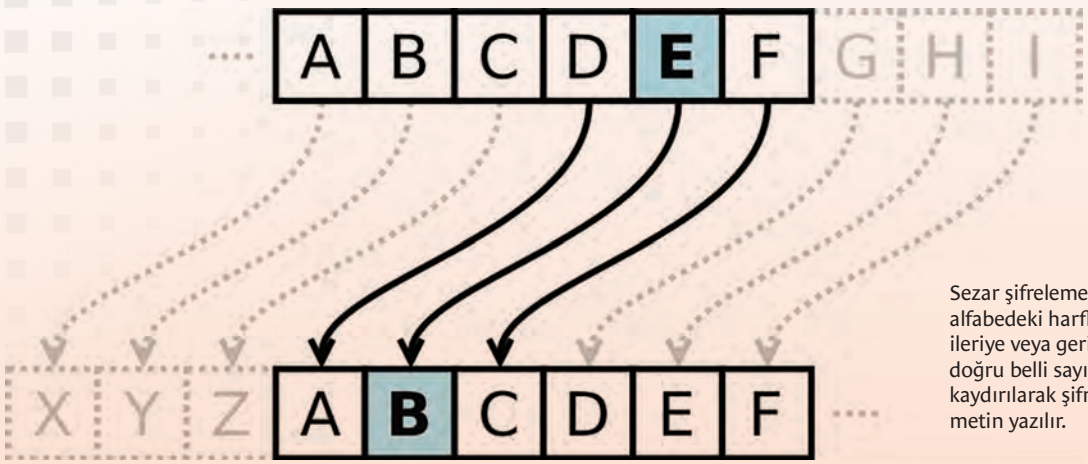
KRİPTOLOJİ

Gürkan Caner Birer [*Bilgisayar Mühendisi*

Birkaç asır öncesinde kriptoloji çok az sayıda kişinin bilip katkı sağladığı özel bir alandı. Bugün ise günlük hayatımız dijital dünya ile o kadar iç içe hâle geldi ki dijital cihazları kullanmadan neredeyse bir gün bile geçiremez olduk. Her ne kadar farkında olmasak da televizyon, telefon, tablet ve bilgisayar gibi tüm cihazlar çalışmak için kriptografiye bel bağlamış durumda. Şifre bilimi olarak da bilinen kriptoloji; mesajların belli bir sisteme göre şifrelenmesi, bu mesajların güvenlikli bir ortamda alıcıya iletilmesi ve iletilmiş mesajın deşifre edilmesi anlamına geliyor. İlk başta karmaşık ve fazla teknik bir alan gibi görünse de basit temeller üzerine inşa edilmiş bir bilim dalıdır. Kriptolojinin temellerini ve çalışma mantığını anlamak günümüz dünyasında güvenli iletişim ve verilerimizi kötü niyetli kişilerden korumak için son derece önemli. Bu yazıda kriptolojinin keyifli dünyasına birlikte göz atacağız.

Kriptolojinin Geçmişi

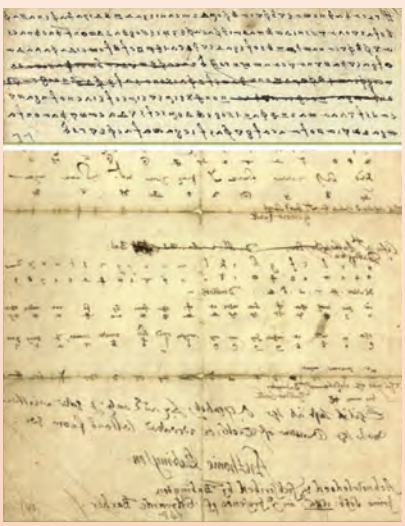
İletişime geçen iki kişi arasında başkalarının öğrenmesini istemedikleri bazı mesajlar olabilir. Tarihin başından bu yana insanlar bu tür mesajları gizli tutmanın yollarını aradı. Bu amaçla kullanılan en eski yöntemlerden biri, alfabedeki harflerin belli sayıda kaydırılarak başka bir harfle yer değiştirilmesiyle mesajların şifrelenmesidir. Roma hükümdarı Jül Sezar tarafından sıklıkla kullanılan bu yöntem Sezar şifreleme olarak da bilinir. Örneğin, 3 harf atlamalı Sezar şifresinde "BABA" yerine "EDED" yazılır. Öte yandan, Sezar şifresini (çevrimsel alfabe) kırmak görece kolaydır: Bir filolog (dil bilimci), bir dilde en çok kullanılan harfleri tespit edebilir. O harfler ile mesajda en sık geçen harfler karşılaştırılarak hangi harfin hangi harf ile değiştirildiği bulunabilir. Bu adımların ardından şifreli mesaj da çözülmüş olur.



Sezar şifrelemede alfabedeki harfler ileriye veya geriye doğru belli sayıda kaydırılarak şifreli metin yazılır.

Antik Yunan'da Spartalılar tarafından kullanılan Scytale. Bir sopanın etrafına sarılan parşömen şeride yazılan mesaj, şerit çözülüp de yukarıdan aşağıya okunduğunda anlamsız görünse de aynı çapta bir sopanın etrafına yeniden sarıldığında okunabilir hâle geliyor.

Bir başka benzer yöntem de harflerin başka sembollerle değiştirilmesidir. Ancak bu yöntemde de Sezar şifrelemeye benzer bir zayıflık vardır. Sık kullanılan sözcüklerin ve harflerin denenmesiyle bu şifreleme de hızla çözülebilir. 1587'de İskoçya kraliçesi Mary, kuzeni I. Elizabeth'e suikast girişimi için Sör Anthony Babington'a bu yöntemle şifrelenmiş bir mesaj gönderdi. İlk başta anlaşılmaz görünen bu mesaj, detaylı şekilde incelendiğinde bazı sembollerin çeşitli sıklıklarda tekrarlandığı tespit edildi. İngilizce metinlerde harflerin sıklık oranına bakılarak kolayca çözülebilecek bu şifreli metin, Kraliçe I. Elizabeth'in ajanları tarafından çözüldü ve bu nedenle hem Babington hem de Kraliçe Mary idam edildi.



Kraliçe Mary tarafından Sör Anthony Babington'a yazılan şifreli mektup ve çözümü

Sonraki dönemlerde kullanılan nispeten daha güvenilir ve popüler bir şifreleme yöntemi ise Blaise de Vigenère tarafından 1586'da yazılan bir kitapta anlatılan Vigenère şifrelemedir. Bu yöntemde bir anahtar sözcük, metindeki her bir harfin şifrelenmesi için kaydırılarak kullanılır. Anahtar sözcüğün sonuna gelince tekrar başa dönerek şifreleme işlemine devam edilir. Bu sayede her bir harf için her seferinde aynı şifreli harf kullanılmamış olur, dolayısıyla da sıklık analizi yapılamaz. 300 yıl boyunca çok güvenli bir şifreleme yöntemi olarak kabul gören Vigenère şifreleme, 1863'te Friedrich Kasiski tarafından kırıldı. Kasiski'nin yöntemi anahtar sözcüğün harf sayısını tahmin etmekle başlıyordu. Anahtar sözcüğün uzunluğu tahmin edildikten sonra ise iş sıklık analiziyle çözülebilecek bir yer değiştirme şifrelemesine dönüşüyordu.

Geçtiğimiz yüzyılın başında ise çok daha güçlü bir şifreleme yöntemi olan Enigma Almanlar tarafından geliştirildi. Bu kriptoloji yönteminde Enigma adı verilen elektromekanik bir alet yardımıyla bir anahtar sözcük ve makinenin başlangıç durumuna göre her bir harfin farklı bir harfe dönüştürüldüğü çok daha karmaşık bir sistem kullanılıyordu. II. Dünya Savaşı'nda Almanlar Enigma'nın kırılamaz olduğunu düşünüyorlardı. Hatta Enigma'nın kırılamayacağına o kadar inanmışlardı ki bazı Alman generalleri savaştan sonra bile Enigma'nın kırıldığına inanmayı reddettiler.

