GÜNÜMÜZDE KRİPTOLOJİ

Uğur Kaşif BOYACI

İllüstrasyonlar : Berke SOYUER

Bu yazı kriptoloji bilimine yeni ilgi duymaya başlayan okurlarımıza konunun temel kavramlarını keyifli bir şekilde anlatmayı ve kriptolojinin günümüzde çalışma ve kullanım alanlarından kısaca söz etmeyi amaçlamaktadır. Konuya ilişkin daha bilgi sahibi olan okurlar için de yazının aralarına daha az bilinen fakat önemli bazı terimler yerleştirilmiştir. Kriptografik terimlerin ilk kullanımları kalın yazılmıştır.

Yazı "alışılagelmiş" kriptoloji ile başlayıp, çığır açan asimetrik sistemler ile sürecektir. Bazı temel kavramlar ve temel sorular irdelendikten sonra sık kullanılan bazı çözümlerden söz edilecektir. Günümüzdeki yaygın bazı uygulama alanları tanıtılıp, kriptolojinin geleceği hakkında bazı öngörülerde bulunulacaktır.

KRİPTOLOJİ DENİLİNCE...

Kriptoloji kelimesi Yunanca "saklanmış, gizli" anlamına gelen "kriptos" ve "söz, us, bilgi, bilim" gibi birçok anlamı olan "logos" kelimelerinden türetilmiştir.

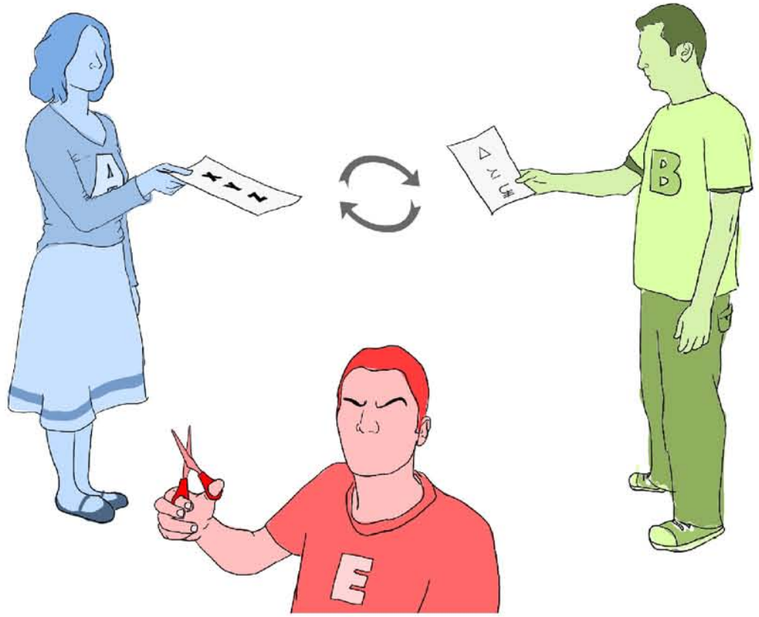
Yakın zamana kadar kriptoloji denilince askerlerin veya casusların gizli mesajlaşmaları dışında bir uygulama alanı pek akla gelmezdi. Bugün kriptoloji herkesin hayatına girmiş durumdadır. Bankamatik kartları, bilgisayar parolaları, alışveriş siteleri, şifreli televizyon kanalları, otoyol geçişleri, elektronik pasaportlar hemen akla gelen uygulamalardan sadece birkaçıdır.

"Verilerin yalnızca istenilen kişiler tarafından anlaşılabilmesi ve diğerleri için anlaşılmaz olması" anlamında kullanılan gizlilik, kriptoloji biliminin hâlâ en önemli uğraşıdır; fakat bu bilim dalı bize çok daha fazlasını vadetmektedir.

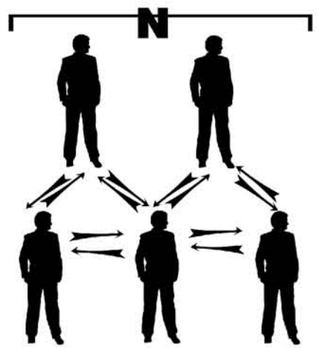
Kriptoloji biliminin bize sağladığı diğer hizmetlere geçmeden önce, **gizlilik** hizmetini sağlayan şifreleme üzerinde biraz duralım.

Simetrik Şifreleme Sistemleri

Ayşe ve **Bora**; mesajları dinleyebilen, kesip yapıştırabilen veya değiştirebilen **Erol** ile yalnızca dinleyebilen **Melahat** gibi kötü niyetli insanlardan gizli haberleşmek istesinler. (Kriptolojide bu düşmanlara genellikle **saldırgan**, bazı özel durumlarda da **hilekâr kullanıcı** denir.) Ayşe ve Bora **kriptolog** olmadıkları için yeni bir gizli haberleşme yöntemi icat edecek durumda olmasınlar; herkes tarafından bilinen bir yöntem kullansınlar: Ayşe göndereceği metni matematiksel bir fonksiyondan geçirerek **şifrelesin** ve Bora'ya yollasın; Bora da bu fonksiyonu kullanarak **şifreli** mesajı **çözsün**. Kullandıkları yöntem, yani **şifreleme algoritması** herkes tarafından biliniyorsa Erol da biliyor demektir. (Kriptolojide kullanılan matematiksel fonksiyonların genel adı **algoritma**dır.) O halde, bu algoritmanın Erol'dan saklanan



bir (ya da birkaç) girdisi olmalı ki, Erol mesajları okuyamasın ya da mesajları okuyabilmek için uğraşsın, yani **kriptoanaliz** yapsın. Mesajı Erol'un



gözünde anlaşılmaz yapan bu "sihirli" girdiye **anahtar** diyoruz. Şifreyi çözen anahtarların kolayca **tahmin edilememesi** gerekir. Dolayısıyla hem yöntemimiz yeterince güçlü olmalı hem de anahtarlar rastgele üretilmelidir ya da diğer bir deyişle, anahtarların **entropi**leri yüksek olmalıdır. Yoksa Erol anahtarı tahmin ederek mesajı okuyabilir.

