Hakan Çakar, Asaf Varol, "Bilgi Güvenliği ve RSA Şifreleme Algoritmasının İncelenmesi", Ulusal Teknik Eğitim, Mühendislik ve Eğitim Bilimleri Genç Araştırmacılar Sempozyumu (UMES 2007), 20-22 Haziran 2007, Kocaeli Üniversitesi, Kocaeli, Bildiriler Kitabı, S. 29-32

4.43. BİLGİ GÜVENLİĞİ VE RSA ŞİFRELEME ALGORİTMASININ İNCELENMESİ

*** Hakan ÇAKAR, * Asaf VAROL**

***Fırat Üniversitesi, Teknik Eğitim Fakültesi, Elektronik-Bilgisayar Eğitimi Bölümü-ELAZIĞ**

avarol@firat.edu.tr , hcakar@firat.edu.tr

ÖZET

Bilgi güvenliği, bilgilerin güvenliğini sağlamak amacı ile yürütülen her türlü çaba ya da faaliyet olarak tanımlanmaktadır. Bilginin korunmasında gizlilik, bütünlük ve kullanılabilirlik hedefleri esastır. Bu esasların sağlanabilmesi için, bilginin uygun bir şifreleme tekniğiyle anlaşılamaz hale getirilmesi gereklidir.

Bu çalışmada, günümüzde özellikle bankacılık sistemlerinde sayısal verileri şifrelemede kullanılan RSA algoritması incelenmiştir. Ayrıca nesne tabanlı bir programlama dili kullanılarak RSA algoritmasının çalışmasını gösteren yeni bir ara yüz tasarımı gerçekleştirilmiştir.

Anahtar Kelimeler: Güvenlik, Şifreleme, RSA Algoritması

INFORMATION SECURITY AND ANALYSIS OF RSA ENCODING

Hakan Çakar, Asaf Varol, "Bilgi Güvenliği ve RSA Şifreleme Algoritmasının İncelenmesi", Ulusal Teknik Eğitim, Mühendislik ve Eğitim Bilimleri Genç Araştırmacılar Sempozyumu (UMES 2007), 20-22 Haziran 2007, Kocaeli Üniversitesi, Kocaeli, Bildiriler Kitabı, S. 29-32

SUMMARY

Information security is described as the all sorts of actions and efforts to ensure the safety of the information. Targeting privacy, integrity and employability is the principal of the securing information. In order to provide these bases, information has to be encoded to an unknown structure.

In this study, the RSA encoding algorithm, which is especially employed in banking systems, is investigated. Moreover, a GUI based object oriented program is developed to present the operation of the RSA algorithm.

Key Words: Encoding, RSA Algorithm, Security

1.GİRİŞ

Bilim ve teknoloji uzun bir süre ayrı olarak yollarına devam etmişlerdir. Sanayi devrimine kadar teknoloji, mucitlerin kontrolünde daima bilimden önde gitmiştir. Ancak, sanayi devriminden sonra bilim ve teknoloji, birbirini tamamlayan kavramlar haline gelmiştir. Bu sebeple atölyelerin yerlerini, bilim adamlarının laboratuarları ve araştırma merkezleri almıştır. Bu gelişmeler, insanların sosyal hayatına ve insanların evreni algılamasında farklı bakış açılarına yönelmelerine sebep olmuştur [1].

MÖ. 3500 yılı civarında yazının, MÖ. 170 yılında ilk kağıt (parşömen) ve 1454 yılında da matbaanın icadı ile bilgi yeni bir boyutta gelişme gösterirken; daktilo, telgraf, telefon, sabit resimlerin elektromanyetik dalga ile dijital halde iletimi, televizyon yayını, haberleşme uydusu, denizaşırı fiber optik kablo ile yazılı metinlerin yanında ses ve hareketli görüntüyü de kapsayan Internet' in ortaya çıkması ile bilgi yeni bir

boyut kazanmıştır. Haberleşme teknolojilerinin gelişmesi sayesinde bilginin iletilmesi, işlenmesi, depolanması gibi yeni alanlar ve bununla ilgili yeni teknolojiler ortaya çıkmasına neden olmuştur. Bu teknolojiler sayesinde insan yaşadığı dünyaya alternatif olan farazi (sanal) bir dünya oluşturmuştur. Bu hayali dünyanın neredeyse tamamını bugün Internet oluşturmaktadır [2].