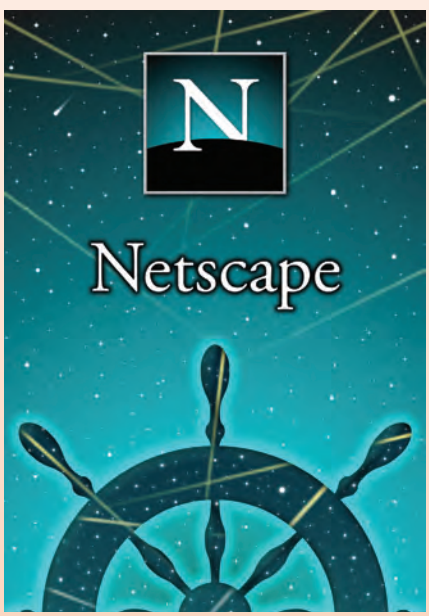
Enigma

Ancak Enigma bilgisayar biliminin öncülerinden Alan Turing'in de içinde bulunduğu bir ekip tarafından kırılmıştı. Enigma'nın kırılmasında bazı dikkatsizlikler ve hatalar da bu ekibe yardımcı olmuştu. Örneğin hemen her mesajın "Heil Hitler" ifadesiyle bitmesi önemli bir ipucu sağlamıştı. Ayrıca Enigma hiçbir zaman bir harfi kendisiyle eşleştirmiyordu. 1941'de Enigma'yı çözmeye çalışan İngiliz ekibi uzun bir şifreli metin aldı. Bu metinde hiç L harfi geçmiyordu. Bu kadar uzun bir metinde L gibi Almancada sık kullanılan bir harfin bulunmaması mümkün değildi. Bunun tek bir açıklaması vardı, o da aslında bu metnin sadece L harfinden oluşan bir test mesajı olmasıydı. Bir operatör muhtemelen L harfini test etmek için L'ye basılı tutarak uzunca bir şifreli metin oluşturmuştu. Bu sayede bir sonraki mesaj çözüldü ve Cape Matapan muharebesi kazanıldı.

Enigma'nın nasıl çalıştığını ayrıntılı olarak anlatan bir videoyu izlemek için https://youtu.be/ybkkiGtJmkM adresini ziyaret edebilir ya da aşağıdaki kare kodu akıllı cihazınızdaki barkod okuyucuya okutabilirsiniz.

Güvenli Şifreleme

II. Dünya Savaşı sonrasında "bilgisayar çağı" başladı ve kriptoloji artık savaşlarda kullanılan veya üst düzey devlet yöneticilerinin ihtiyaç duyduğu bir alan olmaktan çıkarak herkesin kullandığı bir sisteme dönüştü. Bunun için çok daha güvenli şifreleme yöntemlerine ihtiyaç vardı. Geçmiş kriptoloji sistemleri şifreleme yöntemini gizlemeye dayanıyordu. Şifreyi çözmeye çalışan kişinin mesajın nasıl şifrelendiğini bilmemesinin önemli bir güvenlik önlemi olduğu düşünülüyordu. Ancak her defasında farklı şifreler kullanıyor olsanız da aynı yöntemin tekrar tekrar kullanılması sonucunda eninde sonunda kullandığınız yöntem tespit edilebilir. Bu nedenle temel bazı ilkeler ortaya kondu. Bunlardan biri, "Bir kripto sistem, şifreleme anahtarı bilinmediği sürece o sistemle ilgili her şey biliniyor olsa bile güvenli olmalıdır." ilkesidir. Bunu gerçekleştirebilmek için rastgele üretilen gizli anahtarlar kullanılır.

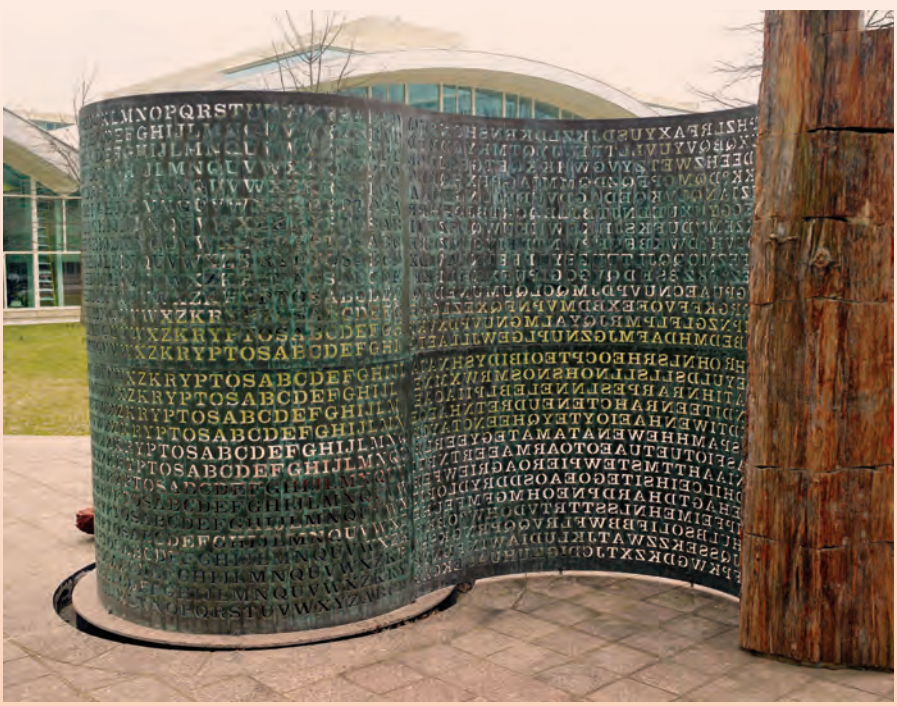


Bir dönemin en popüler internet tarayıcısı Netscape kriptolojide ihtiyaç duyduğu rastgele sayıyı üretme konusunda kolaya kaçınca büyük bir güvenlik açığı ortaya çıkmıştı.

Tüm modern kripto sistemler gizli anahtarlar üzerine inşa edilir. Bu anahtarlar tahmin edilememelidir. Kriptolojide gizlilik için rastgelelik çok önemlidir. Bilgisayar üzerinde rastgele bir sayı üretmenin bir yolunu bulmanız gerekir. Rastgele sayı üretmek için bilgisayar ağında yaşanan gecikmeyi referans almak, kullanıcıların klavye kullanımı ve fare hareketlerini dikkate almak gibi yöntemlerden tutun da termal sıcaklık dalgalanmalarını veya nükleer bozunmayı ölçen donanımlar kullanmaya kadar birçok yöntem geliştirilmiştir. Eğer rastgele sayı üretme yönteminiz zayıfsa kurduğunuz kripto sistem de zayıf olur. Örneğin; Netscape tarayıcısı, SSL iletişimi için bilgisayardaki işlem numarasını (ProcessID) ve günün saatini dikkate alıyordu. Kaynak kodunun gizli olmasına güvenen Netscape'in kaynak kodu tersine mühendislik yöntemleriyle çözülünce SSL şifrelemesi de çözüldü. 2012'de bazı güvenlik uzmanları internetteki güvenli şekilde şifrelenmiş metinleri analiz ettiklerinde bunların bir

kısmının kolayca kırılabildiğini tespit ettiler. Problemin kaynağı; klavye, fare ve sabit disk gibi donanımların aksine rastgele sayı üretmede entropi sağlayacağı düşünülen imkânlara sahip olmayan yazıcı gibi cihazların ürettiği şifrelenmiş metinlerdi. Bu cihazlar tam olarak rastgele bir sayı üretemediklerinden şifreli metinleri kolayca kırılabiliyordu.

