ŞİFRELEME ALGORİTMALARININ SINIFLANDIRILMASI VE BİR KREDİ KARTI UYGULAMASI

Mehmet Tektaş[1] ,Fevzi Baba[2] ,E. Müslim Çalışkan[3]
[1] Marmara Üniversitesi Teknik Bilimler Meslek Yüksekokulu ,Göztepe Kampüsü 81040 İstanbul.
e-mail: tektas@marmara.edu.tr
[2] Marmara Üniversitesi Teknik Eğitim Fakültesi, Elektronik Bilgisayar Bölümü, Göztepe Kampüsü 81040 İstanbul. e-mail: fbaba@marmara.edu.tr
[3] Bahçelievler Erkan Avcı Anadolu Teknik, Teknik, Endüstri Meslek Lisesi, Bilgisayar Bölümü, Bahçelievler -İstanbul . e-mail: mslm76@yahoo.com

Özet:Şifreleme Algoritmalarının Sınıflandırılması ve Bir Kredi Kartı Uygulaması

Bilginin güvenli iletimi yani iletim esnasında bilginin gizliliğinin ve bütünlüğünün korunması önemli bir gereksinim haline gelmiştir. Özellikle, e-ticaret ve e-devlet projeleri, internet üzerinden askeri, özel ve resmi yazışmalar, ulusal güvenlik, internet bankacılığı v.b. gibi alanlarda bilginin güvenliğini sağlamak amacıyla çeşitli algoritmalar ve bunları kullanan donanım ve yazılımlar geliştirilmiştir.

Günlük hayatta karşılaştığımız uygulamalardan da anlaşılacağı gibi bilgi güvenliği denilince akla ilk gelen, şifreleme ve şifreleme algoritmalarıdır. Bu nedenle çalışmamızda, literatürde yaygın olarak kullanılan şifreleme algoritmaları sınıflandırılmıştır. Sınıflandırma işleminde; algoritmaların anahtar kullanıp kullanmaması, şifreleme - çözme işlemlerinde kullanılan anahtar sayısı ve algoritmaların gizlilik yada anonimliği göz önüne alınarak bunların genel yapısı incelenmiştir. Şifreleme ve çözme işlemi bir kredi kartı uygulamasında gösterilmiştir.
Anahtar Kelimeler: Kriptoloji, şifreleme, dijital imza, RSA, PGP, algoritma.
Abstract: Classification of Encryption Algorithms and A Credit Card Application

The secrecy and completeness in the communication of information has become an important necessity in modern communication systems. In order to provide the security of information, various algorithms, hardware and software systems based on these algorithms have been developed. These systems have been used in many business areas such as e-trade, e-state projects, military, private or formal e-mails, international security, the internet banking, etc. where the secrecy of information is important.

The secrecy of information requires encryption and encryption algorithms. Therefore, in this study, we classified commonly used encryption algorithms existed in literature. In the classification process, some features of the algorithms such as whether they use key or not, the number of keys used in encryption – decryption, and the privacy or publicity of information was considered. These algorithms were structurally analyzed and examined. Finally, they were used in a sample credit card application.

Keywords :Cryptography, digital signature, PGP, security algorithms

1.Giriş

Elektronik iletişim, günümüzde kağıt üzerinde yazı yazarak yapılan her türlü iletişimin yerine geçmeye adaydır. Çok uzak olmayan bir gelecekte kişi, kuruluş ve toplumlar, özel, kamusal ve resmi haberleşmelerini elektronik iletişim ağları üzerinden yapabilecekler.

