ISTANBUL UNIVERSITY ENGINEERING FACULTY **YEAR : 2001 (169-178)**
JOURNAL OF ELECTRICAL & ELECTRONICS VOLUME : 1
NUMBER : 2

ELEKTRONÝK TÝCARET'TE SAYISAL ÝMZANIN KULLANIMI

M. Nusret SARISAKAL[1] K. Göksel MARANGOZ[2] Osman N. UÇAN[3]

[1] Ýstanbul Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliði Bölümü, 34850, Avcýlar, Ýstanbul
[2]DataMarket Bilgisayar Servis Hizmetleri A.ª ., Sistem Destek Bölümü
[3] Ýstanbul Üniversitesi, Mühendislik Fakültesi, Elektrik-Elektronik Mühendisliði Böl. 34850, Avcýlar, Ýstanbul

[1]e-posta: nsarisakal@istanbul.edu.tr [2]e-posta:gmarangoz@datamarket.com.tr
[3]e-posta:uosman@istanbul.edu.tr

ABSTRACT

This exercise has been a solution to the security problem of electronic commerce by using digital signature systems in which DSA and RSA algorithms have been analyzed. With the help of DSA and signature systems a like, users will be able to exchange messages with each other, build up trade links and in line with the expansion of the electronic commerce. In this exercise a digital signature system has been created by using RSA algorithm.

Key Words: *Security, Digital Signature, e-Commerce, RSA, DSA*

ÖZET

Bu çalýþmada, e-ticaret'te bir sorun olan güvenlik problemine çözüm olabilecek sayýsal imza sistemlerine genel bir giriþyapýlmýþDSA ve RSA algoritmalarý incelenmiþtir. DSA ve benzeri sayýsal imza sistemlerinin oluþturulmasýyla kullanýcýlar birbirlerine güvenli bir ºekilde mesaj gönderebilecek, iþ baðlantýlarý kurabilecek, e-ticaret'in yaygýnlaþmasý saðlanacaktýr. Bu çalýþmada RSA algoritmasýnýn kullanýldýðý bir sayýsal imza sistemi geliþtirilmiþtir.

Anahtar Kelimeler: Güvenlik, Sayýsal Ýmza, e-Ticaret, RSA, DSA

1. GÝRÝÞ

Günümüzde, Internet üzerinde, güvenlik ön plana çýkmaya baþlamýþtýr. Verilerin güvenilir bir biçimde aktarýmý ve eldesi için, kriptografi bilimi aracýlýðý ile çeþitli þifreleme, anahtarlama ve çözümleme algoritmalarý bulunmaktadýr. ª ifreleme, gerçekten deðerli bilgiyi organize suç örgütlerine, kötü niyetli kiºilere ve büyük hükümetlere karþý korumak için kullanýlabilecek bir yöntemdir. Kriptografi; kiºisellik, güven, eriºim kontrolü, elektronik ödeme, toplu (ºirket, ulus, vs.) güvenlik ve pek çok alan için ana araçlardan biri olmuºtur.

Kriptografi literatüründe kullanýlan terimleri sýrasý ile açýklayalým: Gönderici, bir mesajý gönderen, alýcý ise mesajý alan kiþi olarak tanýmlanýr. Bir mesajý, doðrusal olmayan fonksiyonlar kullanarak deðiþtirmeye, þifreleme denir. ª ifrelenmiº bir metni çözümlemeye, ters ºifreleme, yani matematiksel fonksiyonun tersini kullanarak, ºifrenin çözümlenmesi denir.

Gönderilecek metni M, ºifrelenmiº metni ª ile, ºifreleme fonksiyonunu da F ile gösterelim. Þifrelenmiþ metnin uzunluðu, gönderilecek metnin uzunluðundan fazla olabilir. Bu durumda, þifrelenmiþ metni sýkýþtýrma algoritmalarý yardýmý ile boy olarak küçültmeye çalýþýrýz. Bu tanýmlamalara göre þifreleme olayýnýn matematiksel modeli;

$$F(M) = {}^{a}$$

biçiminde verilir. ^{a} ifrenin çözümlenmesi için kullanýlacak ters þifreleme fonksiyonu ise aþaðýdaki gibidir:

$$^{a}(M) = F$$

Genel olarak her °ifreleme ve °ifre çözümleme algoritmasýnýn birbirlerinin ters fonksiyonlarý olmalarý gerektiði ortadadýr. Fakat, bu fonksiyonlarýn lineer olmamasý da iþleri ayrýca zorlaþtýrmaktadýr.

Kriptografi uzun süre, askeri ve diplomatik haberle°mede kullanýlmaktaydý. Fakat, veri þifreleme standartý (DES) 1974 yýlýnda bir IBM çalýþma takýmý tarafýndan geliþtirilip ve 1977'de ulusal bir standart olarak kabul edilince bu bilim dalý aðlar üzerinde iletilen verilerin þifrelenmesine de taþýndý.

Bir ki°i diðer bir kimseye bir mesaj göndermek istiyor ve baþka hiçbir kimsenin mesajý okumadýðýndan emin olmak istiyor. Ancak, baþka bir kiþinin mesajý açmasý veya elektronik iletiþimi duymasý olasýlýðý yüksektir. Mesajýn içeriðini istenmeyen kiþilerden saklamak için þifrelemeye encryption adý verilmektedir. ^{a} ifrelenmi° mesaja ciphertext (°ifreli-mesaj) denmektedir. ^{a} ifreli metinden düz-metni elde etme iþlemine decryption (çözme) adý verilir. ^{a} ifreleme ve çözme i°lemleri genelde bir anahtar kullanýlarak yapýlýr ve þifreleme i°leminden sonra çözme iþlemi sadece doðru anahtarýn bilinmesiyle gerçekle°tirilebilir.

2. ÞÝFRELEME ALGORÝTMALARI

Bazý kriptografik metotlar algoritmanýn gizliliðine dayanýr; bu tip algoritmalarýn þimdilerde sadece tarihi önemi vardýr ve gerçek-dünya ihtiyaçlarý için yeterli deðildirler.