Bir şifreli metni kırmak için ilk akla gelen yol şifreyi tahmin etmektir. Muhtemel bütün olasılıkları denerseniz şifreyi kırabilirsiniz. Ancak çoğu şifreleme yönteminde tüm olasılıklar kümesi pratik olarak denenemeyecek kadar büyüktür. Örneğin, Enigma için olası anahtar kümesi 10^{113} ihtimalden oluşuyordu. Yani tüm galaksimizi ışık hızında çalışan bilgisayarlarla doldursak bile biz tüm olasılıkları denemeye imkân bulamadan Güneş'in tüm enerjisi biterdi. Dolayısıyla çoğu zaman şifreyi tahmin etmek işe yaramaz. Bu nedenle şifreli metni kırmak için bazı olasılıkların mantıksal olarak elenmesi gerekir. Bunun için de tıpkı Enigma'nın kırılmasında olduğu gibi şifreli metnin orijinal metinle ilgili sağladığı bazı bilgilerden faydalanmalıyız. Mükemmel bir şifreleme işleminde şifreli metnin orijinal metinle ilgili hiçbir bilgiyi açık etmemesi gerekir. Bunun için de şifreleme için kullanılan anahtarın da metin kadar uzun olması lazımdır ve bu da pratik olarak mümkün değildir. Yine de modern şifreleme yöntemleri bu ilkeler üzerine inşa edilmiştir.



CIA merkez binasının önünde yer alan Kryptos adlı heykeldeki şifreli mesajlardan üçü çözülse de dördüncüsü hâlâ gizemini koruyor.

Her ne kadar şifrelemenin geçmişi çok eskilere dayansa da günlük hayatta kullandığımız birçok sistem yeteri kadar güvenli değildir. Örneğin internete bağlanmak için kullanılan kablosuz ağlarda kullanılan WEP (Wired Equivalence Privacy) protokolü, 1999'da güvenli iletişim için geliştirilmişti. Ancak iki yıl içinde bu protokolün pek de güvenli olmadığı ortaya çıktı. Öyle ki WEP şifreli modemler bir dakikadan kısa bir sürede kırılabiliyordu. Bu bilgiye rağmen yıllar boyunca üretilen birçok modemde, varsayılan erişim protokolü olarak WEP kullanılmaya devam edildi. 2012'de bile kablosuz modemlerin dörtte biri WEP ile iletişim kuruyordu. Bugün hâlâ WEP kullanan birçok cihaz var. Bu örnek bize güvenli tasarlanmayan bir protokolün yıllar boyu sürecek zararlara yol açabileceğini gösteriyor.

Güvenli şifreleme için yıllar içinde çeşitli kriptoloji yaklaşımları geliştirildi. Geleneksel olarak kripto sistemler gerçekleşen saldırılara karşı yeni önlemler almak suretiyle iyileştirmelerin yapıldığı döngüsel bir modelle tasarlanır. Tasarlanan bir şifreleme modeli saldırıya uğrayınca mevcut hataları iyileştirilerek daha iyi bir model geliştirilir. Gelişimsel bir model olsa da bu modelde de bir kripto sistemin güvenli olduğundan emin olmak mümkün değildir. Yine de yeterince güvenli(!) olduğu düşünüldüğünde söz konusu model kullanılmaya başlanır. Ayrıca geliştirilen sistemin kripto analizini yapabilmek için bilgili ve kabiliyetli uzmanlar yetiştirmek de gerekir, bu da hayli zor bir iştir.

Öte yandan, "hesaplama karmaşası kuramı" diye bilinen bir yaklaşımla, şifreyi çözmeye çalışan kişinin sahip olduğu bilgi işleme gücünü hesaba katarak kripto sistemler tasarlanabilir. Bir başka deyişle, şifreli metin teoride kırılabilir olsa da pratikte gerekli bilgisayar gücü sağlanamadığı için kırılamayacaktır. Bu tür şifreleme için matematiksel problemlerden faydalanmamız gerekir. Bunlar öyle problemler olmalı ki mesajı şifreleyenler fazla zahmet çekmemeli, şifreyi kırmaya çalışanlarsa çok zahmet çekmelidir. Bu tür problemler için bilgisayar biliminde NP-Complete olarak bilinen hesaplaması zor problemler akla gelir. Ancak bunlar şifreleme için iyi bir seçim değildir. Çünkü en kötü senaryoda hesaplaması çok zor olsa da ortalama durumlar için hesaplanmaları o kadar da zor değildir. Bu bağlamda, tek yönlü fonksiyonlar kriptoloji için çok daha ideal problemler. Bu fonksiyonları hesaplaması çok kolay ama geri döndürmesi çok zordur. Tek yönlü fonksiyonları

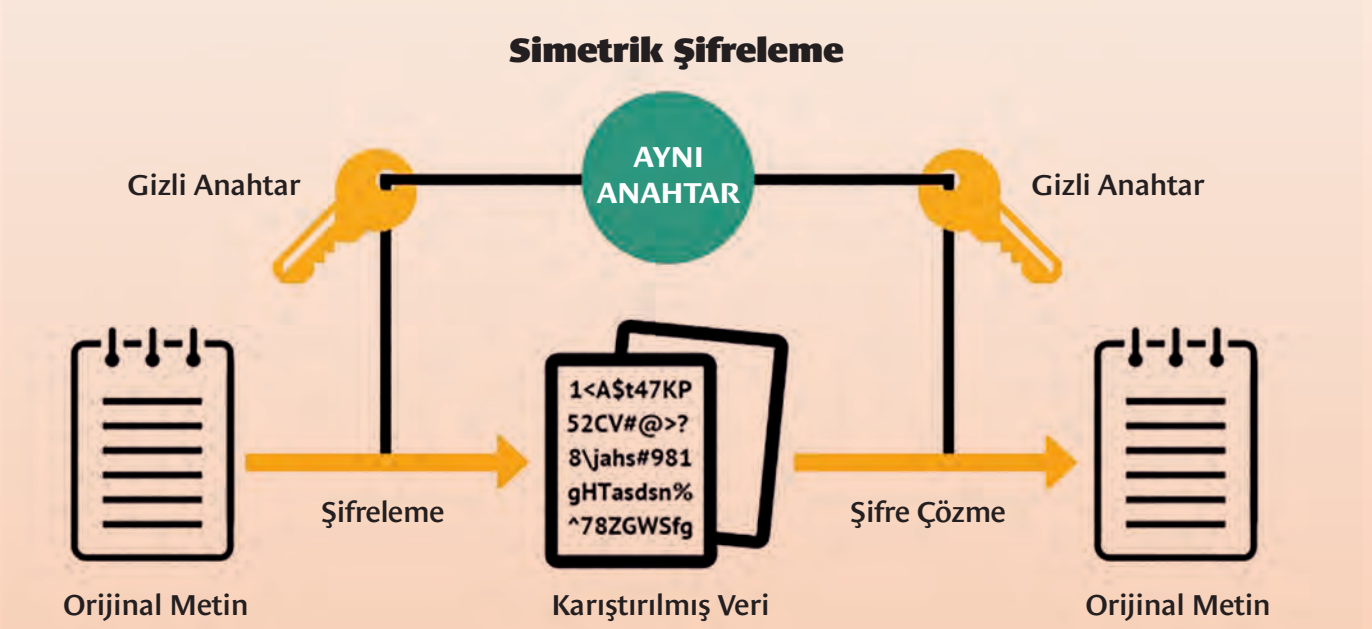
tıpkı cam bir vazo gibi düşünebilirsiniz. Kırması kolay ama tekrar birleştirmesi çok zordur. Bu tür fonksiyonlara en güzel örnek çarpma işlemidir. Bütün sayılar ya asal sayıdır ya da asal sayıların çarpımıyla oluşur. İki sayının çarpımını hesaplamak kolaydır. Ama rastgele verilen bir sayının hangi sayıların çarpımı olduğunu hesaplamak çok çok zordur. Örneğin 20'nin 2x2x5 olduğunu anlamak kolaydır ancak 2.244.354'ün 2 x 3 x 7 x 53.437 olduğunu tespit etmek hayli zordur. Bir bilgisayar için, her biri 100 basamak uzunluğunda iki asal sayıyı çarpmak o kadar da zor değildir. Ancak büyük bir sayıyı asal çarpanlarına ayırmak süper bilgisayarlar için bile oldukça zaman alıcıdır. Bu matematiksel bilgiyi kullanarak bir şifreleme sistemi yani güvenlik modeli geliştirilebilir.

