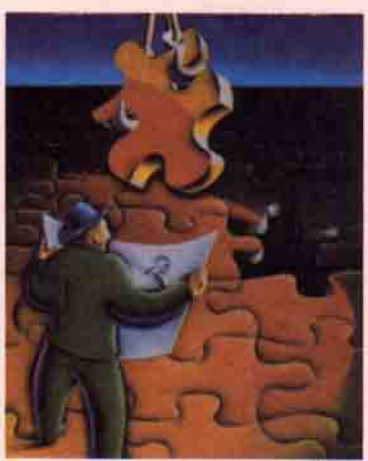
Bilgisayar Dünyası
Sinan Göktepeli

Kişiye Özel?

YURT dışındaki birine birşeyler anlatacaksınız. Ne yaparsınız? Mektup yazabilirsiniz. Ama mektup çok yavaş gider. Bir de bunlar özel ve gizli kalması gereken bilgilerse (şirketinizin gelecek yıl yapacağı yatırımlar veya milyonlarca dolarlık araştırmaların sonuçları ya da aile içi dedikodular), herhangi biri zarfı kolayca açıp, sonra hiç dokunulmamış gibi kapatabilir. Mektup riskini göze alamıyorsanız telefon ya da faksı deneyebilirsiniz. Ancak bu da pek önerilecek bir şey değildir. Ne de olsa iki kabloyu birbirine bağlayabilen herkes, telefon dinlemeyi ve faks mesajını almayı da becerebilir. Kalan seçeneklerin hepsi de ya güvensiz ya da çok pahalıdır.

E-mail'in ne kadar güvenilir olduğuna gelince... ABD'de yapılan bir araştırmada, yöneticilerin % 25'i çalışanlarının bilgisayardaki kütüklerini e-mail ve ses mesajlarını okuduklarını kabul ettiler! Ancak bunlar sadece şirket içinde olanların bir kısmı. Internet üzerinde mesaj aktarılırken onu alabilmek de oldukça kolay olabiliyor.

Her durumda, bilginin mahremiyeti tehlikede. İnsanların bilgilerini güvenlik içinde saklayıp, iletebilmeleri çok zor ve dünya üzerindeki yönetimlerin birçoğu da bunu zorlaştırmaktan zevk alıyor. Ancak insanlar bunu aşmanın birkaç yolunu buldular. E-mail'de mahremiyeti sağlamak için atılabilecek iki adım var şu an. Birincisi, anonim mail aracıları kullanmak; böylece e-mail'i alanlar göndericinin kim olduğunu anlayamazlar (daha fazla bilgi için: alt.privacy.anon-server adlı newsgroup'a bakınız). Ancak bu sizin bilgilerinizi değil, sizi gizler. İkinci yol da, PGP (Pretty Good Privacy: Oldukça İyi Mahremiyet) yazılımı ile kodlanmış mesaj göndermek (alt.security.pgp). Günümüzde de-facto standart olan PGP, gönderdiğiniz e-mail'i ve bilgisayardaki kütüklerinizi kodlamak amacıyla kullanılabilir. Böylece sizden başka kimse bunları okuyamaz.



Kodlama

Kodlama (encryption), bilginin gizli bir açıcı anahtara sahip olmayan kişiler tarafından okunmaz hale getirilmesidir. Amacı, bilgileri okuması istenmeyen kişilerden onların kodlanmış bilgiyi görmesine engel olmadan saklamaktır.

Çok kullanıcılı bir ortamda, kodlama güvenilir olmayan bir yoldan da iletişimi sağlar. Sık karşılaşılan bir olay şöyledir: Ali, Burçak'a sadece onun okumasını istediği bir mesaj göndermek ister. Ali, düz metin denilen mesajı bir kodlama anahtarı ile kodlar. Kodlanmış metin Burçak'a gider. Burçak, açıcı anahtarla elde ettiği düz metni okur. Cemil ise gizli anahtarı ele geçirerek veya kodlu metni anahtarsız açarak metni okumaya çalışır. Güvenli bir kodlama ortamında açıcı anahtar olmadan düz metin elde edilemez.

