KRİPTO ALGORITMALARININ GELİŞİMİ VE ÖNEMİ

Tarık Yerlikaya
Trakya Üniversitesi
Bilgisayar Müh. Bölümü
tarikyer@trakya.edu.tr

Ercan Buluş
Trakya Üniversitesi
Bilgisayar Müh. Bölümü
ercanb@trakya.edu.tr

Nusret BULUŞ
Trakya Üniversitesi
Bilgisayar Müh. Bölümü
nusretb@trakya.edu.tr

ÖZET

Bu çalışmada kriptografi algoritmalrının gelişimini ve günümüzdeki önemini açıkladık.. Öncelikle ilk oluşturulan şifreleme algoritmaları yapılarını ve özelliklerini inceledik. Günümüzde kullanılan şifreleme algoritmalrını sınıflandırdık. Simetrik şifreleme algoritmalarının en önemlisi olan DES şifreleme algoritmasının yapısını ve özelliklerini inceledik. Son olarak asimetrik şifreleme algoritmalarından bir olan ve günümüzde yaygın bir şekilde kullanılan RSA şifreleme algoritmasını açıkladık.

ABSTRACT

In this study, we explain the development and importance of cryptography algorithms. The background of encryption algorithms and the structure of these algorithms is analyzed. We classified the crypto algorithms which are used in daytime. The structure and properties of DES which is most popular of symmetric algorithms is showed. . In the end, we explain the structure and properties of RSA encryption algorithm that is used in daytime and one of most popular algorithms of asymmetric algorithms.

Anahtar Kelimeler: Kriptoloji, Kripto Algoritmaları, Simetrik Şifreleme Algoritmaları, Asimetrik Şifreleme Algoritmaları, DES, RSA

1. GİRİŞ

Kriptoloji, Yunanca krypto's (saklı) ve lo'gos (kelime) kelimelerinin birleştirilmesinden oluşturulmuştur ve iletişimde gizlilik bilimi olarak değerlendirilmektedir.

Ticari ilişkilerde, devlet işlerinde, askeri işlerde ve personel ilişkilerinde güvenli iş çalışması yapmak büyük bir sorundur.

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 kriptoanaliz (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 (haberleşmede) güvenliği sağlamak için bin yıldır kullanılmaktadır. Ancak bugün artık özel sektörde de gereksinim duyulmaktadır. Sağlık hizmetleri, finansal işler (örneğin: kredi oranları) 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.

2.KRİPTOLOJİ TEMELLERİ

Bir mesajın anlaşılabilirliğini gizlemek amacı ile iki yöntem uygulanabilir. Bunlardan birincisi mesajın belirli bir yöntem uyarınca kısaltılması, diğeri ise belirli bir teknikle mesajın anlaşılamaz bir biçime dönüştürülmesidir. Bunlardan ilkine stenografı, diğerine ise kriptografı denir.[1]

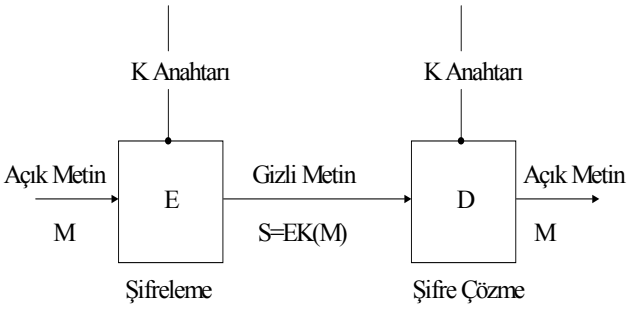
Verinin orijinal biçimindeki haline açık metin denir. Dönüştürülmüş biçimine ise şifrelenmiş metin veya gizli metin denir. Dönüştürme işlemine şifreleme veya kriptolama diyoruz. Dönüştürülmüş metnin ters işlem sonucu açık metin halinin elde edilmesine ise şifre veya kripto çözme denir. M açık metni, E ve D simgeleri de kriptolama ve kripto çözme işlemlerini temsil ettiğinde, gizli metin S,

$$S = E_K(M)$$

olarak gösterilir. Gizli metinden açık metnin elde edilmesi amacı ile kripto çözme işlevinde kullanılması,

$$M = E_K(S)$$

olarak gösterilir. Her iki ifadede kullanılan _K, kripto anahtarını temsil etmektedir. Şekil 1. bu iki işlemi göstermektedir



