*Uğur Kaşif Boyacı**
*Orhun Kara***

**Uzman Araştırmacı,*
***Dr., Başuzman Araştırmacı,*
UEKAE, TÜBİTAK

Bilgi Güvenliği Problemlerine Matematiksel Yaklaşım Getiren Bir Bilim Dalı Kriptoloji

Düşmandan bilgi saklama ve gizli haberleşme insanoğlunun kafasını binlerce yıldır meşgul eden bir problem. Çok eski zamanlarda ilkel haberleşme teknolojisinden ve okuryazar oranının düşük olmasından faydalanılarak bu problemlere kolay çözümler getirilebilmiş. Oysa günümüzün son derece karmaşık ve gelişmiş bilgi ve haberleşme teknolojisinde, kimlik doğrulama, gizliliği sağlama, bilginin kaynağını doğrulama, verinin bütünlüğünü sağlama gibi bilgi güvenliği problemlerini çözmek o kadar kolay değil. Öyle ki, bu problemleri çözmek için bir bilim dalı doğmuş: Kriptoloji

Anahtar Kavramlar

Kriptoloji bir yandan gizlilik, veri bütünlüğü, kimlik doğrulama, inkâr edememe gibi bilgi güvenliği problemlerine matematiksel teknikler kullanarak çözüm getirme, bir yandan da bu çözümleri analiz etme ve çürütme bilimidir. Kriptografik bir çözüm oluşturmayı bir inşaata benzetirsek temel yapıtaşları, belli görevleri yerine getiren "algoritmalar"dır. Bu yapıtaşları çoğunlukla "anahtar"larla kullanılabilir.

Güvensiz bir kripto sistemi güvensiz bir uçak gibidir; ne kadar verimli olursa olsun, o sistemi kimse kullanmaz.

Eğer kripto algoritmanız güvenli ise saldırgan algoritma ile ilgili (algoritmanın işleyişi dahil, ama anahtar hariç) her şeyi bilse bile bir avantaj elde edemez.

Aslında pratikte kullanılan hemen hemen bütün sistemler kırılabilir. Ancak bunun bir maliyeti vardır ve bu maliyet çoğu kez insanlığın hiçbir zaman ulaşamayacağı kadar yüksektir.

