AÇIK ANAHTAR GİZLİ ŞİFRELEME

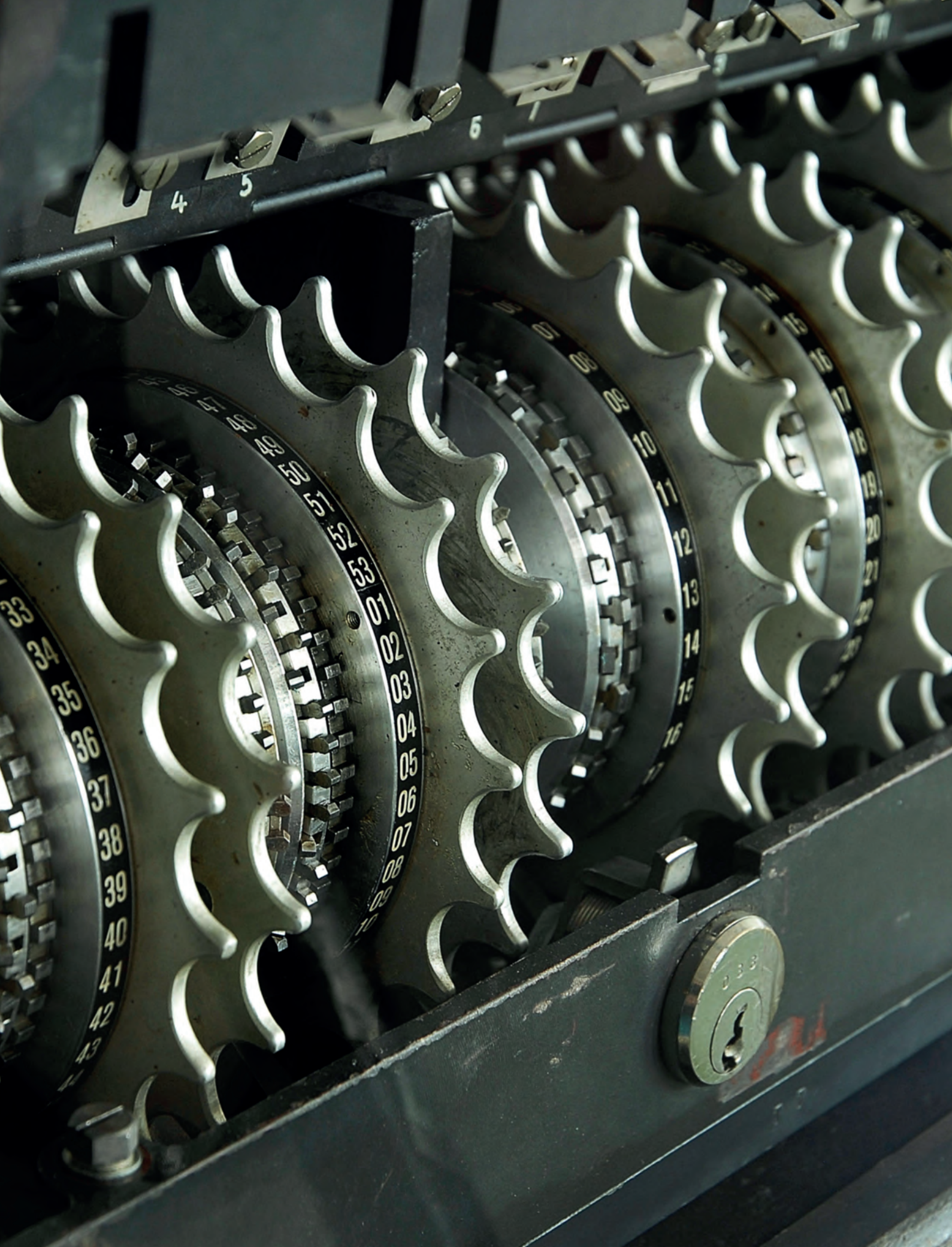
Prof. Dr. Ali Sinan Sertöz [*Bilkent Üniversitesi - Fen Fakültesi - Matematik Bölümü*

Ağustos sıcağında Cenevre'de uluslararası bir toplantı salonundayız. Kıbrıs'ta gerçekleşen sevimsiz bazı olaylardan sonra Türkiye adaya silahlı kuvvetlerini çıkararak adadaki Türklerin güvenliğini kısmen koruma altına almıştı. Uluslararası baskıyla silahlı müdahaleye ara verilmişti. Cenevre'de duruma barışçıl bir çözüm aramak üzere toplantı üstüne toplantı yapılıyordu. Bu sırada Kıbrıs'ta Türk köylerine saldırılar yer yer devam ediyor, karşı tarafın esir aldığı Türkler karşılıklı anlaşmalara rağmen serbest bırakılmıyordu. Türkiye'yi bu toplantıda o sıralar elli iki yaşında olan Dışişleri Bakanı Turan Güneş temsil ediyordu. Toplantıya katılan ülkeler, diplomatik bir dille söylemek gerekirse, konuyu zamana yayıp Türkiye'yi gereksiz yere adaya asker çıkarmış duruma düşürmek için görüşmeleri teknik ayrıntılar etrafında döndürüyordu. Sanki bir sonuç çıkacakmış gibi konferans son derece gergin ve boğucu bir ortamda sürüyordu.

Bir ara Turan Güneş Türkiye'deki yetkililerle bir telefon görüşmesi yapmak istedi. Bu görüşmenin yabancılar tarafından gizlice dinleneceğini bildiği için bu telefon görüşmesinde Türk tarafının gerçek izlenimlerini açığa çıkarmayan sıradan bazı genel bilgiler verdi. Tam telefonu kapatacakken Türk tarafından bakana "Bu arada eşiniz aradı. Kızınız tatile çıkacakmış, izin verir misiniz diye soruyor" dediler. Turan Güneş yorgun bir sesle "Ayşe tatile çıkabilir" dedi.

