Kriptoloji ve Uygulama Alanları: Açık Anahtar Altyapısı ve Kayıtlı Elektronik Posta

Sedat Akleylek[1,3], Hamdi Murat Yıldırım[2], Zaliha Yüce Tok[3]
[1] Ondokuz Mayıs Üniversitesi, Bilgisayar Mühendisliği, Samsun
[2] Bilkent Üniversitesi, Bilgisayar ve Bilişim Sistemleri Bölümü, Ankara
[3] ODTÜ Uygulamalı Matematik Enstitüsü, Ankara
sedat.akleylek@bil.omu.edu.tr, hmurat@bilkent.edu.tr, zalihayuce@gmail.com

Özet: Bu çalışmada, Akademik Bilişim 2011'de verilen "Kriptoloji ve Uygulama Alanları: Açık Anahtar Altyapısı ve Kayıtlı Elektronik Posta" başlıklı bir günde verilen eğitimde anlatılan temel kavramlar özetlenmiştir. Kriptolojinin temelleri, elektronik imzanın kullanıldığı açık anahtar altyapısı ve bunların güncel uygulaması olan kayıtlı posta konusunda açıklayıcı bilgiler verilmiştir. Okuyucunun kriptoloji ve uygulama alanları hakkında daha fazla Türkçe kaynağa erişmesi amacıyla çeşitli kaynaklar belirtilmiştir.

Anahtar Sözcükler: Kriptoloji, E-İmza, Açık Anahtar Altyapısı, Kayıtlı Elektronik Posta

Cryptology and Its Applications: Public Key Infrastructure and Certified Electronic Mail

Abstract: In this study, fundamental concepts presented in Akademik Bilişim 2011 as one day seminar titled "Cryptology and Its Applications: Public Key Infrastructure and Certified Electronic Mail" are summarized. Information about basics of cryptography, Public Key Infrastructure which uses the electronic signature and their current application, certified electronic mail is clarified. We give some directions to the reader for more detail about cryptology and its applications.

Keywords: Cryptography, E-Signature, Public Key Infrastructure, Certified Electronic Mail

1. Giriş

Bilgisayarın keşfi ve Internet kullanımının yaygınlaşması sonucunda geleneksel iletişim yerini elektronik iletişime bırakmıştır. Bunun sonucunda elektronik ortamlarda yapılan işlemler için güvenlik kavramı çok fazla önem kazanmaktadır. Günümüzde çok sık kullandığımız Internet üzerinden yaptığımız haberleşmeler ve işlemlerin güvenliğini sağlamak için disiplinlerarası çalışmalarla geliştirilen birçok yöntemin birlikte kullanıldığı söylenebilir. Yalnız burada kullanılan yöntemlerin birçoğunun dayandığı bir matematiksel tekniklerin bütününe kriptografi denir.

Kriptografi, bir bilginin istenmeyen taraflarca anlaşılmayacak bir hale dönüştürülmesinde kullanılan tekniklerin bütünü olarak açıklanabilir. Kriptografi gizlilik, bütünlük, kimlik denetimi, inkâr edememe gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemleri içermektedir

- Gizlilik : Bilgi istenmeyen kişiler tarafından anlaşılmamalıdır.
- Bütünlük : Bilginin iletimi sırasında hiç değiştirilmediği doğrulanmalıdır.
- Kimlik Denetimi : Gönderici ve alıcı birbirlerinin kimliklerini doğrulamalıdır.
- İnkar Edememe : Gönderici bilgiyi gönderdiğini ve alıcı bilgiyi aldığını inkar edememelidir.