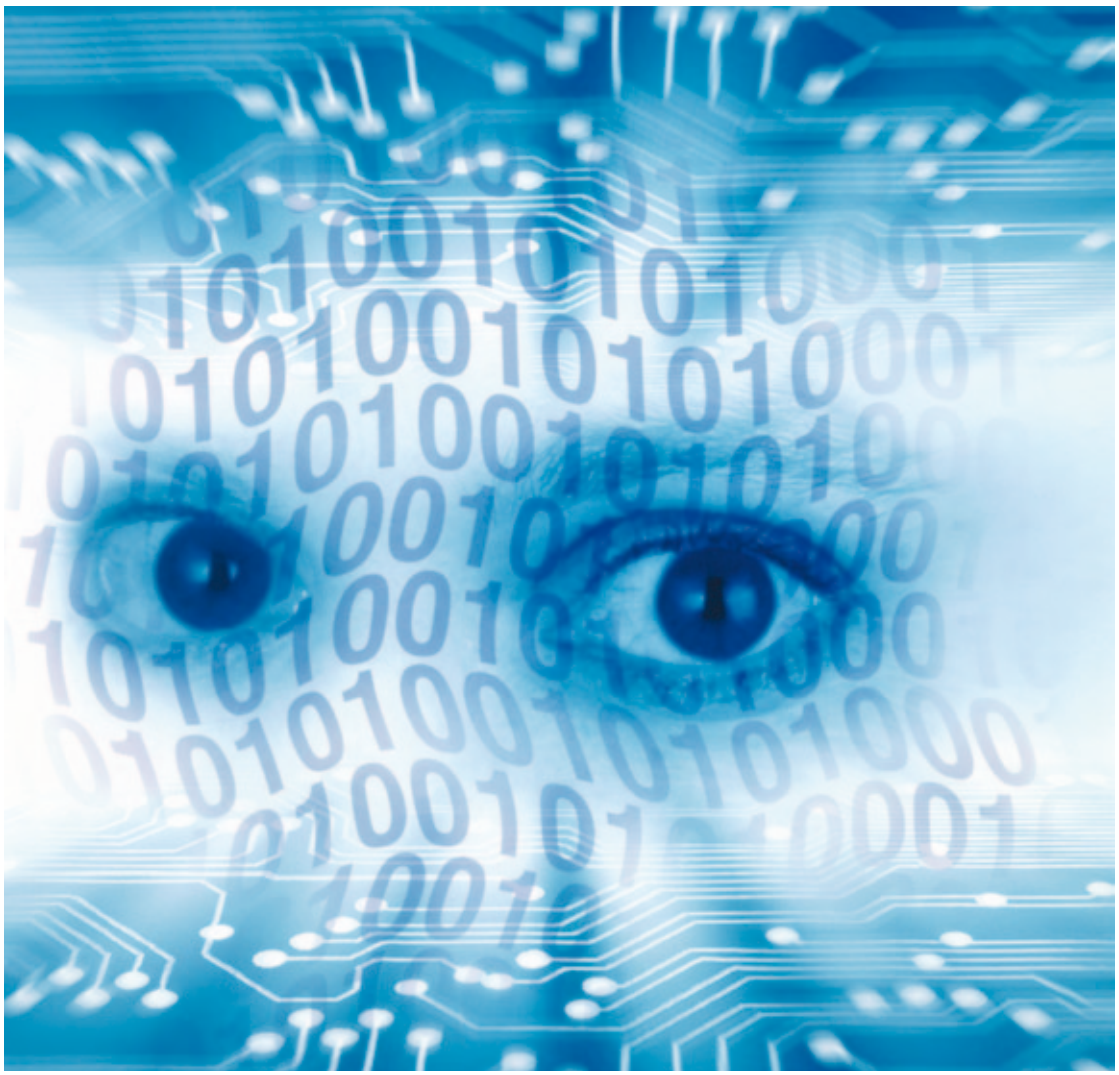
Uğur Kaşif Boyacı, ODTÜ Matematik Bölümü'nden lisans derecesi ve Yıldız Teknik Üniversitesi Matematik Mühendisliği Bölümü'nden yüksek lisans derecesi aldı. Dizi şifreleme algoritmalarının analizi üzerine tez yazdı. Yaklaşık on yıldır kripto algoritmaları ve protokolleri üzerinde TÜBİTAK UEKAE'de çalışmaktadır.

Pek azımız kriptolojinin ne olduğunu, ne anlama geldiğini bilir. Aslında kriptoloji dünyanın en ilgi çekici ve gizemli bilimlerinden biridir. Biraz dar bir tanım olsa da, kriptolojiyi kısaca şifreleme ve şifre kırma bilimi olarak tarif edebiliriz.

"Şifre yapmanın ya da şifre kırmanın bilimi mi olur?" diye düşünebilirsiniz. Şifre kırma deyince büyük ihtimalle kafanızda, Hollywood filmlerinden çıkma cin gibi bir gencin telaş içinde, klavyede aynı anda bir sürü tuşa basarak FBI'ın giriş kodlarını ele geçirmesi canlanmıştır.

İnanın şifre yapmak ya da şifre kırmak sanıldığı kadar kolay bir iş değil. Sadece bu konuda çalışan profesörler bile var. Bu araştırmacılar saniyeler içinde klavyede yüzlerce tuşa basabilecek kadar hızlı değiller, ama aylar ve hatta yıllar süren çalışmalar sonucunda belli şifreleri çözmek için geliştirdikleri matematiksel yöntemlerle gerçek birer şifre kırıcılar.

>>>



Visual Photos

İnternetteki sohbet odalarında, biz farkına varmasak da kulak misafirlerimiz olabilir.

