İSTANBUL AYDIN ÜNİVERSİTESİ DERGİSİ (İAÜD)
Yıl 3, Sayı 12, Sayfa (69 - 82)

GÜVENLİ HABERLEŞME TEKNİKLERİ

Osman Nuri UÇAN[1] Tarık YERLİKAYA[2] Hakan GENÇOĞLU[3]

[1]İstanbul Aydın Üniversitesi Mühendislik Fakültesi, İstanbul

[2]Trakya Üniversitesi, Bilgisayar Mühendisliği Bölümü, Edirne

[3]İstanbul Aydın Üniversitesi, Anadolu Bil Meslek Yüksek Okulu, İstanbul

1. GİRİŞ

Yüzyıllar boyu gizli kalması gereken mesaj iletiminde şifrelemeye başvurulmuştur. İlk kullanılan teknikler basit öteleme veya yer değiştirme üzerine kurulmuştur. Örneğin Sezar şifresi olarak bilinen yöntem belirli bir anahtar değerinde seçilen harflerin ötelenmesi şeklinde çalışmaktadır. Şifreleme konusunda, teknolojinin ilerlemesine bağlı olarak, daha karmaşık matematiksel yöntemler kullanılmaya başlanmıştır.

Şifreleme algoritması oluştururken dikkat edilmesi gereken unsurlardan ikisi hız ve güvenliktir. Simetrik algoritmalar hızlı çalışır, hem şifrelemek hem de şifre çözmek için aynı anahtarı kullanır ve tatmin edici bir güvenlik sağlar, ama anahtar dağıtımı güvenliğin muhtemel zayıf noktasını oluşturur. Asimetrik algoritmalarda ise anahtar dağıtımı problemi yoktur. Çünkü şifrelemek için

kullanılan açık anahtarın herkes tarafından bilinmesinde sakınca yoktur, şifre çözmek için kullanılacak olan gizli anahtarın ise sadece şifre çözmeyi yapacak kişi tarafından bilinmesi yeterlidir. Dolayısıyla simetrik algoritmalara göre daha güvenlidir, ama şifreleme ve şifre çözme süreleri daha uzundur. Bu çalışmada simetrik ve asimetrik şifreleme algoritmalarının güçlü yönleri kullanılarak daha hızlı ve daha güvenli bir yaklaşım denenmiştir.

Anahtar Kelimeler: Kriptografi, RSA, AES, Hibrit

2. RSA

1977 yılında Ron Rivest, Adi Shamir ve Len Adleman tarafından geliştirilen RSA, açık anahtarlı şifreleme düşüncesi üzerine kurulmuştur. Çok büyük asal sayıları kullanarak şifreleme yapmaktadır. Algoritma şu şekilde çalışır:

- p ve q birbirinden farklı olacak şekilde iki asal sayı seçilir.
- n=pq hesaplanır
- Ø(n)=(p-1)(q-1) sayısı hesaplanır.
- 1<e< Ø olacak şekilde bir e sayısı seçilir. Buradaki önemli koşul gcd(e, Ø(n))=1 olmalıdır
- de≡1 mod Ø(n) olacak şekilde d hesaplanır.

Bu işlemler sonucunda elde edilen (n,e) açık anahtardır ve şifreleme için kullanılır, (n,d) ise gizli anahtardır deşifreleme için kullanılır.

Bu işlemleri yaparak anahtarları tespit eden alıcı, göndericiye açık anahtarı gönderir ve gönderici

$C = M^e \bmod(n)$ işlemlerini gerçekleştirerek mesajı şifreler ve alıcıya gönderir.

Şifrelemenin asıl sorunu anahtar üretimi ve dağıtımı olduğu için günümüz bilgisayarlarını çok zorlayan hesaplaması uzun süren işlemlerle yoran RSA deşifreleme yapmak için gerekli olan anahtarı kaba kuvvet saldırısı yaparak bulmayı ve mesajı çözmeyi neredeyse imkânsızlaştırmıştır.

