Alparslan Babaoğlu

TÜBİTAK UEKAE Enstitü Müdür Yardımcısı

Kriptolojinin Geçmişi
Bir Şifreleme Algoritması Kullanmadan Önce Son Kullanım Tarihine Bakın!

İnsanoğlunun gizli haberleşmeye gereksindiği günden beri şifreleme teknikleri var. Binlerce yıllık gizli haberleşme tarihinde teknolojinin gelişimiyle şifreleme sistemleri ve cihazlar da değişti. Ancak bir ilke binlerce yıldır geçerliliğini koruyor: Kırılan bir şifre tarihin tozlu sayfalarında yerini alır ve onun yerine daha gelişmişi tasarlanır. Diğer bir deyişle, bir şifre kırılmadığı sürece varlığını korur. Kriptoloji bu ilkeyle gelişerek günümüze kadar geldi. İnsanoğlu Alberti diskini ya da Jefferson tekerleğini binlerce yıl daha önce icat edecek teknolojiye sahipti. Antik çağda şifre kırma teknikleri iki yüzyıl önceki kadar gelişmiş olsaydı, belki şimdi o dönem insanlarının Alberti diskini de Jefferson tekerleğini de kullandıklarından bahsediyor olacaktık.

Anahtar Kavramlar

Askeri haberleşmelerinde kriptografi kullanan ilk ulus İspartalılardır. MÖ 5. yüzyılda kendi geliştirdikleri bir cihazı tarihin ilk yer değiştirme sistemini uygulamak için kullanıyorlardı.

Şifre anlamına gelen İngilizce "cipher" ve Fransızca "chiffre" kelimeleri bu dillere Arapçadan (cifr ya da cifir) geçmiştir.

Avrupa'da şifre sistemlerinin ilk yaygın kullanım yeri Rönesans'a muhalefet eden Kilise'ydi.

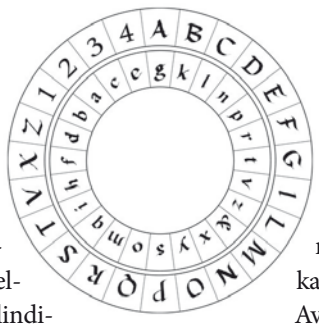
Alparslan Babaoğlu, Manchester Üniversitesi Elektronik Mühendisliği bölümünden 1979'da lisans, 1980'de yüksek lisans derecelerini aldı. TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü müdür yardımcısıdır. Sayısal haberleşme sistemleri, kripto sistemleri, bilgi güvenliği politikaları konularında çalışmaktadır. Bilgi güvenliği konusunda çeşitli kamu kurumlarında seminerler vermektedir.

Bundan 4000 sene önce, Nil nehri kıyısında küçük bir şehir olan Menet Khufu'daki bir kâtip, efendisinin hayatını anlattığı hiyeroglifleri çizerken kriptoloji tarihini başlattığının farkında değildi. Kullandığı sistem modern dünyanın anladığı biçimde bir gizli yazı sistemi olmamasına karşın, metnin rastgele seçilmiş yerlerinde, daha önce hiç kullanılmamış bazı hiyeroglif semboller bulunuyordu.

İlk 3000 yıllık süre zarfında kriptografi sürekli bir gelişim göstermedi. Dünyanın birçok bölgesinde diğer yerlerden bağımsız olarak gelişti ve medeniyetlerin yok olmasıyla birlikte elde edilen birikimler de kayboldu. Antikçağın en ileri medeniyeti olan Çin'de yazının tarihi çok eski olmasına karşın, ideografik yazı (sözleri veya düşünceleri sesleri gösteren harflerle değil çeşitli işaret veya simgelerle yazma sistemi) kullanımına bağlı olarak, bir yazının yazılmasının zaten o yazıyı neredeyse şifrelemekle eş zorluğu olması nedeniyle, kriptografide hemen hemen hiçbir ilerleme kaydedilmedi.

Hrana Janto

Ispartalıların kullandığı kripto cihazı.