Ayşe ve Bora'nın hem şifrelemek hem de şifre çözmek için aynı anahtarı kullandığı **simetrik sistem**lerde (örneğin ABD'de Veri Şifreleme Standardı, *'Data Encryption Standard'*, ***DES***) ya da İleri Şifreleme Standardı (*'Advanced Encryption Standard'*, ***AES***) kullanılan sistemlerde) ortak gizli anahtar başkalarının ulaşamayacağı emin bir yerde saklanmalıdır.

Simetrik sistemlerin büyük bir sorunu N kişinin birbiriyle ayrı ayrı gizli konuşmak istemesi durumunda ortaya çıkmaktadır. Bu durumda kişi başına *(N-1)* tane, toplam olarak da *N(N-1)/2* tane değişik anahtarın saklanması gerekmektedir.

Diffie ve Helmann, 1976'da yayımladıkları **Diffie-Helmann (DH)** algoritması ile anahtar dağıtımı sorununa yepyeni bir çözüm getirdiler. Ancak, Rivest, Shamir ve Adleman üçlüsü, adlarının baş harflerini verdikleri, 1977'de yayımlanan **RSA** algoritması ile, şifreleme için simetrik anahtar dağıtımı zorunluluğunu ortadan kaldırarak kriptolojide çığır açtılar. **Asimetrik** ya da **açık anahtar sistemi** adı

verilen bu tür sistemlerin ortaya çıkmasıyla modern kriptoloji devrine girildi.

Asimetrik Şifreleme Sistemleri: Yeni Bir Devir

Asimetrik şifreleme sistemlerinde her kullanıcının iki anahtarı vardır: Bunlardan biri herkese verebildiği **açık anahtarı**, diğeri de herkesten gizli tuttuğu ve elde edilemeyeceğinden emin olduğu **özel anahtarı**dır. Açık anahtar özel anahtardan, geri dönüşümü pratik olarak olanaksız olan matematiksel bir "formül" ile elde edilmektedir. Kullanılan formül algoritmaya ve bazı **parametre**lere bağlı olarak değişmektedir. Açık anahtar ile yapılan "işlem"i özel anahtar "çözebilmektedir".

Ayşe, Bora ve Erol'a dönelim. **Asimetrik şifreleme sistemi** sayesinde Ayşe **şifreleme açık anahtarı**nı herkese, hatta Erol'a bile yayınlar. Bu anahtar kullanılarak gönderilen mesajları, yalnızca Ayşe okuyabilir. Bu noktada aklınıza takılabilecek bazı soruları biraz erteleyelim ve kriptologların bulduğu farklı asimetrik algoritmaları temel işlevlerine göre sınıflandıralım:

- Açık anahtarı bilinen bir kişiye yalnızca o kişinin çözebileceği gizli mesaj yollamaya yarayan **asimetrik şifreleme** algoritmaları, (örneğin RSA, **PSEC** (*Provably Secure Elliptic Curve encryption*))

- Açık anahtara sahip herkesin, mesajın özel anahtar sahibi tarafından gönderildiğini doğrulayabildiği (**mesaj kaynak doğrulaması**) ve özel anahtar sahibinin mesajı **inkâr edemediği imza** algoritmaları, (örneğin RSA, ***DSA*** (*Digital Signature Algorithm*), ***ECDSA*** (*Elliptic Curve Digital Signature Algorithm*), ***NTRU***(*N-Th Degree Truncated Polynomial Ring*))

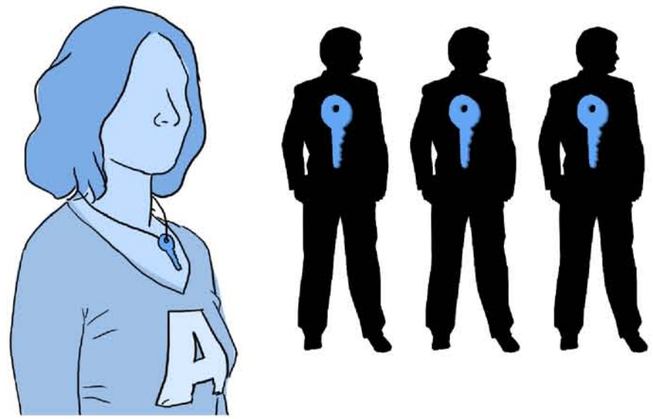
- İki ya da daha çok kişinin yalnız biri tarafından belirlenemeyen **yeni** bir anahtar oluşturulmasını sağlayan anahtar anlaşması algoritmaları, (örneğin ***DH***, ***ECMQV*** (*Elliptic Curve Menezes-Qu-Vanstone*))

- Teorik olarak zor bir probleme dayanan **sözde rastgele sayı üretme** algoritmaları, (örneğin **Blum-Blum-Shub**.)