2.1. RSA Sisteminin Güvenirliği

RSA sisteminin kırılması birkaç değişik şekilde yorumlanabilir. Sisteme en çok zarar verecek saldırı bir saldırganın belli bir açık anahtara karşı gelen gizli anahtarı bulmasıdır. Bu durumda saldırgan mesajları okuyabildiği gibi imzaları da taklit edebilir. Eğer p ve q değerleri bulunabilirse açık üs e kullanılarak d kolaylıkla hesaplanabilir. Ancak buradaki zorluk n=pxq değerinin çarpanlarına ayrılmasıdır. RSA sisteminin güvenliği çok büyük sayıların asal çarpanlarına ayrılmasının zorluğu varsayımına dayanır. Büyük sayıların çarpanlara kolayca ayrılabilmesiyle ilgili henüz kesin ve hızlı bir yöntem yoktur. Son üç yüzyıl içerisinde Fermat ve Legendre gibi ünlü matematikçiler bu konuda çalışmalar yapmışlardır.[1]

P ve q değerleri yeterince büyük seçilirse n değeri çok büyük bir sayı olacağından günümüz teknolojisi ile p ve q yu hesaplamak mümkün olmaz.

RSA'yı kırmanın bir başka yolu mod n'e göre e'inci köklerin hesaplanmasıdır. $c=m^e$ olduğuna göre c'nin e'inci kökü m'dir. Bu durumda gizli anahtar bilinmese dahi şifrelenmiş mesajların deşifre edilmesi ya da imzaların taklit edilmesi sağlanabilir. Şu ana kadar RSA yöntemini bu yolla kırmaya çalışan bir metoda rastlanmamıştır.

Ayrıca saldırganın doğru olanı bulana kadar, olası tüm d'leri denemesi mümkündür. Ancak böyle bir brute-force saldırı n'in çarpanlarına ayrılmasından daha verimsizdir, bir başka yöntem ise (p -1)(q -1)'in değerinin tahmin edilmesi olabilir. Bu da aynı şekilde n'in çarpan1arına ayrılmasından daha kolay değildir.

Bir başka saldırı da n'i çarpanlarına ayırmadan ϕ>(n)'nin hesaplanmasıdır. Eğer bir saldırgan ϕ>(n)'i hesaplayabilirse e'nin ϕ>(n) modülüne göre çarpımsal tersini hesaplayarak d'yi bulabilir. Ancak bu n'nin çarpanlarına ayrılmasından daha kolay değildir çünkü bu yolla kriptanalist ϕ>(n)'i kullanarak n'i kolaylıkla çarpanlarına ayırabilir. Bunun için ϕ >(n) = n -(p + q) + 1 eşitliğinden n bilindiği için. (p + q) hesaplanır.

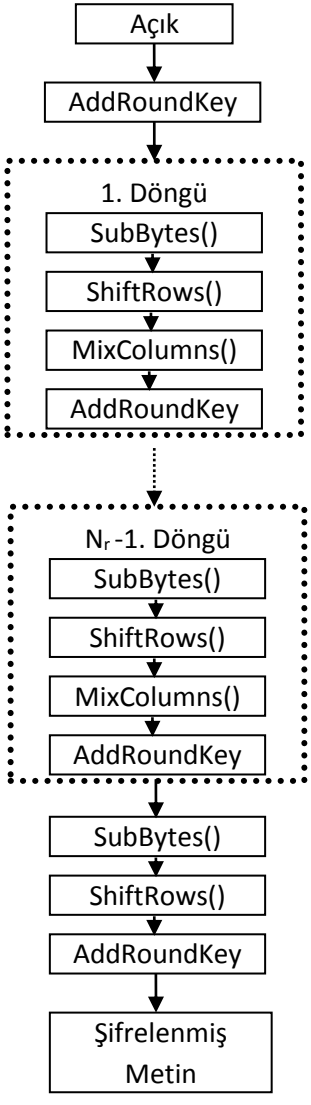
$$(p-q) = \sqrt{([(p+q)^2 - 4n])}$$

olduğundan (p -q) bulunur. Bu iki eşitlikten p ve q hesaplanabilir. d'nin hesaplanmasının n'in çarpanlarına ayrılmasından daha kolay olamayacağı açıktır. Çünkü eğer d bilinirse n kolaylıkla çarpanlara ayrılabilir. [2],[3]