Anahtar temelli algoritmalarýn iki çeþidi vardýr. Bunlar; simetrik (gizli-anahtar) ve asimetrik (açýk-anahtar) algoritmalarýdýr. Simetrik algoritmalarda °ifreleme ve çözme i°lemleri için ayný anahtar kullanýlýr veya çözme anahtarý þifreleme anahtarýndan türetilir. Asimetrik algoritmalarda ise þifreleme ve çözme için farklý anahtar kullanýrlar ve çözme anahtarý þifreleme anahtarýndan elde edilemez.

Simetrik algoritmalar stream cipher (akan °ifre) ve blok cipher olarak ikiye ayrýlabilir. Stream cipher'lar belli bir anda bir bitlik düz-metni þifreleyebilirken, blok cipher'lar pek çok biti alýp (Örneðin 64 bit) bunlarý tek bir blok olarak þifrelerler. Asimetrik þifreleme algoritmalarýnda bir anahtarýn halka açýk olmasý sözkonusudur. Þifreleme anahtarý özel veya gizli anahtar, þifre çözme anahtarý ise açýk anahtar olarak adlandýrýlmýþtýr. En yaygýn simetrik þifreleme algortimasý DES tir. RSA ise çok kullanýlan asimetrik þifreleme algoritmasýdýr.

Açýk anahtar þifreleme algoritmalarýnýn (ing. Public Key Cryptography) saðladýðý baþka bir olanak ise sayýsal imzalardýr. B'nin aldýðý mesajýn gerçekten A'dan gelip gelmediðini öðrenebilmesi için, A'nýn mesajý imzalamasý gerekir. A, mesajý yollarken, gizli anahtarýyla °ifreler. B, A'nýn þifrelediði mesajý A'nýn açýk anahtarýyla çözer. Böylece mektubun A'dan geldiðini ve deðiþtirilmediðini anlar.

3. E-TÝCARET'E GENEL BAKIÞ

Bilgisayar aðlarýnýn gündelik yaþama girmesi, dünyanýn çehresini deðiþtirmekte ve kaðýt üzerinde yapýlmakta olan hemen hemen her þey için, yepyeni bir ortam sunmaktadýr. Bu ortama Elektronik ortam denilmektedir. Ýnsanlarýn birbirleriyle yüz yüze konuþarak yaptýklarý birçok iþ yerini bilgisayarlarýn otomatik olarak yapabildikleri bir haberle°me türüne býrakmaya baþlamýþtýr: 'Elektronik Veri Deðiþimi - EVD', ya da ingilizcede kullanýldýðý gibi 'Electronic Data Interchange - EDI'. EDI sayesinde bilgisayarlar, kendilerine belirli bir yazýlýmla önceden öðretildiði þekilde ve kullanýcýlarýnýn istediði konularda, birbirleriyle otomatik olarak veri deðiþ tokuþu yapmakta, otomatik olarak yollanan ve alýcýsýna ulaþan verileri yine otomatik olarak deðerlendirmektedirler.

Günümüzde, teknolojinin etkilediði ticaretin yeni ismi olan Elektronik Ticaret, ürünlerin genelde bir að üzerinden elektronik olarak alým, satým, sipariþ ve bazen de ulaþtýrýlmasý olarak tarif edilebilir [1].

Elektronik ticaretin temel araçlarý olarak telefon, fax, televizyon, elektronik ödeme ve para transfer sistemleri, elektronik veri deði°imi (Electronic Data Interchange - EDI) ve Internet olarak altý ana araç sayýlabilir [1].

Klasik elektronik ticaret araçlarýndan, Telefon esnek ve interaktiftir. Faks ise interaktif olmasýna

raðmen gönderilen dokümanýn görüntü kalitesi iyi deðildir. Televizyon çok yaygýn olmasýna raðmen tek yönlü bir iletiþim aracýdýr. Ticaretin önemli destekleri olan elektronik ödeme ve fon transfer sistemleri (ATM, kredi kartlarý, borç kartlarý ve akýllý kartlar) sadece para aktarýlmasýnda kullanýldýðýndan ticaret sürecinde sýnýrlý bir bölüme hitab etmektedir [1].

Genel de elektronik ticaret, internet ve diðer aðlar üzerinden yapýlan ticaret olarak anlaþýlmaktadýr. Elektronik ticaretin çok yeni bir kavram olmamasýna karþýn, ticari iþlemler de bir veya daha fazla insan tarafýndan ses, görüntü ve yazýlý metinlerin ayný anda interaktif bir biçimde iletilmesi, zaman ve mekan sýnýrýnýn olmayýþý ve nispeten daha düþük maliyetlerle çalýþýlabilmesi þeklinde internet ortamýnýn sunduðu olanaklar, elektronik ticaret kavramýný hýzla gündeme getirmiþtir. Bu olanaklar internetin; diðer elektronik ticaret araçlarýna göre daha esnek olmasýný saðlar. Internet ortamý iletiþim ve ticaretin önündeki engelleri azaltmaktadýr [1].

Örneðin, internetten bir shareware tipi programýn indirilip beðenildiðinde bunun ücretinin ödenmesi bir elektronik ticarettir. Bir ürünü, örneðin bir kitabý, elektronik ortam kitapçýlarýnýn raflarýnda bulmak, bunun hakkýnda bilgi almak ve sipariºini vermekte bir elektronik ticarettir [1].

Daha detaylý olarak Elektronik Ticaret, elektronik ortamda açýk ve kapalý aðlar üzerinden yapýlan; mal (taþýnýr, taþýnmaz) ve hizmet (bilgi servisleri, danýþmanlýk, finans, hukuk, saðlýk, eðitim, ulaþtýrma vb.) ticareti, sayýsal biçime çevrilmiþ yazýlý metin, ses, video görüntülerinin iþlenmesi ve iletilmesi, ürün tasarýmý, üretim, doðrudan tüketiciye pazarlama, üretim izleme, sevkiyat izleme, tanýtým, reklam ve bilgilendirme, sipariº verme, sözleºme yapma, banka iþlemleri ve fon transferi, ortak tasarým geliºtirme ve mühendislik, kamu alýmlarý, elektronik para (sanal para) çýkarma, elektronik hisse alýþveriþi ve borsa, açýk arttýrma, sayýsal imza, e-noterlik, güvenilir üçüncü taraf iºlemleri, vergilendirme ve vergi toplama, fikri mülkiyet haklarýnýn transferi, kiralanmasý vb. iþlemler olarak belirtilebilir [1].