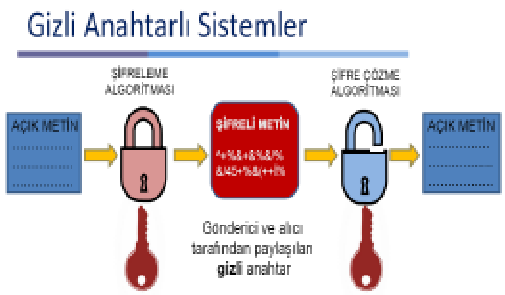
Kriptanaliz, şifrelenmiş yani anlamsız bir metinden doğru metni bulma yöntemidir. Kriptoloji ise kriptografi ve kriptanalizin birlikteliği için kullanılmaktadır. Başka bir deyişle Kriptoloji, haberleşmede veri güvenliğini sağlayan kripto cihazlarını, bu cihazlarda kullanılan algoritmaların güvenilirliğini araştıran, matematik bazlı elektrik ve elektronik mühendisliği, bilgisayar bilimleri, bilgisayar mühendisliği, istatistik ve fizik bölümlerini ilgilendiren disiplinlerarası bir alandır.

Bu yazımızda kısaca kriptografinin gelişimden, gizli ve açık anahtarlı sistemlerden, elektronik imza ve açık anahtar altyapısından, kayıtlı elektronik posta, kriptografik algoritmaların bazı günümüz uygulamalarında kullanımlarından bahsedeceğiz ve kriptografi eğitimi için kaynaklar önereceğiz.

2. Kriptolojinin Gelişimi

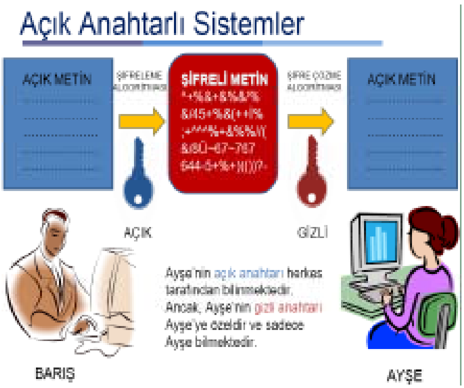
1970'lere kadar sadece askeri ve resmi kurumların kullandığı kriptografik yöntemler, 1976 yılında Diffie ve Hellman'ın önerdiği "Açık Anahtarlı Sistemler" kavramıyla bir devrim geçirmiştir. 1976 yılına kadar var olan şifre sistemlerinin güvenilirlikleri anahtarın gizliliğine dayanmaktaydı. Gizli Anahtarlı Sistemler olarak adlandıracağımız bu sistemlerde, şifreleme ve şifre çözme işlemi için önceden belirlenen anahtarlar kullanılmakta ve şifre sistemlerinin de hep bu tür olabileceği düşünülmekteydi. Ancak, Açık Anahtarlı Sistemlerin keşfiyle aynı anahtarın hem alıcı hem de gönderici tarafından bilinmeden de güvenli haberleşmenin sağlanabileceği ortaya çıkmıştır. Ayrıca, Açık Anahtarlı Sistemler gizliliğin yanı sıra veri bütünlüğü, kimlik kanıtlama ve inkâr edememe konularına da çözüm getirerek birçok yeni uygulamaları da beraberinde getirmiştir.

Gizli Anahtarlı Sistemlerin çalışma prensibi Figür 1'de gösterilmiştir. Gizli Anahtarlı Sistemlerin işleyişinde en çok yer değiştirme ve karıştırma işlemleri kullanılmaktadır. Örneğin, en çok bilinen basit şifrelerden birisi olan Sezar şifresinin çalışma mantığı, şifrelenmek istenen harfin, kendisinden sonra gelen 3. harf ile yer değiştirilmesidir. Sezar şifresi ile ABC, ÇDE olarak şifrelenebilir. Günümüzdeki hesaplama gücünün yüksek olması ve iletişimin bilgisayar ortamında yapılmasından ötürü, bu tip yer değiştirme ve karıştırma işlemleri şekil değiştirmiştir. Bu tip yer değiştirmeler için çeşitli matematiksel uygulamalar bulunmaktadır. Örneğin, tüm dünyada kullanılan ve güvenilir olduğu bilinen AES (Advanced Encryption Standard) algoritması eski tip yer değiştirme işlemlerini kullanmasının yanı sıra, matematiksel yöntemleri de kullanmaktadır. Gizli Anahtarlı Sistemler yer değiştirme ve karıştırma işlemlerini temel aldığından ötürü çok kısa sürede çok büyük boyutlardaki verileri şifreleyebilirler. Aynı hızda şifre çözme işlemini de gerçekleştirebilirler.



