

RSA Şifreleme Algoritmasının

Pollard RHO Yöntemi ile Kriptanalizi

Tarik Yerlikaya, Ercan Buluş, H. Nusret Buluş

Trakya Üniversitesi, Bilgisayar Mühendisliği Bölümü, 22030, Edirne
tarikyer@trakya.edu.tr ercanb@trakya.edu.tr nusretb@trakya.edu.tr

Özet: Bu bildiri de şifreleme algoritmalarını sınıflandırılacak ve asimetrik şifreleme algoritmalarından günümüze kadar yaygın olarak kullanılan RSA şifreleme algoritması incelenecektir. RSA şifreleme algoritmasının performans sonuçları verilerek, bu algoritmanın gücünden bahsedilerek algoritmaya karşı yapılan saldırıların üstünde durulacaktır. Pollard Rho yöntemi kullanılarak RSA şifreleme algoritması üzerine yapılan kriptanaliz çalışması incelenerek, Delphi 7.0 programlama dili ile yazılmış kriptanaliz uygulaması, örnekleri ve sonuçları verilecektir.

Anahtar Kelimeler: Simetrik Şifreleme Algoritmaları, Asimetrik Şifreleme Algoritmaları, RSA, Anahtar Değişimi, Kriptanaliz, Pollard Rho Algoritması, GCD

Cryptanalysis of RSA Cryptographic Algorithm by Pollard RHO Method

Abstract: This paper presents crypto algorithms' basic structures and classifications. Importance of cryptology science is mentioned and symmetric and asymmetric crypto algorithms' basic structure is given. Widely used today RSA crypto algorithm is one of most important asymmetric algorithm. RSA crypto algorithms structure is examined. Attack method performed to this algorithm is studied and Pollard Rho attack method on RSA algorithm is examined in detail

Keywords: Symmetric Encryption Algorithms, Asymmetric Encryption Algorithms, RSA, Key Exchange Algorithms, Cryptanalysis, Pollard Rho Algorithm, GCD

1. Giriş

Şifreleme teknikleri Sezar döneminden başlayarak günümüze kadar çok büyük aşamalar kaydetmiştir. Basit yer değiştirme teknikleriyle başlayan şifreleme teknikleri teknolojinin hızla ilerlemesiyle birlikte bir bilim haline gelmiştir. Bilgisayarların gelişimi ve internet ağının oluşmasıyla birlikte, verilerin bir noktadan diğer bir noktaya gönderilmesi ve bu verilerin üçüncü şahıslardan saklanarak gönderilmesi kriptoloji biliminin gelişimini hızla gerçekleştirmesini sağlamıştır. Günümüze kadar oluşturulan şifreleme algoritmaları kriptoloji büzerine çalışan bilim adamları tarafından iki ana gruba ayrılmıştır. Bunlar, tek anahtar kullanan Simetrik şifreleme algoritmaları ve biri gizli diğeri

açık anahtar olarak kullanılan Asimetrik şifreleme algoritmalarıdır. [1],[2]

Günümüze kadar oluşturulan şifreleme algoritmaları her zaman bir önceki şifreleme algoritmasının dez avantajlarını ortadan kaldırmayı amaçlamıştır. Bu dez avantajlar algoritmanın hızlı çalışmaması yani yeni donanımlarla uyumlamaması veya teknolojinin gelişimiyle birlikte daha hızlı bilgisayarlar sayesinde güvenliğinin azalması yani daha kolay kırılması şeklinde verilebilir.

Bu bildiri de şifreleme algoritmalarını sınıflandırılacak ve asimetrik şifreleme algoritmalarından günümüze kadar yaygın olarak kullanılan RSA şifreleme algoritması incelenecektir. RSA şifreleme algoritmasının gücünden bahsedile-

rek bu algoritmaya karşı yapılan saldırıların üstünde durulacaktır. Pollard Rho yöntemi kullanılarak RSA şifreleme algoritması üzerine yapılan kriptanaliz çalışması incelenerek, Delphi 7.0 programlama dili ile yazılmış kriptanaliz uygulaması ve örnekleri verilecektir.