Güvenlik Modeli

İdeal senaryoda iletişime geçmek isteyen iki kişi başka hiçbir kimsenin haberdar olamayacağı bir kanal üzerinden iletişim kurabilmeli. Ancak gerçek hayatta böyle bir kanal yerine internet ve telefon gibi başkalarına da açık kanallar üzerinden iletişim sağlanıyor. Kriptolojinin temel işlevi bu şekilde açık kanallar üzerinden yapılan iletişimi güvenli kılmaktır. Kriptoloji ideal bir kanalın tüm özelliklerini sağlamaya çalışmak yerine mahremiyet, mesajın gerçekliği ve bütünlüğü gibi en önemli konulara odaklanır. Bu amaçları gerçekleştirebilmek için taraflar bir iletişim yöntemi, yani "protokol" üzerinde anlaşmalıdır. Kullanılacak şifreleme yöntemlerinin yanı sıra yazılımlar ve cihazlar gibi unsurların tümü protokol kapsamında belirlenir. Kriptolojide sadece güvenli iletişim kuran kişilerin bildiği, ancak başkalarının bilmediği özel bazı bilgilerden faydalanılır. Kriptolojide kullanılacak güvenlik modeli başlangıçta kimin hangi anahtar şifrelere sahip olduğunu belirler. Temel olarak iki güvenlik modeli vardır: Simetrik (paylaşılan anahtarlı) ve asimetrik (açık anahtarlı) model.

Simetrik Model

En basit ve yaygın model gönderici ve alıcının başkalarının bilmediği bir anahtar kullanarak şifreleme yapmasıdır. Simetrik model denilen bu yöntemde, tüm şifreleme ve şifre çözme işlemleri bu anahtara göre yapılır. Gönderici ve alıcı taraflar güvenli iletişime başlamadan önce bir şekilde ortak bir anahtar (şifre) belirlemelidir. Bir şekilde iki tarafın



da bu şifreyi bildiği ve üçüncü tarafın bu şifreyi ele geçiremeyeceği varsayılır. Simetrik algoritma, bir şifreleme algoritması ve anahtar şifre kullanarak açık bir metni anlamsız bir metne çevirir. Ayrıca mesajın yolda değiştirilmediğini doğrulamak için mesaj kimlik kodu (MAC) adı verilen bir etiket de mesaja eklenir. Gönderici bu etiketi oluşturmak için şifreli metin ve anahtarı birlikte kullanır. Eğer metin içerisinde küçük bir kısım değişse bile bu etiket geçersiz olacaktır. Bu şifrelenmiş metni ele geçiren üçüncü bir kişi başlangıçtaki açık metinle ilgili hiçbir bilgiye ulaşamamalıdır.

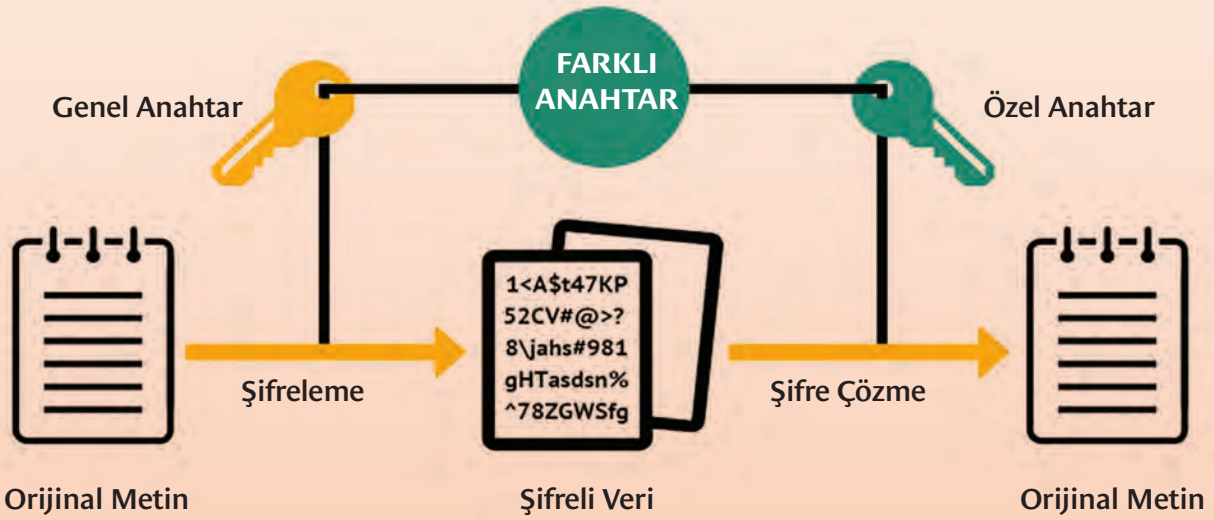
Öte yandan simetrik modelde bir saldırgan şifreli metnin uzunluğunu analiz ederek orijinal metnin uzunluğunu çözebilir. Ayrıca taraflarla ilgili sahip olduğu ek bilgiler (kim oldukları, ne amaçla konuştukları, konunun ne olduğu gibi) şifrenin kırılmasına yardımcı olabilir.

Asimetrik Model

50 yıl öncesine kadar kriptoloji, şifrelemek için kullanılan anahtarın şifreyi çözecek kişilerle önceden paylaşılması esasına dayanıyordu. Sezar şifrelemede kaç karakter kaydırılması gerektiği taraflarca önceden belirleniyordu. Enigma'da da şifrelenen mesajı çözebilmek için bir Enigma cihazına ve şifre defterine ihtiyaç vardı. Peki ya böyle bir imkân yoksa? Yani taraflar güvenli iletişim için kullanacakları şifreyi önceden paylaşmamışlarsa o zaman ne olacak? 1974'te Berkeley'de üniversite öğrencisi olan Ralph C. Merkle bir ders için verdiği proje önerisine şöyle başlamıştı:

"Bugüne kadar doğru kabul edilen, *'İki kişi güvenli iletişim kurmak için önceden bir şifreli iletişim yöntemi üzerinde anlaşmalıdır, aksi takdirde herkese açık bir iletişim kanalını kullanarak güvenli şekilde iletişim kuramazlar.'* varsayımının yanlış olduğunu düşünüyorum. Hayır şaka yapmıyorum…"

Her ne kadar Merkle'ın proje önerisi okul tarafından reddedilse de sonrasında Merkle ile tanışan Whitfield Diffie ve Martin Hellman bu fikri geliştirip adına "açık anahtar kriptografisi" (public key cryptosystem) diyerek 1976'da yayımladıkları makaleyle bugün Diffie-Hellman anahtar değişim protokolü diye bilinen yöntemi dünyaya tanıttı.



Açık anahtarlı model olarak da bilinen asimetrik modelde, iletişim kurmak isteyen taraflar arasında önceden bilinen bir anahtar şifre kullanılmaz. Her iki tarafın da herkesle (üçüncü kişiler dâhil) paylaştığı bir açık anahtarı ve kimseyle paylaşmadığı bir gizli anahtarı olur. Gönderici gizli bir mesaj göndermek istediğinde alıcının açık anahtarını kullanarak bu mesajı şifreler. Bu şifreyi çözmek için ise alıcının gizli anahtarı gerekir, aksi takdirde bu şifre çözülemez (daha doğrusu çözülmesi mevcut bilgisayarların kapasitesiyle son derece zordur). Alıcı ise kendi gizli anahtarını kullanarak şifreli metni anında çözebilir. Mesajın belirli bir göndericiden geldiğini teyit etmek için şifreli mesaja bir imza bölümü eklenir. Bu bölüm göndericinin gizli anahtarıyla şifrelenmiş olsa da göndericinin açık anahtarıyla çözülebilir. Böylece alıcı mesajdaki imza bölümünü göndericinin açık anahtarıyla çözerek bu mesajın gerçekten de o belirli göndericiden geldiğini anlar. Bir önceki bölümde bahsettiğimiz asal çarpanlara ayırma konusu burada kullanılır. Açık anahtar büyük sayı iken, gizli anahtar bu sayıyı oluşturan asal sayılardır. Asal sayılardan açık anahtara ulaşılabilirken, açık anahtardan çarpanları oluşturan sayılara ulaşılamaz.