Figür 1. Gizli Anahtarlı Sistemlerin İşleyişi

Gizli Anahtarlı Sistemlerde, alıcı ve gönderici aynı anahtarı kullandığından, bu gizli anahtarın paylaşılması bir problemdir. Gizli anahtar öyle bir paylaşılmalıdır ki, sadece alıcı ve gönderici gizli anahtarın ne olduğunu bilsin. Gizli Anahtarlı Sistemlerdeki anahtar paylaşım problemine Açık Anahtarlı Sistemler ile çözüm gelmiştir. Açık Anahtarlı Sistemlerin işleyişi Figür 2'de resmedilmiştir. Açık Anahtarlı Sistemlerde, açık (herkes tarafından bilinen) ve gizli (kişiye özel) anahtar olmak üzere iki çeşit anahtar kullanılmakta ve bu sayede, Açık Anahtarlı Sistemler ile herkesin birbirlerini tanımadan bile gizli bir şekilde haberleşmesi sağlanmaktadır. İki farklı anahtarın kullanıldığı Açık Anahtarlı Sistemlerin çalışabilmesi için matematiksel problemlere ihtiyaç duyulmaktadır. Ayrıca, bu sistemlerin güvenilir olarak adlandırabilmesi için bu problemlerin çözümünün de zor olduğunun gösterilmesi gerekmektedir. Bunlara bağlı olarak günümüzde en çok kullanılan açık anahtarlı sistemlerden RSA çarpanlara ayırmanın zorluğuna, DSA (Digital Signature Algorithm) ve ECDSA (Elliptic Curve Digital Signature Algorithm) ise sonlu cisimler ve eliptik eğri üzerindeki ayrık logaritma probleminin zorluğuna dayanmaktadır. Açık Anahtarlı Sistemlerin en çok kullanıldığı alanlar Gizli Anahtarlı Sistemler için anahtar paylaşımı ve elektronik imza uygulamalarıdır.



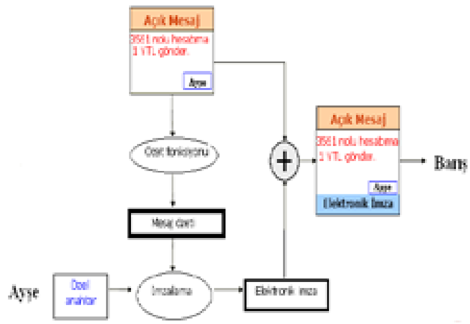
Figür 2. Açık Anahtarlı Sistemlerin İşleyişi

3. Elektronik İmza ve Açık Anahtar Altyapısı

Kamu kurumlarında yapılan birçok işlem için kimlik kanıtlanması ve imza atılması gerekmektedir. Bu tür işlemler elektronik ortamda yapılmak istendiği zaman ortama uygun kimlik kanıtlama ve imza atılması gerekmektedir. Elektronik imza (e-imza) elektronik ortamlarda ıslak imzanın yerine geçmekte ve bireyin kimliğini içermektedir. E-imza, gönderilmek istenen belgeye eklenen, kimlik doğrulama amacıyla kullanılan elektronik veridir.

E-imza, Açık Anahtarlı Sistemlerin en yaygın kullanılan bir uygulamalarından birisidir. E-imza oluşturmak ve doğrulamak için çeşitli bilgilere ihtiyaç bulunmaktadır. E-imza oluşturmak için öncelikle hangi e-imza algoritmasının (RSA, DSA, ECDSA) kullanılacağının belirlenmesi gerekmektedir. Buna ek olarak, e-imzanın hangi platformda başka bir deyişle, kriptografik donanımlar ile atılacağı önemlidir.