3.1. E-Ticaret'in Güvenliði

Kullanýcýlarýn E-ticarete güven duyabilmesinin önündeki en önemli teknik sorun, Internet üzerindeki bilgi güvenliðinin saðlanmasý ve güvenli ödeme yapýlabilmesidir. Bilgi güvenliðinden kastedilenler;

- Kimlik kanýtlanmasý,
- Bilginin bütünlüðünün bozulmamasý,
- Bilginin gizliliðidir.

Bilgi güvenliðinin saðlanabilmesi için, her kullanýcýya biri gizli diðeri açýk iki anahtar (sayý dizisi) veren açýk anahtarlý þifreleme algoritmalarý kullanýlmasý ve dünya üzerine yayýlmýþ bir açýk anahtar altyapýsýnýn (public key infrastructure) kurulmasý gereklidir.

Açýk anahtarlý þifrelemede kimlik kanýtlanmasý ve bilgi bütünlüðü, sayýsal imza (digital signature) ile saðlanmaktadýr. Sayýsal imza, yollanan mesajýn özetinin, imzalayanýn gizli anahtarýyla þifrelenmesiyle oluþur. Ýmzayý doðrulamak için, imzalayanýn açýk anahtarý kullanýlýr. Bu nedenle, açýk anahtarlar herkesin kullanýmýna açýk bir veri tabanýnda tutulmalý ve sürekli olarak güncellenmelidir. Bu veri tabanlarýný güncelleyen, anahtar üretimi, daðýtýmý ve yönetimini saðlayan, kiþilerin açýk anahtarlarý ve kimlik bilgilerini içeren elektronik kimlik belgelerini hazýrlayan onay kurumlarý veya güvenilir üçüncü kuruluºlar, birbirleriyle eþgüdüm içinde çalýþmalý, ulusal ve uluslararasý düzeylerde, kendilerine benzer kuruluºlarla karþýlýklý olarak birbirlerini tanýmalýdýrlar.

Dünya pazarýndaki en tanýnmýþ onay kurumu olan VeriSign, RSA Bilgi Güvenliði, Ameritech ve Visa þirketlerinin ortaklýðýyla kurulmuþtur. Açýk aðlar üzerinden birbirine ulaþmak isteyen iki kullanýcý, örneðin Avrupa'de, ABD'de veya Avustralya'da olabileceði gibi, kimliklerini karþýlýklý olarak hýzlýca kanýtlayabilmeleri, bütün onay kurumlarýnýn uyum içinde çalýþýyor olmasýna baðlýdýr. Açýk anahtar altyapýsýndan amaçlanan da, eºgüdüm ve etkileºim içinde çalýþmasý gereken onay kurumlarý, güvenilir üçüncü kuruluþlar, sayýsal noterler, zaman damgasý vurma veya anahtar bulma kurumlarý gibi kuruluþlarýn saðladýðý ulusal ve küresel hizmetlerin bütünüdür.

ABD'de açýk anahtar altyapýsý kurma sorumluluðunu üstlenen Ulusal Standartlar ve Teknoloji Geliºtirme Enstitüsü – NIST; AT&T, Motorola, VeriSign gibi kuruluþlarýn da bulunduðu 10 onay kurumunun yazýlýmlarýný inceleyerek, bütün bu yazýlýmlarýn uyum içinde çalýþmasý için gerekli kýsýtlarý belirlemektedir.

Onay kurumlarýnýn önemli bir bölümünü de banka ve benzeri kuruluþlarýn oluþturmasý çok doðaldýr. Örneðin, SET(Secure Electronic Transactions) standardýný geliþtiren MasterCard ve Visa, bu standardýn gerektirdiði onay kurumu, sertifika otoritesi hizmetlerini de verenmektedir.

E-Ticaret'teki güvenlik sorunu güvenli ileti°im saðlayan SSL, SHTTP gibi protokolleri kullanýlmasý veya bilginin þifreleme algoritmalarý ile °ifrelenmesiyle çözülebilir.

Sayýsal sertifikalardan oluþan yapýsý ile kredi kartýnýn gerçek sahibinin alýþveriþ yaptýðýný garanti etmesi ve E-ticaret'te hem satýcý, hem alýcý hem de aracý finansal kurumlar arasý bir güvenlik tamponu oluº turan SET (Secure Electronic Transaction) standardý ile temel ödeme sistemlerinin yaygýnlaþmasý ve on-line alýþveriþte bir sorun olan, güvenlik probleminin büyük ölçüde çözülmesi hedeflenmi°tir.

4. SAYISAL ÝMZALAR

Bazý açýk-anahtar algoritmalarý sayýsal imzalar üretmek için kullanýlmaktadýr. Bir sayýsal imza, bazý gizli anahtarlar kullanýlarak oluþturulmuþ küçük bir bilgi parçasýdýr ve imzanýn gerçekten uygun bir özel anahtar kullanýlarak üretildiðini doðrulamak için kullanýlabilecek bir açýk-anahtar vardýr. Ýmzayý üretmek için kullanýlan algoritma öyle olmalýdýr ki gizli anahtarý bilmeden geçerli sayýlabilecek bir anahtar üretmek mümkün olmasýn.

Sayýsal imzalar mesajýn gerçekten istenilen göndericiden geldiðini doðrulamak için kullanýlýr. Bunlar ayrýca dokümanlarý timestamp (zaman-pulu) ile i°aretlemek için de kullanýlabilir; güvenilen bir kiþi dokümaný imzalar ve kendi anahtarý ile zaman pulunu imzalar, böylece dokümanýn belirtilen zamanda var olduðu doðrulanýr. Sayýsal imzalar bir açýk-anahtarýn belirli bir kiþiye ait olduðunu doðrulamak veya onaylamak için kullanýlabilir. Bu iþlem, anahtarýn ve bunun sahibi hakkýndaki bilginin kombinasyonunun (combination), güvenilen bir anahtar ile imzalanmasý suretiyle yapýlýr. Üçüncü bir kiþinin (güvenilen anahtarýn sahibi) sayýsal imzasý, açýk anahtar ve açýk-anahtarýn sahibi hakkýndaki bilgiler genelde sertifikalar (certificates) olarak adlandýrýlýr. Üçüncü kiþi (Third Party) anahtarýna güvenilmesinin sebebi, bunun ba°ka bir güvenilir anahtar ile imzalanmýþ olmasýndan dolayýdýr. Sonuçta bazý anahtarlar güven hiyerarþisinin kökü olmalýdýr.