Klasik kriptografi yöntemlerinde mesajın göndericisi ve alıcısı bir tek gizli anahtara sahiptir. Gönderici bununla mesajı kodlar ve alıcı da aynı anahtarla kodu açar. Bu yöntem gizli anahtar kriptografisi (ya da simetrik kriptosystem) olarak bilinir. En önemli problem göndericinin ve alıcının bir gizli anahtar üzerinde anlaşmasını sağlamaktır. Eğer farklı fiziksel ortamdalarsa, bir kuryeye veya telefona güvenmek zorundadırlar. Ancak anahtarı bir şekilde elde eden biri, o anahtarla kodlanmış tüm mesajları okuyabilir. Anahtarların üretimi, aktarımı ve saklanmasına anahtar yönetimi denir ve bu tüm kriptosistemlerin dikkate alması gereken noktalardan biridir. Gizli anahtar kriptografisi güvenilir bir anahtar yönetimine sahip değildir.

Günümüzde Kriprografi

1976'da Whitfield Diffie ve Martin Hellman anahtar yönetimi sorununu çözmek amacıyla açık anahtar kriptografisini geliştirdiler. Yeni sistemde herkesin kişisel anahtar ve açık anahtar adı verilen bir çift anahtarı vardı. Açık anahtarı herkes bilebiliyor, ancak kişisel anahtar gizli tutuluyor; böylece herkesin bir gizli anahtarı bilmesine gerek kalmıyordu. Gizli bir mesaj göndermek isteyen, onu açık anahtarla kodluyordu ve sadece kişisel anahtarın sahibi olan alıcı tarafından açılabiliyordu. Bu sistem aynı zamanda kişinin dijital imzası olarak da kullanılabilmektedir.

Kodlamanın nasıl olduğuna bir bakacak olursak: Ali, Burçak'a kodlanmış bir mesaj göndermek istediğinde, bir kütükten Burçak'ın açık anahtarına bakar ve bunu metni kodlamak amacıyla kullanır. Burçak, kişisel anahtarı ile mesajı açar ve okur. Bu anahtarın sahibinden başka kimse de mesajı açamaz. Ancak, önemli bir nokta kişisel anahtarın iyi gizlenmesinin gerekliliğidir.

Aynı şekilde, Ali gönderdiği mesajı imzalamak istediğinde, mesajı ve kişisel anahtarını içeren bir hesaplama işleminin ardından ortaya çıkan dijital imzayı gönderdiği mesaja ekler. Burçak, bu imzanın doğruluğunu görmek için, mesajı, imzayı ve Ali'nin açık anahtarını içeren bir hesaplama yaptırır. Eğer sonuç bu üçünü içeren basit bir matematiksel ilişkiyi sağlıyorsa, imza gerçektir. Yoksa, ya mesaj değiştirilmiştir ya da imza sahtedir. Böylece mesajın Ali'den gelmediği ortaya çıkar.

Kısa Tarih

1977'de ABD yönetimi IBM tarafından geliştirilmiş olan bir kodlama yöntemini standart olarak seçti. DES (Data Encryption Standart: Bilgi Kodlama Standartı) olarak bilinen bu sistem, gizli anahtar, simetrik kriptosistemiydi ve bugüne kadar en çok kullanılan ve denenmiş kriptosistemlerden biri oldu. 64 bitlik bilgi bloklarını 54 bitlik bir anahtar aracılığı ile kodlayan DES, donanımda uygulanmak üzere geliştirilmişti. Günümüze kadar da DES kodunu kırmak için kolay bir yol bulunamamıştır. Ancak kaba kuvvet denilebilecek, tüm olası kodların baştan itibaren denenmesi gibi, bir süper bilgisayar için bile çok yorucu olan bir yöntemin bazı varyasyonları kullanılmaktadır.

ABD'de NIST (National Institute of Standarts and Technology: Ulusal Standartlar ve Teknoloji Enstitüsü) tarafından, resmi makamlarca kullanılacak kriptosistemler, beşer yıllık süreler için standart olarak belirlenmektedir. DES'in standart olarak kullanım süresi de, en son 1993'te, bir beş yıl daha uzatılmıştı. Ancak 1998'den itibaren yeni bir sisteme geçilmesini isteyen NIST, bu konuda dijital imzaları (DSS) ve bilgi kodlanmasını (Clipper çipi) içeren Capstone projesini başlattı.