Şekil 1: Şifreleme ve şifre çözme işlemleri

Burada K anahtarını kullanmanın amacı, eğer M açık metni sadece E kripto işlevi ile şifrelenirse gizliliği sağlayacak olan tek parametrenin kripto algoritması olması ve iletişim güvenliğini arttırmak için alıcı tarafın her yeni kripto işlevi için farklı bir kripto algoritmasını bilmesinin gerekmesidir. Eğer mesajın şifrelendiği E işlevi kaybolacak olursa yeni bir algoritma tasarlanmak durumundadır. Bu durumda zaman kaybı da göz önüne alınacak olursa bu oldukça pahalı bir yöntemdir. Bunun yanı sıra K anahtarı mesajın kripto algoritması bilinse de ikinci bir güvenlik parametresi olduğundan iletişim güvenliğini arttırmaktadır.[3],[4]

3. KRİPTO ALGORITMALARI

Şifreleme işlevinin güvenli bir şekilde gerçekleştirilmesi kriptolama sırasında kullanılan tüm yöntem ve bilgilerin gizliliğine dayanır. Ancak herhangi bir nedenle krıpto işlevlerinin açığa çıkabileceği düşünülerek iletişim güvenliği ,kripto anahtarı denen ek bilgi ile arttırılmıştır. Bu durumda kriptolama işlemi sırasında açık mesaj ,kripto anahtarı aracılığı ile şifrelenir. Bir başka deyişle açık mesaj ile kriptolanmış mesaj arasındaki geçişler kripto algoritmasına bağlı olduğu kadar kullanılan anahtar bilgisine de bağlıdır,

Günümüzde kullanılan kriptografık algoritmalar ikiye ayrılır. Bunlar, kullandıkları anahtar biçimine göre simetrik veya asimetrik olarak adlandırılırlar. Simetrik algoritmalarda verinin kriptolanmasında kullanılan anahtar bilgisi ile kriptolanmış verinin kriptosunun çözülmesinde kullanılan anahtar aynıdır. Bu sebeple açık kullanılan anahtarın üçüncü kişilerden gizlenmesi gerekmektedir. Bu algoritmalara örnek olarak DES'i verebiliriz. Asimetrik algoritmalarda ise her iki kullanıcı ver iyi farklı anahtar bilgisi ile kriptolar ve çözerler. Bu amaçla her bir kullanıcı biri gizli diğeri açık iki anahtar kullanır. Açık anahtar bilgisi alıcı tarafa herhangi bir koruma yapılmadan iletilir. Açık anahtarı alan taraf bu bilgiden kriptoyu çözmek amacı ile kullanacağı gizli anahtarı üretir. Açık anahtarın üçüncü bir kişinin eline geçmesi tek başına hiç bir şey ifade etmez. Her ne kadar bu yöntemin, anahtarların alıcı tarafa iletilmesi işlemini basitleştirdiği düşünülse de asimetrik algoritmaların işlem süresinin yüksek oluşu, veri kriptolama da yaygın olarak kullanılmalarını engellemektedir. Hem simetrik hem de asimetrik algoritmaların temel özelliği yapılarının açık olarak bilinmesidir. Böylece kripto algoritmalarının tasarımında, kriptolanmış verinin anahtar bilgisi olmadan şifrenin çözülememesi ilkesi göz önüne alındığından, iletişim güvenliği, kripto anahtarlarının güvenliği problemine indirgenmiştir.