Daðýlmýþ bir altyapýda evrensel olarak kabul edilmiþ köklerin olmasýna gerek yoktur ve her kesimin farklý güvenilir kökleri olabilir. Keyfi bir dokümanýn bir sayýsal imzasý tipik olarak dokümandan alýnan bir mesaj özeti (message digest) hesaplamasý ve imzalayan hakkýnda bilgi, bir zaman-pulu, vs. ile ili°kilendirilerek oluþturulur. Ortaya çýkan dizi uygun bir algoritma kullanýlarak imzalayanýn özel anahtarý kullanýlarak þifrelenir. Sonuçta elde edilen þifrelenmiþ bitler bloðu imzadýr. Bir imzayý onaylamak için önce anahtarýn, anahtara sahip olduðu düþünülen kiþiye ait olup olmadýðýnýn belirlenmesi ve sonra da kiþinin açýk-anahtarý kullanýlarak imzanýn çözülmesi gerekir. Eðer imza uygun bir °ekilde çözülürse ve bilgi mesajýnkiyle uyuþursa (uygun mesaj özeti vs.) imzanýn geçerli olduðu kabul edilmektedir.

4.1 SAYISAL ÝMZA SÝTEMLERÝ

Sayýsal imza sistemi, bir imzalama ve bir doðrulama iþlemlerinden oluþmaktadýr. **A** imzalayan **B** ise alýcý, **M** imzalanacak mesaj, S_A A'ya ait imzalama transformasyonu, V_A A'ya ait doðrulama transformasyonu olarak kabul edilir ve sonuçta doðru yada yanlýþ þeklinde bir çýktý üretir. S_A, A tarafýndan imza üretmek için kullanýlmakta ve gizli tutulmaktadýr.

4.1.1. Ýmzalama Ýþlemi

A tarafý M mesajý için aþaðýdaki þekilde bir imza oluº turur.

$s = S_A(M)$ hesaplanýr.

(M,S) çifti B'ye gönderilir. S'ye M mesajýnýn imzasý adý verilir [2].

4.1.2. Doðrulama Ýþlemi

Mesajdaki S imzasýnýn A tarafýndan üretildiðini doðrulamak için B tarafýnda aþaðýdaki iþlemler yapýlmaktadýr;

A'nýn doðrulama fonksiyonunu (V_A) elde eder.

$U = V_A(M,S)$'i hesaplar

Eðer U="doðru" ise imza A tarafýndan üretilmi°tir.

5. SAYISAL ÝMZA MEKANÝZMALARI

5.1. DSA (DÝGÝTAL SÝGNATURE ALGORÝTHM)

Aðustos 1991'de ABD Ulusal Standartlar ve Teknolojileri Enstitüsü Sayýsal Ýmza Standardýnda (DSS) kullanýlmak üzere, Sayýsal Ýmza Algoritmasýný (DSA) önerdi [2]. DSA bir hükümet tarafýndan önerilen ilk sayýsal imza sistemidir. Ayný zamanda Elgammal sisteminin deðiþik bir versiyonudur.

5.1.1. DSA Parametreleri

DSA aþaðýdaki parametreleri kullanmaktadýr.

- **P**, bir asal modüldür. $2^{L-1} < p < 2^{L}$, **512 £ L £ 1024** ve **L**, 64'ün bir katý olmalýdýr.
- **q, (p-1)'ý**n bir asal çarpanýdýr. $2^{159} < q < 2^{160}$
- $g=h^{(p-1)/q} \bmod p$. **h**, **1<h<p-1** ve $h^{(p-1)/q} \bmod p>1$ olan herhangi bir tamsayýdýr.
- **x** rastgele bir sayýdýr. **0 < x < q**
- $y = g^{x} \bmod p$
- **k** rasgele bir sayý. **0 < k < q**

p, q ve **g** tamsayýlarý herkese açýk olabilir ve bir grup kullanýcý tarafýndan ortak olarak kullanýlabilir. Bir kullanýcýnýn gizli ve açýk anahtarlarý sýrasýyla **x** ve **y** dir. k parametreleri her imza için yeniden üretilmelidir.

5.1.2 Ýmza üretimi

Bir **M** mesajýnýn imzasý aþaðýdaki eþitliklere göre üretilen **r** ve **s** sayýlarýdýr.

$$r = (g^{k} \bmod p) \bmod q$$
$$s = (k^{-1}(SHA(M) + xr)) \bmod q$$

Yukarýda k^{-1}, **k**'nýn **q** modülüne göre çarpýmsal tersidir.SHA(M) güvenli çýrpma algoritmasýnýn ürettiði 160 bitlik bir katardýr.

5.1.3. Ýmzanýn Doðrulanmasý

Ýmzalanmýþ bir mesajdaki imzanýn doðrulanmasýndan önce **p, q** ve **g** ile imzalayanýn açýk anahtarý doðrulamayý yapacak tarafa asýllanmýþbir þekilde duyurulmalýdýr.

M', **r'** ve **s'**, sýrasýyla **M**, **r** ve **s**'nin alýcý tarafýndan alýnmýþ versiyonlarý olsun. Alýcý önce **0 <r' <q** ve **0 < s' < q** olup olmadýðýný kontrol eder. Eðer bu þartlar saðlanmýyorsa imza reddedilir. Eðer saðlanýyorsa alýcý aþaðýdaki hesabý yapar.

$$w = (s')^{-1} \bmod q$$
$$u_1 = ((SHA(M'))\, w) \bmod q$$
$$u_2 = ((r')\, w) \bmod q$$
$$v = (((g)^{u_1} (y)^{u_2}) \bmod p) \bmod q$$

Eðer **v = r'** ise imza doðrulanmýþtýr. Aksi taktirde mesaj reddedilir.