Simetrik sistemler tarafından sağlanamayan inkar edememe özelliği, yalnızca asimetrik sistemlerde vardır.

Şimdi, aklınıza takılabilecek olası soruları sıralayarak ilerleyelim. İlk iki soru sadece asimetrik algoritmalara özgü değildir; bütün kriptografik çözümler için geçerli çok temel sorulardır.

Soru 1: Kullanılan yöntem (algoritma) güvenli midir? Güvenliyse ne kadar güvenlidir?



Asimetrik algoritmalar genel çözümü çok güç bazı matematiksel problemlere dayanır. (Örneğin **çarpanlara ayırma, Knapsack, ayrık logaritma, kafeslerde** (*lattice*) **en kısa vektörü bulma**) Genel çözümün güç olması özel çözümlerin hepsinin güç olduğunu göstermez. Nitekim, genel çözümü çok zor (*'nondeterministic polynomial-time hard'*, ***NP-hard***) olan Knapsack problemine dayanan **Merkle-Hellmann** sisteminde özel anahtarı ele geçirmek için saldırganın "beklenen"den daha az iş yapması yeterli olmaktadır; diğer bir deyişle, bu sistem **kırılmış**tır. Bir sistemin kırılması için ne yapılması gerektiği sistemden sisteme değişmektedir. Formel dilde kırılma, "hatırı sayılır" **avantaj** elde etmektir.

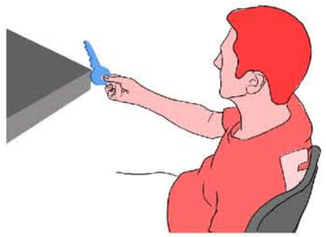
Genel olarak, herhangi bir kriptografik sistemin (örneğin simetrik, asimetrik, ileride bahsedeceğimiz protokollerin ya da özet algoritmalarının) ne kadar güvenli olduğu, güvenliyse güvenliğinin ispatı, güvensizse kırılma yolunun gösterilmesi kriptolojinin en temel dallarından biri olan kriptoanalizdir.

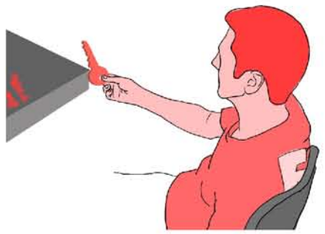
Soru 2: Kullanılan sistem saldırganı ne kadar uğraştırır?

Bu sorunun yanıtı, seçilen algoritmada neyin kırılmak istendiğine ve anahtarların boyuna bağlıdır.

Güvenli bir simetrik sistemin şifresinin çözülmesi için saldırganın olası anahtarları tek tek denemesi (**kaba kuvvet saldırısı**) yani ortalama $2^{<\text{anahtar boyu}>}$ işlem yapması gerektiği kabul edilir.

1024 bitlik RSA algoritmasının ya da 160 bitlik **eliptik eğri** algoritmasının cebirsel saldırılar yardımıyla özel anahtarının bulunarak kırılması için gerekli işlem sayısı, kabaca 80 bitlik simetrik algoritma kırmak için gerekli işlem sayısı kadardır. Bu aynı zamanda 160 bitlik güvenli bir özet algoritmasının **çakışma** bulunarak kırılması ile **eşdeğer güvenlik**tedir.





"Eşdeğer güvenlik" daha çok asimptotik (**büyük "O" gösterimli**) bir ölçüttür; çünkü karmaşıklık birimleri aynı değildir.

İlk sorunun, yani sistemin ne kadar güvenli olduğunun yanıtı, sistemi kırmak için gerekli işlem sayısını doğrudan hesaplamadan da bulunabilir. **Kanıtlanabilir güvenlik tekniklerin**den en çok kullanılanı, sağlamlığı araştırılan bir sistemin, güvenliği bilinen başka bir sistem ya da bir problemle eşdeğer ya da en az onun kadar zor olduğunun gösterilmesidir. Örneğin, birçok asimetrik sistem RSA'ya denktir. RSA probleminin çarpanlara ayırmaya denk olduğu kanıtlanamamakla birlikte bugüne dek daha kestirme bir genel çözüm bulunamamıştır.

Soru 3: Açık anahtarın gerçekten "iddia edilen" sahibine ait olduğundan nasıl emin olabiliriz?

Erol kendi şifreleme açık anahtarını başkalarına Ayşe'nin açık anahtarı olarak kabul ettirirse, sadece Ayşe'nin okuması gereken mesajları okuyabilir. Dahası, Erol kendi **imzalama açık anahtarını** Ayşe'ninkiymiş gibi kabul ettirirse Ayşe adına belgeler düzenleyebilir.

Üçüncü soruya ilişkin bir çözüm yöntemi, açık anahtarların, ait oldukları kullanıcıya ilişkin kimlik bilgileri ve diğer bazı bilgileri içerecek biçimde, herkesin güvendiği **Güven** adlı biri tarafından imzalanması ve yayımlanması olabilir. Kullanıcının açık anahtarını içeren, Güven tarafından sağlanan imzalı veriye **sertifika**, Güven'e de **sertifika otoritesi** adı verilir.

İsterseniz önceki sorulara yenilerini de ilave ederek devam edelim. Devam etmeden önce, Güven'in sertifika otoritesi değil, **Güvenilir Üçüncü Şahıs** (*Trusted Third Party*) olduğu senaryolar bulunduğunu da ekleyelim.

Soru 4: Ayşe, özel anahtarını çaldırırsa ya da kaybederse bunu diğerlerine nasıl duyuracak? (Biri kopyalayabilir, dolayısıyla kaybetmese de çaldırabilir.)