Kriptoloji kelimesinin kökü Eski Yunancadan gelir ve "gizem bilimi" anlamı taşır. Kriptolojiyi, bilgi güvenliği alanında matematiksel çözümler üreten ve bunları analiz eden bir bilim olarak düşünebiliriz. Kriptolojinin bilgi güvenliği sağlamak için çözüm üreten alt bilim dalına kriptografi, önerilmiş çözümleri analiz eden ve çürütmeye çalışan alt bilim dalına ise kriptoanaliz denir.

Kriptolojinin uğraşı alanlarını bir örnekle ifade etmek daha açıklayıcı olacaktır. Ankara'da bir kimya profesörü Zürih'teki bir ilaç firması için ilaç formülleri geliştiriyor olsun. Geliştirilen formüllerin firmanın Zürih'teki laboratuvarlarında test edilmesi gerekmektedir. Ya profesör belli aralıklarla Zürih'e gidecek ya da Zürih'ten Ankara'ya araştırmacılar gelecek. Bu görüşmeler sırasında profesör hazırlanan raporları elden teslim edecek ya da alacak. Firma yetkilileri geliştirilen yüzlerce formülün yolda kaybolabileceği endişesini taşıyor. Üstelik seyahat masrafları ve gecikmeler, firma için oldukça maliyetli olmaya başlamış. Başka ülkelerde ortak çalıştıkları diğer profesörleri de hesaba katınca seyahat masraflarının altından kalkılamaz hale geldiğini gören firma, bu duruma bir çözüm bulmaya karar veriyor. Seyahate ne gerek var? Zaten internet bilgileri kolayca transfer etmeye yaramıyor mu? Bunun üzerine, çalışanlar arasında formülleri paylaşmaları için sanal sohbet odaları kuruluyor. Böylece çalışanlar birbirlerine zahmetsizce yazı, ses ve görüntü iletme imkânına kavuşuyor.

İlaç firması raporları hızlı iletmenin yolunu buldu, ama güvenliği sağlayabildi mi? Muhtemelen hayır. Profesörümüzü internet ortamında bekleyen bir takım tehlikeler var. Profesör sanal sohbet odasında kendi firmasından arkadaşları ile sohbet ettiğini zannederken, aslında rakip ilaç firmasının araştırmacıları ile sohbet ediyor olabilir. Yani profesör sohbet ettiği kişilerin kimliğini doğrulayabilmeli. Bir diğer tehlike, rakip firmadakilerin sohbet odasında geçen konuşmalara "kulak misafi-

Visual Photos

Şifreleme algoritmanızın sağlamlığı şifrelediğiniz metinleri kime karşı koruduğunuza bağlıdır. Eğer uzaylılar varsa ve galaksileri aşıp Dünya'yı ziyaret ettilerse, muhtemelen insanoğlunun modern şifrelerini kırabilecek hesapsal güce sahip teknolojiyi de geliştirmişlerdir.

ri" olması. Formüller sadece profesör ve kimliğinden emin olduğu sohbet arkadaşları arasında gizli kalmalı. Rakip firmadakiler izlerini fark ettirmeden formülleri, gizli olsalar bile, değiştirebilir ya da bozabilir. Bunun önlenmesi için sohbet odasından giden verilerin bütünlüğünün sağlanması gerekir.

Yukarıda verilen örnekte bahsedilen problemleri çözsek dahi, bilgi güvenliğini tam olarak sağlamış sayılmayız. Daha verinin kaynağının doğrulanması, verilerin taze bilgi olduğunun yani daha önceki haberleşmeden kalma bilgi olmadığının doğrulanması, profesörümüzün ilaçlar kötü sonuç verirse "bunlar benim formüllerim değil ki" diye inkâr etmesinin önlenmesi gibi işler ve daha pek çok güvenlik problemi bizi bekliyor.