Bugünkü internet ortamının, gerçek dünyada olduğu gibi tehlikeli ve kötü niyetli kişiler tarafından da farklı amaçlar için kullanıldığını görmekteyiz. Açık bir ağ olan internet, ticari amaçlı kullanımının da yaygınlaşmasıyla, saldırıların hedef noktası olabilmektedir. Kurum ve kişiler, internet ortamına güvenlik endişesiyle girmekten kaçınabilmekte, bir yandan da böyle bir ortamda bulunmamanın büyük bir eksiklik olacağını bilmektedirler. İnternet kullanıcıların birbirlerine karşılıklı güvendiği, çalışmalarını ve edindikleri bilgileri paylaştığı akademik bir ortam olarak tasarlanmıştır [3].

Günümüzde, teknolojinin gelişimiyle birlikte bilgisayarlar ve internet hayatımızda çok büyük yer sahibi olmaya başlamıştır. Daha çok insanın online olduğundan beri internet üzerinden işlemler yapmak kaçınılmaz bir hal almıştır. Bunun en önemli sonucu olarak e-ticaret büyük bir önem kazanmıştır. IP ağlarındaki dezavantajlarından biride güvenliktir, güvenliği sağlamanın yolu da şifreleme ve kimlik denetiminden geçmektedir. E-ticaret ve bankacılık sisteminin gelişimi ile birlikte bu sistemlerin güvenliğinin sağlanması için şifreleme algoritmaları kullanılmaya başlanmıştır [4].

Şifreleme algoritmaları açık anahtarlı (asimetrik) ve gizli anahtarlı (simetrik) olmak üzere iki kategoride sınıflandırılmaktadır. Anahtarlar, şifreleme ve deşifreleme işlemlerinin kontrolünü gerçekleştiren, farklı uzunluk ve yapıdaki gereçlerdir. Açık anahtarlı sistemlerin kullanımı, gizli anahtarlı sistemlerin aksine henüz yenidir. Açık anahtarlı şifreleme

sistemlerinin amacı, belli bir anahtar üzerinde anlaşmanın ve alıcı tarafa bu anahtarı ulaştırabilmenin zorluğunu ortadan kaldırmaktır. Gizli anahtarlı algoritmalarda, şifreleme ve deşifreleme işlemleri için gönderici ve alıcının birlikte paylaştığı tek bir anahtar kullanılırken, açık anahtarlı algoritmalarda şifreleme ve deşifreleme için birbirinden farklı anahtarlar kullanılmaktadır. Dolayısıyla gizli anahtarlı şifrelemede, anahtar açıklanırsa haberleşmede güvenlik sorunu ortaya çıkar [5].

Açık anahtarlı şifrelemede mesaj gönderen kişi, alıcı tarafa ait herkesçe bilinmekte olan açık anahtarı kullanarak, göndereceği mesajı şifreler ve alıcıya gönderir, mesajın alıcısı da yalnız kendisinin bildiği gizli anahtar ile mesajı açar. Gizli anahtar yalnız alıcı tarafından bilindiği için, başka biri tarafından mesajın açılması söz konusu değildir.

Şifre anahtarı halka açık tutulduğu için, Asimetrik şifreleme algoritmaları aynı zamanda Halk Anahtarlı Kripto sistemler (public key cryptosystem-PKS) olarak da bilinir [6].

Asimetrik şifreleme sistemlerinin çoğunluğu, sayılar teorisini temel almaktadır. Sayılar teorisinin bazı kısımlarını bilmek, açık anahtarlı şifreleme algoritmaları hakkında kesin bir yargıya varmak için gereklidir [7]. Açık anahtarlı kripto sistemleri üzerine ilk öneri, 1976 yılında Diffie ve Hellman tarafından yapılmıştır. Ardından Rivest, Shamir ve Adleman RSA kripto sistemini bulmuşlardır [8].

