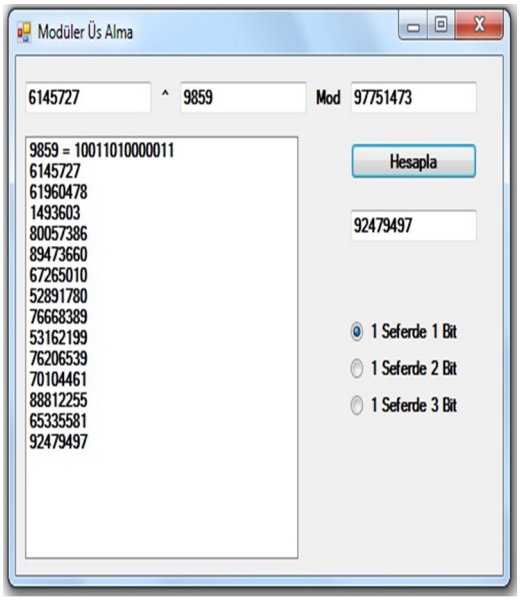
4. MODÜLER ÜS ALMA ALGORİTMALARI

RSA`ya yönelik en çok tartışılan kripto analiz yöntemi, N sayısını kendisini oluşturan iki asal çarpanına ayırmaktır. Günümüzde, verilen N ve E için D değerini hesaplayan algoritmalar üs alma problemi gibi zaman ile de ilgili bir problem yaratmaktadırlar. Bu nedenle çarpanlara ayırma performansını, RSA`nın güvenliği için bir tehdit olarak düşünebiliriz.

Çok büyük asal sayılardan oluşturulmuş çok büyük bir N`i çarpanlarına ayırmak çok zor bir işlem olacaktır; fakat bu zorluk N`in kullanımından daha büyük bir zorluk değildir. Projemizde çeşitli üs alma algoritmaları işlenerek karşılaştırılmıştır. Bu karşılaştırmalar sonucunda en hızlı olan Modüler Üs Alma yöntemi seçilmiştir.

4.1. İkili Üs Alma (Binary Method)

Bu yöntem yaygın olarak kullanılan bir yöntemdir. Üs değeri ikili olarak yazılır. Her bit değerine göre işlem yapılarak sonuca gidilir.



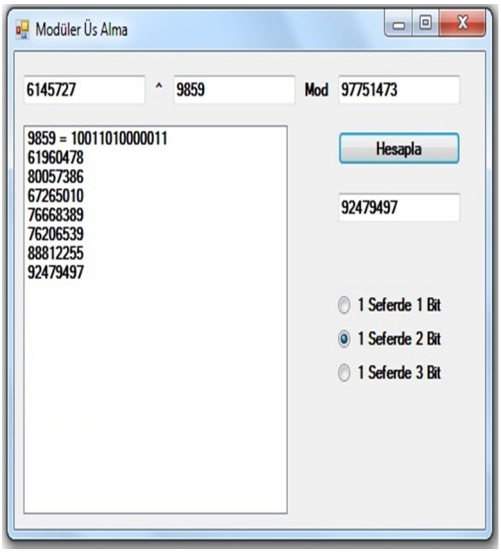
Şekil 2-İkili Üs alma Modeli

Şekil 2 ‘ de ki programda görülmek üzere ikili üs alma methodu kullanılarak, üs alma işlemi gerçekleştirilmektedir. 6145727 ^ 9859 işlemi normalde 6145727 in 9859 kere bir biri ile çarpımından elde edilmektedir. Fakat kullanılan modül sayesinde bu işlem 14 adımda gerçekleştirilir.

4.2.Bir Seferde 2 Bit (Quaternary Method)

Bu metotta E değerinin bitleri gruplara ayrılarak incelenir. Her seferde 2 bit işlenilerek üs alma işlemi tamamlanır.

Şekil 3 te görüldüğü üzere 9859 sayısı 14 bit yapmaktadır. Her seferde 2 bit işleneceği için 14 işlem yerine 7 kez işlem yapılacaktır. İkili biçimde yazılan üs değeri ise 2 li gruplara ayrılarak işleme alınır.