Kriptoloji, sayısal ortamda işte bu tür güvenlik problemleriyle uğraşan disiplinlerarası bir bilim dalıdır. Daha biçimsel bir tanım verecek olursak kriptoloji bir yandan gizlilik, veri bütünlüğü, kimlik doğrulama, inkârın önüne geçme gibi bilgi güvenliği problemlerine matematiksel teknikler kullanarak çözüm getirme, bir yandan da bu çözümleri analiz etme ve çürütme bilimidir.

Kriptografik bir çözüm oluşturmayı bir inşaata benzetirsek, temel yapıtaşları belli görevleri yerine getiren "algoritmalar"dır. Bu yapıtaşları çoğunlukla "anahtar"larla kullanılabilir. Sadece güçlü yapıtaşlarını kullanarak bir inşaat yapamayız. İnşaat için yapıtaşlarının belli bir plan-proje çerçevesinde, belli sırayla, belli kişiler tarafından bir araya getirilmesi gerekir. Bu plan ve iş kurallarına "protokol" denir.

Kriptoanaliz Nedir?

Bütün kripto algoritmalarından, protokollerinden ve uygulamalarından mühendislik açısından iki temel özelliğe sahip olmaları beklenir: Güvenlik ve verimlilik. Bu iki gerekliliği sıraya koymak gerekirse, önce gelen güvenliktir. Güvensiz bir kripto sistemi güvensiz bir uçak gibidir; ne kadar verim-

li olursa olsun, kimse kullanmaz. Sesten birkaç kat hızlı bir uçak tasarlayın. Emin olun, uçağınız güvenli değilse, Ankara'dan New York'a iki saatte varsa bile, kimse onunla uçmayacaktır.

Algoritmaların verimliliği, genel olarak kriptonun çalışacağı platformdaki hızı, hafızada ya da devre şemasında kapı sayısı olarak kapladığı yer ve tükettiği güç ile ölçülür. Uygulama platformunun kısıtlarına göre bu kıstaslardan bazıları öne çıkar. Örneğin RFID etiketlerinde koşacak bir algoritmanın kısıtlı yonga alanı nedeniyle az yer kaplaması ve etiketlerin dışarıdan yani elektromanyetik ortamdan elde ettikleri enerjiyi tüketmelerinden dolayı az güç harcaması gerekir. Burada hız ikinci planda kalır.

Çok çeşitli RFID etiketleri vardır, ama genel olarak RFID etiketlerini mağazalarda ürünlere yapıştırılan ve kapıda alarmları çaldıran, içinde labirent gibi, sarmal şeklinde bir antenle sarılmış küçücük bir yongadan oluşan etiketler olarak düşünebilirsiniz. Kutusuna RFID etiketi yapıştırılmış bir ürün aldığınızda (örneğin bir DVD filmi) etiketi kutudan ayırın. İçindeki labirent gibi anteni sökün. Masrafsız bir şekilde bozup kurcalamanın tadını çıkarın. Büyütecinizle antenin ortasındaki küçücük yongayı yakından inceleyin. O yongada bir kripto algoritmasının koştuğunu hayal edin ve bu algoritmanın şifrelediği metinleri milyarlarca TL'lik süper-bilgisayarların bile çözemediğini düşünün.