Askeri haberleşmede kriptografi kullanan ilk ulus Ispartalılardır. MÖ 5. yüzyılda geliştirdikleri bir cihazı tarihin ilk yerdeğiştirme sistemini uygulamak için kullanıyorlardı. Bu cihaz belli kalınlıkta bir tahta silindirden ve silindirin etrafına eğik biçimde sarılmış papirüs ya da ince, deri bir şeritten oluşuyordu. Gizli mesaj silindir boyunca silindire sarılı şerit üzerine yazılıyor, daha sonra şerit silindirden çözülüyordu. Birbirinden ayrılan harfler yeniden aynı kalınlıkta bir tahta silindire sarılmadıkça hiçbir anlam ifade etmiyordu.

Askeri haberleşmelerde kriptografinin bir diğer önemli kullanımı Roma döneminde oldu. Büyük Roma İmparatoru Julius Caesar, komutanlarıyla kendi geliştirdiği bir yerine koyma sistemini kullanarak haberleşiyordu. Bu sistemde, alfabedeki her harf kendisinden sonra gelen üçüncü harfle (örneğin A, D ile D, G ile) değiştiriliyordu. En temel şifre kırma yöntemlerinden olan ve şifreli metindeki harflerin gözükme sayılarındaki sapmaya dayanan sıklık analiziyle, hiç açık metin olmadan ve hatta şifreleme algoritmasını dahi bilmeden Caesar şifresini kırmak mümkündür. Ancak o dönemde sıklık analizi bilinmiyordu ve Ceasar şifresi Roma ordusunun gereksinimlerini karşılıyordu.

Avrupa'da ortaçağa kadar hiçbir gizli yazışma üzerinde kriptoanaliz yapılmadı. Bu nedenle birkaç istisna durum dışında kriptoanalizle ilgili ciddi bilimsel çalışma olmamış, ancak kriptografi hep var olmuştur.

İlk ciddi kriptoanaliz çalışmaları Araplar tarafından yapıldı. Araplar kriptografi çalışmalarına edebiyatta ve matematikte çağın ilerisinde oldukları MS 600'lü yıllarda başladılar. Şifre anlamına gelen İngilizce "cipher" ve Fransızca "chiffre" sözcükleri bu dillere Arapçadan (cifr ya da cifir) geçmiştir.

Arapların kriptografi konusunda yazdıkları ilk eser, Abdurrahman el-Halil İbn-i Ahmed tarafından MS 718 yılında kaleme alınan *Kitab-ül Muamma* adlı kitaptır. Bu kitapta Abdurrahman el-Halil, Bizans imparatoru tarafından gönderilen Yunanca bir şifreli mektubun çözümünü verir.

wikimedia

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vigenère Karesi

Arapların kriptoloji bilimine en önemli katkısı ise Abdullah Kalkaşandî tarafından 1412'de tamamlanan *Subhu'l A'şâ* adlı 14 ciltlik ansiklopedinin kriptografiyle ilgili bölümleridir. Bu eserde kriptoanalistin ilgilendiği dili bilmek zorunda olduğundan söz edilir ve Arapça'da asla yan yana gelmeyen harflerin bir listesi verilir.

Batı'da günümüze kadar kesintisiz olarak gelen politik kriptografi ortaçağda başladı. Feodal yönetimlerin hâkim olduğu bu dönemde kriptografinin kullanımı ilkel, seyrek ve düzensiz olmakla birlikte sürekli bir gelişim göstermiştir. Avrupa'da kriptografinin ilk günlerinden beri her iki temel yöntem, yani hem kodlar (açık metni oluşturan kelimelerin anlamlı ya da anlamsız başka kelime ya da sayılarla yer değiştirmesi) hem de şifreler (açık metnin belli bir algoritmaya göre şekil değiştirmesi) kullanılmıştır. Şifre sistemlerini yaygın olarak önce Kilise kullandı. 1363 yılında Napoli Kardinali Pietro di Grazie'nin, Papalık ve diğer kardinallerle olan yazışmalarında sesli harfleri kodladığı bir şifre sistemi kullandığını biliyoruz.

Batı dünyasında kriptografinin babası olarak anılan İtalyan Leon Battista Alberti'nin geliştirdiği, iç içe iki diskten oluşan şifreleme cihazında 24 hücre vardı ve cihaz tek alfabeli şifreleme sistemlerinden çok alfabeli şifreleme sistemlerine geçişin ilk örneğini teşkil ediyordu. Kriptoloji tarihi için kritik olan bu başarıdan sonra Alberti kodlamayı ve şifrelemeyi birleştirerek bir başka önemli başarıya daha imza attı: Şifreli kod. Alberti'nin disklerinde harflerle birlikte bulunan dört rakam kodlama amacıyla kullanılıyordu (Bkz. bir önceki sayfa).