Konuşmayı dinleyen yabancı istihbarat yetkilileri ve bu konuşma metinlerini okuyan diğer diplomatlar Turan Güneş'in bu kadar yoğun ve gergin bir ortamda görev yaparken dahi ailesiyle ilgilenmesini onun kişiliğindeki asalete verdiler.

Ertesi sabah Türk ordusu Kıbrıs'ta kapsamlı bir askeri harekâta başladı ve Kıbrıs'ta bugün hâlâ geçerli olan sınırları çizdi. Ayşe tatile çıkmıştı!



Turan Güneş (1922-1982)

...
Tam telefonu kapatacakken
Türk tarafından bakana
"Bu arada eşiniz aradı.
Kızınız tatile çıkacakmış,
izin verir misiniz diye soruyor"
dediler.

Turan Güneş yorgun bir sesle
"Ayşe tatile çıkabilir" dedi.
...

Gizlilik Hep Gerekliydi

Türk tarafının Cenevre'deki toplantılardan bir sonuç çıkmayacağı izlenimini edindiğini açık etmesi durumunda Türkiye'nin bir askeri harekâtı düşünmeye başlayacağı belli olacak ve bu harekâtın engellenmesi için dış baskılar ve tehditler devreye girecekti. Oysa böyle bir askeri harekât ancak aniden yapılıp oldu bittiye getirilirse bir sonuç verebilecekti. O yüzden Turan Güneş'in toplantıların gidişatı hakkındaki izlenimlerini Türkiye'ye şifreli bir mesajla bildirmesi uygun görülmüş ve Ayşe'nin tatile çıkıp çıkmayacağı sorusu bu izlenimin gizlice aktarılması için kullanılmıştı. O zamanın teknik olanakları içinde zekice kurgulanmış bir gizli haberleşme yöntemiydi bu.

Bu çeşit "bir atımlık barut" misali yöntemler çok acil durumlarda hayati mesajların aktarılmasını sağlar, ama daha ayrıntılı bir mesaj iletilmesi için uygun değildir. Eğer Turan Güneş o gün uzun ve mutlaka gizli kalması gereken bir öneri iletmek ve örneğin Türkiye'nin siyasi tavrında bazı değişiklikler önerip bu değişikliğe İngiltere'nin göstermesi muhtemel tepkilerin Yunanistan'ı zor bir konuma iteceğini söylemek istese, açıkça dinlenen bir telefon görüşmesi sırasında "çaktırmadan" bunu yapamazdı.

İşte şifreleme tarih boyunca bu çeşit durumlarda kullanılmak için icat edilmiştir.

Turan Güneş Cenevre Konferansı'nda

İlk Şifreleme Tekniği

Tarihte bir mesajı şifreleme ihtiyacını ilk kimin ve neden duyduğunu ve hangi tekniği kullandığını bilmek pek mümkün değil. Hiç kimse "ileride tarihçiler benim ne yaptığımı merak eder, onlara kolaylık olsun diye her yaptığımı belgeleyeyim, kaydedeyim" dememiştir. Özellikle şifreleme gibi gizli kalması gereken konularda kayıtlı delil bulmak hemen hemen imkânsız. Yine de ilk şifreleme işlerini yapanların Spartalılar olduğu iddia edilir.

Spartalılar göreve gönderilen bir generale silindir şeklinde yontulmuş kalın bir sopa verir ve bu sopanın bir kopyasını merkezde tutarlarmış. Generale gizli bir mesaj gönderileceği zaman parşömenden ya da benzer bir maddeden yapılmış bir şeridi bu silindire sarıp mesajı şeridin üzerine ve sopanın uzunluğu doğrultusunda yazarlarmış. Sonra şeridi söküp generale gönderirlermiş. Yolda bu şerit başkalarının eline geçse bile art arda gelen harfler bir anlam oluşturmadığı için anlaşılmazmış. General bu şeridi alıp elindeki sopaya sarınca elbette mesaj kendiliğinden okunur hale gelirmiş.

Sopalı bir şifre mesajı
Kaynak: Simon Singh, *The Code Book*, s. 8)

Örneğin ulağın taşıdığı mesaj şeridinde şöyle bir yazı olabilir:

UĞKAVULIASULANFIRA

Bu şeridi kalın bir sopaya sarınca, sopanın uzunluğuna sol alttaki örnekte olduğu gibi sekiz değil de sadece üç harf sığdığını varsayarsak, general şunu görecek:

ULA
ĞIN
KAF
ASI
VUR
ULA

Bu hikâyeyi -miş'li geçmiş zamanda anlatmamın nedeni ise kaynaklarda göreceğiniz Thomas Kelly'nin ayrıntılı araştırma makalesidir. Kelly'ye göre Spartalılar asker bir toplumdu ve sözlü bir gelenekleri vardı. Aralarında okuryazar olanlar çok azdı ve bir şifreleme mekanizmasına gerek bile duymamışlardı. Bir mesaj gönderilecekse birini gönderip mesajı sözlü olarak iletiyorlardı. Kelly bu uzun makalesinde o dönemlere ait onlarca kaydı inceleyip bu sopa şifresine ait hiçbir ima olmadığını anlatır.

Amerikan Kriptografi Kurumu'nun logosu

Yine de Amerikan Kriptografi Kurumu'nun logosunda silindir bir sopaya sarılmış bir mesaj resmi vardır.

Sezar (MÖ 100-44)

Sezar Şifresi

Sezar'ın generalleriyle yaptığı yazışmalarda alfabedeki harfleri kaydırmaya dayalı bir şifre kullandığı söylenir. Sezar her harf yerine alfabede o harften sonra gelen üçüncü harfi kullanmıştır. Yani Türk alfabesi kullanırsak A yerine Ç, B yerine D, C yerine E kullanmıştır. Alfabenin son harflerine gelince de elbette saymaya devam etmek için Z'den sonra A B C geliyormuş gibi davranmıştır. Örneğin bir şehri almak üzere yola koyulan bir generale okunması zor olsun diye kelimeler arası boşluklar kaldırılarak aşağıdaki mesaj gönderilebilir.