3. AES

AES (Rijndael) değişik anahtar boyutları ile şifreleme yapabilen bir algoritmadır. Şifrelenmek istenen mesajı 128 bitlik bloklara ayırarak 4 katmandan oluşan işlemden geçirir. Bu işlem seçilen anahtar boyutuna göre (128 bitlik anahtar için 10, 192 bitlik anahtar için 12, 256 bitlik anahtar için 14) tekrarlanarak şifreleme işlemi yapılmış olur. [4]

AES en küçük işlem birimi olarak baytları kabul eder. Şifrelenecek metin, şifrelenmiş metin ve anahtar bilgileri bayt dizileri olarak kabul edilirler. Bu diziler 4 satır ve Nb adet sütündan oluşur ve her bir hücre baytlık bilgi tutar. Metin 4 baytlık sütün vektörleri şeklinde, yani 128 bit için 4x4 (Nb= 4), 192 bit için 4x6 (Nb= 6) ve 256 bit içinde 4x8'lik (Nb= 8) matrislerle ifade edilir. 128 bitlik bir metin için aşağıdaki gibidir. [3]



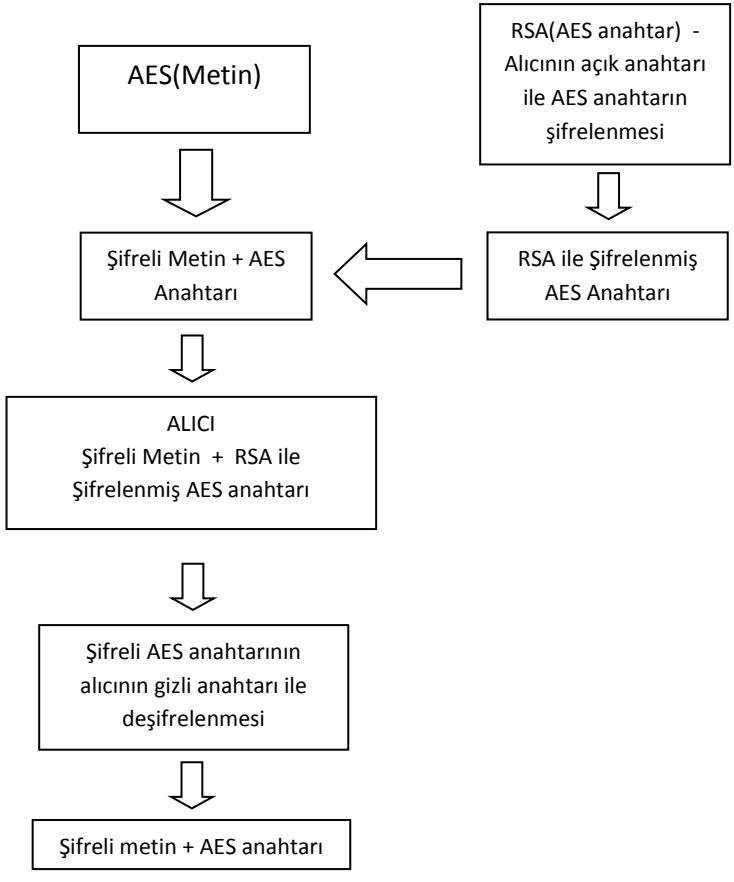
Şekil 1. AES (Rijndael) akış şeması

Osman Nuri UÇAN[1] Tarık YERLİKAYA[2] Hakan GENÇOĞLU[3]

4. Hibrid Algoritma

Simetrik ve Asimetrik algoritmalarını avantajlı özelliklerinin birleştirilmesi düşüncesi ile ortaya çıkmıştır. AES algoritmasının hızı ve bilinen ataklara karşı güvenliği ile RSA algoritmasının anahtar üretimi ve anahtar paylaşımındaki güvenliği birleştirilmiştir. Böylece hem hızlı hem de anahtar paylaşımı güvenli olan bir algoritma elde edilmiştir. Aşağıdaki akış şemasında açık metnin AES ile şifrelenmesi ve şifrelemede kullanılan AES anahtarının alıcının açık anahtarı kullanılarak RSA ile şifrelenmesi ve şifreli metin ile birlikte güvenli bir şekilde alıcıya gönderilmesi anlatılmıştır.

