

ISBN: 978-625-7587-36-5
© 2018 Ketebe Kitap ve Dergi Yayıncılığı A.Ş.

ketebe.com

Ketebe Yayınları: 501

Kültür



Yayın Yönetmeni
Furkan Çalışkan

Yayıma Hazırlayan
Dilâra Yabul İşleyen

Düzeltili
Hande Yıldırım Önsöz

Kapak
Harun Tan

Mizanpaj
Nilgün Sönmez

1. BASKI

Temmuz 2021
İstanbul

Ketebe Yayınları
Sertifika No. 49619
Maltepe Mahallesi Fetih
Caddesi No: 6 Dk: 2
Topkapı 34010 İstanbul
Tel: 212 612 29 30
e-mail: ketebe@ketebe.com

Baskı ve Cilt
Matsis Matbaa Hizmetleri
San. ve Tic. Ltd. Şti
Sertifika No: 40421
Tevfik Bey Mah. Dr. Ali Demir Cad.
No: 51 Sefaköy Küçükçekmece /
İstanbul Tel: 212 624 21 11

© Özgün adı *The Story of Codes* olan bu kitabın Türkiye hakkı Kalem Ajans aracılığıyla Ketebe Kitap ve Dergi Yayıncılığı A.Ş.'ye aittir. İzinsiz yayınlanamaz. Kaynak gösterilerek alıntı yapılabilir.





içindekiler

önsöz..... 8

kısım 1: özgünlük 11

Antik Mısır'dan İskoçya Kraliçesi Mary'ye kadar hem din hem cinsellik şifreleri. Basit ikame şifrelemeleri, yer değiştirmeler, sıklık analizleri

kısım 2: yaratıcılık..... 43

Kriptoloji; çılgın keşifler, diplomatlar ve papa danışmanlarının nasıl başını döndürdü? Ayrıca şifre kırma disiplininin devlet memurlarınca uygulanışı

kısım 3: pratik zekâ..... 63

Teknoloji birçok şifre devrimini beraberinde getirdiyse de bazı şifreler çözülemeden kaldı. * İki Harf * Doğru (Playfair) Şifre * Elgar'ın Diğer Enigması

kısım 4: sabır 87

Eli kanlı biri Enigma ve diğer savaş dönemi şifrelerinin çözülmesine yardım etti. * Zimmerman Telgrafı * ADFGX Şifresi * Soğuk Savaş Şifreleri * Venone Kodları * Navajo Kodlu Konuşanları





kısım 5: sürat.....127

Bu bilgisayar çağında verileri suçlulara karşı koruyan tek şey güçlü dijital şifrelemeler oluyor. * Açık Anahtar Şifrelemeleri

* Çarpanlara Ayırma Şifreleme Standardı

kısım 6: önsezi146

Kuantum şifrelemeleri kırılmaz olduğuyla övülür;

bu, şifre kırıcıların sonunun geldiğini anlamına gelir mi?

Artık şifreler kuantum fiziğinin ve kaos teorisinin boyunduruğunda.

kısım 7: gerçeklik164

Dijital çağda gözetim ile özel hayat arasındaki savaş, şifrelemenin önemini her zamankinden çok artırdı. * Bitcoin * Mesaj Özü (Hash) Algoritmaları

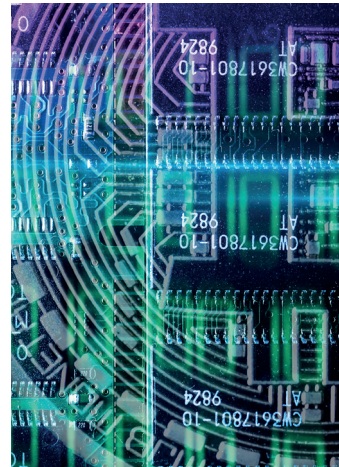
* Edward Snowden

terimler sözlüğü186

dizin.....188

ilave kaynaklar191

resim kaynakları.....191



önsöz

Günümüz dünyasında ne tarafa dönsek şifrelenmiş bir veriye toslarız. Cep telefonundan yaptığımız her arama, izlediğimiz her kablolu televizyon kanalı, bankada yaptığımız her çevrimiçi işlemde meraklı göz ve kulaklardan uzak olabilmek için gelişmiş bilgisayar şifreleme sistemlerine bel bağlarız.

Fakat bu gizlilik sadece günümüz dünyasına mahsus değildi. İki bin yıldan fazla bir süredir şifreler ve kodlar, siyasetten kanlı savaş alanlarına, suikastlardan suça karşı savaşmaya kadar birçok alanda hayati, hatta belirleyici rol oynamıştır. Gizlice iletilen bir mesajla savaşlar kazanılmış ya da kaybedilmiş, imparatorluklar kurulmuş ya da yıkılmış, insanların hayatları kararmış ya da kurtulmuştur. Kaybedilecek bunca şey söz konusuysen, bir bilgiyi kod veya şifrelerin ardına gizleyen şifre koyucularla (kriptolog) o şifrelerin ardındaki gerçeği açığa çıkarmaya yemin etmiş becerikli ve kurnaz şifre çözümleyiciler (kriptoanalist) arasında sonu olmayan bir mücadelenin süregeldiğini tahmin etmek zor olmasa gerek.

Şifre koyucular her bir şifre ya da kod ürettiğinde şifre çözücüler karanlığa gömülür. Şifresi o zamana dek şipşak çözülen mesajlar bir anda aşılamaz duvarlara dönüşür. Sü (asker) uyur, şifre savaşçıları uyumaz. Şifre çözücüler yılmaz bir kararlılık ya da göz alıcı bir ilham parıltısıyla en sonunda zırhın zayıf noktasını bulur ve gizli mesaj ifşa olana dek bıkmadan usanmadan çalışırlar.