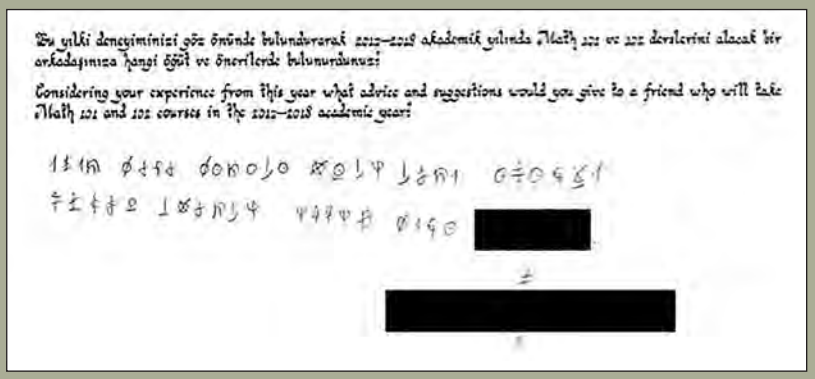
JHÖHPTRÖÇBÇGSP

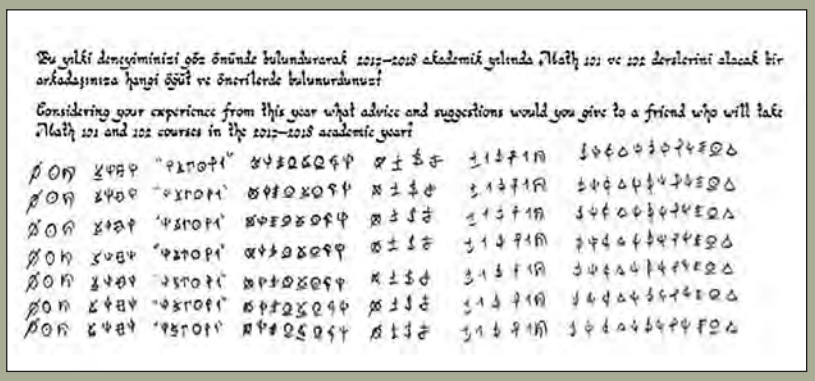
Burada her harfin yerine alfabede kendisinden önce gelen üçüncü harfi koyarak mesajı çözebilirsiniz.

Bu çeşit mesajları çözmek kolay olmasına rağmen Sezar zamanındaki genel eğitim düzeyi göz önüne alınınca bu şifreleme yönteminin etkili olduğu düşünülüyor.

Bir harfin yerine başka harf koyarak yapılan şifrelemeler bugün fazla zorlukla karşılaşmadan çözülüyor. Özellikle mesaj uzunsa ve hangi dilde olduğu biliniyorsa o dildeki harflerin kelimelerde kullanılma sıklıklarına bakarak mesajı çözmek zor değil. Bu tekniğe frekans analizi adı verilir. Öte yandan Osmanlı devletinin bir dönem resmi yazışmalarda kullandığı şifrelerin yabancılar tarafından, mesajın "arz ederim" kelimeleriyle biteceği tahmin edilerek çok kolay kırıldığı söylenir. Tıpkı bazı Alman kodlarının kırılmasında mesaj sonlarında "Heil Hitler" sözlerinin bulunmasının işe yaraması gibi. Bu arada şifreleme konusundaki ilk ciddi çalışmaların 800'lü yıllarda yaşamış el-Kindi'ye ait olduğunu da hatırlayalım.

el-Kindi





Şifreyi çözebilecek misiniz?

Güncel Bir Örnek

Bilkent Üniversitesi'nin efsanevi hocalarından Okan Tekman her dönem sonunda öğrencilere bir kâğıt dağıtıp seneye bu dersi alacak yeni öğrencilere bu ders hakkındaki tavsiyelerini yazmalarını ister. Bu kâğıtları sonra Okan bize de gösterir. Öğrenciler öyle aklı başında ve yerinde tavsiyeler verirler ki madem bunları biliyorlardı kendileri niye uygulamadılar diye şaşarız. Bir keresinde Okan şifreli bir mesajla karşılaşır. Öğrenci şifresinin çözülemeyeceğinden öylesine emindir ki hem edepsiz bir kelime kullanmış hem de adını da kendi şifresiyle yazmaktan çekinmemiştir.

Elbette Okan Hocamız bu şifreyi derhal çözer, bir kâğıda o şifreyi kullanarak bir cümle yazar ve öğrenciyi odasına çağırıp o cümleyi ceza olarak yedi kez yazmasını ister. Öğrenci bir yandan bu taşkınlığını bu kadar hafif bir cezayla atlatmanın sevincini yaşarken bir yandan da ceza cümlesini her yazdığında "Hocam nasıl çözdünüz" demekten kendini alamaz. Bakalım siz de, o kötü kelimenin ve öğrencinin adının kapatıldığı şifreli mesajı ve Okan Hocanın ceza cümlesini çözebilecek misiniz?

Pierre de Fermat (1607-1665)

Kırılması Zor, Kurulması Kolay Şifreli Mesajlar

Yukarıdaki örneklerdeki mesajlar kolayca kuruldu ve kolayca kırıldı. Oysa bir harfin yerine başka harf yazmanın çok karışık yolları bulunabilir ve şifreyi kırmak daha da zor hale getirilebilir. Üstelik şifreleme yöntemi sık sık değiştirilerek mesajları anlamaya çalışanların işi yokuşa sürülebilir. Ama yine de bu çeşit şifreler kırılabilir. Üstelik bu yöntemleri kullanmanın başka zorlukları da vardır.