4. KRİPTO ALGORİTMALARININ GELİŞİMİ

Kripto algoritmalarının kullanım M.Ö. ye dayanmaktadır. B u bölümde ilk oluşturulan şifreleme algoritmalarını inceleyeceğiz.[2]

4.1 Sezar Şifresi

En eski kripto algoritmalarından biri olan Sezar şifresi adını Julius Caesar'dan almaktadır. Orijinal olarak kripto algoritması şu şekilde ifade edilebilir:

S=M+3 (mod26)

Burada S açık metin harfini M gizli metin harfini göstermektedir. Daha sonra bu algoritma genelleştirilerek şu biçimi almıştır,

S = M + i (mod 26), 0 <= i < = 25

Burada i öteleme katsayısı genel anlamda bir kriptografik anahtara karşılık düşmektedir. Burada kullanılan i anahtarının tanım aralığının 25 sayısı ile kısıtlı olması algoritmanın güvenilirliğinin düşük olmasına yol açmaktadır.

4.2 Tekli Alfabetik Yer Değiştirme

Daha yüksek güvenlikli kripto sistemleri düşünüldüğünde alfabede bulunan her harfin yerine başka bir harfin, belirli bir tablo uyarınca yerleştirildiği yapılar ortaya çıkmıştır. Bu tekniğe tekli alfabetik yer değiştirme adı verilir . Bu teknik özel bir alt uygulaması olarak Sezar şifresini de içermektedir. Olası uygulama sayısının yüksekliği göz önüne alındığında tekli alfabetik yer değiştirme güçlü bir algoritma olarak düşünülebilir. Ancak şifrelemeden sonra ortaya çıkan gizli metinde bulunan harflerin dağılım sıklığı, kullanılan diller göz önüne alındığında

bazı istatistiksel ipuçları verdiğinden dolayı, bu tür şifrelemenin de çözülebilmesi oldukça basittir.[6]

4.3. Çoklu Alfabetik Yer Değiştirme

Çoklu alfabetik yer değiştirme tekniğinde, alfabede bulunan her bir harf üzerine n periyotlu bir dizi yer değiştirme uygulanır. Bu yöntem, dilin istatistiksel olarak tahmin edilebilen yapısından kaynaklanan birebirliği bozmayı amaçlamaktadır.

Çoklu alfabetik yer değiştirme yönteminin bir uygulaması olan Vigenere şifresi periyodik olarak belirli bir anahtar değerinde yer değiştirme uygular. Bu uygulamada K anahtarı bir dizi harf olar ak belirlenir. Bu durumda $K = k_1, k_2,.... k_d$ olarak gösterilen ifadede kullanılan k; değeri i=l,2,...,d olmak üzere, alfabede yapılması gereken i'nci ötelemeyi gösterdiğinde, şifreleme sonucu elde edilen harf,

$f(a) = a + k_i \pmod n$ $(n = 26)$

biçiminde gösterilir.

Yer değiştirme şifrelerinde sistemin güvenilirliği anahtar uzunluğuna bağlı olarak değişir. Eğer anahtar uzunluğu mesaj uzunluğunda olur ise bu duruma, çalışan anahtar şifresi adı verilir.

4.4. Tek Kullanımlı Şerit Yöntemi

Analitik olarak koşulsuz güvenli tek şifreleme yöntemidir. Bunu gerçekleştirmek amacı ile tek bir kez kullanılmak üzere, mesaj uzunluğuna eşit veya daha uzun, tümüyle rassal bir anahtar seçilir . Anahtar, ikili sayı düzeninde düşünülen mesaj ile dış veya'lanır. Ancak bu sistem bir çok uygulama için oldukça kullanışsızdır. Çünkü her bir kullanım için en az mesaj uzunluğunda olan anahtarın, haberleşme öncesi her iki tarafa da ulaştırılması gerekmektedir.