Akıllı kartlar (Smart card) en çok kullanılan ve bilinen kriptografik donanımlardan birisidir ve kredi kartı boyutlarındadır. Akıllı kartlar üzerinde, şifreleme, şifre çözme, imzalama, imza doğrulama ve anahtarları depolama gibi hizmetleri sunmaktadır. Akıllı kartı kullanabilmek için bilgisayar ile uyumlu çalışacak akıllı kart okuyuculara ihtiyaç vardır. Akıllı kartın içine bireyin gizli anahtarı yüklendikten sonra e-imza atılmaya hazırdır. Bireyin gizli anahtarı kendisine özel üretildiğinden ve sadece kendisinde olduğundan, attığı imzaların kopyası yapılamaz. Ayrıca, göndericinin yolladığı mesaj iletişim anında değiştirilirse, alıcı bunu e-imzada kullanılan algoritmalar sayesinde anlayabilir. Figür 3 e-imzanın nasıl atıldığını anlatmaktadır.



Figür 3. e-imza ile gönderilen veri için yapılan işlemler

E-devlet uygulamaları ve kriptolojinin ortak çalışma sahası sadece e-imza ile sınırlı değildir. E-devlet ile kağıt üzerinde yapılan her işlem elektronik ortama geçtiğinden, daha önceden fiziksel olarak korunan kağıt üzerindeki bilgilerin elektronik ortamda yetkisiz kişiler tarafından görünmesini, değiştirilmesini engellemek gerekmektedir. Güvenli elektronik arşivleme olarak adlandırılabilecek bu saklama işlemi için verinin özelliğine göre (kim/kimler tarafından oluşturuldu, geçerlilik süresi gibi) çeşitli güvenlik seviyeleri belirlenmelidir. Bu tip işlemler için Gizli Anahtarlı Sistemler ile Açık Anahtarlı Sistemler belli bir sıraya göre kullanılmalı ve kullanılan şifrelerin/algoritmaları anahtar boyları ihtiyaca uyumlu bir şekilde seçilmelidir.

4. Kayıtlı Elektronik Posta

Klasik posta sisteminde herhangi birisi postaneye gidip, zarfın üzerindeki gönderici bölümüne herhangi bir isim yazarak size mektup yollayabilir. Bu tip istenmeyen mektupların önüne geçmek ve mektubun alıcıya ulaştırılıp ulaştırılmadığından emin olunmak amacıyla iadeli taahhütlü posta sistemi geliştirilmiştir. Bu sistemde, gönderici, mesajının alıcıya ulaştırılıp ulaştırılmadığı bilgisine sahiptir ve aynı zamanda alıcı da gönderici bölümünde yazan ismin kesinlikle gönderici olduğunu bilmektedir. Kamu kurumlarının, özellikle Adalet Bakanlığı, Çalışma ve Sosyal Güvenlik Bakanlığı'nın kişilere özel bildirimleri (tebligat) bildiğimiz iadeli taahhütlü posta yoluyla yapılmaktadır. İletişim tekniklerinde elektronik postanın yaygın kullanımının klasik tebligat ile birleştirilmesi, bireylerin bu tip bildirimlerden anında haberdar olmasını sağlayacaktır. Bu tip sistemlere kayıtlı elektronik posta (KEP – Registered e-mail) adı verilmektedir. KEP sistemlerinin kullanım alanlarının, sadece bireylere yapılan resmi tebligatlar olmadığı bilinmektedir. Klasik posta yoluyla elimize ulaşan her haber ve fatura (su, elektrik, telefon, doğalgaz, v.b.) KEP sistemleri ile iletibilir. Bu sistemin en önemli avantajı, istenilen mesajın karşı tarafa iletildiğinden emin olunmasıdır. Alıcı ise bu mesajın kesinlikle mesajın gönderici bölümünde yazandan geldiğinden emin olmaktadır. Bu kimlik denetimi e-imza kullanımı ile gerçekleşmektedir. Kâğıt ortamında yapılan bildirimlerin, çevre ve ekonomiye olan zararı bilinmektedir. Her yıl bu tip bildirimler için binlerce ağaç kesilmekte ve bunların kamu kurumlarına olan maliyetleri milyonlarca TL'yi bulmaktadır. Elektronik ortamda yapılan bu bildirimler için bu tipte sorunlar bulunmamaktadır.