Örneğin Sezar şifresinde anahtar 3 sayısıdır. Harfleri üç kaydırarak şifreler ve tersini yaparak çözeriz. Bu 3 sayısının hem mesajı yazan hem de alan tarafından bilinmesi gerekir. Daha sonra biz 3 sayısının mesajları okuyan yabancılar tarafından tahmin edildiğini fark edince 3 yerine 7 sayısını kullanmaya karar verirsek bu 7 sayısını da mesajı iletecegimiz kişiye bildirmemiz gerekir. Bu bildirim gizlice yapılmalı ama nasıl? Eski şifremiz çözüldüğüne göre onu kullanıp 7 sayısını göndermek güvenli olmaz. Üstelik mesajlaşacağımız kişiler birden fazla olunca sorun daha da büyüyecek.

Bu sorunun bir çözümü açık anahtar şifreleme yönteminin kullanılmasıdır. Bu yöntemde herkes kendisine gönderilecek mesajın nasıl şifrelenmesi gerektiğini herkese ilan eder ama yöntem öyle ayarlanmıştır ki şifrelenmiş mesajı pratikte ancak o mesajın nasıl şifreleneceğini söyleyen kişi çözebilir.

Böyle bir şeyi ilk duyduğumuzda olmaz öyle şey diyebiliriz. Ama matematik işte böyle durumlarda imdadımıza koşar. Binlerce yıllık bir geçmişi olan ve sadece sayıların gizemli büyüsüne kapılan insanların ürettiği sayılar kuramı hiç umulmadık bir şekilde yirminci yüzyılda şifreleme konusunun en önemli aktörü olmuştur.

Önce Biraz Matematik

Bazı matematikçilerin adını çok sık duyarız. Onların hepimizden daha zeki ve yetenekli olduğu için meşhur olduklarını düşünür, Tanrı isteseydi bize de zekâ ve yetenek verirdi, biz de büyük matematikçi olurduk diye teselli bulabiliriz. Oysa gözden kaçırdığımız küçük ve can sıkıcı bir ayrıntı vardır. O meşhur matematikçiler çok çalışmıştır. Yoksa birbirinden farklı pek çok konuda hep onların adlarının çıkması başka nasıl açıklanabilir?

Günümüzün en gözde şifreleme yöntemi olan açık anahtar şifreleme tekniğinin arkasında da Pierre Fermat'nın 1640'ta sadece merak ettiği için araştırıp bulduğu, doğal sayılarla ilgili bir özellik yatar. Fermat'nın Küçük Teoremi olarak anılan bu teorem tam sayılarda şu özelliğin olduğunu ileri sürer: Eğer p bir asal sayıysa ve a da p'ye bölünmeyen pozitif tam sayıysa, o zaman a^p sayısı p'ye bölündüğünde mutlaka a artar. Bunu matematik jargonunda şöyle yazarız:

p asal ve $(a,p)=1$ ise $a^p \equiv a \bmod p$ olur.

Örneğin $p=7$ ve $a=45$ alırsak

$a^p = 373.669.453.125$ olur.

Fermat teoremi sayesinde biz bu sayıyı 7'ye bölmeden eğer bölseydik 45 artacağını biliyoruz. Gerçekten de,

$45^7 = 373.669.453.125 =$

$7 \times 53.381.350.440 + 45$

olur.

Bu ne işimize yarayacak?

Dikkat ederseniz Sezar şifreleme yöntemi aslında bir toplama işlemiydi. Her harfe karşılık gelen sayıya 3 ekliyorduk. Şifreyi çözmek için de 3 çıkarıyorduk. Burada 3 yerine hangi sayıyı kullanırsak kullanalım şifreyi çözmek için toplama işleminin tersi olan çıkarma işlemini kullanırız.

Şimdi tersinin uygulanması daha zor bir operasyon kurmaya çalışıyoruz. Örneğin 373.669.453.125 sayısını gördüğümüzde bir çırpıda hangi sayının yedinci kuvveti olduğunu bilmek kolay değil. Hele 45 yerine kırk beş basamaklı bir sayı kullansaydık yedinci kuvvetine bakarak o sayıyı hemen çıkaramazdık. Biraz uğraşmamız gerekirdi ama sonunda yine o sayıyı bulabilirdik. Öyleyse işleri biraz daha karıştıralım.

Leonhard Euler (1707-1783)

Hepimizin Ustası: Euler

Fermat'dan yüz yıl sonra Euler Fermat'nın Küçük Teoremi'nin altında yatan mekanizma üzerine düşünürken yeni bir şey keşfetti. Bunu anlatmak için önce Euler'in kendi adıyla da anılan şu meşhur φ fonksiyonuna bakalım.

Kalanlar aritmetiğiyle oynarken bir sayı seçeriz ve tüm aritmetik işlemlerden sonra sonucu o seçtiğimiz sayıya bölüp sadece kalanı alır ve o işlemin sonucu olarak o kalan sayıyı yazarız. Örnek olarak 6 seçelim. O zaman $2 + 4 \equiv 0 \bmod 6$ yazarız. Demek ki sadece 0, 1, 2, 3, 4, 5, sayılarıyla oynayacağız. Burada hemen gözümüze çarpan bir özellik var: 2 sayısını kendisiyle istediğimiz kadar toplayalım yine de buradaki tüm sayıları elde edemiyoruz. Sadece 2, 4 ve 0 sayılarını elde edebiliriz. Aynı "isteksizliği" 3 ve 4 sayılarında da görüyoruz. Oysa 1 sayısını kendi kendisiyle toplayarak diğer sayıların hepsini elde edebiliriz. Aynı verimliliği 5 sayısı da gösteriyor. Demek ki kalanlar aritmetiğinde, 6 sayısını seçersek kullanacağımız tüm sayıları üretebilen iki sayı var.