Bu konuda NIST, NSA (National Security Agency: Ulusal Güvenlik Ajansı) adlı ABD hükümeti kuruluşuyla da yardımlaştı. NSA, 1950'lerin başlarında kurulan ve çok uzun süre gizli tutulan bir kuruluştu. Görevi gereği ABD'nin tüm dış iletişimlerini kontrolü altında tutarak (örneğin telefon konuşmaları) o ülkenin güvenliği ile ilgili olanları ayırmaktadır. Kodlanmış mesajların onun bu görevini zorlaştırması sebebiyle günümüzün gelişmiş kriptografi sistemlerinin yayılmasını da elden geldiğince engellemeye çalışmaktadır. Bunun için kriptografi yöntemlerinin ve programlarının ABD'den dışarı çıkarılmasının yasaklanmasını sağlamış; aynı zamanda NIST'ye yaptığı "danışmanlık" aracılığı ile kullanılacak bilgisayar güvenliği sistemleri konusunda da söz sahibi olmuştur. NSA, büyük bir alıcısı olması nedeniyle, kriptografik ürünler pazarına da belirli ürünlerin yayılması (veya kaldırılması) yolunda baskılar uygulayarak, burayı kontrol etmeye çalışmaktadır.

1977'de atılan önemli adımlardan biri de, Ron Rivest, Adi Shamir ve Leonard Adleman tarafından RSA (soyadlarının baş harfleri) adlı kriptosistemin üretilmesiydi. Fazla karmaşık olmayan mod ve üs hesaplamalarına dayanan matematiksel işlemlerin sonucunda iki büyük asal sayıdan birer tane açık ve kişisel anahtar üreten bu sistemin en büyük özelliklerinden biri; kişisel anahtarın açık anahtarı oluşturan parçalardan üretilmesinin olanaksız olmasıydı (henüz aksi yönde bir kanıt yok).

RSA, DES'in bir alternetifi olarak üretilmemişti. Hatta DES'in daha verimli kullanılmasını sağlamaktadır. RSA ile bir metinin tamamını kodlamak, gereken işlemlerin çokluğu nedeniyle oldukça uzun bir zaman alacaktır. Ancak, ondan çok daha hız-

lı olan DES ile bir düz metnin kodlanması ve sonra da DES anahtarının RSA ile kodlanarak kodlu metne eklenmesi, işlemi oldukça hızlandırmaktadır. Ancak güvenliğin çok önemli olduğu ortamlarda sadece RSA kodlamaları de kullanılmaktadır.

RSA'yı kırmak için bir büyük sayıyı oluşturan iki asal çarpanın bulunması gerekmektedir. İlk ortaya çıktığında 125 basamaktan oluşan bir sayı için çözümü bir kaç trilyon yıl sürüyordu. Ancak, 1994'de yapılan bir denemede, dünya üzerindeki 1600 bilgisayarda sekiz ay süren bir çalışma sonucu, 129 basamaklı bir sayının iki asal çarpanı bulunabildi.

RSA'ya alternatif olarak bir çok kodlama sistemi üretildi; ancak bunlardan bir kısmı kırıldı. ElGamal tarafından üretilen ve Schnorr tarafından geliştirilen bir sistem NIST'nin projesinde yer alan DSS imza sistemini oluşturdu. Ancak bu sistem oldukça fazla eleştiri aldı; çünkü DSS, pek fazla denenmemiş ve kırılmazlığı yeterince kanıtlanmamış bir sistemdi.

Ancak, RSA'nın en büyük avantajlarından biri olan, hem anahtarları, hem de dijital imzayı aynı anda üretme kapasitesine sahip olan diğer sistemler RSA'nın güvenilirliğini yakalayamadılar.

Bu gücü sayesinde RSA, Unix sistemlerinin neredeyse tümünde ve Novell, Apple, hatta Microsoft tarafından kullanılmakta veya kullanılması düşünülmektedir. ISO (International Standarts Organization: Uluslararası Standartlar Organizasyonu) ve CCITT (Consultative Committee in International Telegraphy and Telephony: Uluslararası Telegraf ve Telefonculuk Danışma Komitesi) tarafından standart kriptosistemlerden biri olarak kabul edilmiştir. Internet üzerinde, PEM (Privacy Enhanced Mail: Mahremiyeti Arttırılmış Mail) ve PGP tarafından da kullanılmaktadır. Ancak ABD hükümeti, NSA'ya ABD dışına çıkacak kriptosistemleri kontrol yetkisi verdi ve NSA da tüm kriptosistemlerin ABD dışına çıkartılmasını yasakladı!