Günümüzde asimetrik şifreleme için en yaygın kullanılan yöntem RSA algoritmasıdır. RSA'da açık anahtarla şifrelenen metin gizli anahtarla çözülür, gizli anahtarla şifrelenen metin de açık anahtarla çözülür. Böylece size mesaj göndermek isteyen kişi mesajı sizin açık anahtarınızla şifreleyerek gönderir. Gizli anahtar sadece sizde olduğu için bu şifreyi sizden başkası çözemez. RSA anahtarları genellikle 1.024 veya 2.048 bit uzunluğunda olur. İki yıl süren bir denemede, çok yoğun işlemci gücü ve birçok kişinin desteğiyle 768 bitlik bir RSA şifresi kırıldı. İşlemci kapasitesindeki hızlı artış dikkate alındığında önümüzdeki yıllar içerisinde 1.024 bitlik şifrelerin kırıldığını görebiliriz. Dolayısıyla artık 2048 bit veya daha uzun şifrelerin kullanılması tavsiye ediliyor. İnternet erişiminde sıklıkla kullanılan TLS (Transport Layer Security) de RSA üzerine kuruludur.

Hash

Hash bir verinin matematiksel özetini ifade eden değer olarak tanımlanabilir. Elimizde internetten indirdiğimiz bir dosya olduğunu varsayalım, bu dosyanın orijinal dosyanın bire bir aynısı olduğundan nasıl emin olabiliriz? Elbette orijinal dosya indirilip bütün veri bitleri tek tek karşılaştırılarak sağlama yapılabilir ama bu son derece zahmetli bir yöntemdir. İşte bu noktada Hash fonksiyonları devreye girer. Bu fonksiyonlar veri boyutu ne kadar büyük olursa olsun hep aynı uzunlukta bir özet çıkarır. Verideki bir bit değişmiş olsa bile farklı bir özet ortaya çıkar. İki ayrı dosyanın aynı hash özetine sahip olma olasılıkları hayli düşüktür. Hash fonksiyonları bir veriyi sabit uzunluktaki başka bir

veriye dönüştüren algoritmalardır. Bu fonksiyonlar deterministik olarak çalışır. Yani bir veri için her defasında aynı sonucu verir. İki dosyanın aynı olup olmadığını kontrol etmek için faydalı bir yöntem olsa da işin içine gizlilik girdiğinde bu fonksiyonlar yetersiz kalabilir. Her ne kadar özet veriden orijinal veriye ulaşmanın doğrudan bir yolu olmasa da (çünkü bu veri özettir) dolaylı yöntemlerle orijinal veri tahmin edilebilir.

Çevrim içi sistemlere giriş yapmak için kullandığımız parolalar veri tabanlarında hash'lenerek saklanır. Örneğin Adana909 şeklinde bir parolanız olduğunu varsayalım. Bu parola bir hash fonksiyonundan geçirilerek ZHHHHXXHXGSUYTK şeklinde bir metne dönüştürülür ve veri tabanında saklanır. Siz sisteme her girmeye çalıştığınızda girdiğiniz parola aynı yöntemle hash'e dönüştürülür ve hash'ler kıyaslanır. Eğer hash'ler aynı ise girmenize izin verilir. Bu sistemin veri tabanını ele geçiren kötü niyetli bir bilgisayar korsanı çokça bilinen parolaların hash'lerini kıyaslayarak var olan parolaları kırabilir. Bu sorunu çözmek için tuz (salt) adı verilen bir anahtar sözcük kullanılır. Kullanılan hash fonksiyonuna sadece sistemin sahibinin bildiği özel bir metin kullanılarak dönüşüm sağlanır. Böylece veri tabanı ele geçirilse bile bu parolalar orijinaline dönüştürülemez. Hatta kimi sistemlerde her kullanıcı için farklı bir tuz oluşturulur ve bu tuz değerleri de veri tabanında saklanır. Böylece aynı parolayı kullanan kişilerin hash'leri bile farklı olur. Bu durumda veri tabanını ele geçiren bir bilgisayar korsanının her bir kullanıcının şifresini çözmesi için ayrı ayrı bütün bilinen parolaları denemesi gerekir ki bu da çok çok maliyetli bir işlemdir. Dolayısıyla bu yöntemle parolalar güvenli şekilde saklanmış olur. MD5, SHA-1, SHA-2, SHA-3, bcrypt, ve BLAKE3 gibi algoritmalar en popüler hash algoritmalarıdır.

Blok Şifreleme

Blok şifreleme belli uzunluktaki veri bloklarını şifrelemek için kullanılan algoritmadır. Bu algoritma bir açık metni, bir anahtar metin yardımıyla aynı uzunluktaki farklı bir metne dönüştürür. Şifrelenmiş metin aynı anahtar metin kullanılarak bir şifre çözme algoritmasıyla tekrar açık metne de dönüştürülebilir. Şu anda kullanılan en popüler blok şifreleme metodu İngilizce Advanced Encryption Standard (İleri Şifreleme Standardı) ifadesinin kısaltması olan AES'dir. Bu algoritma, DES adındaki blok şifreleme metodunun yeterli gelmemesi üzerine herkesin katılımına açık olarak düzenlenen bir yarışma sonucunda ortaya çıktı ve geniş bir çevre tarafından kabul gördü. AES'de blok uzunlukları 128 bit, anahtar uzunluklarıysa 128, 192 ve 256 bit uzunluğunda olabilir.

KUANTUM KRİPTOLOJİ

Kuantum fiziğinin kriptolojide kullanımı yeni gibi gelse de aslında 1960'lara kadar uzanıyor. 1968'de Stephen Weisner'in kuantum para uygulaması kuantum fiziğinin kriptolojiye dönük ilk uygulaması olarak literatüre geçti. Kuantumla ilgili temel kavramları anlamak

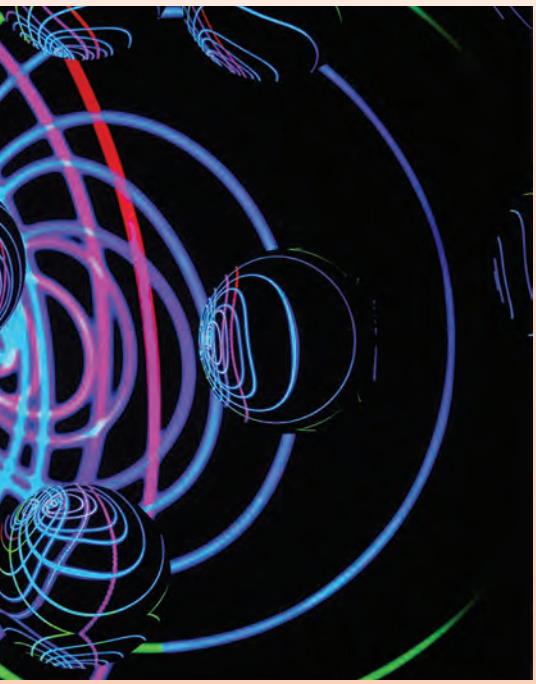
biraz güç. Örneğin bir cisimciğin aynı anda iki yerde veya durumda bulunabilmesi olarak adlandırılan süperpozisyon, cisimciklerin arasında uzun mesafeler olsa bile etkileşim hâlinde olduğu kuantum dolanıklığı ve kuantum bilinmezliği gibi ilkeler klasik fizikten çok farklı olduğu için bu konuları anlamak ve üzerlerinde çalışmak hayli zor olabilir.