Peki, 6 yerine 60 seçseydik kalanlar aritmetiğinde kullanacağımız tüm sayıları üreten kaç sayı olacaktı? İşte Euler bu soruya bir cevap buldu ve bu cevabı veren fonksiyona φ dedi.

$\varphi(6) = 2$, $\varphi(60) = 16$

$\varphi(n)$ sayısı genel olarak n'den küçük ve n ile 1'den büyük ortak çarpanı olmayan sayılardan kaç tane olduğunu söyler. Toplama işleminden çarpma işlemine geçersek $\varphi(n)$ sayısı n elemanlı döngüsel bir grubun üreteç sayısını verir. Yani işe yarar bir fonksiyondur.

Euler-Fermat Teoremi

Fermat'nın sadece asal sayılar kullanmasının hikmetini anlamaya çalışan Euler, asal bir p sayısı yerine rastgele bir n sayısı alırsa ne olacağını araştırdı. Yine Fermat'nın yaptığı gibi n ile en büyük ortak çarpanı 1 olan bir a sayısı aldı ve a sayısının kuvvetlerini n ile bölünce kalanlara baktı. Bir süre sonra tekrarlayan bir düzen gördü. Eğer a sayısının $\varphi(n)$'inci kuvveti alınırsa n'ye bölündüğünde mutlaka 1 artıyordu. İşte bugün Euler-Fermat Teoremi diye anılan teorem şöyle yazılabilir:

$(a,n) = 1$ ise $a^{\varphi(n)} \equiv 1 \bmod n$

Bu sonuç Fermat'nın teoremini genellediği gibi bize şifreleme konusunda da yardımcı olacak. Bu sonucun çok işimize yarayacağını düşünmemizin nedeni karışık bir işlemden sonra 1 elde ediyor olmamız. Şimdi biz o denklemin iki tarafının da 100'üncü kuvvetini alırsak sol taraf çok büyük bir sayı olacak, ama sağ tarafta yine 1 olacak ve o kocaman sayı kalanlar aritmetiğinde yine 1'e eşit olacak. İleriki paragraflarda her iki tarafın k'inci kuvvetini alırken bunu hatırlayın.

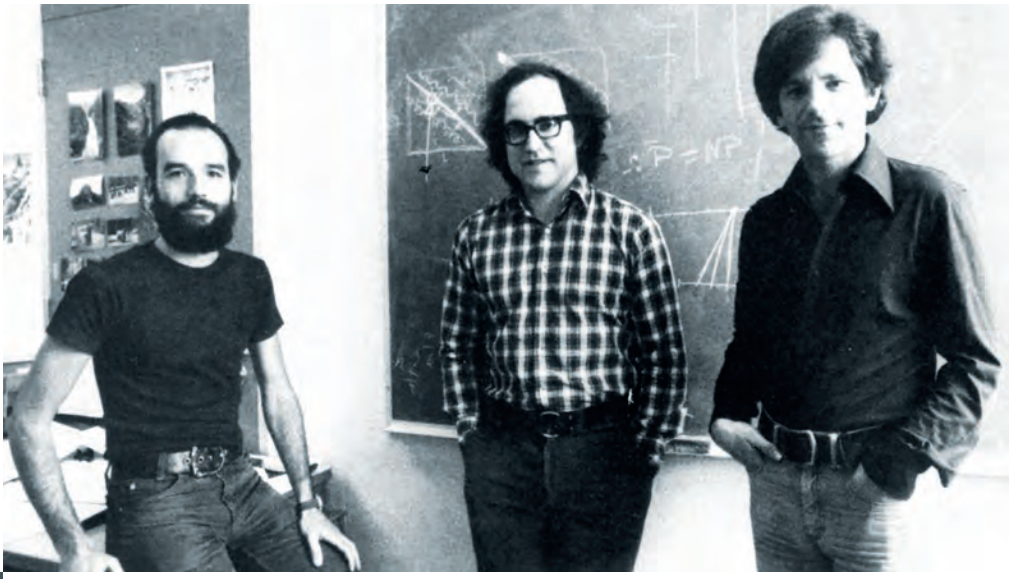
Şimdi bu özelliği şifre geliştirmek için kullanalım.

Açık Anahtar Şifreleme - Ana Fikir

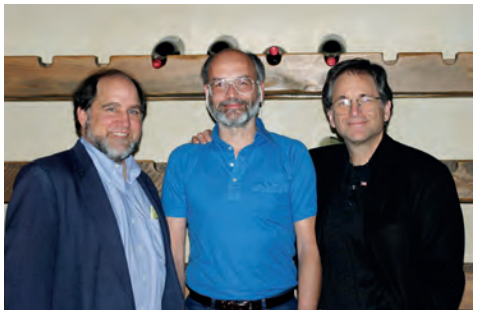
Şifreleme yaparken önce bir metin sayılara dönüştürülür. Sonra bu sayılar belli kurallara göre değiştirilir. Buna şifreleme diyoruz. Şifreli mesajı alan taraf bu sayıları değiştirmek için kullanılan yöntemin tersini kullanarak tekrar eski sayıları bulur ve elde etiği sayıları metne dönüştürür.

Biz bu sürecin, metinlerin nasıl sayılara dönüştürüldüğü ve o sayılardan metnin nasıl geri kazanıldığı kısmıyla ilgilenmeyeceğiz, sadece gönderilmek istenen sayıların kimsenin anlamayacağı şekilde şifrelenmesi işiyle ilgileneceğiz.

Sezar şifresi ya da "Ayşe tatile çıksın" türü şifreleme yöntemlerinde taraflar karşılıklı olarak bir şifre ya da parola belirlemek zorundadır. Eğer bir firma yüz ayrı ülkedeki temsilcilikleriyle haberleşirken şifre değiştirmek isterse merkezden her ülkeye bir kurye ile yeni şifreyi göndermesi gerekir. Yolda bu şifrelerin çalınmayacağını kim garanti edebilir?