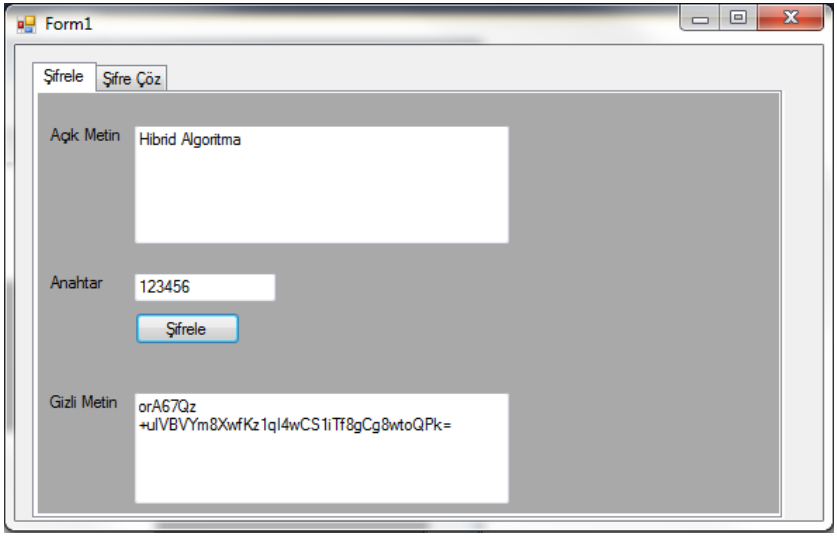
Osman Nuri UÇAN[1] Tarık YERLİKAYA[2] Hakan GENÇOĞLU[3]



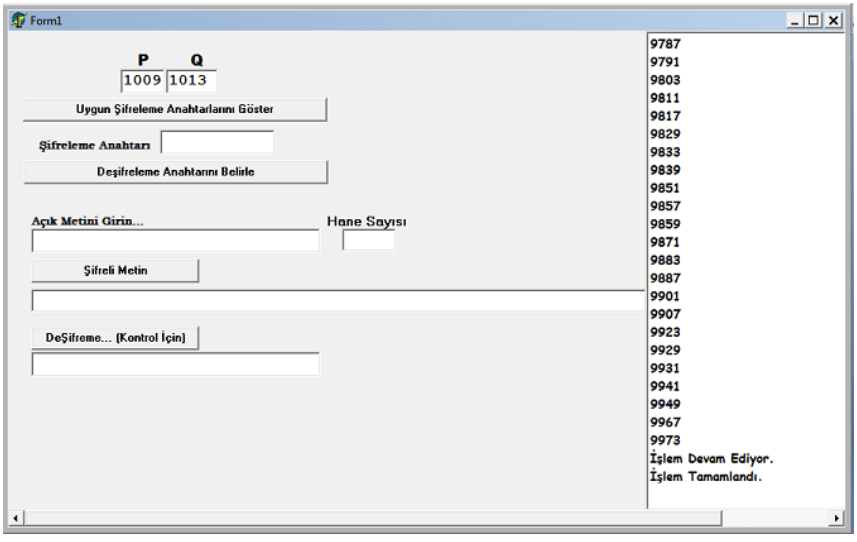
Şekil 3. Hibrid Algoritma Akış Şeması

5. Hibrid Algoritma Uygulama Örneği

Açık metin "Hibrid Algoritma" olarak seçilmiş ve "123456" simetrik anahtarı ile AES kullanılarak şifrelenmiştir.