4.5.Dönüşüm Şifreleri

Yer değiştirme şifreleri açık metinde bulunan tüm sembollerin yerini değiştirmezken sadece bu sembollerin yerine şifreleme amacı ile kullanılacak olan yeni sembolleri belirler. Ancak dönüşüm şifrelerinde açık metnin harfleri de yer değiştirir. Bu yöntem ilk olarak Eski Yunanda kullanılmıştır. Uzun dar bir şerit üzerine yazılan açık metnin, çapı anahtar bilgisi olan bir silindire spiral olarak dolandırılması ile elde edilen gizli metnin çözülmesi ancak aynı çaplı bir silindire gizli mesajın sarılması ile mümkün oluyordu. Bu sistemde, kullanılan harflerin dağılım sıklığı korunuyordu. Ancak dilin yapısında olan ikili, üçtü ve daha yukarı seviyede harflerin bir araya gelmesi olasılığı bozulduğundan, bu yöntem, dil üzerinde basit yer değiştirmeye dayalı kripto yöntemlerine göre daha güvenli olarak kabul edilir.

5. GÜNÜMÜZDE KULLANILAN ŞİFRELEME ALGORİTMALARI

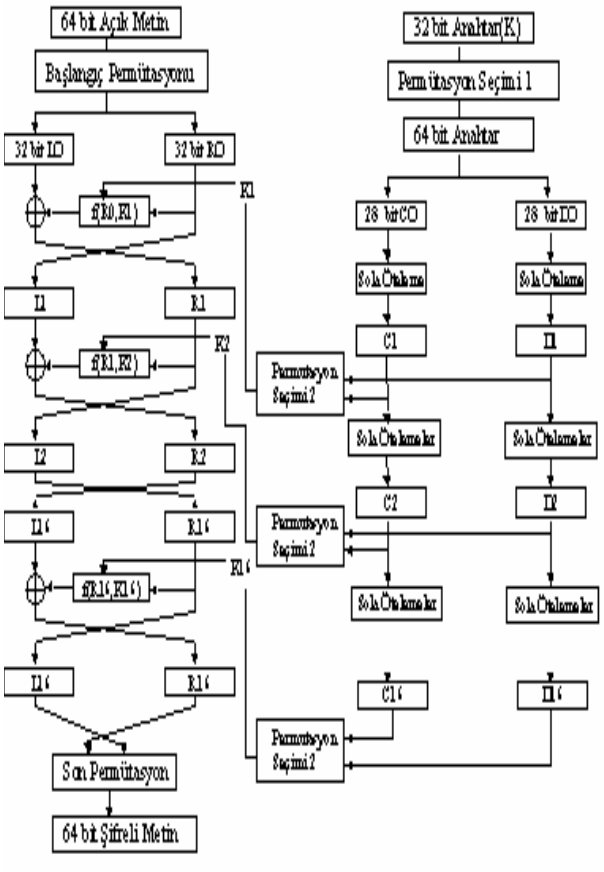
Günümüzde kullanılan kriptografik algoritmalar ikiye ayrılır. Bunlar, kullandıkları anahtar biçimine göre simetrik veya asimetrik olarak adlandırılırlar. Simetrik algoritmalarda verinin kriptolanmasında kullanılan anahtar bilgisi ile kriptolanmış verinin kriptosunun çözülmesinde kullanılan anahtar aynıdır. Bu sebeple açık kullanılan anahtarın üçüncü kişilerden gizlenmesi gerekmektedir. Bu algoritmalara örnek olarak DES'i verebiliriz. Asimetrik algoritmalarda ise her iki kullanıcı ver iyi farklı anahtar bilgisi ile kriptolar ve çözerler. Bu amaçla her bir kullanıcı biri gizli diğeri açık iki anahtar kullanır. Açık anahtar bilgisi alıcı tarafa herhangi bir koruma yapılmadan iletilir. Açık anahtarı alan taraf bu bilgiden kriptoyu çözmek amacı ile kullanacağı gizli anahtarı üretir. Açık anahtarın üçüncü bir kişinin eline geçmesi tek başına hiç bir şey ifade etmez. Her ne kadar bu yöntemin, anahtarların alıcı tarafa iletilmesi işlemini basitleştirdiği düşünülse de asimetrik algoritmaların işlem süresinin yüksek oluşu, veri kriptolamada yaygın olarak kullanılmalarını engellemektedir. Bu algoritmalara örnek olarak RSA'ı verebiliriz Hem simetrik hem de asimetrik algoritmaların temel özelliği standart haline gelebilmesi için algoritma yapılarının açık olarak bilinmesidir.