Her açık anahtar tabanlı şifreleme sistemi matematiksel zor problemlere dayanır. Örneğin RSA sisteminin güvenliği, büyük sayıların faktorizasyonunun zorluğuna dayanmaktadır. Açık anahtar tabanlı şifreleme algoritmaları ile yapılan işlemler (şifreleme, deşifreleme, sayısal imzalama ve imza doğrulama işlemleri) yavaş işlemlerdir. Uygulamanın çalıştırıldığı

platform, kullanılan algoritma ve anahtar uzunluğu işlemlerin hızını belirleyen önemli etkenlerdendir. Ancak her ne koşul altında olursa olsun, tek anahtarlı simetrik algoritmalar, asimetrik algoritmalara göre kat kat daha hızlı olabilmektedir. Buna rağmen açık anahtar tabanlı algoritmaların tercih edilmesinin nedeni, sunduğu kripto analiz direnci ve anahtar dağıtımdaki kolaylıklardan dolayıdır [9].

Bu çalışmada Asimetrik şifreleme algoritmalarının en önemlisi ve günümüzde kullanılan, R.Rivest, A.Shamir ve L.Adleman tarafından geliştirilen RSA şifreleme algoritması incelenmiştir.

2.GEREÇ VE YÖNTEM

RSA Algoritması açık anahtar şifreleme tekniğinin temel bir uygulamasıdır. Önceden aralarında hiçbir görüşme yapmamış olan alıcı ve göndericinin aralarındaki haberleşmenin güvenli bir ortamda (güvenli gönderim ve mesajların doğrulanması) gerçekleştirilmesi, bu şifreleme yönteminin iyi yönlerinden birisidir. Bu noktada elbette RSA algoritmasının çalışmasından bahsetmek gereklidir.

Bu şifreleme sistem tasarımı için, öncelikle p ve q olmak üzere iki tane asal sayı üretilir. Bunların birbiriyle çarpılması neticesinde n=p*q işleminden n elde edilir. Bundan sonra n sayısından küçük ve (p-1)*(q-1) sayısıyla 1 dışında herhangi bir ortak böleni bulunmayan bir e sayısı seçilir. Daha sonra (E*D=1) sayısının (p-1)*(q-1) çarpımına tam olarak bölünmesini sağlayan bir D sayısı bulunur.

E ve D değerleri, sırasıyla, açık ve gizli anahtar olarak adlandırılırlar. Açık anahtarı (n,E) çifti, gizli anahtarı ise (n,D) çifti oluşturur. p ve q sayıları ya yok edilmeli ya da gizli anahtar ile birlikte saklanmalıdır.

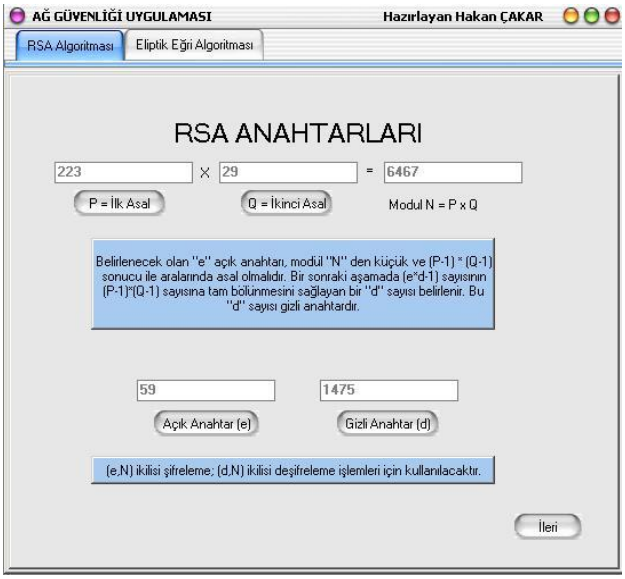
Gizli anahtar olan D sayısının (n,E) sayılarından elde edilmesi zor bir işlemdir. Eğer bir kişi n sayısını çarpanlarına ayırarak p ve q sayılarını elde edebilirse, gizli anahtarı da kolaylıkla bulabilir. Bu sebeple RSA sisteminin güvenliği çarpanlarına ayırma probleminin zorluğu temeline dayanır. Çarpanlarına ayırma işleminin kolay bir yönteminin bulunması, RSA algoritmasının kırılması anlamına gelir [10].