Elektronik ileti kullanımında karşılaştığımız en büyük sorunlardan birisi reklâm veya başka içerikli istenmeyen mesajlardır (spam elektronik posta). KEP sistemlerinin hayata geçirilmesi ile istenmeyen içerikli mesajların da önüne geçirilecektir. Kısacası, KEP ile daha verimli, çevreci ve maliyeti düşük elektronik haberleşme sağlanacağı öngörülmektedir. Ayrıca, KEP sistemlerinin farklı yorumlanması ile kurumlar arasındaki güvenilir ve kayıtlı iletişim ve arşivleme sorunlarına çözüm bulunacağı açıktır. Önümüzdeki senelerde KEP sistemleri ve türevlerinin günlük hayatımızda nasıl aktif olarak yer alacağını hep birlikte göreceğiz.

5. Kriptografik Algoritmaların Günlük Yaşamdaki Diğer Uygulamaları

Kriptografik algoritmaların çalışacağı ortamlar ihtiyaca yönelik olarak farklılık göstermektedir. Örneğin, kredi kartları, akıllı kartlar, uydu alıcıları. Burada sadece akıllı kartların bazı kullanım alanlarından bahsedeceğiz. Akıllı kartların uygulama alanları oldukça geniştir : e-kimlik (Akıllı kart tabanlı elektronik kimlik kartı), e-pasaport (elektronik pasaport). Bu tip uygulamalarda sayısal kimlik bilgileri ve biometrik bilgiler akıllı kart içine yerleştirilmektedir. Kimlik doğrulama yöntemleri ve akıllı kart üzerindeki verinin saklanması için de kriptografik yöntemlerin düzgün bir biçimde kullanılması gerekmektedir.

Kriptolojinin günlük yaşamdaki kullanım alanı sadece e-devlet ve elektronik ileti ile sınırlı değildir. Günlük yaşamımızın bir parçası olan elektronik ticaret (e-ticaret – online alışveriş), İnternet bankacılığı, kablosuz cihazlar, cep telefonları, kredi kartları, CD/DVD gibi teknolojik uygulamalarda güvenliğin sağlanması oldukça önemlidir.

E-ticaret, mal ve hizmetlerin satınalınması veya satılması işleminin elektronik ortamlarda yapılması olarak tanımlanabilir. Yapılacak bu işlemlerden önce örnek e-ticaret sitesinde verilerin korunması için bazı önlemler alınması gerekmektedir. E-ticaret sisteminde müşteriler çeşitli kişisel bilgilerini sisteme girmektedirler. Web tarayıcı kullanılarak yapılan bu işlem sonucundaki veriyi işleneceği ortama güvenilir olarak götürmek için SSL (Secure Sockets Layer) protokolü kullanılır. SSL, Netscape firması tarafından geliştirilen ve İnternet üzerinden güvenli veri aktarımı sağlayan kriptografik teknikleri içermektedir. SSL ile gizlilik, bütünlük ve kimlik denetimi gibi web ortamındaki güvenlik problemlerine çözüm bulunmuştur. SSL'nin uygulanabilmesi için sunucu sertikasına ihtiyaç vardır. Bir sunucu sertifikasında, sertifikayı veren kurum ve organizasyon sahibi hakkında bilgi bulunur. SSL'in çalışma mantığı temelde 3 aşamadan oluşur. İlk aşamada kullanılacak olan şifreleme algoritmaları üzerinde anlaşılır. Sonraki aşamada üzerinde anlaşılan Açık Anahtarlı Sistem kullanılarak anahtar değişimi ve sertifika doğrulanması gerçeklenir. Son aşamada ise ikinci aşamada elde edilen anahtar ile Gizli Anahtarlı Sistem kullanılarak veriler şifreli bir biçimde karşı tarafa yollanır.

Internet bankacılığı günümüzde herkes tarafından yaygın olarak kullanılmaktadır. İnternet bankacılığı, şubeye gidilerek alınan hizmetlerin Internet üzerinden sunulması ile meydana gelmiştir. Günün her saat diliminde kullanılabilinen Internet bankacılığının güvenliğini sağlamak için çeşitli uygulamalar bulunmaktadır. Veriler transfer işlemleri sırasında mutlak suretle şifrelenmelidir. Bunu sağlamak için SSL uygulamasının aktif hale getirilmesi gerekmektedir. Ayrıca e-imza ve sertifika kullanımı güvenliği arttırıcı diğer önlemlerdir. İnternet bankacılığına girişi daha güvenli hale getirmek için tek kullanımlık anahtarlar (one time pad) üreten kriptografik donanımlar bankalar tarafından müşterilerinin hizmetine sunulmuştur. Tek kullanımlık anahtar ile Internet şubesine her seferinde farklı bir şifre ile girme olanağı sağlanmaktadır.