2. Şifreleme Algoritmaları

Şifreleme algoritmaları iki ana gruba ayrılmaktadır.[3]

1. Simetrik Şifreleme Algoritmaları
2. Asimetrik Şifreleme Algoritmaları

Simetrik şifreleme algoritmaları, şifreleme ve deşifreleme işlemleri için tek anahtar kullanmaktadır. Açık metni şifreledikten sonra şifreli metni alıcıya gönderir. Şifreli metni alan kişi gizli anahtarı bilmeden açık metne ulaşamaz. Bu noktada haberleşen iki kişi anahtar paylaşımı gerçekleştirmek zorundadır. Bu simetrik şifreleme algoritmalarının en büyük dezavantajıdır. Bu dezavantaja karşın simetrik şifreleme algoritmaları yer değiştirme üzerine kurulduğu için çok hızlı şifreleme ve deşifreleme işlemlerini gerçekleştirmekle birlikte kırılması zor algoritmalarıdır.

Asimetrik şifreleme algoritmaları, Simetrik şifreleme algoritmalarının gizli anahtar problemini ortadan kaldıracak sistemler gerçekleştirebilirler. Bu şifreleme algoritmaları, şifreleme ve deşifreleme işlemleri için iki ayrı anahtar kullanmaktadır. Şifreleme işlemini gerçekleştirmek için açık anahtar ve deşifreleme işlemini gerçekleştirmek için gizli bir anahtar kullanmaktadır. Böylece gizli anahtarı paylaşmaya gerek kalmamaktadır. Asimetrik şifreleme algoritmaları çok kullanıcı sistemleri için çok büyük avantajlar sağlamaktadır. Ayrıca asimetrik şifreleme algoritmaları şifreleme ve deşifrelemenin yanı sıra dijital imza ve kimlik denetimi içinde kullanılmaktadır. İnternetin bu kadar yaygın olması asimetrik şifreleme algoritmalarının sağladığı dijital imza sayesinde bu algoritmaların güncel uygulamalarına olanak sağlamaktadır.

Asimetrik şifreleme algoritmalarının en büyük dezavantajı hızlı algoritmalar olmamalarıdır. Kriptoloji bilimi bu dezavantajı ortadan kaldırmak için çalışmalarını sürdürmekte ve yeni algoritmalar geliştirmektedir. [4]

Aşağıdaki şekil de 1000 kullanıcı bir ortamda, simetrik ve asimetrik şifreleme algoritmaları kullanıldığında ortaya çıkan anahtar dağılımı görülmektedir. Simetrik şifreleme algoritmaları kullanıldığında, 1000 kullanıcı bir ortamda 499,500 anahtar gereklidir. Asimetrik şifreleme algoritmaları kullanıldığında, 1000 kullanıcı bir ortamda 1001 anahtar yeterli olacaktır.[4],[5],[12]



Şekil 1. Anahtar dağılım sistemi

3. RSA Şifreleme Algoritması

RSA (RIVEST-SHAMIR-ADLEMAN) asimetrik şifreleme algoritması 1977 yılında R.Rivest, A.Shamir ve L.Adleman tarafından bulunmuş ve daha sonra asimetrik şifreleme algoritmalarına (genel anahtar şifrelemesi) uygun biçimde geliştirilmiştir. Bu algoritma, açık anahtarlı şifreleme sistemlerini ve sayısal imza işlemlerini işlemlerinde güvenli bir şekilde kullanılmaktadır. [1],[2]

RSA şifreleme algoritmasında şifrelenecek olan açık metni öncelikle $[0, n-1]$ arasındaki pozitif tamsayı bloklar haline dönüştürülür. Şekil 2 de ayrıntılı olarak matematiksel işlemler gösterilmektedir.[6],[7]

Bundan sonraki işlem gizli anahtar ve açık anahtar çiftlerini elde etmektir. Bunun için p ve q şeklinde çok büyük iki tane birbirinden farklı asal sayı bulunur.

$$n = p \cdot q \text{ ve } Z = (p-1) \cdot (q-1) \quad (1)$$

hesaplanır. Z ile ortak böleni 1 olacak şekilde bir E sayısı bulunur. Açık anahtar (Public key) $\{E,n\}$ olarak belirlenir.

$$D=E^{-1} \text{ mod } Z \quad (2)$$

olacak şekilde bir D sayısı bulunur. Gizli anahtar (Private key) $\{D,n\}$ olarak belirlenir.