Simetrik anahtar kullanılıyorken sadece o anahtarı paylaştığı kimseleri haberdar etmesi yeterli idi. Şimdi tanımadığı insanları da uyarmak zorundadır.

Soru 5: Ayşe, özel anahtarını "sonsuza kadar" saklamak zorunda mıdır?

Soru 6: Herkesin güvendiği bir Güven nasıl bulunacak? Ayşe sadece Güven1'e, Bora ise yalnızca Güven2'ye güveniyorsa ne olacak?

Soru 7: Güven Ayşe'ye nasıl güvenecek? Karşısındakinin Ayşe olduğundan nasıl emin olacak?

Gördüğünüz gibi sorular arttıkça artıyor. Asimetrik sistemlerin açık anahtarlarının dağıtımını sağlayan ve diğer bazı sorunlarını gideren sistemlere **Açık Anahtar Altyapısı** (**AAA**) sistemleri denir. Bu sistemlerin kısaca anlatılması, derginin ilerideki sayılarından birinde yayımlanacak ayrı bir yazı dizisine bırakılmıştır. Aradığınız soruların yanıtlarını bu yazı dizisinde bulabileceksiniz.

Simetrik ya da asimetrik anahtarların üretilmesi, saklanması, paylaşılması, taşınması, kayıp anahtarlardan diğer kullanıcıların haberdar edilmesi, muhasebesi, yok edilmesi gibi anahtar ile ilgili işlemlerin tümüne verilen genel ad **anahtar yönetimi**dir. Anahtarlar bütün kripto sistemlerinin kalbi olduğundan anahtar yönetimi de güvenlik sistemlerinin en hassas noktasıdır.

Asimetrik Sistemlerin Diğer Sorunları

Asimetrik sistemlerin eşdeğer güvenlikteki simetrik sistemlerle kıyaslandığında yüzlerce kat yavaş olmaları, anahtar boylarının çok daha uzun olması, anahtar üretimlerinin görece zorluğu gibi başka sorunları da vardır. Bu sorunların bazıları kısmen aşılmıştır.

Gerekli anahtar boyu, RSA, *DSA* gibi algoritmalar ile yüksek gizlilik düzeylerinde eşdeğer güvenlik sağlayan simetrik sistemlere kıyasla gerçekten de çok uzundur. Eliptik eğri sistemlerinin anahtar boyu simetrik sistemlere oranla yalnızca bir kaç kat fazladır. Dolayısıyla günümüzde eliptik eğri sistemleri giderek daha çok yaygınlık kazanmaktadır. Bir başka çözüm de, uzun bir mesajın tamamının asimetrik algoritmadan geçirilmesini önlemektir. Örneğin imzalama fonksiyonuna, mesajın kendisi yerine, simetrik algoritma kadar hızlı olan özet fonksiyonundan geçmiş hali girilebilir. Özet fonksiyonları, uzunluğu ne olursa olsun, bir veriyi sabit uzunlukta bir veriye dönüştüren, bunu da çıktıdan girdinin tahmin edilemeyeceği (**geriye dönülemez**, *pre-image resistant*) ve aynı çıktıyı veren iki girdinin bulunamayacağı (çakışma olmayacak, '*collision resistant*') biçimde yapan fonksiyonlardır.

Uzun bir mesajın asimetrik şifrelenmesi yerine yalnızca **Anahtar Şifreleme Anahtarı (AŞA)** asimetrik şifrelenir. Mesajın kendisi AŞA ile simetrik şifrelenebilir. Bu çözümün mesajın kısa, fakat alıcı sayısı çok olduğu durumlarda da kullanışlı olduğuna dikkat ediniz. Elektronik posta çözümlerinin çoğu bu ilkeyle çalışır.

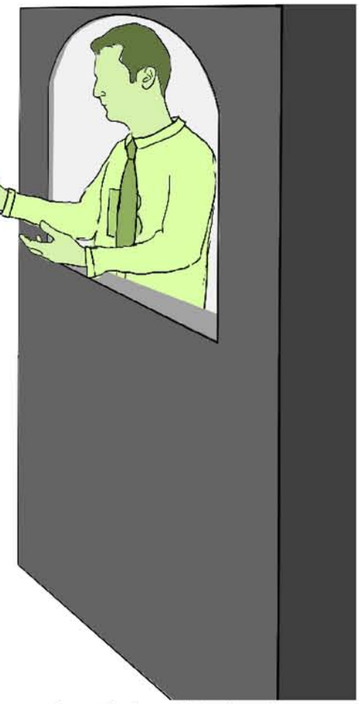
Yeni nesil bilgisayar işlemcileri "makul" asimetrik işlemlerin üstesinden rahatlıkla gelebilir. Asimetrik işlemlerin hızlı yapılabilmesi yalnızca işlemcilerin yeteneklerinin artırılması ile değil, aynı zamanda, asimetrik algoritma içinde geçen, örneğin **modüler üs alma** ya da **eliptik eğri çarpma** algoritması gibi temel yapıtaşlarının matematiksel olarak daha verimli yapılmasını sağlayan yöntemlerin de keşfedilmesiyle mümkün olmuştur.