Günümüzde cep telefonları her yerde kesintisiz haberleşmeyi sağlayabilmek için bir ihtiyaç haline gelmiştir. İnsanların telefon konuşmalarının dinlenmesinin popüler olduğu bu dönemde, bunları engellemenin temel yolu kriptografiden geçmektedir. Cep telefonları aracılığıyla yaptığımız görüşmeler Gizli Anahtarlı Sistemlerin bir üyesi olan A5 şifresi veya türevleri ile şifrelenmektedir. Kriptoloji alanındaki gelişmeler ışığında, burada kullanılan şifrelerin güvensiz oldukları ispatlanmıştır. Kablolu telefon hatları başka bir deyişle, sabit hatlar üzerinden yapılan görüşmeler içinde benzeri şifreler kullanılmaktadır. Bu çerçevede, telefon görüşmelerinin dinlenememesi için kriptografik anlamda güvenlik ölçütlerini sağlayan şifrelerin kullanılması ihtiyacı bulunmaktadır.

6. Öneriler

Bu yazımızda, kriptografinin tarih boyunca insanların ihtiyaçlarına bağlı olarak sürekli değişim geçirdiğini ve günümüzde birçok alanda uygulamasının olduğunu anlatmaya çalıştık. Kâğıt-kalem ortamından elektronik ortama geçiş ve verilerin taşınması, depolanmasıyla birlikte bilgi güvenliği kavramının önemi ortaya çıkmıştır. Elektronik ortamlarda yapılan işlemlere güven kriptografik yöntemler ile sağlanmaktadır. Ülkemizde Internet kullanımının yaygınlaşması, klasik posta sistemlerinin elektronik ortamlardaki uyarlamaları ve akıllı kartların daha etkin kullanımı ile bu ortamlardaki güvenlik sorununa önem verilmesi gerektiğini bir kez daha göstermektedir. Bu ortamlardaki olası güvenlik sorunlarının önüne geçebilmek ve yeni teknolojileri güvenli bir biçimde uygulamaya geçirebilmek için Kriptografi alanında çalışmaların takip edilmesi ve güncel gelişmelerin uygulanması bir ihtiyaçtır.

Kriptoloji konusunda eğitim almak isteyenler, Tübitak Bilgem "Kriptoloji Eğitimleri" web sayfasındaki [8] duyuruları düzenli olarak takip edebilirler. Bir kriptografi eğitimi/dersi beraberinde, eğitim amaçlı, temel kriptosistemleri uygulamalar ile anlatan ve kriptanalizleri sunan ve de modern kriptografik algoritmalar ve protokollerin animasyonlarına yer veren Cryptool yazılımı [9], ODTÜ Uygulamalı Matematik Enstitüsü (UME) Kriptografiye giriş notları [10], D.R. Stinson'ın kitabı [11] ve de uygulamalı kriptografi el kitabı [12] kullanılabilir. Kriptoloji, e-imza, X.509 sertifikalar ve Açık Anahtar Altyapısı konularında temel tanımlar için bir başvuru kaynağı "Tübitak UEKAE, Açık Anahtar Altyapısı Eğitim Kitabı" dır [13]. Kapak konusu Kriptoloji olan TÜBİTAK Bilim ve Teknik Dergisi'nin 500. sayısındaki kriptoloji ile ilgili makaleler [14] ve ODTÜ UME AAA grubunun web sayfasında önerilen makaleler [15] okunabilir, E-imza mevzuatları

[16] ve standartları [17] incelenebilir. Bunlara ek olarak, bilgi güvenliği ve kriptoloji alanındaki akademik gelişmelerin paylaşıldığı Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı [18] ve Ağ ve Bilgi Güvenliği Sempozyumu [19] ülkemizde düzenlenmektedir.