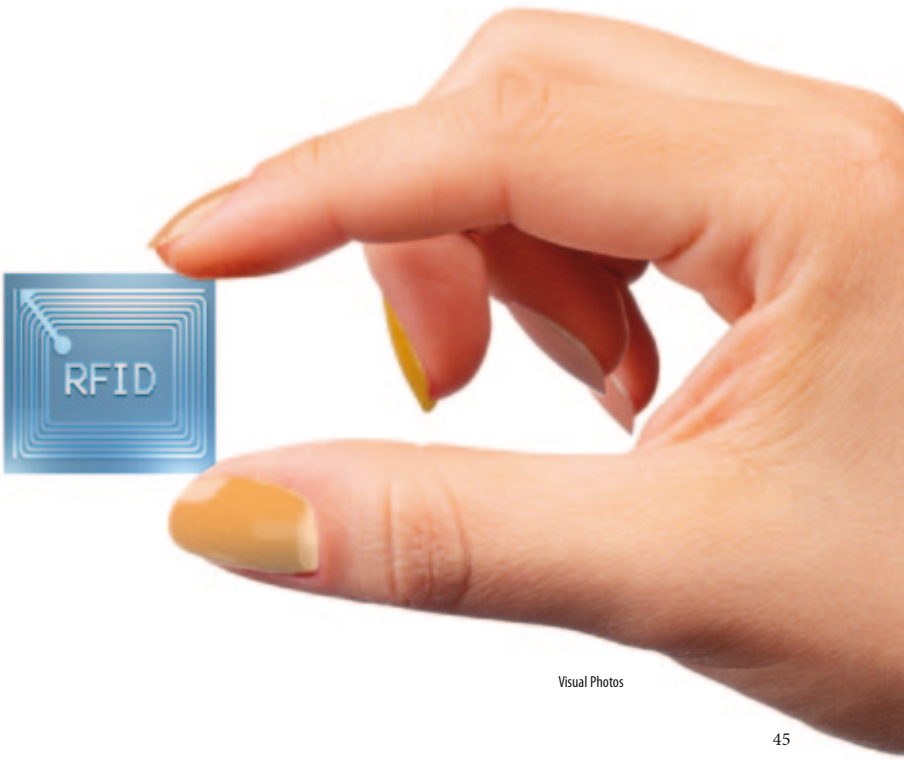
Algoritmaların güvenliğini ölçmek son derece zordur ve ayrı bir uzmanlık gerektirir. Bir algoritmanın ne kadar güvenli olduğu algoritmayı kırmaya çalışan varlığın entelektüelliği ile ilgilidir. Yani insanoğlu akıllı bir varlık olan insanoğluna karşı önlem almaya çalışmaktadır.

Mühendisliğin birçok alanında güvenlik problemleri çok daha açık ve nettir. Köprü, bina ya da tünel yapımında mühendisler zor hava şartlarına ya da depreme karşı nasıl önlem alacaklarını hesaplayabilir. En zorlu koşullara göre tasarımlarını yaparlar ve bu koşullardan daha zorlu koşullarla karşılaşmayacaklarından emin olabilirler. Oysa kripto algoritma ya da protokol tasarımında tehditler belirsiz olduğundan alınacak önlemler de açık değildir. İşte güvenli bir kripto sistemi tasarlamanın altında yatan kavramsal zorluk buradan gelir. Yıllarca güvenli olduğu düşünülen bir şifreleme algoritması, yeni çıkan bir saldırı metoduna maruz kalarak bir günde güvensiz hale gelebilir. Dünyanın en tanınmış ve önde gelen kriptologlarının protokol tasarımları bile kırılabilir. Literatür bu tür örneklerle doludur. Diğer tasarım bilimlerinde pek rastlanmayan bu olguyla kriptografide sık sık karşılaşırız.

Kripto algoritmalarının güvenliğini ölçme bilimine kriptoanaliz denir. Bir algoritmanın güvenliğini ölçmek, o algoritmanın ne kadar sağlam olduğunu ispatlamak gibi pozitif yönde olabileceği gibi, algoritmayı kırmak gibi negatif yönde de olabilir. Genellikle kriptoanaliz negatif yönde çalışmalarla, yani kripto sistemlerini kırmakla özdeşleşmiştir. Halbuki bir kripto sisteminin güvenliği hakkında yapılan her çalışma, olumlu olumsuz elde edilen her sonuç, bir kriptoanaliz faaliyetidir..

Bir kriptolog tasarladığı algoritmanın ne kadar sağlam olduğunu matematiksel ya da biçimsel olarak kanıtlama yoluna gidebilir. Bu yönde yaptığı çalışmalar ve algoritmasının sağlamlığı ile ilgili elde ettiği bulgular, kendi tasarımı için bir kriptoanaliz çalışması demektir. Güvenlik ispatı yapılırken önce genellikle olası saldırganın kabiliyeti modellenir. En yaygın kullanılan modellemeler "standart" ve "kâhin" modellemeleridir.