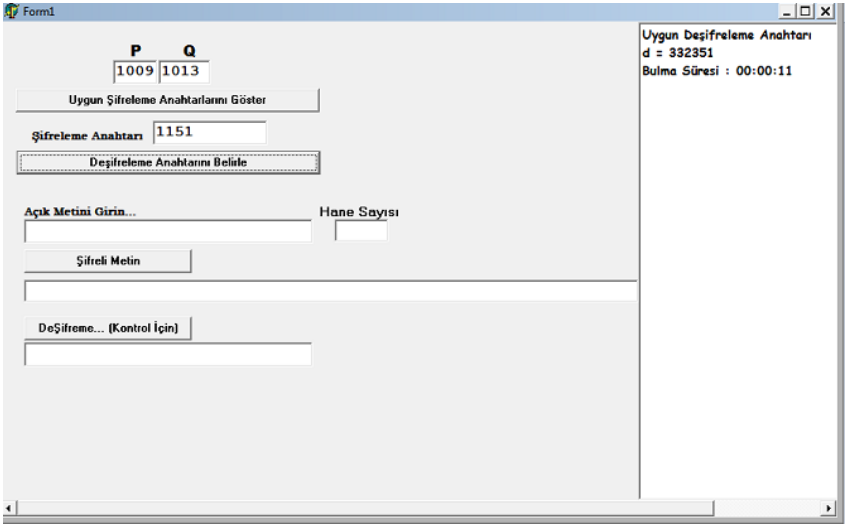


Alıcı tarafından RSA anahtar üretimi için 1009 ve 1013 asal sayıları seçilmiş ve olası e (şifreleme anahtarları) listelenmiştir.

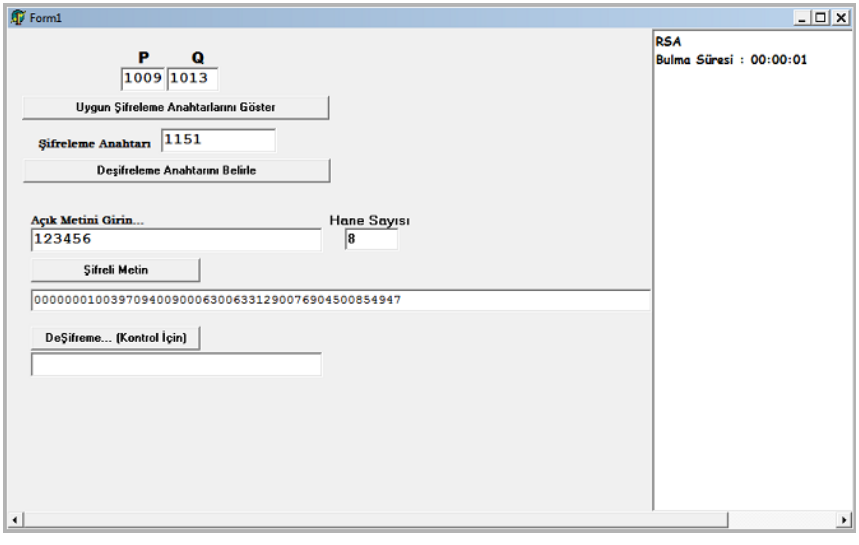


Alıcı e anahtarı olarak 1151'i seçmiş ve AES de kullanılan şifreleme anahtarını RSA ile şifrelemesi için göndericiye bildirmiştir. Seçilen e=1151 şifreleme anahtarına karşılık deşifreleme anahtarı d=332351 olarak hesaplanmıştır.

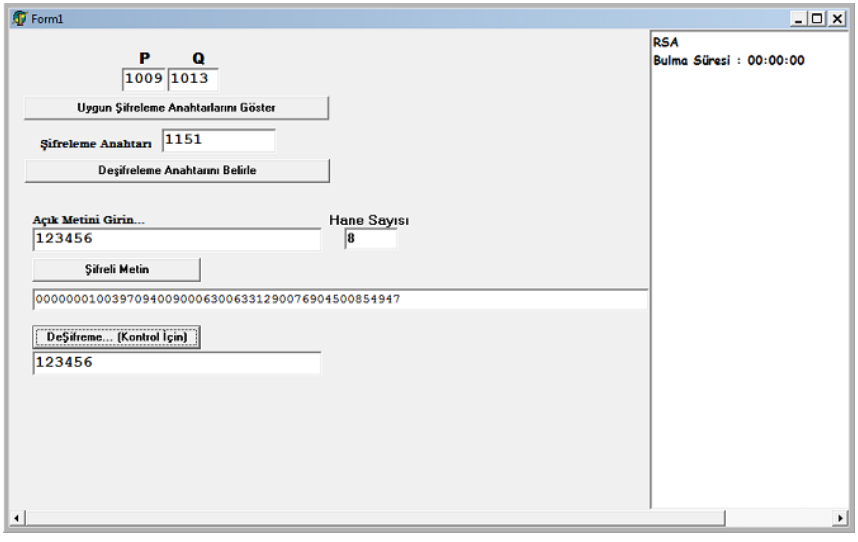
Osman Nuri UÇAN[1] Tarık YERLİKAYA[2] Hakan GENÇOĞLU[3]