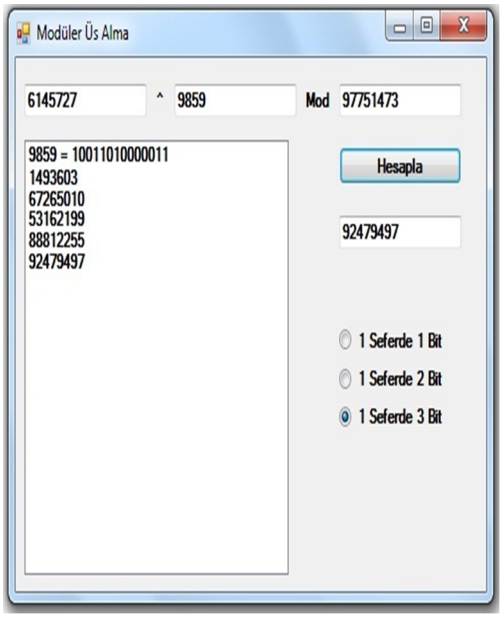


Şekil 3- Bir Seferde 2 Bit Modülü

4.3.Bir Seferde 3 Bit (The Octal Method)

İkili sayı 3'lü bloklara ayrılarak işlem yapılır. Örneğin 9859 üs değeri hesaplanır.

010011010000011 Tam bölünmeme durumundan dolayı sola eklenen 0 değeri sayesinde s=k/r=3 bulunur. M^W (Mod N) değerleri hesaplanır. C=M^F3=M^3 (Mod N) ataması ile algoritma çalıştırılır ve M^9859 değeri hesaplanır.



Şekil 4-Bir Seferde 3 Bit Modülü

5.UYGULAMA

5.1.Verilerin Analizi Ve Metot Seçimi

Belirli bir tabana göre verilen sayının hızlı yani kısa sürede tersini bulmak için uygulamamızda Uzatılmış Öklit Algoritmasını kullanacağımızı bölüm 3 te belirtmiştik.

Bir diğer sorun ise üs alma işleminin büyük asal sayılarla gerçekleştirilmesi sırasında çok zaman kaybının olmasıydı. Yapılan program modülleri ve çalışmalara göre, Bir Seferde 2 Bit ve Bir Seferde 3 Bit metotları İkili Üs Alma metoduna göre daha hızlıdır. Nedeni işlem yapılacak bitlerin gruplandırılarak daha hızlı bir çözüm elde edilecek olmasıdır.

Şekil.2 ve Şekil.3 teki işlem adımları ve zamanlama dikkate alındığında, modüler üs alma metotlarından Bir Seferde 3 Bit metodunun daha hızlı olduğu görülmektedir.

5.2.RSA Şifreleme Uygulaması

Rsa yönteminin güvenliği, daha önce de bahsedildiği gibi gücünü çarpanlara ayırma işleminin zorluğuna dayandırmasıdır. Bu yöntemin formülü ve uygulamamızın en basit çalışma şekli şöyledir;

i. P ve Q olmak üzere iki büyük asal sayı seçilir.

ii. E, 1’ den büyük, PQ değerinden küçük, (P-1)(Q-1) ile aralarında asal olan bir sayı

seçilir.

iii. D, (P-1)(Q-1) ile tam bölünebilecek bir

(DE-1) sayısından D elde edilir.

iv. C=(T^E) Mod PQ şifreleme fonksiyonudur. C şifreli-metin T düz metindir.