Bankacılık Oynayalım

Şimdiye dek açıkladığımız kriptografi bilgileriyle gerçek hayatta karşılaşabileceğimiz bir problemi çözelim: Banka müşterisi Ayşe ile banka görevlisi Bora arasında "güvenli" bir ödeme yönteminin kurulması istensin. Ayşe ve Bora'dan herhangi biri, diğerinden mesaj aldığında kabul edilebilir bir sürede yanıt yollayabilsin. Ayşe mesajlarını, işlem verisini başkalarından gizlemek için şifrelesin. Yine de Erol, Ayşe'nin yolladığı şifreli mesajın bazı yerlerini, örneğin işlem tutarının geçtiği yeri değiştirerek Bora tarafından kabul edilebilir bir mesaja dönüştürebilir. Şifreli de olsa birçok elektronik veri formatında hangi verinin nerede olduğu kolayca tahmin edilebilir. Dolayısıyla Erol'un işine yarayan bir yeri değiştirmesi varsayımımız gerçekçidir. Bu nedenle mesajın **bütünlüğü korunmalı**dır.

Öneri 1: Ayşe, mesajı şifrelesin. Daha sonra da imzalasın. Peki bu yeterli midir?

Hatırlarsanız, Erol anahtarlara sahip değil, fakat istediği mesajı kaydedebiliyor ve istediği mesajı tekrar yollayabiliyor. Erol, Ayşe'nin herhangi bir mesajını kaydedip tekrar yollayabilir ve bir **tekrar gönderme saldırısı** düzenleyebilir. Bora, gelen mesajda Ayşe'nin imzası olduğundan mesajın Ayşe'den geldiğine inanır; Ayşe ile kendisinden başkasının bilmediği miktarı öder. Dikkat edilirse, şifreleme ya da imzalama algoritması ne kadar güçlü olursa olsun, Erol başarılı olur; çünkü sistemi kırması için anahtarlardan birini



bulmasına bile gerek kalmadan Bora'nın gerekli miktardan fazla ödemesini sağlar. Bora'nın ikinci kez aynı miktar için ödeme yapmayacağını iddia edebilirsiniz. Ancak Bora bu mesajın daha önce gönderildiğini nasıl anlayabilir? Mesaj üzerindeki zamana bakarak mı? Mesaj üzerinde zaman olduğunu nereden biliyoruz? Ya da mesaj üzerindeki zamanın doğruluğundan emin miyiz? Ya Bora'nın veya Ayşe'nin güvenilir saati yoksa?

Öneri 2: Ayşe ve Bora, mesajların belli bir zamandan sonra oluşturulmadığını, mesajı oluşturanın inkar edemeyeceği biçimde doğrulayan güvenilir bir **Zaman Damgası Sunucusu**'ndan (ZDS) yardım alırlar.

Önerimiz başka birine yani ZDS'ye güven duyulmasını gerektirir; dolayısıyla başka sorunlar çıkarabilir, ama güvenilir saat sorununu belki çözebilir.

Öneri 3: Ayşe ve Bora taze oluşturdukları rastgele sayılarla ve daha önceden aralarında paylaştıkları simetrik anahtarı kullanarak **sorgu-yanıt** (*challenge-response*) ile **kimlik doğrulama** yaparlar. Karşı tarafın kimliğinden - ve hazır bulunduğunda - emin olduktan sonra şifreli ve bütünlüğü sağlanmış mesaj alışverişi başlayabilir.

Öneri 4: Ayşe ile Bora kendi aralarında uzun süre bir anahtar paylaşmış olmasınlar ve anahtar üretiminde diğer tarafa, hatta kendilerine bile güvenmesinler; fakat bir **Anahtar Dağıtım Merkezi** (ADM) ile anahtar paylaşmış olsunlar ve her bağlantıda yeni bir anahtar istesinler.

Bu çözüm de ADM'nin sürekli çevrimiçi olması, ikisinin birden güvendiği bir ADM bulunması, ADM'nin anahtarları ele geçerse eski konuşmaların ele geçmesi gibi başka sorunları da beraberinde getirir; fakat kullanıcıların başkaları ile anahtar paylaşma yükünü hafifletir. Ayrıca, her bağlantıda yeni bir anahtar kullanılmasını engelleyebilecek başka önlemler bulunabilir. (Örneğin belirli **geçerlilik süresi** olan bir **bilet** alabilirler.)

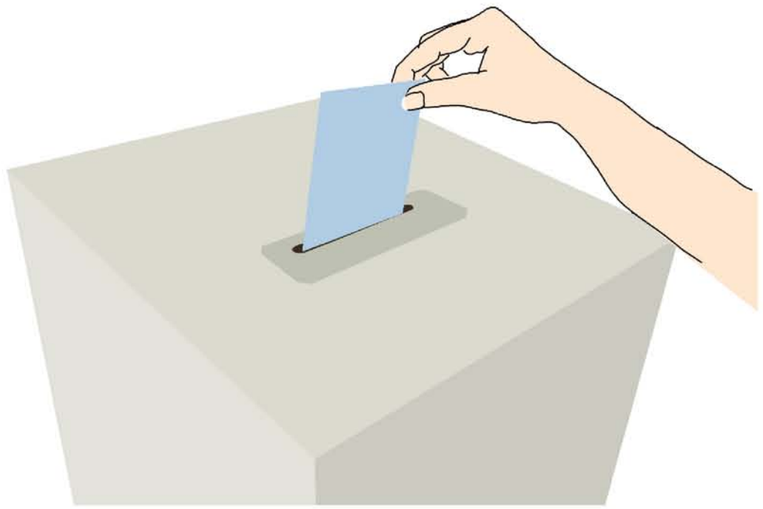
Öneri 5: Ayşe ve Bora bir **anahtar anlaşması** yöntemi, örneğin DH ile taze anahtar oluştursunlar. Daha sonra yollayacakları mesajların gizliliğini bu yeni anahtardan türettikleri bir şifreleme anahtarı kullanarak simetrik şifrelemeyle, bütünlüğünü ise yine bu yeni anahtardan türettikleri başka bir kimlik doğrulama anahtarı ile (**simetrik şifreleme tabanlı**) **mesaj kaynak doğrulama** ('*Message Authentication Code*', *MAC*) algoritması ya da **özet algoritmalı mesaj kaynak doğrulama** ('*Hash-Based Message Authentication Code*', *HMAC*) algoritması kullanarak sağlasınlar.