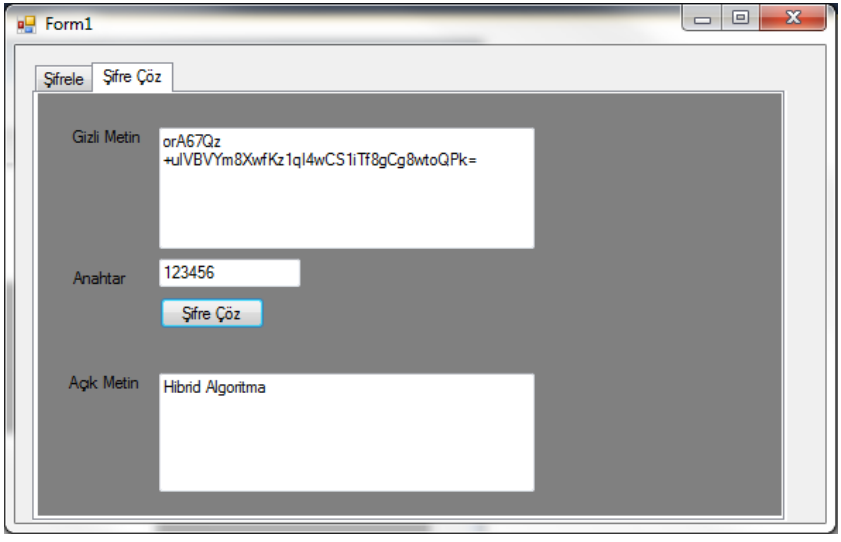
Gönderici, alıcının e=1151 anahtarı ile AES şifreleme anahtarını (123456) şifrelemiş ve şifreli mesaj ile alıcıya göndermiştir.



Alıcı e=1151 açık anahtarına karşılık gelen d=332351 gizli anahtarı ile deşifreleme yaparak AES açık anahtarına ulamıştır.



AES anahtarına ulaşan alıcı "123456" şifresini kullanarak gizli metni çözmüştür.



6. SONUÇLAR:

Bilgi hırsızlığından en etkin korunma yolu şifreleme algoritmalarından geçmektedir. Donanım alanındaki gelişmeler bilgisayarların işlem yapma yeteneğini geliştirmiş ve bilgisayarların hızlarını artırmıştır. Bu artış hem olumlu hem de olumsuz sonuçları bir arada getirmiştir. Simetrik şifreleme algoritmaları güvenli ve hızlı olmakla birlikte anahtar dağıtımı problemi yaşamaktadır. Asimetrik algoritmalarda bu problem çözülmüş fakat bu sefer bilgisayarlara çok fazla işlem yüklendiği için performans problemi doğmuştur. Bu çalışmada yeni bir yaklaşımla şifreleme simetrik (AES - Rijndael) algoritma ile yapılmış, AES deki anahtar da tekrar asimetrik (RSA) ile şifrelenerek güvenlik sağlanmıştır.

İlerleyen çalışmalarda bu algoritmanın çeşitli eş zamanlı sohbet programlarına implement edilmesi ve web üzerindeki kullanımı ile ilgili çalışma yapılması düşünülmektedir.

7. KAYNAKLAR:

[1] P1398, "Standard Specifications For Public−Key Cryptography", IEEE, October 1998.

[2] Knuth, D.E., "Art of Computer Programming Volume 2 Seminumerical Algorithms", Addison Wesley, 1969.

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

[4] YERLİKAYA, Tarık - Doktora Tezi Trakya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Bölümü – 2006