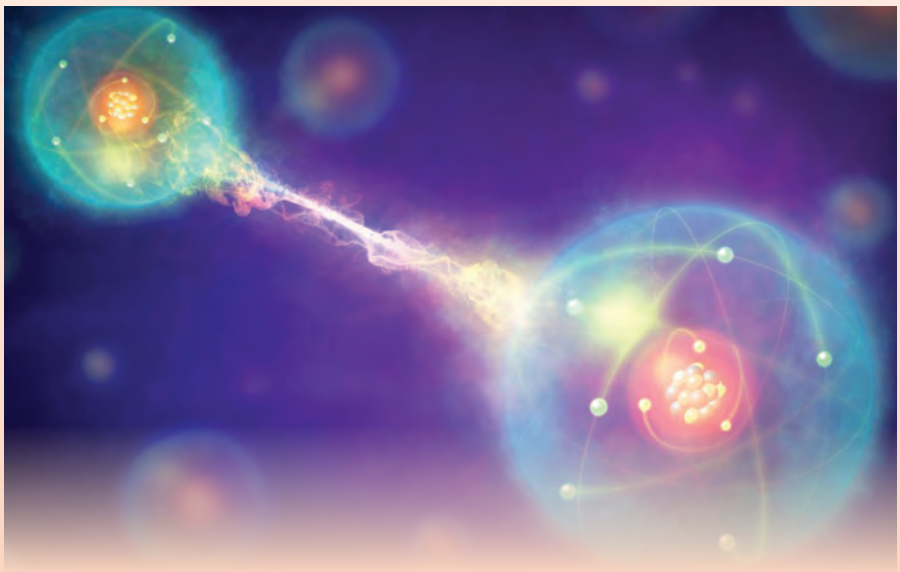
Klasik bilişimde her şey 0 veya 1 değeri alabilen bitler üzerine inşa edilmiştir. Kuantum bilişimdeyse bit yerinde kübit (qubit) vardır. Bit 0 veya 1 değerlerinden biri olmak zorundadır ancak kübit için böyle bir zorunluluk yoktur, her ikisi birden olabilir. Biraz kafa karıştırıcı olsa da kuantum bilişimi güçlü yapan bu temellerdir. Bir kübite ölçüm işlemi uygulandığında 0 veya 1 olarak bir değer elde edilir. Yani artık kübit klasik bir bite dönüşmüş olur. Bir bakıma ölçerek kuantum sistemi bozmuş oluruz.

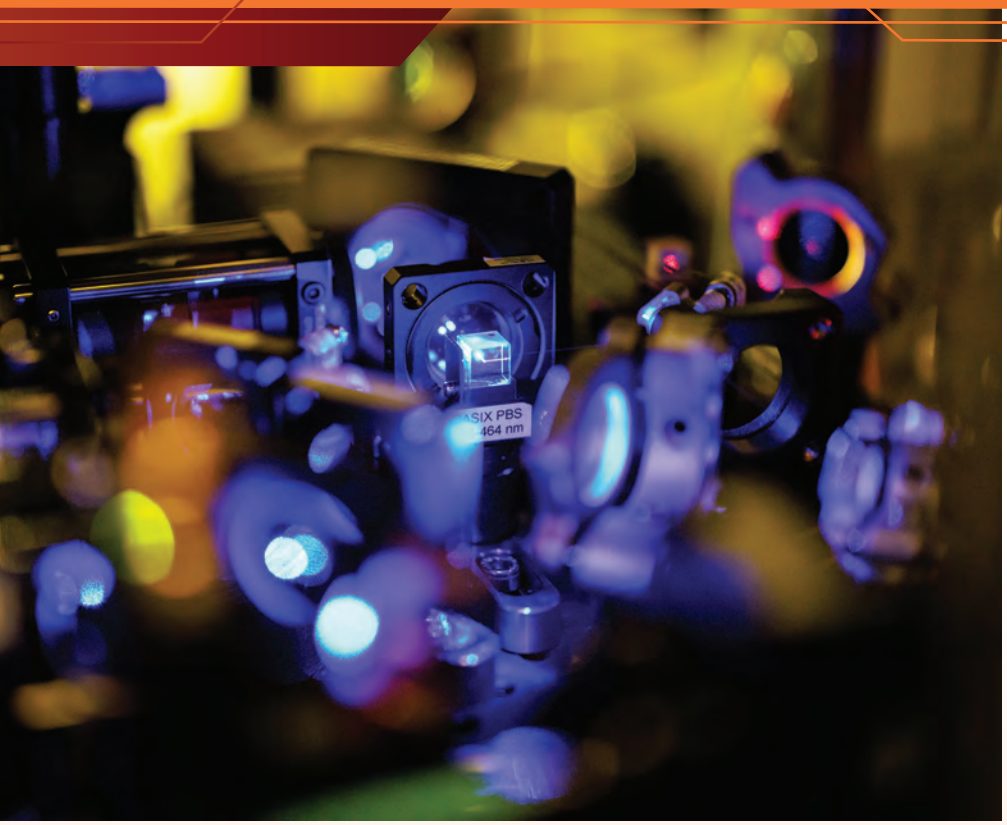
Diğer yandan, bir kuantum sistemi fiziksel olarak klonlamak mümkün değildir. Bir başka deyişle bir kuantum verisini alıp iki eşit kopya olarak veren bir sistem yoktur. Çünkü kopyalamak için okuduğunuz anda kuantum sistem bozulur. Kuantumu ilginç kılan bir başka unsur da kuantum dolanıklığıdır. Elimizde bir kübit olduğunu düşünelim. Bunu ölçerek kuantum sistemini çökerttiğimizde ilgisiz gibi görünen bir başka kübit de bundan etkilenir ve aynı anda o da çöker. Bir bakıma görünürde birbiriyle bir bağı olmayan ama ortak hareket eden iki kutunuz var gibi düşünebilirsiniz.

Kuantum kriptolojinin temelleri eşlenik kodlama (conjugate coding) veya kuantum kodlama diye adlandırılan yönteme dayanıyor. Bu yöntem daha önce bahsedilen iki anahtar özelliğe göre çalışır. İlk olarak, eşlenik kübitlerden birini okumak diğerinin de yıkılmasına neden olur. İkincisi, kuantum kodlamayı doğrulayabilmek için kodlama algoritmasını bilmek gerekir; aksi takdirde kodlanmış veri okunduğunda yapısı bozulacağı için onu doğrulamak mümkün olmayacaktır. Wiesner'in yıllar önce ortaya attığı kuantum para, tam da bu ilkeler üzerine kuruluyordu ve asla sahtesi yapılamayacak dijital jetonlar üretmeyi hedefliyordu.

Kuantum anahtar dağılımı (Quantum Key Distribution -QKD) ise güvenli iletişim kurmak isteyen iki tarafın rastgele üretilmiş kuantum







temelli ortak anahtarların mesajları şifrelemek ve şifreyi çözmek için kullanılmasıdır. Bu yönüyle geleneksel kriptografik sistemlere benzese de gönderilen mesajların üçüncü bir kişi tarafından okunması durumunda çöken kuantum sistemlerden dolayı mesajlar bozulacak ve birilerinin araya girdiği anında anlaşılacaktır. Geleneksel açık anahtar sistemleri hesaplama zorluğuna dayanarak çalışırken QKD tamamen kuantum fiziğinin temel yapısına dayalı olarak çalışır. Ancak QKD yönteminde ortak anahtarın önceden biliniyor olması gerekliliği bir sınırlılık olarak değerlendirilebilir. Kuantum şifrelemede ilk akla gelenin QKD olmasındaki en büyük etken, laboratuvar ortamında test edilebiliyor olmasıdır.