Aslında kullanılan hemen hemen bütün sistemler pratikte kırılabilir. Ancak bunun bir maliyeti vardır ve bu maliyet de çoğu kez insanlığın hiçbir zaman ulaşamayacağı kadar yüksektir. Diğer taraftan, teoride kırılamayacağı ispatlanabilen şifreler vardır. Örneğin 1918'de bir AT&T mühendisi olan Vernam'ın önerdiği Tek Kullanımlık Istampa (OTP-*One Time Pad*) şifrelemesinin, 1949'da başka bir AT&T mühendisi Shannon tarafından şartsız güvenlik sağladığı ispatlanmıştır. Düşmanın sonsuz bir hesaplama gücü olsa bile, şifreyi kırması mümkün değildir. Ancak şifreleme için açık me-



Bir RFID etiketi

Visual Photos

tin kadar bir anahtar da gerektiğinden ve bir anahtarla sadece bir kere şifreleme yapılabildiğinden, Vernam'ın tek kullanımlık ıstampası pratik değildir. İlginç olan, bu şartlar sağlanmadığı zaman Vernam şifrelemesinin son derece zayıf kalmasıdır.

Kriptologlar şartsız güvenlik yerine, uygulaması çok daha kolay olan hesapsal güvenliğe yoğunlaşır. Günümüzde hemen hemen bütün kripto sistemleri ve algoritmaları bu güvenlik kriterine göre tasarlanır. Hesapsal güvenliğe göre tasarlanmış bir algoritmanın sağladığı güvenlik, belirlenmiş bir hesapsal zorluk ile ifade edilir. Bu zorluğu aşacak hesapsal güce sahip olanlar sistemi kırabilir.

Hesapsal zorluk derecesi genellikle günümüz teknolojisiyle, hatta 50-100 yıl sonrasının teknolojisiyle dahi ulaşılamayacak bir hesapsal güç gerektirecek şekilde belirlenir. Örneğin bir şifreleme standardı olan AES şifreleme algoritması, en düşük seviyede 128 bitlik, en yüksek seviyede 256 bitlik güvenlik sağlar. Kaba kuvvet (yani anahtarları tek tek deneme) saldırısı ile 2'nin 128. kuvveti kadar (yani 128 tane 2'nin çarpımı kadar) şifreleme yapmak, günümüz teknolojisi ile ve hatta 15-20 yıl sonrasının teknolojisiyle bile, hesaplama biliminde çok önemli bir gelişme olmayacağını varsayarsak, mümkün gözükmemektedir. Bu hesapsal güce kimsenin ulaşamayacağını kabul edersek, AES kaba kuvvet saldırısına dayanıklıdır. Ama tabii kimbilir, belki uzaylılar vardır ve onların teknolojileri çok daha gelişmiştir. Bu uzaylılar belki kuantum bilgisayar da imal etmiş olabilir ve insanoğlunun AES ile yaptığı şifrelemeleri çözebiliyorlardır. Hesapsal güvenlikte, düşmanın hem günümüzdeki hem de gelecekteki hesapsal gücünü dikkate almak ve teknolojinin geleceğini öngörmek gerekir.


JUPITERIMAGES

Güvenlik İspatında Kâhin Modeli

Tipilere ve hırçın rüzgârlara meydan okuyup yalçın kayalıkların arasındaki, bulutlara tepeden bakan mağaraya ulaştınız. Ulu kâhinin huzuruna çıkıyorsunuz. Size kâhinin soracağınız tüm sorulara cevap vereceği müjdelendi. Yalnız asıl cevabını aradığınız soru hariç: Mutluluğun anahtarı nedir?