Öneri 5'de ciddi bir tehlike vardır, şöyle ki:

DH algoritmasının olduğu gibi uygulanılması **aradaki adam saldırısı**na olanak sağlar. Bu saldırıda Erol Ayşe'ye kendini Bora, Bora'ya kendini Ayşe gibi tanıtır. İki tarafla ayrı ayrı DH anlaşması yaparak iki farklı anahtara sahip olur. Birinden (örneğin Ayşe'den) gelen mesajı aralarında paylaştıkları anahtarla çözer, diğeriyle (Bora ile) paylaştıkları anahtarla şifreleyerek kendini gizler. Dolayısıyla anahtar anlaşma mesajlarından en az birisi için kaynak doğrulamasının yapılmış olması gerekir.

Öneri 5, aralarında daha önce bir **gizem** (anahtar, parola, anahtar çekirdeği vb.) paylaşmamış iki tarafın güvenli haberleşmesine imkan verir. Gerçekten de internet dünyasında en çok kullanılan güvenlik uygulamalarından biri olan ***SSL/TLS*** (*Security Socket Layer/Transport Layer Security*) çalışma ilkesi kabaca bu şekildedir.

Belli bir güvenlik hedefinin (bu problemde, iki taraf arasında güvenli mesaj iletişiminin) farklı kısıt ve kabiliyetler ile çok farklı, kriptografik çözümler bulunabileceğine örnekler vermiş olduk. Mesajlarda **sayaç** kullanarak güvenli bir ödeme önerisi getirmeyi okuyucuya bırakıyoruz. Çözümünüzde esas önemli olan mutlak güvenlik sağlamak değil, önerinizin getireceği **varsayımları**, **güven ilişkileri**ni ve **zayıf noktaları**nı belirleyebilmenizdir.



Yukarıdaki çözüm önerileri bizi kriptolojinin bir diğer önemli kavramına getirdi.

Protokoller

Belli bir güvenlik hizmetini sağlamayı hedefleyen, iki ya da daha fazla tarafın belli bir sırayla takip etmesi zorunlu adımlar silsilesinden oluşan çözümlere (**kriptografik**) **protokol** denir.

Bankacılık oynarken çözümlerin sadece "anafikirler"ini vermiştik. Uygulama için tarafların adımlarını iyi belirlemiş olması, yani protokolün iyi tanımlanmış olması gerekmektedir. Bununla birlikte, yalnızca anafikirlere de protokol denilebilmektedir.

Kriptografik protokoller çok çeşitli şekilde sınıflandırılabilirler: Katılan taraf sayısına göre (iki, üç ya da **çok taraflı**), katılan tarafların niteliğine göre (istemci-sunucu, güvenilir kişi destekli, **hilekar kullanıcıların bulunduğu** vb.), hedeflenen hizmete göre (kimlik doğrulama, anahtar anlaşma, **e-oylama, sıfır bilgi, çoklu yayın**), ağırlık verilen kriptografik algoritma ya da gizeme göre (simetrik algoritma tabanlı, asimetrik algoritma tabanlı ya da **parola tabanlı**), haberleşme ortamının kısıtlarına göre (geniş alan ('*Wide Area Network*', ***WAN***), **kablosuz ağ**, (yarı) **çevrimdışı**, **akıllı kart**).

Protokoller bazen birkaç hizmeti birden sağlasa da genellikle temel görevleri ile anılırlar. Daha önce gizlilik, bütünlük, inkar edememe, kimlik doğrulama gibi hizmetlerden söz etmiştik. Şimdi başka hizmetler ve farklı kullanım alanlarından bahsetmeye devam edelim.

Daha Değişik Hizmetler / Kullanım Alanları

Son yıllarda en çok istenen hizmetlerden biri de protokole katılan tarafın yaptığı

işlemin başkaları tarafından izlenmesinin engellenmesidir. Burada söz konusu olan **mahremiyet** (özel hayatın gizliliği) kavramıdır. Bir diğer benzer kavram ise, yapılan işlemin ne olduğunun bilindiği, fakat yapanın bilinmediği **anonimlik** kavramıdır.

Örneğin **elektronik oylama** protokolünde kime oy atıldığı belli olabilir, fakat verilen oydan yola çıkılarak oy atanın kimliğinin belirlenememesi (anonimlik) gerekir. Elektronik oylamada seçmenin kime oy attığının başkaları tarafından anlaşılamaması mahremiyet ile ilgilidir.

Elektronik oylama protokollerinin oy verenin oyunun sayıldığından emin olması (**geçerlenebilirlik**, *validation*), her oy verenin tek sefer oy atabilmesi, oylamanın tekrar sayım kolaylığı, oylama bitene kadar oy sonuçlarının açığa çıkmaması, kullanıcı kolaylığı gibi bir çok koşulu daha sağlaması beklenmektedir.