Elektronik iletişimin artmasıyla beraber başta finans kurumları olmak üzere birçok kuruluş ticari işlemlerini elektronik iletişimin en yaygın aracı olan İnternet'e taşımaya başlamıştır. Örneğin, bankacılık sektörü internet üzerinden para yatırma işlemi hariç her türlü faaliyeti gerçekleştirebilen sanal şubeler kullanmaktadırlar. Böylece, bilgilerin herkese açık bir ağ üzerinde dolaşmasının doğurduğu haklı tedirginlik gündeme gelmiş, bu konu yoğun bir şekilde tartışılmaya başlanmıştır.
Internet'in iletişim teknolojisinin en yoğun kullanıldığı platform olması yüzünden parasal işlemlerinin güvenilirliği oldukça önemli bir hal alıyor. Para transferleri sırasında önemli bilgilerin Internet üzerinde bunu kötü amaçlarla kullanabilecek insanların eline geçmemesi, geçerse bile kullanamayacağı şekilde olması sorunun büyük bir oranda çözülmesi demektir. Bunun için, para akışı sırasında kullanılacak olan bu tür bilgilerin belirli mantıklarla şifrelenmesi gerekir.
Yine bilgi teknolojilerinin gün geçtikçe artarak hayatın içine girişi, her adımımızın ilgili yada ilgisiz birileri tarafından izlenebileceğimiz ihtimalini gündeme getirmektedir.
Kredi kartı şirketleri, kredi kartlarımız ile yaptığımız tüm alışverişleri takip ediyor; bu sayede bizler ile yada alışveriş yaptığımız mağazalar ile kendileri için daha karlı anlaşmalar yapmayı hedefliyor. Kredi kartı şirketleri ile ilgili gizlilik problemlerimiz bu kadarla sınırlı kalmıyor. Şirket bize ait bilgileri, alışverişlerimize ilişkin olanlar dahil olmak üzere, istediği kişi ve kuruluşlara verme hakkına da sahiptir. Kredi kartı başvuru formuna eşlik eden sözleşmenin bir maddesi bizleri bunu peşinen kabul etmeye zorluyor. Size hiç tanımadığınız firmalardan doğum günü yada bayram tebrik kartları gelmiyor mu?
İnternet'te gezerken izlendiğinizi hiç düşündünüz mü? Web sitelerinin sizin web istemcinize gönderdiği cookie'ler aracılığı ile sitenin en son hangi kısmını ve ne zaman ziyaret ettiğinizi takip etmesi ve kayıt altına alması mümkündür. Web'de bir çok belgeye yada programa erişmeden web sunucu tarafından önce bir form doldurarak kişisel bilgilerinizi vermeniz isteniyor. Bu formlar aracılığı ile kişisel bilgilerinizi ne kadar sık açığa vurduğunuzun farkında mısınız?
ABD'de uluslararası ihalelere girecek Amerikan şirketlerinin rakiplerin ticari sırlarını çalmak için de internet sistemini kullandığı öne sürülmektedir. İddiaya göre, ABD firmalarının katılacağı ihalelerde rakip şirketlerin iletişimi dinleyerek milyarlarca dolarlık kazanç sağladığı iddia edilmektedir. İngiltere dışında Avrupa Birliği, bu ağa karşı engelleme çalışmalarını yoğun şekilde sürdürüyor.
Bundan başka, E-devlet projesi, devletle olan ilişkilerimizde, bürokrasiyi azaltarak büyük yararlar sağlamasına karşın internet üzerinde dolaşabilecek gizli Devlet bilgileri ve askeri bilgilerin gizliliği de bilgi güvenliğinin önemini göstermektedir.
Buraya kadar, anlatılanlar internet'te bilgi güvenliğinin ne kadar önemli olduğunu açık bir şekilde göstermektedir. Ayrıca, bu bilgilerden şu sonucu da çıkartmak mümkündür

"Şirketler, finans kurumları, devlet kurumları, kişiler ve internet'te bilgi transferi yapan özel yada tüzel kişilerin internet'te bilgi güvenliği ve şifreleme teknikleri konusunda ciddi bir şekilde bilgi sahibi olmaya ihtiyaçları vardır.

2.Bilgi Güvenliği Sorunları

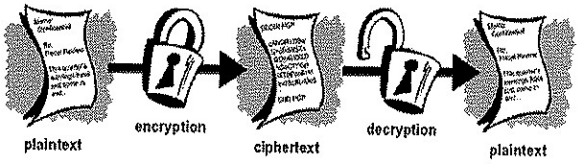
Bilgi güvenliğinden bahsedildiğinde akla gelen sorunlar bilginin gizliliği, bütünlüğü ve inkar edememedir. Bilgi gizliliği; verinin alıcısı dışında hiç kimse tarafından okunamaması, bilgi bütünlüğü; verinin değişmeden alıcısına ulaşması ,inkar edememe ise; gönderenin gönderdiği bir mesajı daha sonra inkar edememesi, etse bile alıcının gönderenin bu mesajı gönderdiğini üçüncü kişilere ispat edebilmesi anlamına gelmektedir .