İşte, kriptografik ispatlarda saldırganın yeteneğini modellemekte en çok kullanılan yöntemlerden biri de saldırganın böyle bir bilgeye danıştığı varsayımını kabullenen "Rastsal Kâhin Modeli"dir (random oracle model). Efsanedeki kâhin her şeyi bilse de, rastsal kâhinin bilgisi sınırlıdır.

Kâhinin huzurunda soru sormanın adabı nedir?

Başlıca kuralları sıralayalım: Kâhine doğrudan aranan cevabı verecek (örneğin "bu algoritmanın anahtarının tersi nedir?" ya da "Sayın kâhin, bana şu özet fonksiyonunda bir çakışma verir misiniz?" gibi) sorular sorulamaz. Kâhinden bilmediği soruların cevabı beklenmez. Örneğin kâhin sadece özet alabiliyorsa, özet çıktıya bakıp giren metni söylemesi beklenmez. Aynı sorunun birden fazla cevabı varsa, kâhin aynı soruya hep aynı cevabı verir. Örneğin bir fonksiyon çıktısına giden farklı girdi değerleri arasından hep aynısını seçer, fakat siz hangi cevabı vereceğini ilk soruyu sormadan tahmin edemezsiniz. Çünkü ilk seçim rastsaldır.

Kâhin modelinin kullanılışına bir örnek verebilir misiniz?

Diyelim ki, bir blok şifreleme algoritmasının anahtarını ele geçirmek istiyorsunuz. Kâhine istediğiniz açık metinlerin şifreli karşılığını sorabilirsiniz. Hatta seçtiğiniz şifreli metinlere karşılık gelen açık metinleri de sorabilirsiniz. Daha da ileri gidip, seçtiğiniz bazı özel açık metin çiftlerinin (örneğin sadece bir karakteri farklı, açık metin çiftleri) şifreli karşılığını isteyip, sonra bu şifreli metin çiftlerindeki eşlerden her birinin birer karakterlerinin değiştirilmiş hallerine karşılık gelen açık metinleri de isteyebilirsiniz. Kâhinden öğrendiğiniz açık-kapalı metin çiftlerini analiz edip

Aslında şu ana kadar bir kripto sistemini kırmanın ne anlama geldiğini henüz açıklamadık. Bir kripto sistemini kırmak, belirlenmiş bir hesaplama gücüne karşı sağlandığı iddia edilen bir kripto hizmetinin, daha az hesaplama gücüyle engellenmesi olarak tanımlanabilir. Belki kısa bir yol vardır; AES'i kırmak için 2'nin 128. kuvveti kadar şifreleme yapmaya gerek olmayabilir. Kim bilebilir ki! AES on yıldır literatürde olmasına ve yoğun kriptoanaliz çalışmalarına maruz kalmasına rağmen, şu ana kadar daha kısa bir yol bulan çıkmadı. İşin ilginç yanı, daha kısa bir yolun olmadığını ispatlayan da çıkmadı.

Yukarıda verdiğimiz kripto sistemi kırma tanımı teorik bir tanımdır. Bir kripto sistemindeki hiç hesapta olmayan, o ana kadar kimsenin fark edemediği bir özellikten kaynaklanan bir zayıflığın sömürülmesiyle o sistem kırılmış sayılabilir. Ancak atağı uygulamak pratikte mümkün olmayabilir. Bir AES şifrelemesinde kullanılmış anahtarı 2'nin 120. kuvveti kadar şifreleme yaparak ele geçirecek bir yöntem keşfetmiş olabilirsiniz. Bu durumda AES'i kırmış sayılırsınız. Kripto dünyasında meşhur olursunuz ve kripto tarihine geçersiniz. Ancak AES'in sağlaması gereken hesapsal güvenliği 256 kat aşağı çekmiş olsanız dahi, atağınız pratikte uygulanamayacaktır. 2'nin 120. kuvveti kadar şifreleme yapabilecek teknolojiyi elde etmek (bunun için milyarlarca TL harcamaya hazır olsanız dahi) şu anda ve yakın gelecekte mümkün gözükmüyor.

buradan anahtarı tahmin etmeye çalışırsınız. Hâlâ anahtarı ele geçirecek bir yöntem aklınıza gelmiyorsa, algoritmanın sağlam olduğuna kanaat getirebilirsiniz. Bu kanaatiniz henüz bir teorem değil. Eğer anahtarın ele geçirilemeyeceğine dair bir ispatınız varsa, o zaman başka. Bu durumda kâhin modeliyle güvenlik ispatı yapmış olursunuz.