Yukarýda **q** parametresinin sayýsý 160 bit olarak gösterilmiþti. Ancak p'nin uzunluðu 512 ve 1024 arasýnda 64'ün bir katý olacak þekilde deðiþebilir. 512 bitlik bir **p** saldýrýlara karþý yeterince güvenli olmayacaktýr [2,3]. **p** için tavsiye edilen uzunluk 768 ya da 1024 bittir.

5.2. SHA-1 Mesaj Doðrulama Algoritmasý

Güvenli hash algoritmasý (SHA-1 - Secure Hash Algorithm), sayýsal imza standardýnda (DSS - Digital Signature Standart) açýkça belirtildiði gibi, federal uygulamalarda güvenli bir Hash algoritmasý ihtiyaç duyulduðunda, sayýsal imza algoritmasý (DSA – Digital Signature Algorithm) ile birlikte kullanýlýr. 2^{64} bitten daha kýsa uzunlukta bir mesaj için SHA-1, mesajýn 160 bit uzunluðunda, "mesaj özeti" isminde bir özet tanýmýný içerir. Mesaj özeti, mesaj için bir imza üretimi sýrasýnda kullanýlýr. SHA-1 ayný zamanda imzanýn doðrulanmasý iþlemi sýrasýnda, alýnan mesaj sürümü için bir mesaj özeti hesaplamak için de kullanýlýr. Ýletim sýrasýnda mesajda oluþacak herhangi bir deðiþiklik, yüksek ihtimalle, farklý bir mesaj özeti ile sonuçlanacak ve imzanýn doðrulanmasý baþarýsýz olacaktýr.

SHA-1 takip eden özelliklere sahip olmasý için tasarlanmýþtýr. Verilen bir mesaj özetine karþýlýk gelen bir mesajýn bulunmasý veya ayný mesaj özetini üretecek iki farklý mesajýn bulunabilmesi cebirsel olarak olasý deðildir [4].

5.2.1. Bit Dizileri ve Tam Sayýlar

Aþaðýdaki terimler dizgesi, kullanýlacak olan bit dizileri ve tam sayýlarla ilgilidir :

a. *Onaltýlýk bir rakam*, {0, 1, … , 9, A, … , F} kümesinin bir elemanýdýr. Bir onaltýlýk rakam, 4 bitlik bir diziyi temsil eder. **Örnek:** 7 = 0111, A = 1010.

b. Bir *kelime*, 8 onaltýlýk rakam dizisi þeklinde temsil edebilecek bir 32 bitlik diziye eþittir. Bir kelimeyi 8 onaltýlýk rakama çevirmek için, her 4 bitlik dizi, yukarýda (a)'da belirtildiði gibi, onaltýlýk eþdeðerine çevrilir.
Örnek : 1010 0001 0000 0011 1111 1110 0010 0011 = A103FE23

c. *0 ile $2^{32} - 1$ arasýndaki (sýnýrlar dahil) bir tam sayý*, bir kelime olarak gösterilebilir. Tam sayýnýn en düþük anlamlý dört biti, kelime gösterimindeki en saðdaki onaltýlýk rakam ile gösterilir.
Örnek : tam sayý $291 = 2^8 + 2^5 + 2^1 + 2^0 = 256 + 32 + 2 + 1$, onaltýlýk kelime 00000123 ile gösterilir.

Eðer z, $0 \quad z < 2^{64}$, aralýðýnda bir tam sayýysa,
$z = 2^{32} x + y$,
$0 \quad x < 2^{32}$ ve $0 \quad y < 2^{32}$.
'x' ve 'y', kelime X ve Y olarak gösterilebildiðinden 'z', kelime çifti (X, Y) olarak temsil edilebilir.

d. *blok* = 512 bitlik dizi. Bir blok (örneðin B), 16 kelimelik bir seri ile gösterilebilir.

5.2.2 Kelimeler Üzerinde Ýþlemler

Aþaðýdaki mantýksal iþlemler, kelimelere uygulanabilir :

a. Bit düzeyinde mantýksal kelime iþlemleri
$X \wedge Y$ = X ve Y'nin bit düzeyinde mantýksal "ve"si
$X \vee Y$ = X ve Y'nin bit düzeyinde mantýksal "veya"sý
X XOR Y= X ve Y'nin bit düzeyinde mantýksal "XOR"u
$\sim X$ = X ve Y'nin bit düzeyinde mantýksal tersi

Örnek :
01101100101110011101001001111011
XOR
01100101110000010110100110110111

=00001001011110001011101111001100

b. *Ýþlem X + Y* þu þekilde tanýmlanýr : X ve Y kelimeleri, x ve y tam sayýlarýný $0 \quad 2^{32}$ ve $0 \quad y < 2^{32}$ aralýðýnda temsil eder. Pozitif tam sayýlar n ve m için n mod m, n'in m'e bölünmesi sonucu kalan olsun. Hesaplarsak,

$$\mathbf{Z = (x + y) \bmod 2^{32}}$$

O halde, $0 \quad z < 2^{32}$ aralýðýnda z'yi bir kelimeye dönüþtürürsek,

Z = X + Y olur.

c. *Dairesel sola kaydýrma iþlemi* $S^n(X)$, X bir kelime ve n, $0 \quad n<32$ aralýðýnda bir tam sayý, þu þekilde tanýmlanýr :

$$\mathbf{S^n(X) = (X << n) \acute{U} (X >> 32-n)}$$

Yukarýda X << n þu þekilde elde edilir : X'in en solundaki n biti atýlýr ve sonucu saðdan itibaren sýfýrlarla doldurulur (sonuç hala 32 bittir). X >> n, X'in en saðýndaki n bitin atýlýp sonucun soldan itibaren sýfýrlarla doldurulmasý ile saðlanýr. Böylece $S^n(X)$, X'in sola doðru n pozisyon dairesel kaymasýna denktir.