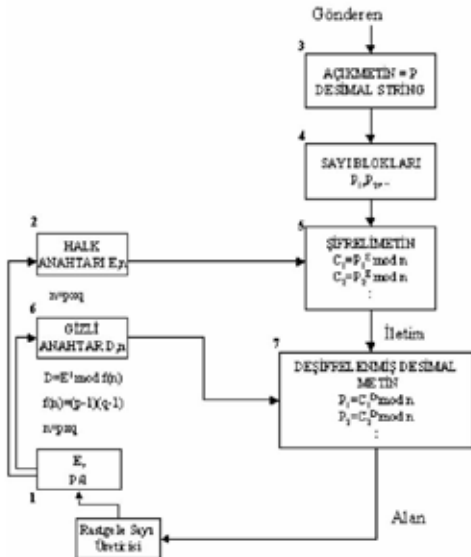
Şifrelenecek mesajı m kabul edersek bu mesaj ikilik olarak $2^k < N$ olacak şekilde k bitlik kısımlara ayrılır.

$$m=m(1)+m(2)+m(3)+\dots+m(n) \quad (3)$$

Daha sonra şifreleme için her bir kısma $C(i)=m(i)^E \text{ mod } N$ işlemi uygulanır. Böylece şifreleme işlemi bitmiş olur. Girişte kullanılan açık metin m şifrelenmiş olarak C şeklinde elde edilir. Belirlenen D gizli anahtarı ile elimizde bulunan şifrelenmiş C metnini çözülmesi gerekmektedir. Bunun içinde şifrelemek için kullanılan bir matematiksel işlem kullanılır. [4],[7],[10]

Gizli anahtar $\{D,n\}$ kullanılarak şifre çözümü:

$$m(i)=C(i)^D \text{ mod } N \quad (4)$$



Şekil 2. RSA Şifreleme Algoritması

4. RSA Algoritmasına Karşı Kriptanaliz Yaklaşımları

Asimetrik şifreleme algoritmaları çözülmesi zor matematik teoremleri üzerin oturtulmuş sistemlerdir. RSA şifreleme algoritması modül aritmetiğini ve çok büyük asal sayıları kullanmaktadır. Bu algoritmanın gücü çok büyük asal sayıların kullanımına bağlıdır.

RSA sisteminin “kırılması” birkaç değişik şekilde yorumlanabilir. Sisteme en çok zarar verecek saldırı bir kriptanalistin belli bir açık anahtara karşı gelen gizli anahtarı bulmasıdır. Bunu başarabilen bir “hasım” hem şifrelenen bütün mesajları okuyabilir hem de imzaları taklit edebilir. Bunu yapmanın en akla gelen yolu n’nin asal çarpanlara ayrılması, yani p ve q’nun hesaplanmasıdır. p, q ve açık üs e kullanılarak d kolaylıkla hesaplanabilir. Ancak buradaki zorluk n modülünün çarpanlarına ayrılmasıdır. RSA sisteminin güvenliği çok büyük sayıların asal çarpanlarına ayrılmasının zorluğu varsayımına dayanır. Büyük sayıların çarpanlarına ayrılmasının zorluğu ispatlanmış değildir. Son üç yüzyıl içerisinde Fermat ve Legendre gibi ünlü matematikçiler bu konuda çalışmalar yapmışlardır.[8],[10]

Bu çalışmada n’i çarpanlara ayırmak için Pollard rho algoritması kullanılacaktır. P ve q ulaşılarak, d gizli anahtar bulunacaktır.

5. Pollard RHO Algoritmasında Kullanılan Teoremler

Bu algoritma için öncelikle modüler aritmeti ve Modül işlemleri tanımlanmalıdır[9]