Şifre çözücülük mesleğine gönül vermiş birçok dâhi kadın ve erkek, bu tehlikeli ve zorlu işi kotarabilmek için nice ender özelliklere sahip olagelmıştır. Bir kere oldukça çarpıcı bir özgün düşünce yeteneğine sahiptirler. Tarihteki en ünlü şifre çözücülerden olan ve II. Dünya Savaşı'nın seyrinin değişmesinde parmağı olan Alan Turing zamanının en özgün düşünürlerindendi. Başarılı bir şifre çözücü, aynı zamanda yüksek motivasyon seviyesiyle kendisini gösterir. İnsan aklını hiçbir şey sırlar kadar büyüleyemez. Bazı şifre çözücüler için şifreyi çözmek adına ortaya konması gereken çaba bile kendi başına motivasyon kaynağıdır. Fakat vatanseverlik, intikam,

açgözlülük ya da daha ileri bilgilere sahip olma sevdası gibi başka motivasyon kaynakları da yok değildir.

Gizli mesajları açığa çıkarmak gelip geçici bir hevesten çok daha fazlasını gerektirir. Jül Sezar tarafından benimsenen ilk dönem şifreleme anahtarı olan ve şimdilerde çocukların bile çözebileceği “harf kaydırma yöntemi” o dönemde Sezar’ın düşmanlarını epeyce uğraştırmıştı. Ne de olsa bu tip durumlarda şifre çözücülüğünde sözde kalan özentiler bir süre sonra sapır sapır dökülürdü.

Şifre çözmede hız da hayati önem taşır. Öyle ki birçok şifre ya da kod kırılabilir fakat üzerinde çalışmak için yeterince zamanınız olması gerekir. RSA Algoritması buna klasik bir örnektir. Algoritma, istenilen herhangi iki sayının çarpılması üzerinedir. İki sayıyı çarpmak kolay olsa da hangi sayıların çarpıldığını bilmeyen kişi için onları bulmak bilgisayarla bile çok uzun zaman alabilir.

Şifre çözücülerin sahip olması gereken diğer bir özellikse vizyondur. Çoğu zaman resmî ya da cezai gizlilik altında çalışmak zorundadırlar ve yaptıkları işin hassas doğası genelde yalnız çalışmalarını gerektirir. Nihai amaca giden yolda vizyonları olmadan yaptıkları işler verimsiz ve nafiledir.

Bu kitap, şifrelerin üretilmesi ve kırılmasıyla tarihin nasıl yön değiştirdiğini gösterecek. Şifreleme mefhumunun insanın hayal gücünde kendi çapında sağlam bir yer kaplaması tuhaftır ve aslında bu durum şifrelerle bezenmiş romanların başarısına ya da şifre çözücülerin sürekli televizyonda ya da filmlerde görünmesine de açıklık getirmektedir. Gerçek dünya o kurgusal hikâyelerden çok farklı olsa da kriptolojinin -ve bilhassa şifre çözücülerin- gerçek tarihi, herhangi bir roman yazarının hayalinde canlandırıp kâğıda dökebileceğinden çok daha acayip olaylarla doludur. İlerleyen sayfalarda şifre çözücülerin ne kadar olağandışı insanlar olabileceğini keşfedecek, tarihe geçmiş bazı şahsiyetlerle tanışacak ve bir şifre çözücünün mühimmatı haline gelen temel yeteneklere göz atma fırsatı bulacaksınız.



özgünlük

*Antik Mısır'dan İskoçya Kraliçesi Mary'ye
kadar hem din hem cinsellik şifreleri. Basit ikame
şifrelemeleri, yer değiştirmeler, sıklık analizleri.*

İnsanın olduğu yerleri sırlar, entrikalar, komplolar, siyasi ihanetler, savaşlar, ticari kazançlar, aşk ilişkileri olmadan kafada canlandırmak zordur. Tabii bunların bir getirisi olarak örtülü mesajların ya da gizli yazışmaların tarihinin en eski medeniyetlere kadar uzandığını söylememiz o kadar da şaşırtıcı olmayacaktır.

Şifrelemenin tarihi 4000 yıl öncesine, yazıcıların büyük taş anıtların üstüne oydukları tarihlerin, hiyerogliflerin kullanımını yavaş yavaş değiştirmeye başladığı Antik Mısır dönemine dayanır.

Yaptıkları işin amacı muhtemelen kelimelerin anlamını gizlemek değil, belki gelip geçen okuyucuların kafalarını bulandırmak, eğlendirmek veyahut da dinî yazıtların gizem ve büyüsunü artırmaktı. Fakat bu durum, ilerleyen yüzyıllarda şifreli yazı sisteminin evrileceği yolun habercisi olmuştu.

Gizli yazışmaların gelişmesine aracı olan tek topluluk Antik Mısırlılar değildi. Örneğin günümüz Dicle Nehri'nin kıyısındaki Bağdat şehrine 30 kilometre mesafedeki Seleucia'daki kazılarda bulunan kitabelerden anlaşıldığı kadarıyla bazı şifreleme teknikleri Mezopotamya'daki sosyal yaşamda da kullanılıyordu. M.Ö. 1500 tarihli cep boyutundaki kitabe, çömlek sırlamasına dair şifreli bir formül içeriyordu. Tarifi her kim yazdıysa bu kıymetli ticaret sırrını

Resim: Şifreli yazıların ilk örnekleri Mısır hiyerogliflerinde görülebilir.