5.2.3. Mesaj Doldurma

SHA-1, giriþ olarak saðlanan bir mesaj veya veri dosyasý için bir mesaj özeti hesaplamak için kullanýlýr. Mesaj veya veri dosyasý bir bit dizisi olarak ele alýnmalýdýr. Mesajýn uzunluðu, mesajýn içindeki bitlerin sayýsýdýr (boþ mesaj, 0 uzunluðuna sahiptir). Eðer mesajýn içindeki bitlerin sayýsý 8'in katýysa, sadelik için mesajý onaltýlýk olarak ifade edebiliriz. Mesaj doldurmanýn amacý, doldurulmuþ bir mesajýn toplam uzunluðunu, 512'nin katý yapmaktýr. SHA-1 mesaj özetini hesaplarken, 512 bitlik bloklarý sýrasal olarak iþler. Aþaðýda, bu doldurmanýn nasýl gerçekleþtirildiði açýklanmýþtýr. Bir özet olarak, 512 × n uzunlukta doldurulmuþ bir mesajýn üretilmesi için, mesajýn sonuna sýrasýyla bir "1", m adet "0" ve 64 bitlik bir tam sayý eklenir. 64 bitlik tam sayý *l*, orjinal mesajýn uzunluðudur. Bundan sonra mesaj, SHA-1 tarafýndan 512 bitlik n blok olarak iþlenecektir.

Bir mesajýn $l < 2^{64}$ uzunluðunda olduðunu varsayalým. SHA-1'e giriþ olmadan önce, mesaj saða aþaðýdaki þekilde kaydýrýlýr :

a. "1" eklenir. Orjinal mesaj "01010000" ise, "010100001" olur.

b. "0"lar eklenir. "0"larýn sayýsý, mesajýn orjinal uzunluðuna baðlýdýr. Son 512 bitlik bloðun son 64 biti, orjinal mesajýn uzunluðu *l* için ayrýlýr.

Örnek : Aþaðýdaki bit dizisi orjinal mesajýmýz olsun :

01100001 01100010 01100011 01100100 01100101.

Adým (a)'dan sonra mesaj þu hale gelir :

01100001 01100010 01100011 01100100 01100101 1.

l = 40 iken, yukarýdaki bitlerin sayýsý 41 olduðundan, 407 adet "0" eklenir ve toplamda 448 bit olur. Bu, onaltýlýk olarak, aþaðýdaki diziyi verir :

61626364	65800000
00000000	00000000
00000000	00000000
00000000	00000000
00000000	00000000
00000000	00000000
00000000	00000000.

c. Orjinal mesajdaki bitlerin sayýsý *l*'nin 2 kelimelik gösterimi ile saðlanýr. Eðer $l<2^{32}$ ise, ilk kelime tamamýyla sýfýrdan oluþur. Bu iki kelime doldurulmuþ mesaja eklenir.

Örnek: Orjinal mesajýn (b)'deki gibi olduðunu düþünelim. O zaman *l* = 40 olur (*l*, hiçbir doldurma iþlemi yapýlmadan önce hesaplanýr). 40'ýn iki kelime gösterimi, onaltýlýk düzende, 00000000 00000028 dir. Artýk doldurulmuþ mesajýmýzýn son hali, onaltýlýk düzende, aþaðýdaki þekildedir :

61626364	65800000
00000000	00000000
00000000	00000000
00000000	00000000
00000000	00000000
00000000	00000000
00000000	00000000
00000000	00000028.

Kaydýrýlmýþ mesaj, her n > 0 için, 16n kelime içerir. Kaydýrýlmýþ mesaj, onaltýlýk kelime ve mesajýn ilk karakterlerini (veya bitlerini) içeren her M_i için, M_1, M_2, …, M_n'den oluþan n bloklu bir dizi olarak ele alýnýr.

5.2.4. Kullanýlan Fonksiyonlar

SHA-1'de bir dizi mantýksal fonksiyon, f_0, f_1, …, f_{79}, kullanýlýr. Her f_t, 0 t 79, 32 bitlik kelimeler üzerinde iþlem yapar ve çýkýþ olarak 32 bitlik bir kelime üretir. f_t, B, C ve D kelimeleri için þu þekilde tanýmlanýr:

$f_t(B,C,D) = (B \wedge C) \vee (\sim B \wedge D)$ (00 t 19)

$f_t(B,C,D) = B$ XOR C XOR D (20 t 39)

$f_t(B,C,D) = (B \wedge C) \vee (B \wedge D) \vee (C \wedge D)$ (40 t 59)

$f_t(B,C,D) = B$ XOR C XOR D (60 t 79)

5.2.5. Kullanýlan Sabitler

SHA-1'de bir dizi sabit, K_0, K_1, …, K_{79}, kullanýlýr. Onaltýlýk olarak aþaðýdaki gibi listelenebilirler:

K_t = 5A827999 (00 t 19)
K_t = 6ED9EBA1 (20 t 39)
K_t = 8F1BBCDC (40 t 59)
K_t = CA62C1D6 (60 t 79)

5.2.6. Mesaj Özetini Hesaplamak

Mesaj özeti, doldurulmuþ mesajýn son hali kullanýlarak hesaplanýr. Hesaplama, her biri 5 tane 32 bitlik kelimeden ve 80 adet 32 bitlik kelimenin oluþturduðu bir diziden oluþan iki tampon kullanýr. Ýlk 5 kelimelik tampondaki kelimeler, A, B, C, D, E olarak adlandýrýlýr. Ýkinci 5 kelimelik tampondaki kelimeler, H_0, H_1, H_2, H_3, H_4 olarak adlandýrýlýr. 80 kelimelik dizideki kelimeler, W_0, W_1, …, W_{79} olarak adlandýrýlýr. TEMP isimli tek kelimelik bir tampon da, ayrýca kullanýlýr.

Mesaj özetini oluþturmak için, 16 kelimelik bloklar, M_1, M_2, …, M_n, sýrasýyla iþlenir. Her M_i'nin iþlenmesi, 80 adýmdan oluþur.

Herhangi bir blok iþlenmeden önce H_j'ler, onaltýlýk düzende, aþaðýdaki þekilde atanýr :

H_0 = 67452301
H_1 = EFCDAB89
H_2 = 98BADCFE
H_3 = 10325476
H_4 = C3D2E1F0

[a] imdi M_1, M_2, …, M_n, aþaðýdaki þekilde, iºlenebilir :

a. M_i'yi, W_0 en soldaki kelime olacak ºekilde 16 kelimeye bölün : W_0, …, W_{15}.

b. t = 16'dan 79'a kadar, $W_t = S^1(W_{t-3}$ XOR W_{t-8} XOR W_{t-14} XOR $W_{t-16})$ olsun.

c. A = H_0, B = H_1, C = H_2, D = H_3, E = H_4 olsun.