Açık anahtar şifreleme tekniklerinden RSA tekniğine adlarını veren **Rivest, Shamir** ve **Adleman**



İşte açık anahtar şifreleme yöntemi bu zorluğu ortadan kaldırır. Herkes kendisi için bir şifreleme anahtarı ilan eder. "Bana mesaj göndereceksenız bu anahtarı kullanarak şifreleyip gönderin" der. Şifrelenip gönderilen mesajı herkes görebilir ama sadece şifreleme anahtarının sahibinde şifreyi çözen ikinci anahtar vardır ve ondan başkası da o mesajı pratikte çözemez. Aslında isteyen evrenin kalan yaşından kat kat daha uzun bir süre deneme yapacak kadar zamanı olsa çözer, ama bugünkü bilgisayar teknolojileriyle bu şifrelerin makul bir sürede çözülmesi beklenmiyor.

Açık Anahtar Şifreleme - İşin Püf Noktası

İşe iki tane çok büyük asal sayı seçerek başlıyoruz. Bu asalları p ve q ile gösterelim. Çok büyük derken en az yüz basamaklı olsun demek istiyoruz. Yoksa bu işin sonunda ortaya çıkacak şifre bir ev bilgisayarıyla bile çözülebilir. Bu iki asalı çarpıp bir n sayısı elde ediyoruz.

$n = p \times q$

Bu n sayısını herkese açıkça söylüyoruz. Kullandığımız asalların büyüklüğü nedeniyle kimsenin p ve q sayılarını bulamayacağına güveniyoruz. Eğer p ve q bilinirse şifremiz hemen çözülür.

Burada Euler'in φ fonksiyonunu kullanacağız. İki tam sayı seçeceğiz. Bunlara b ve c diyelim, öyle ki bunlar $\varphi(n)$ sayısından küçük olacaklar ve $\varphi(n)$ ile en büyük ortak çarpanları 1 olacak. Yetmedi bir de

$b \times c \equiv 1 \bmod \varphi(n)$

şartının sağlanmasını isteyeceğiz. Bunu sağlamak zor gibi görünse de yine çok meşhur başka bir matematikçi imdadımıza yetişecek. Öklid'in kendi adıyla anılan, en büyük ortak çarpan bulma algoritması yardımıyla eğer önce b sayısını seçersek yukarıdaki şartları sağlayan c sayısını kolayca bulabiliriz.

Şimdi bulduğumuz bu iki sayıdan birini gözümüz gibi koruyacak ama öbürünü herkese söyleyeceğiz. Diyelim ki b sayısını herkese söylemeye karar verdik.

Herkese ilan ettiğimiz açık anahtar bilgilerimiz: n ve b sayıları

Bu bilgileri kullanarak herkesin görebileceği ama sadece bizim çözebileceğimiz bir şifreli mesaj nasıl oluşturulur?

Diyelim ki arkadaşımız bize bir M sayısını mesaj olarak göndermek istiyor ama kimsenin bu sayıyı görmesini istemiyor. Önce bu M sayısının b'ninci kuvvetini hesaplayacak, sonra bu sayıyı n'e bölüp kalanı bize gizli mesaj olarak gönderecek. Arkadaşımızın bize gönderdiği gizli mesaj sayısını G ile gösterirsek

$G \equiv M^b \bmod n$

eşitliği sağlanır. Bu G sayısını herkes görür ve kuramsal olarak deneme yanılma yöntemiyle M sayısını bulmaları mümkündür. M için 1'den başlayarak sırayla tüm sayıları tek tek alıp her birinin b'ninci kuvvetini n'ye bölüp kalan G mi diye bakarlar. Sonunda elbet bir yerde M sayısını bulurlar. Ama n ve M sayıları yüzlerce basamağı olan sayılarsa, G ve n kullanarak deneme yanılma yöntemiyle M sayısını bulmak pratikte milyonlarca yıl sürebilir. Şifrenin sağlamlığı burada yatıyor.

Biz bu G sayısını alınca hemen bizde gizli olan c sayısını kullanarak G^c sayısını hesaplarız. Bu sayıyı n'e bölüp kalanına baktığımız zaman gördüğümüz sayı arkadaşımızın bize göndermek istediği M'dir!

Bu mucize nasıl gerçekleşti?

Bizdeki gizli anahtar c ile açık anahtarlardan b çarpıldığında, $\varphi(n)$'e bölünmesi 1 artan veren bir sayı elde ediyoruz. Yani öyle bir k tam sayısı var ki $bc = 1+k\,\varphi(n)$ oluyor. O zaman:

$$G^c = M^{bc} = M^{1+k\,\varphi(n)} = M \times M^{k\,\varphi(n)} = M \times (M^{\varphi(n)})^k \equiv M \bmod n$$

olur, çünkü Euler-Fermat Teoremine göre $M^{\varphi(n)}$ sayısı n'e bölününce 1 artan verir ve yukarıdaki çarpımda M sayısını değiştirmez.

Arkadaşımız kendisinden başka kimsenin bilmediği M sayısından herkesin gördüğü n ve b sayılarını kullanarak G sayısını elde etti ve kimseden gizlemeden bize G sayısını gönderdi. Biz de kimseye göstermediğimiz c sayısını kullanarak bu G sayısından arkadaşımızın kimseye göstermeden bize iletmek istediği M sayısını elde ettik.

Bu yöntemle yüz ayrı ülkede temsilciliği bulunan bir firmanın her temsilcisi kendi şifresini kendi ilan eder ve istediği zaman da istediği gibi değiştirebilir. Şifresini değiştirdiği zaman tek yapması gereken şey bunu kendi sitesinde ilan etmek.