7. Teşekkür

Bu çalışma [1] ve [2] nolu kaynakların verilen eğitim içeriğine uygun bir şekilde güncellenmiş halidir. Bu çalışmanın hazırlanmasında bizden desteğini esirgemeyen ve yorumları ile katkıda bulunan Prof.Dr. Ersan Akyıldız'a teşekkür ederiz.

8. Kaynaklar

[1] Akyıldız, E., Akleylek, S., "Kriptolojideki Gelişmeler", TMMOB Sanayi Kongresi, 2007, s.173-178.

[2] Akleylek, S., Akyıldız, E., "Bilgi Güvenliğinde Matematik: Kriptografi", Popüler Bilim Dergisi, 2011.

[3] Çimen, C., Akleylek, S. ve Akyıldız, E., "Şifrelerin Matematiği : Kriptografi", ODTÜ Geliştirme Vakfı Yayıncılık, İstanbul, 2007.

[4] Diffie, W. ve Hellman, M., 1976, "New Directions in Cryptography", IEEE Transactions on Information Theory, vol.IT-22, pp.644-654.

[5] West, D., "Global E-Government, 2007".

[6] Elgamal, T., ve Hickman, K., Secure Socket Layer Applciation Program Apparatus and Method, US Patent No. US 5,657,390, 1997.

[7] Akademik Bilişim 2011, Kriptoloji Eğitim Notları, [Çevrim içi]: http://www.ab.org.tr/ab11/sunum/Kriptoloji-Egitim/

[8] "BİLGEM - Kriptoloji Eğitimleri - Kriptoloji Eğitimleri." [Çevrim içi]: http://www.kamusm.gov.tr/dosyalar/kitaplar/aaa/index.html [Erişim: 10-06-2012].

[9] "CRYPTOOL1 – Kriptografi Eğitim Yazılımı", [Çevrim içi]: http://www.cryptool.org/en/cryptool1 [Erişim: 10-06-2012].

[10] "ODTÜ Uygulamalı Matematik Enstitüsü, Kriptografiye Giriş Notları" , [Çevrim içi]: http://www3.iam.metu.edu.tr/iam/images/6/69/Kriptolojiyegiri%C5%9F-ersanali.pdf [Erişim: 10-06-2012].

[11] Stinson, D. "Cryptography Theory and Practice.", [Çevrim içi]: http://cacr.uwaterloo.ca/~dstinson/CTAP.html [Erişim: 10-06-2012].

[12] Menezes, A.J., van Oorschot, P. C. ve Vanstone, S. A. , "Handbook of Applied Cryptography.", [Çevrim içi]: http://cacr.uwaterloo.ca/hac/ [Erişim: 10-06-2012].

[13] "Açık Anahtar Altyapısı Eğitim Kitabı.", [Çevrim içi]: http://www.kamusm.gov.tr/dosyalar/kitaplar/aaa/index.html [Erişim: 10-06-2012].

[14] "TÜBİTAK Bilim ve Teknik Dergisi'nin 500. Sayı", [Çevrim içi]: http://www.tubitak.gov.tr/sid/80/cid/15027/index.htm;jsessionid=8AB1AA13B69DA451AF8F4B3568108808 [Erişim: 10-06-2012].

[15] "Yazı / Makale, AAA - Araştırma Grubu.", [Çevrim içi]: http://www.pki.iam.metu.edu.tr/yazi_makale.html [Erişim: 10-06-2012].

[16] "E-imza Mevzuat, AAA - Araştırma Grubu." [Çevrim içi]: http://www.pki.iam.metu.edu.tr/mevzuat.html [Erişim: 10-06-2012].

[17] "E-imza Standartlar, AAA - Araştırma Grubu." [Çevrim içi]: http://www.pki.iam.metu.edu.tr/standartlar.html [Erişim: 10-06-2012].

[18] "Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı" [Çevrim içi]: http://www.iscturkey.org [Erişim: 10-06-2012].

[19] "Ağ ve Bilgi Güvenliği Sempozyumu" [Çevrim içi]: http://www.abgs.org.tr [Erişim: 10-06-2012].