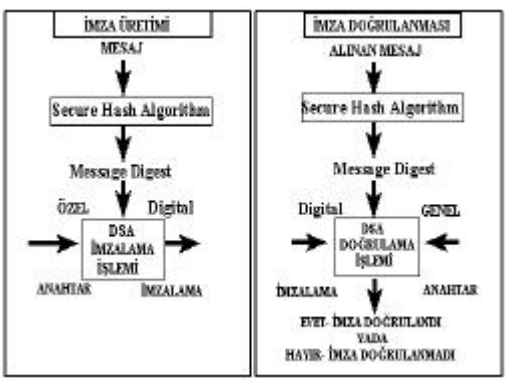
d. t = 0'dan 79'a kadar, aþaðýdaki iþlemler gerçekleºtirilir:
TEMP = $S^5(A)$ + $f_t(B,C,D)$ + E + W_t + K_t;
E = D; D = C; C = $S^{30}(B)$; B = A; A= TEMP;

e. $H_0 = H_0 + A$, $H_1 = H_1 + B$, $H_2 = H_2 + C$, $H_3 = H_3 + D$, $H_4 = H_4 + E$ olsun.

M_n iºlendikten sonra, 160 bitlik mesaj özeti, aþaðýdaki 5 kelime ile gösterilebilir :

H_0, H_1, H_2, H_3, H_4

Aþaðýdaki þekilde Secure Hash Algorithm(SHA) ile DSA nýn birlikte nasýl kullanýldýðý gösterilmiºtir.



6. YAYGIN OLARAK KULLANILAN BÝR SAYISAL ÝMZA MEKANÝZMASI - RSA ALGORÝTMASI

RSA public-key algoritmasý 1977 yýlýnda R.**R**ivest, A.**S**hamir ve L.**A**dleman tarafýndan bulunmuº ve daha sonra public-key cryptography (açýk anahtar þifrelemesi) ye uygun biçimde geliºtirilmiþtir. Bu algoritma, açýk anahtar þifreleme sistemleri ve sayýsal imza sistemlerinde güvenli bir þekilde kullanýlmaktadýr. Internet üzerinde elektronik iletiºimde ºifreleme iþlemlerinde yaygýn olarak kullanýlmaktadýr. Bu algoritma ayný zamanda Netscape Navigator ve Microsoft Explorer web tarayýcý programlarýnýn uygulamalarý olan Secure Socket Layer (SSL) ve kredi kartý iþlemleri için Secure Electronic Transaction (SET) protokollerinde de kullanýlmaktadýr. Ayrýca S/MIME, PEM, MOSS ve PGP gibi gizli haberleºme protokolleri temel olarak RSA kullanmaktadýr.

RSA Algoritmasý açýk anahtar þifreleme yönteminin temel uygulamasýdýr. Bu þifreleme algoritmasýnýn diðer bir iyi yönüde, önceden aralarýnda hiçbir görüþme yapmamýþ olan alýcý ve vericinin kendi aralarýndaki iletiþimin güvenli bir ortamda yapýlmasýdýr. Ýnternet iletiþimi güvenliði tam olmayan kanallar üzerinden iºlemektedir. Bu durumda açýk anahtar þifreleme yöntemleri ile internet üzerinde güvenlik saðlanmýþtýr.

6.1. RSA ALGORÝTMASININ ÝÞLEYÝÞÝ

RSA Algoritmasý aþaðýdaki gibi iþlemektedir [4].

- Özel ve Açýk anahtar çifti üretilir.

1. **P** ve **Q** ºeklinde çok büyük (mesela,1024 bit) iki tane birbirinden farklý asal sayý bulunur.
2. **N = P*Q** ve **Z = (P-1) * (Q-1)** hesaplanýr.
3. **Z** ile ortak böleni 1 olacak ºekilde bir **E** sayýsý bulunur.
4. Açýk anahtar **[E,N]** olarak belirlenir.
5. **D = E^1 mod Z** olacak ºekilde bir **D** sayýsý bulunur.
6. Özel anahtar ise **[D,N]** olarak belirlenir.

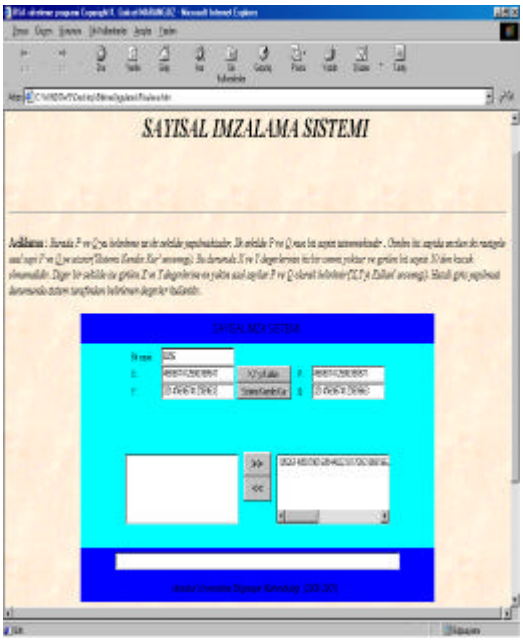
- Þifrelenecek mesajý M kabul edersek bu mesaj ikilik olarak **2^k < N** olacak ºekilde **k** bitlik kýsýmlara ayrýlýr **[M=M(1)+M(2)+M(3)+..+M(n)]** Daha sonra þifreleme için her bir kýsma **C (i) = $M(i)^E$ mod N** iþlemi uygulanýr.
- Özel anahtar **[D,N]** kullanýlarak þifre çözülür. **[$M(i)=C(i)^D$ mod N]**

7. SAYISAL ÝMZA SÝSTEMÝ UYGULAMASI

Geliþtirilen sayýsal imza uygulamasý, dýþarýdan girilen parametreler sonucunda ºifrelenmek istenen metni P ve Q adlý iki asal sayý yardýmý ile

þifreleyen bir uygulamadýr. Bu program içinde birçok class dosyayý çalýþtýran bir java appletinden oluþmaktadýr.