İstenen "alt" hizmetlerin çokluğu, istenen hizmetlerin birbirleriyle teorik ya da pratik bazı **ödünleşim**lerde (*trade-off*) bulunması, mutlaka sağlanması gereken hizmetler üzerinde tam bir uzlaşı olmaması, hemen her çözümde bilinen bir zayıflık ya da pratik uygulama sorunu bulunması elektronik oylama konusunu kriptologlar için ilgi çekici hale getirmiştir. Elektronik oylama, mükemmelden uzak çözümler sunsa da, kriptolojinin günlük hayatımıza daha çok gireceği konulardan sadece biridir.

Kriptolojinin güvenlik çözümleri sunduğu bir başka yeni alan, günümüzde yaygın olarak kullanılan ve gittikçe vazgeçilmez teknolojilerden biri olan ***RFID* etiket** sistemleridir. Barkodlara göre büyük avantajları olduğundan, birçok envanter sistemi bu teknolojiye bel bağlamaktadır. *RFID* sistemleri genellikle kripto kabiliyeti sınırlı **uç cihazlar** kullanmaktadır.

RFID gibi işlemci güçleri genellikle çok sınırlı olan bir diğer veri sistemi **algılayıcı ağ**lardır. Trafik izleme, sınır güvenliği, kritik altyapıyı saklama (barındırma) gibi birçok alanda algılayıcı ağ kullanılmaya başlanmıştır. Bazı durumlarda, *RFID* ile algılayıcı ağlar birlikte kullanılmaktadır.

Gerek *RFID* etiket, gerek algılayıcı ağ sistemlerinde uç cihazlardan gelen bilginin güvenliği ve güvenilirliği büyük önem taşımaktadır. Bu sistemlerde kriptoyu daha etkin gerçekleyebilmek için ya işlem kapasitesinin artırılması (daha iyi piller, daha iyi işlemci) ya da daha az güç isteyen **kolay kriptografi** çözümlerinin bulunması gerekmektedir.

Kriptolojinin farklı uygulamalarına ilginç bir problem ile örnek vermeye devam edelim: N kişi arasından en az k kişinin anlaşması durumunda belli bir hizmetin yerine getirilebilmesine (veya ancak belli bir eşik değeri aşıldığında ortak bir değer oluşturulabilmesine), yoksa bu hizmetin sağlanamamasına çözüm bulmaya çalışan **eşik kriptolojisi** tekniği pratiğe geçirilebilirse, birçok bürokratik işlem hızlandırabilir ya da bazı güvenlik sorunları aşılabilir.

Aralarındaki t hilekâr oyuncuya karşın ortak bir gizem oluşturmayı deneyen N kişi (**Bizans Generalleri**) problemi de kriptolojide kuramsal çözümleri incelenen bilgi teorisinin önemli uğraşlarından biridir.

Açık anahtarlı sistemlerde sertifika yerine açık anahtarın kişinin kimliği olduğu bir sistem güzel olmaz mıydı? Kriptologlar, **eliptik eğri eşleşmeleri** kullanarak teorik ve pratik güzel çözümler üretti bile. **Kimlik tabanlı kriptografi**, gelecekte orta ölçekli birçok kurum için sertifika tabanlı kriptografinin yerini alabilir.

Buraya kadar sözünü ettiğimiz kriptoloji, genellikle matematiksel (daha çok cebirsel) yöntemlerle sistemlerin güvenli olmasını sağlamayı amaçlıyordu. Diğer yandan, **yan kanal çözümlemesi** (*side-channel analysis*) denilen bir mühendislik dalı, algoritmanın **gerçeklenme** (*implementation*) yöntemine bağlı olarak anahtar hakkında bilgi sızdırabilen veriler (örneğin güç tüketimi ya da geçen işlem süresi) yardımıyla anahtarı bulmaya çalışıyor. Artık kriptologlar, yan kanal saldırılarına da dayanıklı mekanizmalar tasarlamaya çalışıyorlar.

Kriptoloji Her Yerde

Bazı kuramsal çözümlerin zamanla pratiğe dökülerek kriptolojinin uygulama alanlarının genişleyeceğini tahmin etmek zor değil. Bugün bilginin saklanması ve güvenli aktarılması için kriptoloji olmazsa olmaz görünüyor. Yazıyı okuyanlara, kriptolojinin kağıt üzerinde bazı matematiksel problemlerin çözümü olmadığını tekrar hatırlatalım. Bilgisayar, telsiz, telefon, cep telefonu, *PDA*, işlemci, elektronik pasaport, akıllı kart gibi elektronik veri ile uğraşan hemen her cihaz kriptoloji teknikleri kullanıyor.

Kişinin şahsının ya da sahip olduğu nesnelerin (örneğin arabasının ya da kredi kartının) elektronik ortamda tanınması giderek yaygınlaşıyor. Bunun güvenli yapılabilmesi yanında kontrol eden kişilere bağımlılığının azaltılması yönünde giderek artan bir istem bulunmaktadır. Dolayısıyla bankacılık, elektronik tanıma sistemleri, e-devlet hizmetleri, elektronik envanter sistemleri, bilgi paylaşan **ızgara** (*grid*) sistemleri, araba alarmları, veri tabanları, ücretli televizyon yayıncılığı gibi birçok alanda kriptoloji kaçınılmaz olmaktadır.