Bilgi gizliliği ve bütünlüğünde karşılaşılan en büyük sorun bilginin açık kanallardaki veri akışı sırasında yada yetkisiz erişimler ile elde edilerek okunması veya değiştirilmesidir. Örneğin, internet üzerinde veri akışı sırasında yada bilgisayar internete bağlıyken, bilgilerin çeşitli teknik açıklar değerlendirilerek kötü amaçlı kullanım için ele geçirilme tehlikesi bulunmaktadır. İnternet kullanıcısının verebileceği bilgilerin arasında kendi güvenliği ve mahremiyeti açısından sakıncalı olabilecek kredi kartı bilgileri, kullanıcı isimleri şifreler, adres ve telefon numaraları bulunmaktadır. Bu bilgiler genellikle, elektronik ticaret veya finansal işlemler (bireysel bankacılık) sırasında internete açılır ve ele geçirilme olasılıkları belirir.
Elektronik ticaret ve finansal işlemlerin yürütüldüğü siteler internet'ten bilgi alışverişini şifreleyerek gerçekleştirdikleri zaman genel olarak güvenlidirler. Şifrelenmiş bilgi internet üzerinde iletilirken ele geçirilse bile, şifrenin kırılması çok büyük bir yatırım ve oldukça uzun bir zaman dilimi gerektirdiğinden güvenli olduğu kabul edilebilir
İlk bakışta pek önemsenmeyen ama bazı uygulamalarda elzem olan diğer bir güvenlik sorunu ise inkar edememe (non-repudiation) sorunudur. Özellikle doğrudan parayla ilgili uygulamalarda ortaya çıkan bu sorun, gönderenin gönderdiği bir mesajı daha sonra inkar edememesi, etse bile alıcının, gönderenin bu mesajı gönderdiğini üçüncü kişilere ispat edebilmesi zorunluluğundan kaynaklanmaktadır. Kerberos gibi uzaktan erişimde kullanılan özel anahtar tabanlı sistemlerin inkar edememeyi sağlaması, ortak anahtar kavramından dolayı imkansızdır. Çünkü, gönderici gönderdiği bir mesajın alıcı tarafından uydurulduğunu iddia edebilir, alıcı da aynı anahtarı bildiği için bu durumun aksini ispatlayamaz. Açık anahtar tabanlı sistemlerde ise şifreleme anahtarı ile şifreyi çözme anahtarı farklı anahtarlar olduğundan inkar edememe sağlanabilir. Bunun en güzel örneği dijital imzalardır.
Dijital imza, veriyi gönderenin ve alanın kim olduğunun kanıtlanmasına imkan tanır. Yani, imzalanmış bir dokümanı yollayan kişi onu yolladığını inkar edemez ve alıcı da aldığını inkar edemez.

Kriptoloji Kavramları

Özellikle internet teknolojisinin yaygınlaşmasıyla adını sıkça duymaya başladığımız kriptoloji gitgide önem kazanmaktadır. Bu bilim dalı Kriptografi, Kriptoloji ve Kriptoanaliz olmak üzere üç ana kısımdan meydana gelir.
Kriptoloji şifreleme algoritmalarının matematiksel temelleriyle ilgilenen bir matematik dalıdır. Kriptografi ise bu algoritmaları kullanarak yapılan gizli mesajlaşma, onaylama, dijital imzalar, elektronik para ve diğer uygulamaların tüm

yönleriyle ilgilidir. Kriptografik algoritmaların açıklarını bulup ortaya çıkartma ve bu açıkların giderilmesiyle ilgilenen dala ise kriptoanaliz denilmektedir. Şifreleme (Encryption), veriyi alıcından başkasının okuyamayacağı şekilde kodlamaya verilen addır. Şifre Çözme(Decryption) ise alıcının kodlanmış veriyi çözüp eski haline getirmesi işlemidir.(Şekil-1)



Şekil-1. Şifreleme ve şifre çözme

Farz edelim ki bir kişi diğer bir kimseye bir mesaj göndermek istiyor ve başka hiçbir kimsenin mesajı okumadığından emin olmak istiyor. Ancak, bir başka kimsenin mektubu açması veya elektronik iletişimi duyması olasılığı vardır. Kriptografik terminolojide mesaj plaintext (düz-metin) veya cleartext (açık-metin) olarak adlandırılır. Mesajın içeriğini diğer kişilerden saklamak için kodlamaya encryption (şifreleme) adı verilir. Şifrelenmiş mesaja ciphertext (şifreli-mesaj) denir. Ciphertext'ten düz-metni elde etme işlemine decryption (şifre çözme) adı verilir. Veriyi şifrelerken ve çözerken kullanılan matematiksel metoda ise şifreleme algoritması denilmektedir. Şifreleme ve çözme genelde bir anahtar(Key) kullanılarak yapılır ve şifreleme algoritması çözme işlemi ancak doğru anahtarın bilinmesiyle gerçekleştirilebilir.