Programýn çalýþma prensibi kýsaca þöyledir:



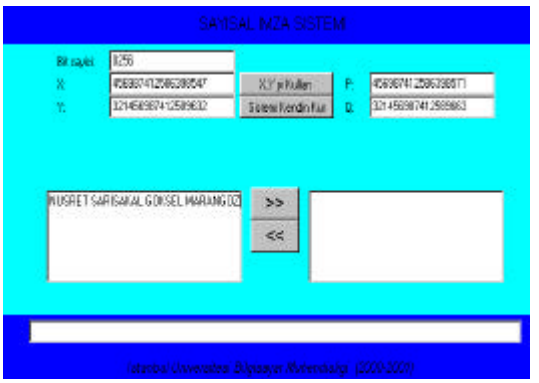
Burada P ve Q yu belirleme iºlemi iki ºekilde yapýlmaktadýr. Ýlk þekilde P ve Q nun bit sayýsý istenmektedir. Girilen bit sayýsý seçilen iki rasgele asal sayý P ve Q ye atanmaktadýr. (Sistemi Kendin Kur seçeneði). Bu durumda X ve Y deðerlerinin hiçbir önemi yoktur ve girilen bit sayýsý 50 den küçük olmamalýdýr. Diðer bir þekilde ise girilen X ve Y deðerlerine en yakýn asal sayýlar P ve Q olarak belirlenir (X,Y'yi Kullan seçeneði).

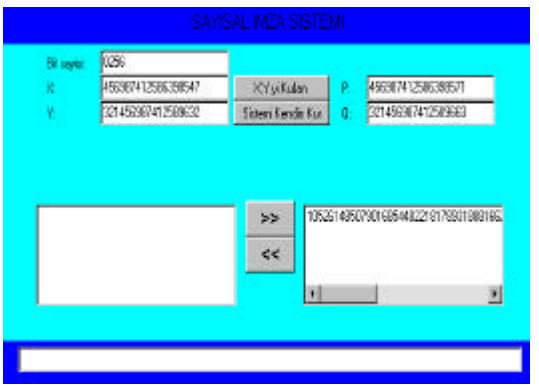
Bit Sayýsý adlý kýsma 50 bit den az olmamak kaydý ile bit sayýsý girilir. Buradaki amaç ºifreleme iºlemini gerçekleºtirmek için kullanacaðýmýz P ve Q asal sayýlarýný oluºturmak için kaç bitlik bir sonuç üreteceðimizin belirlenmesidir.

Girilen deðer neticesinde 'Sistemi Kendin Kur' adlý butona basarak P ve Q asal sayýlarý üretilmiþ olur. Bu üretilen sayýlar kullanýlarak girilecek metin için algoritma ile ºifrelenerek üretilen bir sayýsal imza deðeri bulunur.

Þifreleme iþlemini gerçekleþtirmede kullanýlan P ve Q asal sayýlarýnýn üretiminin bir diðer yolu ise X ve Y adlý dýþarýdan iki parametre girerek olabilir. Bu parametrelere girilen deðerler sonucunda program bize bu sayýlara en yakýn asal sayýlarý üretir. Böylece biraz önce anlatýlan iºlemler tekrarlanarak ºifreleme iºlemi gerçekleºmiº olur.

Aþaðýdaki þekillerde görüldüðü gibi X ve Y parametreleri girildikten sonra P ve Q deðerleri hesaplanmaktadýr. Bu deðerle kullanýlarak girmiþ olduðumuz metinden bir sayýsal imza üretilecektir. Bu uygulama ile e-ticaret'te önemli olan kimlik doðrulama iºlemi gerçekleºtirilmiº olacaktýr.





Yukarýdaki þekilde üretilen sayýsal imza görülmektedir.

9. SONUÇ VE ÝLERÝYE YÖNELÝK ÇALIªMALAR

Hayatýn her alanýnda bilgisayarlarýn yaygýn kullanýmý ve özellikle bilgisayar aðlarýnýn geliþmesi, Dünyanýn dört bir yanýndaki bilgiye eriþmeyi kolaylaþtýrýrken güvenlik sorunlarýný da beraberinde getirmektedir. Gizlilik ile birlikte en önemli sorunlardan olan kimlik doðrulama problemi, kritik iºlemlerin elektronik ortamda yapýlmasýnýn önündeki en büyük engellerdem biridir.

Bu çalýþmada üzerinde durulmayan ancak kimlik doðrulama konusunun kanuni boyutu açýsýndan büyük önem taþýyan sertifika otoriteleri yada güvenilir üçüncü kiþiler konusunda hükümetlere büyük görev düþmektedir. Amerika Birleþik Devletlerinin bazý eyaletlerinde (Utah, Georgia) ve Avustralya'da sayýsal imzalar konusunda yasal düzenlemeler getirilmektedir [5].

E-Ticaret'in yaygýnlaþmasý güvenlik yöntemlerinin artmasýna baðlý olduðu görülmektedir. Bu güvenlik yöntemlerinde sayýsal imzanýn yeri küçümsenmeyecek kadar önemlidir.

Ýnternet uygulamalarýnýn giderek arttýðý günümüzde, geliþmelerin gerisinde kalmamak için ülkemizde de bu konudaki çalýþmalara hýz verilmelidir. Bizler güvenlik konularýnda kullanýlmakta olan diðer algoritmalarýn ve bunlarýn performans analizlerini yaparak yeni yöntemler geliþtirmek için çalýþmalarýmýza devam etmekteyiz.

KAYNAKLAR

1. SARISAKAL M. Nusret, KARAHOCA Adem, DES Algoritmasýný Kullanan Güvenilir Bir E-Posta Ýletim Uygulamasý: Tuðra, Ý.Ü. Mühendislik Fakültesi Elektrik & Elektronik Dergisi, Vol. 1, No. 1, pp 23-31, Mayýs 2001.

2. Menezes, Alfred J., Van Oorschot, Paul C. And Vanstone S. A., 1997,Handbook of Applied Cryptography, CRC Press.

3. Schneier B, 1995, Applied Cryptography:Protocols Algorithms and Source Code in C., Wiley.

4. Stinson D. R., Cryptography Theory and Practice, CRC Press, 1995, Florida

5. TÜBÝTAK-BÝLTEN Sunuþ 1998, Sunuþu gerçekleþtiren : Melek D. Yücel