Kriptolojinin temel öğelerinden birisi de üstlenme şemasıdır. Üstlenme şemasında seçilmiş bir bilgiyi kapalı olarak başkalarıyla paylaşırsınız ve sonrasında o bilgiye erişmek için gerekli anahtarı seçtiğiniz kişiyle paylaşırsınız. Üstlenme şemasını bir mektup yazıp küçük bir kasaya kilitleyerek kasayı bir başkasına göndermeye benzetebilirsiniz. Zamanı geldiğinde anahtarı paylaşarak karşıdakinin mektubun içeriğini görmesini sağlayabilirsiniz ancak o zamana kadar bu bilgi değişmeden kasada saklı kalır. Kuantum kriptolojide bu işin yapılabilmesi için bit üstlenmesinden faydalanılır. Bit üstlenmesinde gönderici alıcıya iki bilgi gönderir. Alıcı bu bilgilerden birisini almayı seçer. Gönderici alıcının bu bilgilerden sadece birini aldığından emin olur. Alıcı da göndericinin bu bilgileri sonradan değiştirmediğinden emin olur. Önceleri bu kavramın kuantum bilişimde yapılabileceği düşünülürken sonrasında bu işlemi güvenli bir şekilde gerçekleştirmeyle ilgili soru işaretleri ortaya çıktı. Bu alanda çalışıldıkça iki yönlü hesaplama ve tarafların karşılıklı güvensizliğinin giderilmesi gibi hususlarda kuantumun sunduğu olanakların yeterli olamayabileceği soruları gündeme gelmeye başladı. Dolayısıyla, kuantum bilişim kriptolojinin temellerini oluşturan ilkeleri sağlayamazsa güvenli bir kriptoloji yöntemi olarak kullanılamayabilir. Buna rağmen QKD'nin başarıyla uygulanabileceği kuantum tabanlı ağların kurulması için çalışmalar devam ediyor. Yani bildiğimiz internet ağının yerine kuantum için uygun hatlarla hazırlanmış yeni bir ağın oluşturulması gerekiyor. Bu konuda DARPA Quantum Network, Vienna QKD, Çin hiyerarşik metropol ağı, Tokyo QKD, 2.000 km'lik Beijing-Shanghai kuantum hattı ve Birleşik Krallık kuantum ağı gibi ağlar üzerine çalışmalar yürütülüyor.

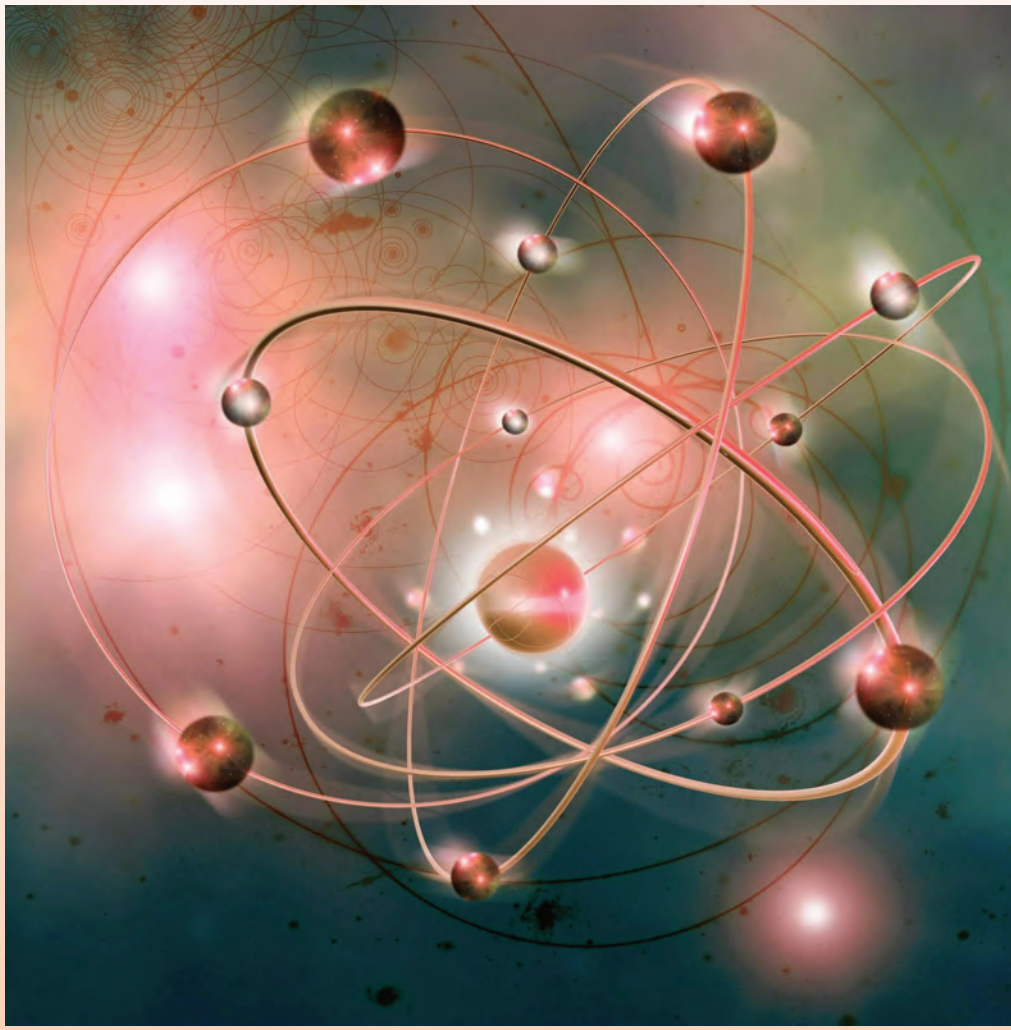
Öte yandan kuantum bilişimin kriptolojiyle iki yönlü ilgisi bulunuyor. Birincisi yukarıda belirttiğimiz kuantum anahtar dağıtımı (QKD) adındaki güvenli iletişim sağlayan kripto sistemin kurulması, diğeri ise kuantum sonrası şifreleme (PQC). Kuantum bilgisayarların teoride sunduğu devasa hesaplama gücüyle, bugünkü süper bilgisayarlarla bile kırılması binlerce yıl sürebilecek şifreler saniyeler içinde kırılabilir.

Bugün için şifrelenmiş bir iletişimi dinleseniz bile veriler şifreli olduğu için içeriğini tespit edemezsiniz. Ancak bu şifreli iletişim kayıtlarını saklayıp birkaç yıl sonra ortaya çıkabilecek yeni bir klasik algoritmayla veya kuantum bilgisayarla çözmek mümkün olabilir. Yani kuantum teknolojisinde yaşanacak gelişmeler sadece gelecekteki iletişimimizi etkilemeyecek. Bugün yapmış olduğumuz şifrelenmiş güvenli iletişimlerimiz kayıt altına alınıp ileride ortaya çıkacak olan kuantum sistemleriyle çözülebilecek. Bir başka deyişle aslında bugünkü güvenli iletişimlerimiz de tehdit altında. Bu nedenle bugünden kuantum güvenliğine sahip şifreleme algoritmalarına geçiş yapmak gerekiyor. PQC günümüzde hesaplaması zor olan faktöriyel ve diskrit logaritma gibi problemlerin kuantum bilgisayarlarla hızlıca çözülmesi anlamına geliyor.

Yine de SHA2, SHA3 ve BLAKE2 gibi kriptografik hash fonksiyonlarının büyük çoğunluğu; HMAC ve CMAK gibi MAC algoritmaları; bcrypt, Scrypt, Argon2 anahtar üretim fonksiyonları kuantum bilgisayarlar tarafından tehdit altında değil. AES-256, Twofish-256 gibi simetrik şifreleme algoritmaları da benzer şekilde kuantum korumalı olarak değerlendiriliyor. Öte yandan RSA, DSA, ECDSA, EdDSA, DHKE, ECDH ve ElGamal gibi açık anahtar kripto sistemleri kuantum bilgisayarlar tarafından kolayca kırılabilir.

Tüm kriptoloji algoritmalarının kuantum saldırılara karşı korumalı hâle getirilmesi pek mümkün görünmüyor. Çünkü koruma için çok daha uzun anahtarlar kullanmak gerekiyor ve bu da internet tüketimini artırıyor. Gerçek manada çalışan kuantum bilgisayarların geliştirilmesi için belki onlarca yıl beklemek gerekecek ama RSA gibi tüm iletişim yöntemlerimize alt yapı sağlayan algoritmaların daha güçlü hâle getirilmesi yine de faydalı olacaktır.

Ortaya atılmasından bu yana geçen yarım asırlık sürede kuantum kriptoloji heyecan verici ve aktif bir alan oldu. Kriptoloji, kuantum fiziği, matematik, bilgisayar bilimi, elektronik gibi alanlardaki güncel yöntem ve algoritmaların uygulanmaya çalışıldığı disiplinler



arası bir alan olan kuantum kriptolojide deneysel çalışmalar hâlâ prototip düzeyinde olsa da kavramsal çalışmalar her geçen gün olgunlaşıyor. Bu alanda çalışılması gereken birçok başlık olsa da aşağıda sıralananlar öne çıkıyor:

► Kuantum algoritmalar hangi tür kripto sistemleri çökertebilir? Kuantum sonrası kripto sistemler nasıl tasarlanmalı?