3. Şifreleme Tekniklerinin Tasnifi

Şifreleme teknikleri algoritmalarına, anahtar sayısına ve şifrelenecek mesajın tipine göre sınıflandırılmıştır. Sınıflandırmada bütün şifreleme algoritmalarını tek tek incelemek yerine her bir algoritma türü için en yaygın olarak kullanılan ve en temel yapıya sahip birkaç algoritma örnek olarak verilmiştir.

3.1. Şifreleme Tekniklerinin Algoritmalarına ve Anahtar Sayısına Göre Tasnifi

Tarihi sürece bakıldığında şifreleme teknikleri önce açık yada gizli algoritma kullanmalarına göre ikiye ayrılırlar.

3.1.1. Algoritması Gizli Olan Şifreleme Teknikleri

Literatürde bulunan en ilkel şifreleme algoritmaları sadece alıcı ile gönderen arasında bilinen ve birbirinin tersi olan gizli bir algoritmaya dayanmaktadır. Bu tip algoritma ilk defa Sezar tarafından generallerine mesaj göndermek için kullanılmıştır. Her bir karakteri belirli bir miktar kaydırma prensibine dayanmaktadır. Bu şifreleme türünün diğer örnekleri ise Yer değiştirme ve Alfabe değiştirme şifreleridir.

3.1.2. Algoritması Açık Olan Şifreleme Teknikleri

Şifreleme algoritmalarının geniş bir kullanım alanına sahip olabilmesi için standart hale getirilmesi gerekir. Gizli algoritmaya dayalı şifreleme sistemleri, algoritmanın gizliliğinin sağlanması zorunluluğu nedeniyle sadece sınırlı bir kullanım alanına sahiptir ve standart hale getirilmesi mümkün değildir. Özellikle, bankalar ve

elektronik ticaret siteleri gibi yaygın iletişim ağlarına sahip kuruluşlar için gizli algoritmaya dayalı şifreleme sistemleri uygun değildir. Ayrıca, şifreleme sisteminin güncellenmesi gerektiğinde gizli algoritmaya dayalı şifreleme sistemleri esnek bir yapıya sahip olmadıklarından eski sistemin tamamen kaldırılıp yerine yenisinin kurulması gerekir.

İşte bu standart hale getirme ve güncelleme gereksinimini karşılamak için algoritması herkes tarafından bilinen şifreleme sistemleri tasarlanmıştır. Bu tip şifreleme sistemlerine, açık metin sadece gönderen ile alıcı tarafından bilinen bir anahtarla şifrelendiği için bir anahtara dayalı şifreleme sistemi denilir. Modern şifreleme tekniklerinin büyük bir çoğunluğu açık algoritmaya sahip teknikler kullanırlar. Anahtara dayalı şifreleme sistemleri anahtar sayısına göre simetrik ve asimetrik şifreleme teknikleri olarak ikiye ayrılır:

3.1.2.1. Simetrik Şifreleme Teknikleri

Hem şifreleme hem de çözme işlemi için tek bir anahtar kullanılır. Aynı zamanda bu teknik; şifreleme işleminde kullanılan anahtarı, gönderen ve alıcıdan başka kimsenin bilmemesi gerektiği için, gizli anahtar, anonim anahtar yada özel anahtar şifreleme olarak da adlandırılır. Ayrıca şifreleme ve çözme işlemlerinde tek bir anahtarla birbirinin simetriği olan algoritmalar kullanarak gerçekleştirildiğinden simetrik şifreleme teknikleri olarak da bilinirler. Bu şifreleme tekniğini kullanan algoritmalara örnek olarak XOR Şifreleme, DES, 3DES, IDEA, DESX, SKIPJACK, RC2, RC4, RC5 algoritmaları verilebilir.

Bunların en meşhuru Veri Şifreleme algoritması (Data Encryption Algorithm) olarak da bilinen DES'tir. DES 64 bit blok boyutu olan bir blok şifrelemedir. 64 bitlik düzyazı bloklarını 56 bitlik anahtarlar kullanarak 64 bitlik şifreli yazı bloklarına çevirir.Simetrik şifreleme tekniğinde gizli anahtarın taraflar arasında iletilmesi problemi bulunmaktadır. Bu gizli anahtar taraflar arasında iletilirken istenmeyen kişiler tarafından ele geçirilebilir.