Bir Sayısal Örnek

Arkadaşım bana M=124 sayısını kimseye göstermeden göndermek istiyor. Benim açık şifre anahtarım b=187 ve n=247. Gizli anahtarım c=67. Anahtar seçimlerimin doğru olduğunu $\varphi(247)$=216 olduğunu kullanarak kontrol edebilirsiniz.

Arkadaşım $G=M^b \bmod 247 = 124^{187} \bmod 247 = 110$ sayısını bana gönderiyor, ben de gizli anahtarım c=67'yi kullanarak $110^{67} \bmod 247 = 124$ buluyorum.

Burada dikkat ederseniz $\varphi(247) = 216$ olduğunu hiç kullanmadık gibi görünüyor. Oysa her önemli matematik kavramı gibi o da arka planda kaldı ve benim b=187 ve c=67 sayılarını kurala uygun seçmemi sağladı.

Dikkatli okuyucu burada durup 187 ve 67 sayıları arasından hangisinin açık hangisinin kapalı anahtar olacağına nasıl karar verdiğimi soracaktır. Cevap: Rastgele. Her iki tercih de çalışır. Eğer 67 açık anahtar olsaydı arkadaşım $124^{67} \bmod 247 = 32$ sayısını bana gönderecekti. Ben de $32^{187} \bmod 247 = 124$ bulacaktım.

Elektronik İmza Atalım

Arkadaşım benim açık şifremi kullanarak bana bir dizi sayı göndermiş olsun. Ben bunları çözüp metne çevirdiğimde de ona olan birikmiş borcumu ödemek yerine Ankara'daki tüm lise son öğrencilerini *Bilim ve Teknik* dergisine ikişer yıllığına abone yapmamı istediğini öğrenmiş olayım. Önce bu mesajın gerçekten arkadaşımdan mı geldiğini yoksa dergi editörlerinin bir muzipliği mi olduğunu öğrenmem gerekir. Arkadaşım bunu fark etmiş olmalı ki "ben şimdi sana 125 sayısını imza olarak göndereceğim" diye yazmış. Bakalım beni nasıl ikna edecek.

Arkadaşımın açık şifre anahtarları n=391 ve b=257. Gizli anahtarı da c=289 ama bunu ondan başka kimse bilmiyor.

Arkadaşım önce kendi gizli anahtarını kullanıp $125^{289} \bmod 391 = 57$ buluyor ve bu sayıyı benim yukarıdaki sayısal örnekte kullandığım açık anahtarımı kullanarak şifreliyor ve $57^{187} \bmod 247 = 190$ bulup bana gönderiyor. Ben mesaj olarak aldığım bu 190 sayısını biliyorum, arkadaşımın yaptığı ara hesapları bilmiyorum.

Bu sayıyı akıllıca kullanıp 125 sayısını elde edebilirsem mesajların arkadaşımdan geldiğine ikna olacağım. Bunun için bu sayıyı kendi gizli anahtarımla çözüp $190^{67} \bmod 247 = 57$ buluyorum ve arkadaşımın açık anahtarını kullanıp $57^{257} \bmod 391 = 125$ buluyorum. Hmmm, bu mesajı kesinlikle arkadaşım göndermiş, çünkü bu hesaplar onun gizli anahtarı olmadan çalışmazdı!

Bu Şifreler Nasıl Kırılır?

Benim şifremi kırmak için gizli anahtarım c=67'yi bulmanız gerekir. Bunun için de $\varphi(247)$=216'yı bilmeniz gerekir. Benim diğer açık anahtarım b=187 olduğuna göre 1/187 mod 216=67 olarak hemen gizli anahtarımı bulabilirsiniz. Genel olarak açık anahtar n çok büyük olacağı için $\varphi(n)$ doğrudan hesaplanamaz ama eğer $n=p\times q$ olduğunu bilirsek Euler'in bir başka teoremini kullanarak

Alan Mathison Turing (1912-1954)
İngiliz matematikçi,
bilgisayar bilimcisi ve kriptolog.

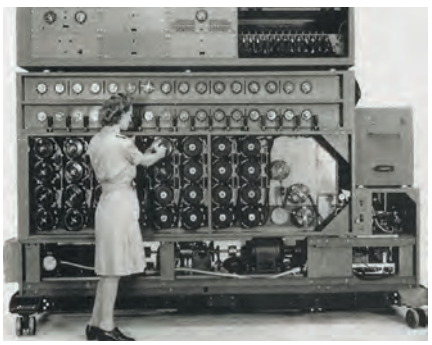
Joan Clarke (1917-1996)
Bletchley Park'ta çalışan şifre çözücülerden ve Alan Turing'in bir dönem nişanlısı

$$\varphi(p\times q)= p\times q- p - q+1$$

olduğunu görürüz. Benim seçimimde n=247 = 13×19 olduğundan $\varphi(247)$ = 216 hemen bulunur. Şifrenin sağlamlığı p ve q yerine yüzer basamaklı asal sayılar kullanmakta yatmaktadır. O durumda $\varphi(n)$'i hesaplamak pratikte mümkün olmayacak, dolayısıyla da benim gizli anahtarım bulunamayacak.

Yüzlerce basamaklı asal sayı üretmenin yolunu bulunca üniversitedeki görevlerinden istifa edip "asal sayı büfesi" açan profesörler olduğunu duymuştum. Baş müşterileri de elbette haberleşme uydularını kullanan kurumlar olmuştu.

Bletchley Park
ENİGMA şifrelerini kırmak için Alan Turing'in Bletchley Park'ta kurduğu makine (sol altta)
Bir ENİGMA makinesi (sağ altta)



ENİGMA

Açık anahtar şifreleme fikrinin kuramsal olarak ilk defa on dokuzuncu yüzyılda konuşulmaya başlandığı yazılsa da yaygın kullanımı ancak 1970'lerden sonra olmuştur. Daha önceleri genellikle "düşmanın aklına gelmeyecek" yöntemlerle şifreleme yapmaya, "öbür taraf ne düşünmüş olabilir" yöntemiyle de şifreler kırılmaya çalışılmıştır.