Kâhin modeli ne kadar "gerçekçi"?
Saldırganın ele geçirdiği, içini açıp anahtara ulaşamasa da istediği mesajları şifreleyebildiği bir kripto cihazını, pratik bir şifreleme kâhini olarak düşünebiliriz. Ayrıca saldırganlar sistemin işleyişini, anahtar hariç, biliyor.

Peki saldırgan kâhine danışabiliyorsa anahtara ne ihtiyacı var?
Dağın tepesindeki bir ölümlü, kâhini sürekli meşgul edemez.
Hem kâhine danışmanın bedava olduğunu kim söyledi? Saldırganın başarısı, kâhine en az sayıda ve niteliği düşük soru sorarak elde etmek istediği sonuca ulaşmakta. Örneğin toptan sorulan n tane soru, her biri eski cevaplardan faydalanılarak sorulan n tane soruya göre daha düşük niteliklidir.

Bir sistem rastsal kâhin sayesinde de çözülemiyorsa güvenli midir?
Kâhin modeli benimsenerek güvenliği ispatlanmış kripto algoritmaları ve protokolleri, bir tür zorlu şartlara dayanıklılık testinden geçmiş gibi algılanabilir. Ama dikkat!
Kriptoloji son derece şaşırtıcı bir bilim. Zorlu teorik koşullarda sağlamlığı kanıtlanmış bir algoritma, pratik hayatta çok daha basit koşullarda güvensiz olabiliyor. Literatürde kâhin modeli benimsenerek güvenliği belli koşullarda ispatlanmış ama ardından pratik saldırılarla kırılmış kripto algoritmalarına ve protokollerine rastlayabilirsiniz.

Bu neden kaynaklanıyor?
Rastsal kâhin çoğu zaman ideal fonksiyonlar kullanıyor. Örneğin özet fonksiyonu gerçekten olması gerektiği gibi, fakat pratik sistemlerde bu tür fonksiyonların çok ufak da olsa kusurları olabiliyor. Ayrıca ispatlardaki varsayımlar, gerçek hayatta rastlayamayacağımız kadar "uçuk" olabilir.

O zaman ispatlarda kâhin modeli neden kullanılıyor?
Bu soru kriptologlar arasında da çok tartışılıyor. Saldırganın sadece işlem gücü ve sorgu sayısı ile sınırlandığı standart modelde ispat yapmak son derece güç, hatta bazı durumlarda imkânsız gibi. Çoğunlukla ispata nereden başlanacağı bile bilinmiyor. Hiç ispatı olmayan bir sistem yerine rastsal kâhine dayanıklı bir sisteme daha çok güvenebiliriz, çünkü pratikte kusurlu parçaları değiştirebiliyorsanız saldırganın eli kolu bağlı demektir.
Hem kriptologlar her geçen gün daha dayanıklı parça üretmenin yolunu öğreniyor. İleride kusurlu tarafları düzelterek, pratikte de güvenli bir kripto sistemine ulaşılabilir.

Kaynaklar
Kahn, D., *The Codebreakers: The Story of Secret Writing,* Scribner, 1996.
Koblitz, N., *Algebraic Aspects of Cryptography,* Springer, 1998.
Mel, H. X., Baker, D., *Cryptography Decrypted*, Addison Wesley, 2001.
Menezes, A. J., Oorschot, P. C., Vanston, S. A., *Handbook of Applied Cryptography*, CRC, 1997.
Vaudenay, S., *A Classical Introduction to Cryptography: Applications for Communications Security*, Springer, 2006.