3.1.2.2. Asimetrik Şifreleme Teknikleri

Simetrik şifreleme tekniğinde bulunan anahtar dağıtım problemini çözmek için şifreleme ve çözme işlemlerinin her birisi için ayrı ayrı anahtar kullanma prensibine dayanan bir şifreleme sistemi geliştirilmiştir. Bu sistemde şifreleme işlemi herkes tarafından bilinen anonim anahtarla yapılır. Bundan dolayı bu sistem anonim anahtar şifreleme sistemi olarak adlandırılır. Şifreleme ve çözme işlemi birbirinin simetriği olmayan (yani aynısı olan) algoritmalarla gerçekleştirildiğinden dolayı da asimetrik şifreleme sistemi olarak bilinir.

Asimetrik şifreleme algoritmalarına örnek olarak RSA, DSA, Diffie-Helman, ElGamal verilebilir. Bunlardan en meşhuru ve en yaygın olarak kullanılanı RSA dır. RSA algoritmasının büyük sayıların modüler aritmetiğine dayalı çok basit bir prensibi vardır. Gücünü ise büyük sayıları asal çarpanlarına ayırma probleminden alır.

Asimetrik şifreleme tekniğinde şifreleme ve çözme işlemi simetrik şifreleme tekniğine göre daha fazla zaman almaktadır. Bu zaman şifrelenecek mesajın ve anahtarların boyutlarına göre üssel olarak artar ve kırılması daha zordur.

3.2. Şifrelenen Mesaj Tipine Göre Şifreleme Tekniklerinin Sınıflandırılması

Şifreleme sistemlerinde, algoritmanın gizliliği ve anahtar kullanımından başka mesajın hangi biçimde şifreleneceği de önemlidir ve bu kritere göre şifreleme teknikleri iki kısma ayrılır.

3.2.1. Stream Şifreleme Teknikleri

Bazı algoritmalar stream şifreleme tekniğini kullanmaktadırlar. Bu algoritmalar mesajı bit bit yada bayt bayt ele alıp şifrelerler. Bu algoritmaların en önemlileri RC4 ve SEAL algoritmalarıdır.

3.2.2. Blok Şifreleme

Bazıları algoritmalar ise blok şifreleme tekniğiyle mesajı bit blokları halinde ele alıp şifrelerler. Algoritmaların büyük çoğunluğu Blok şifreleme kullanırlar.

Blok şifreleme stream şifrelemeye göre daha güvenlidir. Çünkü blok halinde şifrelenen verilerin içerisinden karakterleri tahmin etmek mümkün değildir. Fakat şifreleme ve çözme işleminin zaman karmaşıklığı daha fazladır.
Blok şifreleme tekniğinde güvenliği arttırmak için değişik modlar bulunmaktadır:
Elektronik Kod Kitabı (ECB-Electronic Code Book)
Şifre-Bloğu Zincirleme (CBC-Cipher Block Chaining)
Şifre Geri besleme Modu (CFB-Cipher Feedback Mode)
ECB modda her blok diğerlerinden bağımsız olarak şifrelenir. ECB kullanımında düzyazı kalıpları gizli değildir. Şifre kırıcılar tarafından tahmin edilebilirler.
CBC modda şifreli yazı bloğu, bir düzyazı bloğu ile şifrelenmemiş önceki düzyazı bloğuna şifreleme uygulanarak elde edilir. Bu bütün düzyazı kalıplarını gizler. Bir başlangıç vektörü (IV) işlem için 'tohum' (seed) olarak kullanılır.CFB kullanımında ise şifre nesnesi byte üreteci olarak çalışır. Ayrıca, bu mod stream şifrelemede de kullanılmaktadır.

4. Şifreleme Algoritmalarının Performans Kriterleri

Bir şifreleme algoritmasının performansını şu kriterlere göre belirleyebiliriz.

a) Kırılabilme süresinin uzunluğu.
b) Şifreleme ve çözme işlemlerine harcanan zaman (Zaman Karmaşıklığı).
c) Şifreleme ve çözme işleminde ihtiyaç duyulan bellek miktarı (Bellek Karmaşıklığı).
d) Bu algoritmaya dayalı şifreleme uygulamalarının esnekliği.
e) Bu uygulamaların dağıtımındaki kolaylık yada algoritmaların standart hale getirilebilmesi.
f) Algoritmanın kurulacak sisteme uygunluğu.

Teorik olarak simetrik anahtar kullanan Algoritması açık şifreleme algoritmaları, olası bütün anahtarları sırasıyla denemek yoluyla kırılabilir. Olası anahtarların denenmesi işlemi de, anahtarın uzunluğu arttıkça güçleşecektir.
Tablo. 1'de anahtar uzunluğuna göre şifreyi deneyerek bulma zamanları verilmiştir.