► Pratikte uygulanabilir olan cihazlardan bağımsız protokoller yapabilir miyiz? İletişim kanallarında yaşanacak gerçekçi bir gürültü miktarını tolere edebilen cihazlardan bağımsız protokoller geliştirilebilir mi?

► Dürüst kişilerin kolayca iletişim kurduğu ama saldırganların çözmek için devasa kaynaklar tüketmek zorunda kaldığı kuantum kriptografik sistemler kurulabilir mi?

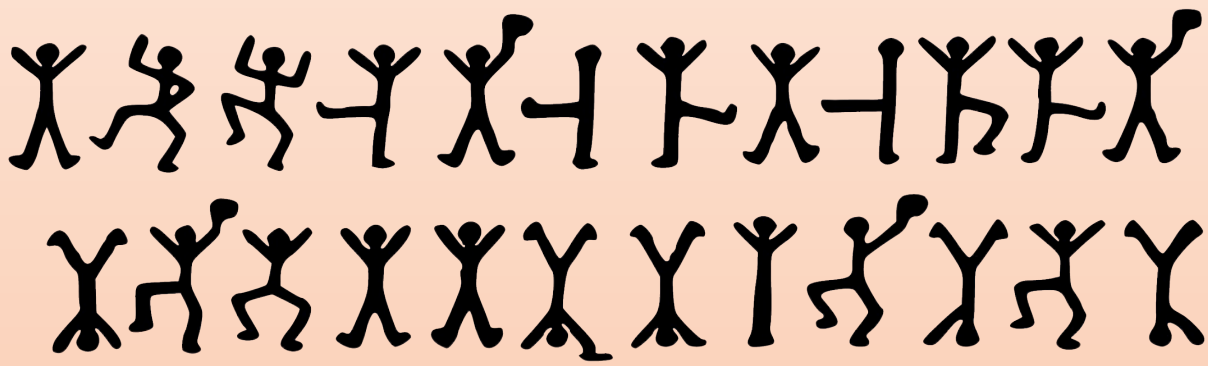
► Açık anahtarlı kuantum para geliştirilebilir mi?

Frekans analizini ilk defa anlatan Kindî'nin yazdığı kitaptan bir bölüm

ŞİFRE KIRMA

Şifrelenmiş bir metni açık metne (şifrelemeden önceki orijinal metin) dönüştürmenin iki yolu vardır. İlki şifre çözme teknikleriyle anahtar kullanarak şifrenin çözülmesidir. Kriptoanaliz olarak bilinen ikinci yöntem ise anahtara sahip olmadan şifreli metnin analiz edilmesiyle kalıpların veya diğer göstergelerin keşfedilerek açık metnin ortaya çıkarılmasıdır. Şifre kırma olarak da bilinen ikinci yöntemde birçok farklı teknik kullanılır.

Şifre kırma tekniklerinden en yaygın kullanılanı frekans analizidir. Ünlü Müslüman bilim insanı Kindî tarafından geliştirilen bu yöntemde amaç, metnin şifrelendiği dildeki harf ve sözcüklerin kullanım sıklığıyla şifreli metindeki harf ve sözcüklerin kullanım sıklığını karşılaştırarak şifreyi çözmektir. Türkçede 29 harf vardır ve genel olarak en çok kullanılan harfler sırasıyla "a", "e" ve "k" harfleridir. Sözcük bazında baktığımızda en sık kullanılan sözcükler "bir", "ve", "bu", "da", "de" ve "için" gibi sözcüklerdir. Bu genel bilgiler kullanılarak harfler ve sözcükler için bir frekans tablosu oluşturulur. Daha sonra şifreli metinde geçen harfler ve sözcükler için de benzer şekilde bir frekans tablosu oluşturulur. Bu iki tablo



Dans Eden Adamların Maceraları başlıklı kitapta, ünlü kurgu dedektif Sherlock Holmes dans eden adam figürlerini inceleyerek ve sıklık analizini kullanarak şifreli metni çözüyordu.

kıyaslanarak örtüşen harf ve sözcükler tespit edilmeye çalışılır. Şifreli metin ne kadar uzun olursa genel ortalamalara yakın frekanslar gösterme olasılığı, dolayısıyla da şifrenin çözülme olasılığı artar. Metni analiz ederken sadece harf ve sözcüklere bakılmaz, aynı zamanda en çok yan yana gelen harfler, sık kullanılan kalıplar, pek yan yana gelmeyen harfler, cümle başında pek fazla yer almayan harfler gibi birtakım kurallar da dikkate alınır.

Bir başka şifre kırma tekniği, açık ve şifreli hâli bilinen bir metinden yola çıkarak şifreleme algoritmasının tahmin edilmeye çalışılmasıdır. Örneğin II. Dünya Savaşı'nda Almanlar her gün aynı saatte hava durumu raporunu birimlerle paylaşıyordu. Hava durumunun Almancası olan "wetter" sözcüğü şifreli metinlerde hep aynı yerde bulunuyordu. Böylece bu sözcüğün şifreli ve şifresiz hâli bilinmiş oluyordu. Ayrıca yerel hava durumu İngilizler tarafında da bilindiği için metnin diğer kısımlarını da tahmin etmek zor olmuyordu. Üstelik her mesajın sonunda "Heil Hitler" ifadesi yer alıyordu. Bazı durumlarda şifreli metinde geçmesi için Alman istihbaratına bazı yer isimleri sızdırılıyordu. Kısa bir zaman sonra şifreli metinlerde bu yer isimleri geçmeye başlayınca şifreleme algoritmasıyla ilgili başka bilgiler de elde ediliyordu. Açık metin saldırısı olarak bilinen bu yöntem özellikle klasik şifreleme yöntemlerine karşı hayli etkilidir.

Bilgisayar teknolojilerinin geliştirilmesiyle hangi algoritmayla şifrelendiği bilinen bir şifreli metni çözmek için olası bütün anahtarlar da denenebilir. Kaba kuvvet saldırısı (brute-force attack) olarak bilinen bu yöntemde amaç bilgisayarın hızını kullanarak olabilecek bütün şifrelerin denenmesidir. Bu tür saldırılarda öncelikle olası şifrelerin bir tablosu kullanılır. Örneğin Türkçede sıkça kullanılan belirli uzunluktaki metinlerden başlanır. ■

Kriptoloji konusuna ilgi duyan okurlarımız için küçük bir bulmacamız var. Aşağıda Sezar şifreleme yöntemiyle şifrelenmiş metni çözüp, doğru cevabı *bteknik@tubitak.gov.tr* adresine gönderen okurlarımızdan birine sürpriz bir hediyemiz olacak.

KTVTY HO FOÜZTÜ NOÇPTDTZTZ TVÜ DJIŞDŞ SJZPT IŞVNJ IJIŞYVJZYŞEFŞÇ

Kaynaklar

Boaz B. (2021). An Intensive Introduction to Cryptography. 46, 52-53, 146, 187-188, 25 Mayıs 2022 tarihinde, https://github.com/boazbk/crypto adresinden erişildi.

Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., … *Gehring, T. (2020). Advances in quantum cryptography, Advances in Optics and Photonics*, Vol. 12, No. 4, 1017. doi: https://doi.org/10.1364/AOP.361502

Rosulek, M. The Joy of Cryptograph. 205, 209. 25 Mayıs 2022 tarihinde, joyofcryptography.com adresinden erişildi.

Bellare, M., Rogoway, P. (2005). Introduction to Modern Cryptography, 9, 50-54. California: University of California Press.

Broadbent A., Schaffner C. (2016), *Quantum cryptography beyond quantum key distribution, Designs, Codes and Cryptography*, 78, pages351–382 (2016) DOI 10.1007/s10623-015-0157-4