PGP

PGP, Philip Zimmermann tarafından yazılmış, RSA algoritmasını kullanarak metinleri kodlayan bir yazılımdır (Zimmermann daha sonra PGP'nin İnternet üzerinden ABD dışına çıkmasına izin verdiği için mahkemeye verildi ve şu an da bu mahkeme devam etmekte). Ancak kodlama yüzünden başı derde giren sadece Zimmermann değil. Fransa, İran ve Irak'ta, kodlanmış metinlerin kullanılması yasak. 3 Nisan'da Boris Yeltsin, Rusya'da hükümet tarafından onaylanmamış olan kodlama yöntemlerinin kullanılmasını yasakladığını açıkladı.

Ayrıca, NSA'nın politikaları yüzünden, ABD'de kullanılan PGP ile dünyada kullanılan PGP arasında da çeşitli farklılıklar var. PGP'nin yasal olmayan son versiyonu 2.3a idi. Daha sonra PGP'yi ABD'de yasallaştırmak için yapılan çalışmalar sonucunda Zimmermann'ın da katkılarıyla MIT, resmi 2.6.2 versiyonunu çıkardı. RSA'nın patentinin sahibi olan RSADSI ile yapılan anlaşmalar gereğince, 2.6.2 ile kodlanan metinler 2.3.a ve daha önceki versiyonlar tarafından okunamıyor. En son ticari versiyonu 2.7.1 olan PGP'nin dünyanın kalanında kullanılan versiyonu ise, Stale Schmacher tarafından geliştirilmiş olan 2.6.2i. Bu versiyon, çeşitli kanuni nedenler yüzünden ABD'de kullanılana göre çeşitli farklılıklar içeriyor.

Özellikle ABD yönetiminin ve NSA'nın yarattığı bu trajikomik duruma daha fazla değinmeden önce, PGP'den ve anahtarların kullanımından bahsetmekte fayda var.

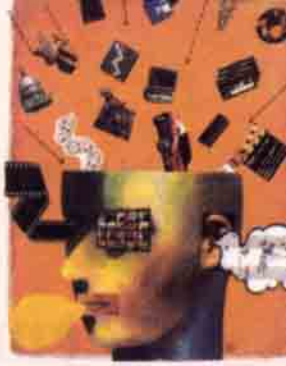
PGP'yi ilk kullanmaya başladığınızda, kendinize ait iki anahtarı yaratmanız gerekir. Anahtarların üretilmesinde kullanılan iki asal sayı, sizin klavyeden gireceğiniz gelişigüzel karakterlere ve harfleri girerken bıraktığınız zaman aralığına göre hesaplanıyor. Daha sonra üretilen kişisel anahtar yine sizin gireceğiniz, istediğiniz uzunlukta bir şifre tarafından korunuyor. Size gönderilen açık anahtarlar da bir açık anahtar kütüğünde saklanıyor.

Yazdığınız bir kütüğü PGP ile ilk olarak kodlayıp daha sonra başka bir program aracılığı ile (örneğin pine) postalamanız gerekiyor. Aynı şekilde, bir kütüğe dijital imza atmanız için de ilk önce dışarıda kodlamanız gerekiyor. Ancak, privtool gibi bazı mail programları sizin istediğiniz işlemleri otomatik olarak yapabiliyor.

PGP'nin bir diğer özelliği ise, size elinizdeki açık anahtarların güvenilirliğini sınıflandırma şansı tanıması. Açık anahtarlar, belki de RSA sisteminin en hassas noktası. Bunların size kodlanmış mail göndermek isteyenlerin elinde olması şarttır. Peki onlar bu anahtarları nasıl elde ediliyorlar? Örneğimize geri dönecek olursak; kötü adam Cemil, Burçak'ın açık anahtarını biliyor olsun. O, yeni bir kullanıcı, yeni bir özel-açık anahtar çifti yaratıp, bunların Burçak'a ait olduğunu iddia ederek yaysın. Ali, bu sahte anahtar çiftiyle mail'lerini kodlayıp, Burçak'a diye sahte kullanıcıya postalar. Cemil, bu mail'i açıp Burçak'ın gerçek açık anahtarıyla kodlayarak onun gerçek kullanıcısına aktarır. Bu arada, mesajdaki herşeyi okuma ve/veya değiştirme şansına da sahip olacaktır. Aynı şekilde sahte dijital imza da atabilecektir. Bu şekilde birçok önemli ve gizli belge kaybedilebilir ve değiştirilebilir.