Tablo - 1 : Anahtar uzunluğuna göre şifreyi deneyerek bulma zamanları

Anahtar Uzunluğu	Sayı Değeri	10^6 şifre/s	10^9 şifre/s	10^{12} şifre/s
32 bit	$\sim 4x10^9$	36 dak	2.16 s	2.16 ms
40 bit	$\sim 10^{12}$	6 gün	9 dak	1 s
56 bit	$\sim 7.2x10^{16}$	1142 yıl	1 yıl 2 ay	10 saat
64 bit	$1.8x10^{19}$	292 000 yıl	292 yıl	3.5 ay
128 bit	$1.7x10^{38}$	$5.4x10^{24}$ yıl	$5.4x10^{21}$ yıl	$5.4x10^{18}$ yıl

Tablo-1'de görüldüğü gibi, teorik olarak kırılabilir kabul edilen algoritmaların pratikte kırılması, anahtar büyüdükçe imkansızlaşmaktadır.Açık anahtarlı şifreleme tekniklerinde kullanılan anahtarların uzunlukları simetrik anahtarlı şifreleme tekniklerinde kullanılanlardan genellikle çok daha büyüktür. Açık anahtar şifrelemeyi kırabilmek için, doğru anahtarı tahmin etmek değil, açık anahtardan ona uygun gizli anahtarı elde etmek gerekmektedir. Örneğin RSA için bu, iki büyük asal çarpanı olan büyük bir sayının çarpanlarına ayrılması anlamına gelmektedir. Bu işlem de teorik olarak yapılabilir olmasına karşın, pratik olarak gerçekleştirilmesi günümüz teknolojisiyle imkansızdır.

Asimetrik şifreleme algoritmaları simetrik şifrelemeden daha dayanıklı olmasına rağmen şifreleme ve çözme zamanının büyüklüğü nedeniyle şifreli veri iletişiminde kullanılmazlar bunların yerine simetrik şifreleme algoritmaları tercih edilir. Bunun yanında dijital imza ve kimlik doğrulama sistemlerinde simetrik anahtar algoritmaları yetersiz kalmaktadır. Çünkü aynı anahtarı bir çok kişiye dağıtmak bilgiyi kimin gönderdiğini sisteme kimin girdiğini tespit etmeyi sağlamaz. Fakat bu sistemlerde asimetrik şifreleme yöntemleri hem gücünden hem de çift anahtarlı yapıya sahip olmasından dolayı daha uygun olmaktadır.

Sonuç olarak; bir algoritmanın diğer algoritmaya karşı üstünlüğü yapılan uygulamaya göre değişmektedir. Yapılan uygulamaya hangi algoritmanın uygun olduğunu bulmak için yukarıda yapılan sınıflandırmada her bir şifreleme türünün avantajları ve dezavantajları yazılmıştır.Bizim uygulamamızda sadece algoritmalarda şifreleme ve çözme işlemine harcanan zaman karşılaştırılmıştır..

5. Şifreleme Uygulamalarının Tasnifi

Şifreleme uygulamaları tipik olarak üç dala ayrılır:

5.1. Gizliliği Sağlayan Şifreleme Uygulamaları

Bu tip uygulamalar bilginin sahibi haricindeki kişiler tarafından okunamamasını sağlarlar. Buna örnek olarak gizli mesajlaşmayı ve şifreli e-mail göndermeyi sağlayan PGP yazılımı verilebilir.Ayrıca elektronik alış verişte kullanıcı, web server, banka arasındaki iletişimin gizliliğini sağlayan SSL ve SET güvenlik protokolleri kullanılmaktadır.

Bu tip verilerin şifrelenerek iletişimini sağlayan uygulamalarda şifreleme ve çözme işlemlerinin harcadığı zaman önemli olduğu için simetrik şifreleme algoritmaları kullanılır. Bu uygulamalarda asimetrik şifreleme algoritmaları daha fazla güvenlik sağlasa da işlem zamanının büyüklüğünden dolayı tercih edilmemektedir.

5.2. Veri Bütünlüğünü Sağlayan Uygulamalar

Bu uygulamalar bilginin sahibine değişmeden gittiğini garanti ederler. Bunlara dijital imza kullanarak imzalı mesaj gönderen uygulamaları (örneğin PGP) verebiliriz. Dijital imzalar mesaj yada dökümlerin içeriğinin değişip değişmediğini sorgulamayı mümkün kılar.