v. Şifreyi çözmek için kullanılan fonksiyon
T= (C^D) Mod PQ dur

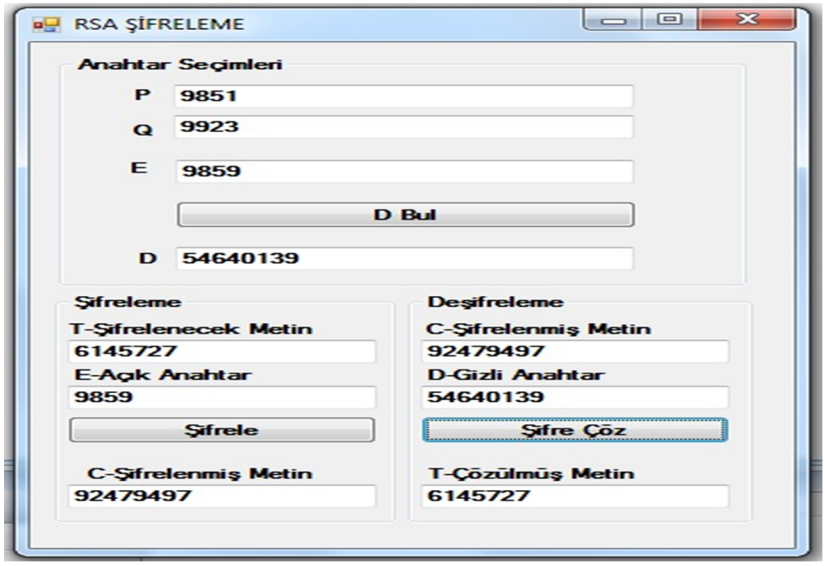
Uygulamadaki örnek bir çözüm Şekil.4 tedir.

6. SONUÇ VE ÖNERİLER

Kullanılan Uzatılmış Öklit Algoritması ve Modüler Üs Alma Metotları ile, RSA Şifreleme Algoritmasından daha fazla verim alınarak, güvenliği arttırılmış, Üs alma işleminin hesap süresi azaltılmıştır.

Uygulamamızda, 3 adet Üs Alma Metodu karşılaştırılarak RSA'ya uyumlu en iyi sonucu veren Bir Seferde 3 Bit işlem yapan Modüler Üs Alma Metodu kullanılmıştır.

Sonuç olarak genel anahtarlı şifreleme algoritmalarında, sistemin güvenliği anahtar uzunluğuna bağlıdır. Bu algoritmalarda çok büyük asal sayıların kullanılması işlemleri yavaşlatmaktadır. Mod ve üs alma işlemi, çeşitli matematiksel metotlar yardımıyla kısaltılmaya çalışılmıştır. RSA şifreleme algoritmasının güvenliği için 512 bit ve daha büyük anahtarların kullanılması önerilmektedir. Bu metotlar kullanılarak büyük asal sayılarla daha kısa sürede işlemler gerçekleştirilebilir. Böylece şifreleme algoritmaları için önemli olan zaman kaybının azaltılması gerçekleşir.



Şekil 5-RSA Şifreleme Örneği

7. KAYNAKLAR

http://banyan.cm.nctu.edu.tw/cn2008/

D.H. Lehmer, The American Mathematical Monthly, Vol.45, No. 4,227-233 "Euclid's Algorithm for Large Numbers", 1938

Daniel Bleichenbacher, "Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1 ", Volume 1 / 1973

Burton Kalinski, "Some Examples Examples of the PKCS Standards ", RSA Laboratories, 1999

IEEE P1363 "Standard Specifications for Public Key Cryptography", IEEE, November 1993

McDonald. M.G, Harbaugh. A.W , "A Modular Three-Dimensional finite-Difference Ground-Water Flow Model", 1988

"RSA Encryption", Tom Davis, tomrdavis@earthlink.net http: // www. geometer.org /mathcircles October 10, 2003

Bruce SCHNEIDER , "Applied Cryptography,second edition",New York, 1996

Kaliski B, "The Mathematics of the RSA Public-Key Cryptosystem" , RSA Laboratories NY, 2001

Yerlikaya T., Buluş E., Buluş N., "Kripto Algoritmalarının Gelişimi Ve Önemi", Akademik Bilişim Konferansları 2006-Ab2006, Denizli-Türkiye, Şubat-2006.

Stallings W., "Cryptography and Network Security: Principles and Practice", ISBN 0-13-869017-0, Prentice Hall, 1998.