Böylesi olayların olmasını engellemek için, açık anahtarları ilk elden veya güvenilen kişilerden almak gereklidir. Ayrıca sahte açık anahtarların dolaşmasını engellemek için birkaç tane açık anahtar merkezi oluşturulmuştur. Buralara gönderilen açık anahtarlara isteyen herkes ulaşabilir. Biri anahtar çiftini yarattığında, bu merkezlere açık anahtarını göndererek, isteyenlerin onun anahtarına en kolay yoldan ulaşmasını sağlayacaktır. Ancak bu merkezler bile ilk el veya güvenilir kişilerin aracılığından daha az emin olacaktır. Diğer bazı Unix kullanıcıları, açık anahtarlarını, finger komutuyla alınmasını sağlayacak şekilde, plan kütüklerine eklemektedirler.

PGP'nin uluslararası versiyonu, neredeyse tüm Unix'lerden, Mac'a, hatta Microsoft'a kadar birçok işletim sisteminde kullanılabilmektedir. Ancak, yeterince dikkatli kullanılması şarttır. Özellikle newgrouplar, kişinin kimliğini kanıtlamak gibi bir şeye genellikle ihtiyaç duymadığı yerlerde mesaja PGP ile imza atması, bir lokantada cep telefonunu çıkarıp herkesin görebileceği bir şekilde masasının üzerine koyması gibi, gösterişe yönelik bir harekettir.



Gizliliğin Geleceği

Ancak, yönetimler kolayca açamayacağı şekilde kodlanmış mesajlarla iletişimi doğru bulmuyor. Bu konuda aldıkları tüm kararlar da, hâlâ bilgi trafiği ve aktarımı bakımından İnternet'in lideri ve geliştiricisi durumunda olmaları nedeniyle tüm dünyayı etkileyebiliyor. İddialarına göre, kötü kişilerin kodlanmış mesajlarla haberleşmesi durumunda bunu rahatlıkla açıp okuyamamaları sonucunda ABD'nin ve insanlığın zararına terörist ve kanun dışı gruplar rahatça haberleşebilecekler. Bunun için verilen örnekler ise çok ilginç: Bir çocuğun pornografik yayınla a ulaşması sonucu açılan davada kanıt, kodlanmış bir kütük olduğu için açıup incelenememiş. Internet üzerinde bazı merkezlerde bomba yapımı hakkında bilgilerin bulunması çok tehlikeliymiş (üstelik dünyanın birçok yerinde, Bombacının El Kitabı'nı veya Encyclopedia Britannica'yı herhangi bir kitapçıda veya kütüphanede bulup çok daha tehlikeli bilgilere ulaşılması mümkünken).

Bu nedenle bir yandan ABD Senatosu'nda oylanan, İletişimde Edep Kanunu (Communications Decency Act, diğer adıyla Exon Amendment) ve Telekom Reformu Önerisi ile insan haklarına karşı gelen yasalar çıkartılmaya çalışılırken, diğer yandan da kodlamayı tamamen kontrollerine almak istiyorlar. Geliştirilmekte olan Clipper sistemi de çip üzerinde dağıtılan çözülmesi neredeyse olanaksız bir kodlama sistemi olacak. Ancak, kişisel anahtarların birer kopyası güvenilir kişilerin veya kuruluşların elinde olacak ve mahkeme kararıyla bu anahtarlar kullanılabilecek.

Bu tip sınırlamalar ile İletişim Çağı'nın, insanlar arasındaki açıklığının soğuk savaş zamanındaki gibi bir ortama dönüştürülmesine karşı, tüm dünya kullanıcıları ortaklaşa ABD Senatosu'na mesajlar göndererek, duyarlığını kanıtladı. Dileğimiz böylesi kontrol yöntemleriyle tehlikeli ve zararlı bilgilerin yayılmasını durdurmak için, İnternet'e sansür getirilmesi yolundaki çalışmaların durdurulması. Bunun bir kaşıkla seli durdurmaya çalışmaktan hiçbir farkı olmadığının biran önce fark edilmesi gerekli.

Kaynaklar

Denning D.E., Resolving the Encryption Dilemna: The Case for Clipper.

Fahn P., Answers to Frequently Asked Questions About Today's Cryptography.

http://www.quadralay.com/www/Crypt/Crypt.html

The World Wide Web Virtual Library: Cryptography, PGP and Your Privacy (http://draco.centerline.com/~franl/crypto/)

Licquia J. PGP Frequently Asked Questions with Answers.

PGP paketi.