5.3. İnkar Edememeyi Sağlayan Uygulamalar

Bu uygulamalar bilgiyi gönderenin, gönderdiğini inkar edememesini sağlarlar. İnkar edememeyi sağlayan uygulamalar dijital sertifika ve dijital imza sistemini kullanırlar. Örneğin SSL ve SET ile iletişimi sağlayan bir web sitesinden yapılan alış veriş dijital sertifikaya dayalı olarak gerçekleştiğinden dolayı inkar edilemez.

Özel anahtar tabanlı sistemlerin inkar edememeyi sağlaması ortak anahtar kavramından dolayı imkansızdır. Çünkü, gönderici gönderdiği bir mesajın alıcı tarafından uydurulduğunu iddia edebilir, alıcı da aynı anahtarı bildiği için bu durumun aksini ispatlayamaz. Açık anahtar tabanlı sistemlerde ise şifreleme anahtarı ile şifreyi çözme anahtarı farklı anahtarlar olduğundan inkar edememe sağlanabilir. Bunun en güzel örneği dijital imzalardır.

5.4. Doğrulama Uygulamaları

Bu uygulamalar karşısındaki nesnenin geçerli nesne olduğunu doğrulamayı sağlarlar. Bunlara kredi kartı bilgilerinin doğruluğunu sağlamada ve bir sisteme girişi denetlemede kullanılan asıllama sistemleri verebiliriz. Bunlar da dijital sertifika sistemlerini kullanırlar.Dijital imza ve dijital sertifika sistemleri ancak asimetrik şifreleme algoritmaları ile gerçekleştirilebilmektedir.

6.Kredi Kartı Uygulaması

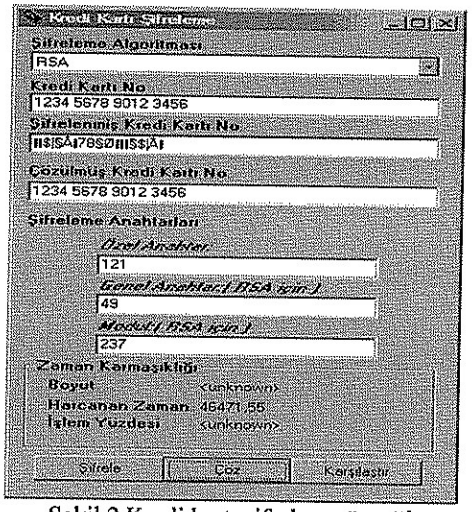
Bu uygulamanın amaçlarından biri simetrik ve asimetrik şifreleme algoritmalarında şifreleme ve çözme işlemlerinin nasıl meydana geldiği hakkında bir fikir vermektir. Diğer bir amacı ise şifreleme algoritmalarının şifreleme ve çözme zamanlarının karşılaştırılmasıdır. Bu iki özellik literatürde bulunan uygulamalarda bulunmaktadır. Bizim uygulamamamızın kendine özgü özelliği ise hem simetrik algoritmalar hem de asimetrik algoritmaların şifreleme ve çözme işlemlerinde harcadıkları zamanı karşılaştırabilmesidir.
Uygulamamızın ana penceresinde kullanılacak şifreleme algoritmasının seçildiği bir açılır kutu bulunuyor. Bu kutudan seçebileceğimiz algoritmalar şunlardır

Tablo – 2 : Uygulamada kullanılan şifrleme türleri

Algoritma Adı	Türü
SkipJack	Simetrik
Blowfish	Simetrik
CryptAPI	Simetrik
Twofish	Simetrik

XOR	Simetrik
Gost	Simetrik
TEA	Simetrik
RC4	Simetrik
DES	Simetrik
RSA	Asimetirk

Şifrelemek istediğimiz kredi kartı numarası ilgili kutuya yazılır. Seçilen algoritmanın kullanacağı anahtarlar şifreleme anahtarları kısmında belirlenir. Bu kısımdaki kutulardan genel anahtar ve modül sadece Asimetrik algoritma olan RSA seçildiğinde kullanılır.Şifrele butonuna basıldığında kredi kartı no şifrelenerek şifrelenmiş kredi kartı no kutusuna yazılır. Çöz butonuna basıldığında ise şifrelenmiş kredi kartı no çözülerek çözülmüş kredi kartı no kutusuna yazılır. (Şekil.2)



Şekil.2.Kredi kartı şifreleme örneği

Karşılaştır butonuna basıldığında 1000 karakterlik rastgele bir bilgi bütün algoritmalarla tek tek şifrelenip çözülerek bunların saniyede şifreleyip çözdükleri bilgi miktarı şifreleme tekniklerinin performansı olarak bir örnek üzerinde denenmiş ve aşağıdaki tabloda gösterilmiştir. (Şekil.3) Bu tabloya bakılarak asimetrik şifreleme algoritmalarının simetrik şifreleme algoritmalarından literatürde de belirtildiği gibi yaklaşık 10 kat yavaş olduğu sonucuna varabiliriz. Fakat bu sonuç karakter şifreleme için geçerlidir. Blok şifrelemede bu oran daha da büyüyecektir.