5.1 Modüler Aritmetik

x ve y birer tam sayı olsun. Eğer $(x-y)$, n’nin bir çarpanı ise x ve y’nin n’ne bölümü ayırdır

$$x = q x'n + rx \quad (5)$$

$$y = q y'n + ry \quad (6)$$

Eğer $rx = ry$

$$q x^n - q y^n + r x - r y = (q x - q y) * n \quad (7)$$

Örnek:

$$x = 37, y = -14 \text{ and } n = 17. \quad (8)$$

$$(x-y) = 37 + 14 = 51 = 3*17 \quad (9)$$

$$x = 2*17 + 3 \text{ and } y = (-1)*17 + 3 \quad (10)$$

5.2 Modül İşlemleri

$$37 + 15 = 3 + 15 = 18 = 1 \pmod{17} \quad (11)$$

$$374 = 34 = (33)*3 = 27 * 3 = 10 * 3 = 30 = 13 \pmod{17} \quad (12)$$

5.3 En Büyük Ortak Bölen

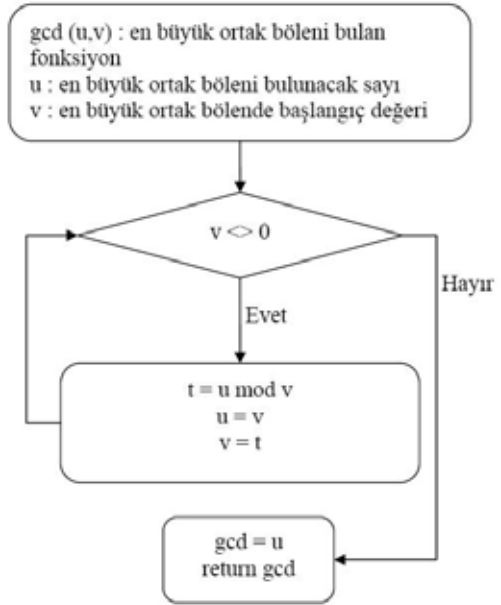
658 ve 154 en büyük ortak böleninin bulunması

$$\begin{aligned} 658 &= 4 * 154 + 42 \\ 154 &= 3 * 42 + 28 \\ 42 &= 1 * 28 + 14 \quad (13) \\ 28 &= 2 * 14 + 0 \end{aligned}$$

6. Pollard RHO Algoritması

Daha öncede söylendiği gibi RSA şifreleme algoritması çok büyük iki asal sayının çarpımı olan n sayısını kullanmaktadır. Bu çalışmada bu n sayısını Pollard Rho yöntemi kullanılarak asal çarpanlarına ayırma işlemi gerçekleştirilecektir. RSA şifreleme algoritmasının yapısından da bilindiği gibi bu asal çarpanlar p ve q değerleri olacak ve bu değerler bulunduğundan sonra d şifreleme anahtarına ulaşılabilecektir.

Örneğin çok büyük bir n sayısı alalım. Bu sayının asal olmadığını biliniyor ve iki asal çarpandan oluştuğunu bilinmektedir. d bu n sayısının bir böleni olsun. d sayısının asal olduğunu, n 'den ufak olduğunu ve kök n den küçük olduğunu biliyoruz.[8],[12]



Şekil 3. En Büyük Ortak Böleni Bulma Algoritması

$$a = b \pmod{n} \quad (14)$$

Bu noktada a ve b hemen hemen aynı sayılara eşit olduğu zaman

$$a = b \pmod{d} \quad (15)$$

denkleminin de doğru olduğunu söylenebilir. $a = b \pmod{d}$ denkleminde yukarıda gösterdiğimiz teoremlerden yola çıkarak $(a-b)$ değeri de d sayısının bir çarpanıdır. d de n 'nin bir çarpanı olduğuna göre $(a-b)$ n 'nin bir çarpanıdır.

Bu algoritmaya göre randam a ve b sayısı alıyoruz. $(a-b)$ ve n sayısının en büyük ortak bölenin 1 den birden büyük değere sahip noktayı bulmaya çalışılır. Bu olmazsa bir c sayısı alınır. $(c-b)$ yada $(c-a)$ sayılarının n ile en büyük ortak bölenini bulmaya çalışılmaktadır.

Görüldüğü gibi bu biraz hantal bir işlem Bundan dolayı Pollard Rho algoritması bunu gidermek için k iterasyonunu ve uygun bir polinom kullanılmaktadır.

Ancak n (asal arpanları olan ok byk sayı) yeterince byk seilirse gnmzn teknolojisıyla n 'nin arpanlarına ayrılması "yeterince" uzun sreceęi iin bu yntemle n 'nin hesaplanması hesaplama aısından verimsiz olacaktır.