5.1. Veri Şifreleme Standardı – Data Encryption Standard (DES)

En çok kullanılan şifreleme tekniği 1977'de şimdiki adı Ulusal Standart ve Teknolojiler Enstitüsü olan Ulusal Standartlar Bürosunda ortaya atılan Veri Şifreleme Standardıdır (DES). DES' de veri, 56-bitlik bir anahtar kullanılarak 64-bitlik bloklar halinde şifrelenir. Algoritma, 64-bitlik bir girişi bazı aşamalar sonucu 64-bitlik bir çıktı oluşturacak şekilde dönüştürür. Şifrelemeyi geri almak için aynı adımlar, aynı anahtar kullanılarak işlenir.

DES' in çok geniş bir kullanım sahası vardır. Güvenilirlik derecesi ise tartışıla gelen bir konu olmuştur.

DES şifrelemesinin tümüyle akışı Şekil 2'de gösterilmiştir. Diğer tüm şifreleme yöntemleri gibi bunda da iki girdi vardır: şifrelenecek düzyazı ve anahtar. Burada düzyazı 64-bit, anahtar ise 56-bit uzunluğunda olmalıdır.[6]



Şekil 2.. *DES Algoritmasının Genel Bir Gösterimi*

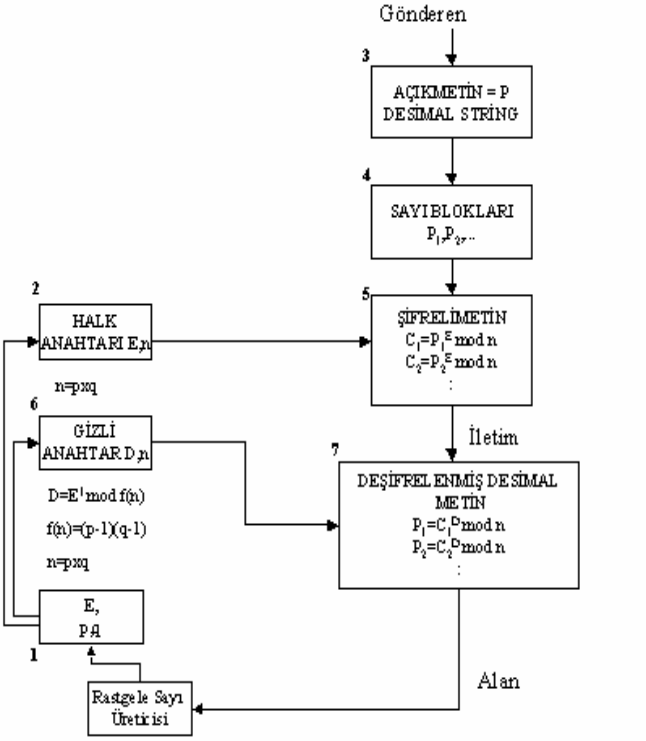
5.2 Rivest-Shamir-Adleman -RSA- Kriptosistemi

RSA 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, asimetrik şifreleme algoritmalarında ve dijital imza işlemlerinde güvenli bir şekilde kullanılır.

Görünüşte son derece basit matematiksel ilişkilerle çalışan bu yöntem de iki ayrı anahtar bulunmaktadır. Anahtarlardan birisi kamuya açık, birisi de gizlidir. Herkes açık anahtarını yayınlar ve kendisine şifreli bir mesaj göndermek isteyen birisi bu anahtarı kullanarak mesajı şifreler ve gönderir. Ancak mesajı sadece gizli anahtar kimde ise o çözebilir. Gizli anahtar da sadece sahibinde bulunur. Böylece, herkes çözüm için gerekli anahtarı bilmeden, güçlü bir şifreyle mesajları gizleyebilir.[5]