Bunun en muhteşem örneği İkinci Dünya Savaşı sırasında Almanların kullandığı ENİGMA şifre makinesidir. ENİGMA yarı mekanik yarı elektronik bir daktiloydu. Bir harfin tuşuna basınca bir elektrik akımı yan yana duran üç rotora gider, o rotorların bulundukları pozisyona göre akım döner gelir bir başka harfin ışığını yakardı. Bazen rotorlardan gelen akım bağlantı şeması ayrıca planlanmış kablolardan geçip ancak ondan sonra bir harfin ışığını yakardı. Daktiloda basılan tuşun gösterdiği harf yerine aslında kâğıda ışığı yanan bu harf basılırdı.

The Imitation Game'den bir sahne.
Önde Benedict Cumberbatch Oscar'lık performansıyla Alan Turing'i canlandırıyor.
Solda da Joan Clarke rolunde Keira Knightley'i görüyoruz.

Eğer ENİGMA'nın tüm mahareti bu olsaydı, yani her harfin yerine başka bir harf bassaydı frekans analizi yapılarak şifre hemen çözülürdü. Oysa ENİGMA'da her harf basıldıktan sonra rotorlar önceden planlanan bir düzene göre biraz dönerdi. Böylece bir harfin yerine her seferinde başka bir harf basılır, frekans analizine fırsat verilmezdi.

Şifrenin çözülmesi için mesajı yazan makinenin rotorlarının ve bağlantı kablolarının başlangıç pozisyonlarının bilinmesi gerekirdi ki alıcı uçtaki ikinci ENİGMA makinesi buna göre mesajı okuyabilsin. Bu pozisyonlar da genellikle her yirmi dört saatte bir önceden belirlenen bir kurala göre değiştirilirdi. Bu kurallar U-bot kaptanlarına pembe kâğıt üzerine suda çözülen kırmızı mürekkeple yazılmış kataloglarla teslim edilirdi. Böylece kataloğun düşman eline geçme tehlikesi belirince kaptan kataloğu suya atarak kodların düşman eline geçmesini engelleyebilecekti.

Almanlar ENİGMA şifresinin kırılamaz olduğuna inanmıştı. Oysa İngiliz gizli servisi, Winston Churchill'in himayesinde ve Alan Turing'in dehasının önderliğinde Bletchley Park'da bu şifreleri kırıyordu. Savaşın son darbesini vuracak olan Normandiya Çıkarması'ndan önce, Almanlar şifreli mesajlarının çözüldüğünü anlamasın diye bazı müttefik birliklerine Almanların ani bir baskın düzenleyeceği haber verilmemiş ve binlerce askerin ölmesine göz yumulmuştur.

Bletchley Park'ta yapılan çalışmalar savaş sonrasında da gizlenmiş, kamuya açıklanmamıştı. Churchill savaşın kazanılmasında çok önemli bir rol oynamasına rağmen hiç sesi duyulmayan bu proje için "altın yumurtlayan ama hiç gıdaklamayan bir kaz" benzetmesini bu yüzden yapmıştır. Orada olanları biraz değiştirerek ama heyecanını koruyarak anlatan 2001 yapımı *ENİGMA* adlı filmde Alan Turing'i Dougray Scott oynamıştı. Bu film daha çok savaş ortamında şifre kırmanın heyecanını Hollywood şablonlarıyla anlatmış, tatmin olmayan seyirciler içinse 2014'te daha gerçekçi olan *The Imitation Game* adlı film çekilmişti. Bu filmde Alan Turing'i oynayan Benedict Cumberbatch performansıyla Oscar adaylığı kazanmıştı.

Her iki film de ENIGMA şifrelerinin kırılması onurunu İngiltere'ye verir. Her ne kadar bu proje Alan Turing'in olağanüstü gayretleriyle sonuca ulaşmışsa da ENIGMA'yı ilk olarak Polonyalı istihbaratçılar çözmüş ama ülkeleri işgal edildiği için bulgularını İngiltere'ye vermek zorunda kalmışlardır. Yukarıdaki filmler için yazılan seyirci yorumlarında da aslında bu şifreyi Amerikalıların kırdığını ama kör olası İngilizlerin bunu karartmaya çalıştığını okursunuz.

The New York Times gazetesinde 27 Kasım 2017'de A. O. Scott imzasıyla çıkan *The Imitation Game* filmi hakkındaki eleştirinin sonunda gazete anne ve babaları filmde yer alan cinsellik, şiddet ve ileri düzey matematik konusunda uyarmış ama bunların açıkça sergilenmeyip sadece ima edildiğini ekleyerek onları teselli etmiştir. ■

Kaynaklar

Kelly, T., "The myth of the skytale", *Cryptologia*, Cilt 22, Sayı 3, s. 244-260, 1998.

Singh, S., *The Code Book*, Fourth Estate, 1999.

Flannery, S., *In Code: A Mathematical Journey*, Workman, 2001.

Alsan, S. (Çev.), "Gizli Haberleşme Aracı: Şifre", *Bilim ve Teknik*, Sayı 104, s. 10-12, Temmuz 1976.

Karadağ, N., "Asallar ve Şifreler", *Bilim ve Teknik*, Sayı 449, s. 84-85, Nisan 2005.

Babaoğlu, A., "Kriptolojinin Geçmişi", *Bilim ve Teknik*, Sayı 500, s. 24-27, Temmuz 2009.

Kara, O., "ENIGMA'dan AES'e", *Bilim ve Teknik*, Sayı 500, s. 28-33, Temmuz 2009.