Bu alıřmada RSA Őifreleme algoritmasının Pollard Rho yntemi kullanılarak kriptanaliz uygulaması gerekleřtirilmiřtir. Gnmzde hala RSA Őifreleme algoritması gcn korumaktadır. RSA Őifreleme algoritması, byk asal sayı deęerleri kullanılarak, bu kriptanaliz ataklarına karřı konulabilmektedir.

Gnmzde RSA algoritmasının daha gvenli hale getirebilmek iin ok byk asal sayılar kullanılmaktadır. Bu algoritmaların daha gvenli hale getirmek iin byk anahtar deęerleri kullanılmaktadır. Byk anahtar deęerlerini kullanmak birok uygulamada Őifreleme ve deřifreleme srelerini uzatmaktadır. Őifreleme algoritmalarının gcl gvenlięe sahip olmaları yanında yeni donanımlarla gerekleřtirilebilmeleri, kolaylık ve performansı yksek olması gz nnde bulundurulmalıdır Aynı Őekilde yazılım olarak ta kolaylıęı ve Cpu' u fazla meřgul etmemesi gerekmektedir. oęu kuruluř alıřanların verimlilięini arttırmak ve aę zerinde uygun bir iřbirlięi saęlamak iin kablosuz aę sistemini yaygınlařtırıyor. Bu aę sistemlerinin korunması byk bir nem teřkil eder. nk kablosuz aę trafięi kolayca engellenmeye aık olabilir. Kablosuz aęlarda bant geniřlięinin verimli bir Őekilde kullanılması iin uygulanacak Őifreleme algoritması bant geniřlięi ve hız bakımından bu sisteme uyumlu olması gerekmektedir. Bu zellik Asimetrik Őifreleme algoritmalarının en byk dezavantajıdır. Son yıllarda yapılan alıřmalarla, asimetrik Őifreleme algoritmalarının bu dezavantajını ortadan kaldırmak veya daha dřk anahtar deęerleriyle aynı gvenlięi saęlayabilme alıřmaları yapılmıřtır. Bu alıřmalar sonucunda Eliptik eęri Őifreleme algoritması (ECC) geliřtirilmiřtir.

Sonuç olarak, RSA Őifreleme algoritması hala gcn korumaktadır. Bilim adamları farklı

matematik teoremleri kullanarak RSA algoritmasına karřı ataklarda bulunacaktır. RSA algoritması bu karřı ataklara karřı daha byk asal sayılar kullanarak gvenlięini saęlamaya alıřacaktır. Fakat ok byk sayılar kullanılması sistemi yavařlatacaktır.

9. Kaynaklar

[1] Schneider B. "Applied Cryptography Second Edition", John Wiley & Sons, Inc., New York

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

[3] Diffie W., Hellman M.E., "New Directions in Cryptography", IEEE Trans. IT-22 1976, no. 6, 644-654.

[4] Tektař M. ,Baba F. ,alıřkan M., ' Őifreleme Algoritmalarının Sınıflandırılması Ve Bir Kredi Kartı Uygulaması ' 3RD International Advanced Technologies Symposium, August 18-20, 2003, Ankara

[5] Yerlikaya T., Buluř E., Arda D., 'Asimetrik Kripto Sistemler Ve Uygulamaları' II. Mhendislik Bilimleri Gen Arařtırmacılar Kongresi-MBGAK'2005, İstanbul-Trkiye

[6] El Gamal T., "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. Advances in Cryptology: Proceedings of CRYPTO 84", Springer Verlag, pp. 10-18, 1988

[7] Rivest R., Shamir A., Adleman L., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, v. 21, n. 2 (Feb 1978), pp. 120-126.

[8] P1398, "Standard Specifications For Public-Key Cryptography", IEEE, October 1998

- [9] Pollard Rho Algorithm www.Csh.rit.edu.Pat/math/rho
- [10] Yerlikaya T., “Şifreleme Teknikleri ve Güncel Uygulama Olanakları”, Yüksek Lisans Tezi Trakya Üniversitesi, 2002
- [11] Yerlikaya T., Buluş E., Buluş N., “Kripto Algoritmalarının Gelişimi Ve Önemi”, Akademik Bilişim Konferansları 2006-Ab2006, Denizli-Türkiye, Şubat-2006.
- [12] Kaliski B., “The Mathematics of the RSA Public-Key Cryptosystem”, RSA Laboratories NY, 2001