Gönderilecek mesaj M şeklinde bir düz metin ise, şifreleme formülü $C = M^E \bmod n$ olacaktır. Alıcı tarafa ulaşan şifreli mesajı çözme işleminde ise, $C^D \bmod n = (M^E)^D \bmod n$ formülü kullanılmaktadır.

RSA şifreleme algoritmasının uygulama programı Delphi 7.0 'da gerçekleştirilmiştir. Bu uygulama programı p ve q değerlerini alarak E şifreleme anahtarı olarak kullanılacak değerleri ve bu değerlerden seçilen şifreleme anahtarına göre deşifreleme anahtarını çıktı olarak vermektedir. Uygulama programı bu değerleri alarak verilerin şifreleme ve deşifreleme işlemlerini gerçekleştirmektedir.

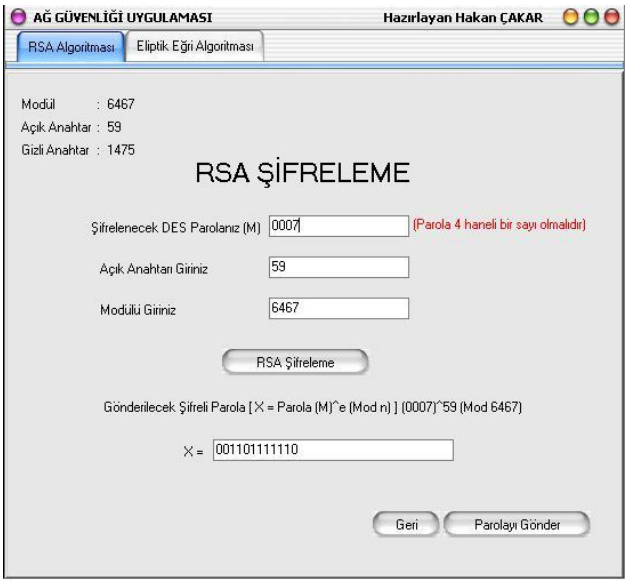
2.1.NESNE TABANLI UYGULAMA YAZILIMININ ÇALIŞTIRILMASI

Şekil 2.1.' de görülen ekran görüntüsünde, RSA anahtarlarının belirlenmesi işlemleri yapılmaktadır. Bunun için P ve Q asal sayıları butonlara tıklanmak suretiyle seçilmekte, daha sonra ekran görüntüsünde de verilen açıklamaya uygun, e açık anahtarı ve d gizli anahtarı tespit edilip, **İleri** butonuna tıklanmalıdır. Eğer P ve Q asal sayıları tespit edilmeden, **Açık anahtar (e)** veya **Gizli anahtar (d)** butonuna tıklanırsa, program uyarı mesajı verecektir.



Şekil 2.1. Açık ve Gizli Anahtarların Belirlenmesi

Şekil 2.2. 'de şifrelenecek olan M parolasının girilmesi sağlanmaktadır. Girilecek olan parolanın 4 haneli olmasında fayda vardır. Uygun parola girildikten sonra, **RSA şifreleme** butonuna tıklanır. Program, ekran görüntüsünde verilmiş olan şifreleme formülüne göre hesaplanan sonucu, ikili sayı sistemine dönüştürmektedir.

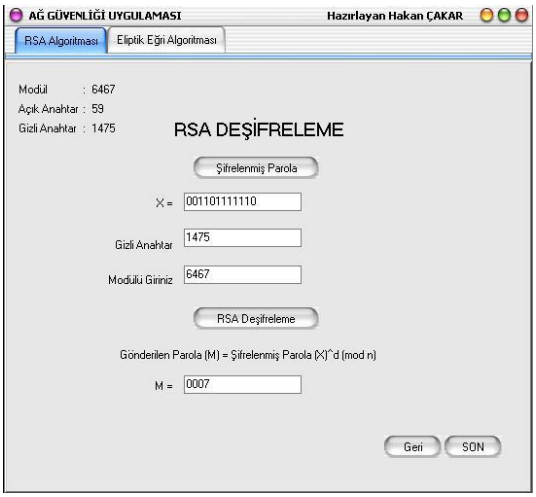


Şekil 2.2. Şifrelenecek Parolanın Girilmesi

Şekil 2.3. ise, şifrelenmiş parolanın alıcı tarafta bulunan kullanıcıya gönderildiği mesajını veren ekran görüntüsüdür. Bu mesaj alındıktan sonra, **Devam** butonuna tıklanmalıdır.