KARŞILAŞTIRMA SONUÇLARI

ALGORİTMA	ŞİFRELEME	ÇÖZME
Blowfish	2879 kbyte/s	2726 kbyte/s
CryptAPI	6919 kbyte/s	8646 kbyte/s
DES (Data	233 kbyte/s	236 kbyte/s
Gost	1257 kbyte/s	1206 kbyte/s
SimpleXOR	16070 kbyte/s	15722 kbyte/s
RC4	24844 kbyte/s	25071 kbyte/s
Skipjack	1113 kbyte/s	1044 kbyte/s
TEA, A Tiny	5855 kbyte/s	5074 kbyte/s
Twofish	1219 kbyte/s	1246 kbyte/s
RSA	92 kbyte/s	27 kbyte/s

Şekil.3.Şifreleme tekniklerinin performansı örneği

7.Sonuç ve Öneriler

Bilgi güvenliği kapsamında değerlendirilen bütün kavramlar bu güvenliği sağlayacak şifreleme tekniklerini kullanırlar. Bilişim teknolojilerindeki gelişime paralel olarak bilgi güvenliği disiplinler arası bir konu olduğundan gün geçtikçe önemi artmaktadır. Bu nedenle, çalışmamızda şifreleme tekniklerinin uygulama alanları, algoritmaları ve anahtar yapılarına göre bir tasnif çalışması yapılmıştır. Bu tasnif çalışmasının bu alanda çalışmak isteyenlere yön vermede önemli bir katkı sağlayacağı inancındayız.

Avrupa ve Amerika'da başlı başına bir bilim dalı olan kriptoloji kapsamında şifreleme algoritmaları lisans, yüksek lisans ve doktora seviyesinde ders olarak okutulmasına karşın ülkemizde sadece birkaç üniversitenin bilgisayar bölümlerinde okutulmaktadır.Bundan dolayı, şifreleme algoritmaları adında bir dersin özellikle teknik programlarda (Elektronik, Bilgisayar v.s) iki dönemlik ders olarak okutulmasının gereğine inanıyoruz.

Çalışmamızda yapılan uygulama ile de pratiğe aktarılacak daha geniş kapsamlı çalışmalara ve verilecek ders içeriğine bir fikir vermenin yanında çok güncel bir konu olan şifreleme tekniklerine ilgiyi arttırmak amaçlanmıştır.

Kaynaklar

1) Cryptography and Network Security, William Stallings Second Edition, 1998, Prentice- Hall
2) Handbook of Applied Cryptography, A. Menezes, S. Vanstone First Edition, 1996, CRC-Press
3) Managing Cisco Network Security, Michael J. Wenstom First Edition, 2001, Cisco -Press
4) RSA Algoritmasını Kullanan Şifreleme/Deşifreleme Yazılımının Tasarımı Metin Erhan Yüksek Lisans Tezi İ.T.Ü. 1993
5) NetLIFE Eylül 2000 Sayısı
6) PGP User's Guide, Essential Topics, Philip Zimmermann
7) Rivest,R.L.,A. Shamir and L. Adleman, "A Method For Obtaining Digital Signatures and Public-Key Cryptosystems, "Commun. ACM, Vol. 21, No.2, Sayfa. 120-126, Şubat 1978.
8) Algoritmalar ve Güvenlik Sistemleri, Ders Notu,M.Tektaş.,V.Topuz ,Marmara Üniversitesi T.B.M.Y.O. 2001, İstanbul
9) InfoNet Security Announcements Web Page
10) http://www.infonet.com.tr/security_anno/marc2002/index1.html
11) Bilgisayar güvenliği, http://www.ege.edu.tr/~bbankasi/dokuman/guvenlik/guvenlik.html
12) Elektronik kimlik belgesi (e-kimlik), http://e-kimlik.bilten.metu.edu.tr/tknyrd/ekimlik.html
13) SSL (Secure Socket Layer), http://www.ssl.com
14) SET (Secure Electronic Transactions), http://www.setco.org