Gelecekte Kriptoloji

Kriptoloji insanlık tarihindeki en büyük rolünü 2. Dünya Savaşı'nda oynamıştı. Yakın gelecekte de, askeri alanda, özellikle **elektronik harp** teknikleri içinde vazgeçilmez yere sahip olacaktır. Günlük hayatta özellikle e-ticaretin yaygınlaşması, kamu ve özel sektör hizmetlerinin elektronik ortamdan verilmesi, akıllı cihazların çoğalması kriptolojinin önemini daha da artıracaktır.

Gelecekte kriptoloji biliminde neler yapılacağını kestirmek için geçmişine bakalım. Aslında kriptolojide olanlar da temel bilimlere dayalı herhangi bir mühendislikten beklendiği gibi cereyan etmiştir:

Belli bir hizmeti sağlayabilmek için bir yöntem aranıyor. Elimizdeki bilinen tekniklerden yararlanarak problem çözülemezse yeni teknikler araştırılıyor. Bu arada, bazı çözümlerin belli koşullarda varlığı ya da yokluğu (çözüm bulunmadan) kanıtlanmaya çalışılıyor. Birçok durumda aranılan hizmeti kısmen de olsa karşılayan pratik ya da teorik çözümler bulunuyor. Bulunan çözümlerin pratik ya da güvenilir olduğu kanıtlanmaya çalışılıyor.

Ortaya atılan çözümler çözülmesi gereken yeni sorunlar ve ucu açık başka sorular yaratıyor ya da umulmayan başka bir soruya yanıt getiriyor. Çözümlerin daha kullanışlı, daha az karmaşık, daha kolay, daha değişik teknikler içeren iyileştirmeleri ya da değişik sürümleri araştırılıyor. Bir çözüm üzerinde yeterince tartışıldıktan ve yeterince olgun bir çözümün varlığından emin olunduktan sonra herkesin birbiriyle ortak dili konuşabilmesi için standartlaşma öneriliyor. Bu arada, çözümleri daha iyi gerçekleyebilmek için yeni teknikler ya da daha kolay alt edebilmek için yeni saldırılar aranıyor.

Örneğin, ilk başta bazı eliptik eğri gruplarına saldırı için kullanılan fakat sonra kimlik tabanlı kriptografinin gelişmesini sağlayan eliptik eğri eşleşmeleri, kimlik tabanlı kriptografinin yolunu açıyor. Unutmayın ki, kriptoloji yalnızca "dürüst insanların" bilimi değil. Aynı zamanda verilen hizmeti kriptografi teknikleriyle alt etmeye çalışıyoruz. Dolayısıyla matematiksel teknikler yalnızca bir hizmeti vermek için değil, o hizmeti "anahtarsız" almanın yollarını bulmak için de kullanılıyor ya da sınanıyor.

Kriptologlardan yakın gelecekte çözüm bekleyen pek çok sorun var zaten: mahremiyet, **yetki devri**, **etkin grup anahtar anlaşması**, kolay algoritmalar, kanıtlanabilir güvenlikli yapıtaşları vb. Dolayısıyla yeni yapıtaşlarına (algoritma ya da protokol) gereksinme bitecek gibi görünmüyor. Değişik yapıtaşlarının araştırılmasını gerektiren bir başka önemli etken ise **kuantum bilgisayarlarının** gelecekteki olası varlığı...

Bildiğimiz işlemcilerden çok farklı yapıya sahip kuantum bilgisayarları ve genel anlamda **kuantum kriptolojisi** için bu sayıda yayımlanan "Kuantum Bilgi Güvenliğine Doğru" başlıklı yazıya bakılabilir. Yalnızca, alıştığımız birçok kripto sisteminin kuantum bilgisayarları ile kırılabileceğini söylemekle yetinelim.

Hem kuantum kriptoloji tehdidi hem de işlem gücü artan saldırganlar yüzünden giderek daha uzun boylu anahtarlar kullanmak zorunda olduğumuzdan, alışılagelmiş asimetrik sistemler yerine alternatif yapıtaşları aranıyor. Bunlardan biri kuantum bilgisayara dayanıklı oldukları bilinen **kafes tabanlı sistemler**. **Çizge grupları, çok değişkenli düşük dereceli polinom sistemleri** umut vadeden diğer matematiksel yöntemlerden bazılarıdır.

Bilgi güvenliğinin en temel taşlarından biri olan kriptoloji, bilgi kuramı, karmaşıklık kuramı, yazılım mühendisliği gibi birçok dalla iç içedir. Örneğin **güvenlik ispatlarında makine geçerlemesi** ya da **otomasyon kanıtlaması**, kriptoloji kadar bilişim teknolojilerinin ve yazılım mühendisliğinin de merakla eğildiği bir konudur. Günlük yaşamda bilgi güvenliğinin hemen her bilim dalına yayılması sonucu kriptoloji de giderek önem kazanacaktır. Kriptoloji kriminoloji, hukuk, biyometri gibi birçok bilim dalı içerisinde şimdiden azımsanmayacak bir yere sahiptir.

Kriptoloji bir zamanlar "yalnızca şifreleme" idi ve "yakın zamana kadar matematik bölümünün altında açılan bir ya da birkaç ders" ile öğretiliyordu. Günümüzde ise, birçok üniversitenin kriptoloji bölümleri bulunmaktadır.

Verinin geçtiği hemen her yerde kriptolojik teknikler uygulanmakta, çok değişik hizmetler sağlanmaktadır. Bu da kriptolojiyi geleceğin en önemli bilim dallarından biri yapacaktır.

Bu yazıyla içinizde kriptoloji bilimine karşı bir merak uyandırabildiysek ne mutlu bizlere...