Daha önce hiç karşılaşmamış, birbirini tanımayan kişiler bile birbirlerine gizli mesajlar gönderebilir. Örneğin Internet'ten alışveriş yapan birisi, kendisini hiçbir şekilde tanımayan bir web sitesine giderek, sitenin kamuya açık anahtarını alır, kart numarasını bu anahtarla şifrelereyek gönderir. Şifreli bilgiyi gönderen dahil hiç kimse çözemez, sadece web sitesinde bulunan gizli anahtarla gelen kart numarasını web sitesi çözebilir. Böylece kart hamili kart numarasının başkası tarafından okunmayacağından emin olacaktır. Ama, acaba Web sitesi gerçekten dürüst bir satıcı mı, yoksa sahte bir site mi ? Bundan emin olamayacaktır, ancak bunun da çözümü SERTİFİKA yöntemiyle sağlanmaktadır[7]

RSA şifreleme algoritmasında şifrelenecek olan açık metni öncelikle [0, n-1] arasındaki pozitif tamsayı bloklar haline dönüştürülür. Şekil 3'te de ayrıntılı olarak matematiksel işlemler gösterilmektedir.



Şekil 3. *RSA Algoritması*

5. SONUÇLAR

Hayatın her alanında bilgisayarların yaygın kullanımı ve özellikle bilgisayar ağlarının gelişmesi, dünyanın dört bir yanındaki bilgiye erişmeyi kolaylaştırırken, güvenlik sorunlarını beraberinde getirmektedir. Bilginin korunması ve güvenli bir şekilde taşınması çok önemli bir sorun haline gelmiştir.

Şifreleme, bilgiyi matematiksel işlemleri kullanarak veya bilgiyi belli bir algoritmaya göre yer değiştirme işlemi yaparak karmaşık hale getirerek gerçekleştirilir. Uygulanan yöntemlere baktığımızda bu iki işlemi gerçekleştiren farlı şifreleme algoritmaları bulunmaktadır. Bugün bankacılık alanında kullanılan RSA şifreleme algoritması matematiksel işlemleri kullanarak, DES yer değiştirme işlemi uygulayarak şifreleme yapmaktadırlar.

Sonuç olarak günümüz teknolojisi kullanılarak daha güçlü şifreleme algoritmaları geliştirilebilir. Bunun yanında farklı matematiksel işlemleri ele alarak şifreleme algoritmasını güçlendirebiliriz. Buna örnek olarak standartlaşması beklenen eliptik eğri ayrık logaritma problemi üzerine kurulmuş ECC (Eliptik Eğri Şifreleme Algoritması) verebiliriz. Önemli olan güçlü, kırılması zor, şifreleme ve deşifreleme işlemlerini hızlı yapabilecek ve her ortamda kullanılabilecek algoritmaya ulaşmaktır. Bu konu üstünde günümüzde çok yoğun çalışmalar vardır

KAYNAKLAR

[1] Schneider B., 'Applied Cryptography, Second Edition', John Wiley & Sons, Inc. 1996 New York, Ny

[2] Salomaa,A.,.'Public-Key Cryptography', Springer-Verlag, 1990 New York

[3] Yerlikaya T., Buluş E., Arda D., 'Asimetrik Kripto Sistemler Ve Uygulamaları' II. Mühendislik Bilimleri Genç Araştırmacılar Kongresi-MBGAK'2005, İstanbul-TÜRKİYE

[4] 'Current Public-Key Cryptographic Systems', Paper of Certicom, dd. April 1997 Updated July 2000.

[5] Koltuksuz A. " Cryptography in Action" ISCIS'99, 1999

[6] **Koblitz, N.,**. 'A Course in Number Teory and Cryptography', 1994 Springer-Verlag, New York

[7] Trappe W., Washington L.,. 'Introduction **to** Cryptography with Coding Theory'**,** 2002 0-13-061814-4 (Hardback)

[8] Salomaa, A**. ,**. 'Public-Key Cryptography', 1990 Springer-Verlag, New York