Şekil 2.3. Şifrelenmiş Parolanın Alıcı Tarafa Gönderilmesi

Şifrelenmiş parola butonuna tıklandığında, **001101111110** şeklindeki şifrelenmiş parola görülür, daha sonra **RSA Deşifreleme** botununa tıklanır. Şekil 2.4' de verilen deşifreleme formülüne göre hesaplamalar yapıldığında, orijinal parola 0007 elde edilmektedir



Şekil 2.4. Şifrelenmiş Parolanın RSA Algoritması Kullanılarak Deşifre Edilmesi

3.SONUÇLAR VE ÖNERİLER

Şifreleme işlemlerinde en çok kullanılan şifreleme algoritması RSA' dır. Bu algoritma günümüzde 160 bit sayısal anahtar büyüklükleri ile gerçekleştirilmektedir. Ancak gelecek için daha hızlı ve daha çok işlem yeteneğine sahip bilgisayarların ortaya çıkması, bu anahtar büyüklüğünün yetersiz kalmasına sebep olacaktır. Bir şifreleme algoritmasının güvenirliğini; şifreleme anahtarının uzunluğuna ve algoritmasının yapısına bağlıdır. RSA şifreleme algoritması uzun anahtar değerlerini kullanabilir ve algoritma yapısı da oldukça güçlüdür. Kripto analistler RSA şifreleme algoritması kırabilmek için her anahtar değerini denemek gerektiğini yada N değerinin asal çarpanlarına ayırmak gerektiğini söylemektedir.

Sonuçta RSA şifreleme algoritmasının matematiksel bir yapısı vardır ve bu işlemi gerçekleştirebilmek için matematiksel teoremlerden yararlanılarak sonuca gidilebilir.

Geliştirilen arayüz yazılımı sayesinde, daha güvenilir bir şifreleme elde edilmiş olup, özellikle kablosuz ağ, mobil iletişim, telekomünikasyon sahalarında rahatlıkla kullanılabileceği gösterilmiştir.

KAYNAKLAR

[1] Varol, A., Alkan, T., 1998, İnternet'e Genel Bakış, Uzaktan Eğitim,10-16

[2] Çakar, H., 2005, Bilgisayar Ağ Güvenliği ve Güvenlik Duvarları, Fırat Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi

[3] Taşdemir, M., 2001, Ağ Güvenliği için PC Tabanlı bir Paket Filtreleme Sisteminin Tasarımı ve Gerçekleştirimi, Hacettepe Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi

[4] Yerlikaya T., Buluş E., 2003, RSA Şifreleme Algoritmasının İncelenmesi ve Kriptanalizi, İstanbul, Türkiye Bilişim Haftası

[5] Tektaş, M., Baba, Fevzi., Çalışkan, E.Müslim., Şifreleme Algoritmalarının Sınıflandırılması ve Bir Kredi Kartı Uygulaması, 3RD International Advanced Technologies Symposium, August 18-20, 2003, ANKARA

[6] RSA Laboratories, www.rsasecurity.com

[7] Kodaz H., 2003, RSA Şifreleme Algoritmasının Uygulaması, Bilgisayar Mühendisliği Bölümü, Selçuk Üniversitesi, Alaeddin Keykubad Kampusü

[8] Rivest, R., A. Shamir ve L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communications of the ACM, vol. 21, no.

2, pp. 120-126, Subat 1978.

[9] Levi, A., Özcan M., Sabancı Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, İstanbul

[10] Bruce SCHNEIDER, 1996.Applied Cryptography, second edition, New York