Kriptoloji konusunda çağının ilerisinde olan bir başka İtalyan ise Giovanni Battista Porta'ydı. Porta, ünlü kitabı *De Furtivis Literarum Notis*'i yazdığında henüz 28 yaşındaydı. Açık metinde geçen harflerin ikişer ikişer tek bir karakterin yerine geçtikleri, yani iki harfin tek bir karakteri temsil ettiği *digraphic* şifre sistemi Porta'nın buluşudur. Kriptografik sistemler tarihte ilk kez Porta tarafından, harflerin yerlerinin değiştirildiği yerdeğiştirme sistemi ve harflerin birbirinin yerini aldığı yerine koyma sistemi adlarıyla ve bugün de doğru kabul edilen bir sınıflandırmaya tabi tutulmuştur.

1523'te Fransa'da doğan Vigenère'in geliştirdiği ve standart alfabenin kullanıldığı şifreleme sistemi, bugün tüm dünyada Vigenère Karesi olarak bilinir. Sistemin gücü periyodik olmayan anahtar kullanılmasına (anahtar olarak bir kelimenin art arda tekrarının kullanılması yerine rastgele bir cümlenin kullanılması) ve bilinen kripto ihlallerine (bir kripto sisteminin kırılmasına yol açan kullanıcı hatası) meydan verilmemesine bağlıdır. Modern sistemlere örnek olduğu ve temel teşkil ettiği için sistemin nasıl çalıştığı aşağıda açıklanmaktadır.

Açık metin,

t a a r r u z d o k u z d a

Anahtar,

K A L E K A L E K A L E K A

olsun.

Vigenère Karesi'nde şifreleme için küçük harflerle yazılan satır açık metindir. En soldaki sütunsa anahtara aittir. Kapatma işlemi için açık metnin ilk harfi ve ona karşılık gelen anahtar harfi karenin ilk satır ve ilk sütununda belirlenerek, bunların kesiştikleri noktadaki harf bulunur. Bu harf açık metnin ilk harfine karşılık gelen kapalı metnin ilk harfidir. Diğer kapalı harfler de aynı şekilde bulunur. Buna göre şifreli metin,

D A L V B U K H Y K F D N A

olacaktır.

Vigenère'den sonra kriptoloji telgrafın icadına kadar büyük bir ilerleme kaydetmedi. Telgrafın bulunmasıyla, posta işletmelerinde gizli telgrafların görevlilerce açılıp okunması ya da telgraf tellerinin dinlenmesi ile şifreli diplomatik ve askeri haberleşmelerin kolay elde edilebilir olması, hem yeni şifreleme sistemlerinin geliştirilmesini hem de bu sis-

temlerin kriptoanaliziyle ilgili çalışmaların yoğunlaşmasını sağladı.

Vigenère'in yöntemi ya da bu yöntemin değişik biçimlerde kullanımı telgrafın icadından sonra da bir süre devam etti. Ancak, Friedrich Kasiski adlı emekli bir Prusyalı piyade 1863'te bu yöntemi kıran bir test geliştirdi. Literatüre Kasiski testi olarak giren bu analiz yöntemi, şifreli metin içinde beklenenden çok daha sık tekrar eden hecelerin aralarındaki uzaklıklardan anahtarın periyodunu tahmin etmeye dayanıyordu. Kasiski testi özellikle askeri şifre kullanıcılarının paniğe kapılmasına ve yeni şifireleme sistemleri arayışına girmelerine neden oldu. Çözüm, Vigenère'in kırılmasından önce, 1797'de Thomas Jefferson tarafından icat edilen Jefferson cihazıyla geldi. Jefferson'ın cihazı her birinde alfabenin harflerinin yazılı olduğu 36 diskten oluşuyordu.

Charles Wheatstone, 1854'te ilk kez gerçek anlamda *digraphic*, yani harflerin ikişer ikişer şifrelendiği ve sonucun her iki harfe birden bağımlı olduğu bir sistemin haberini verdi. Sistem, Wheatstone tarafından icat edilmişti, ancak arkadaşı Baron Playfair'in adını taşıyordu. Bu sistemin üç önemli özelliği vardı. Öncelikle *digraphic* olduğu için harfler artık kimliklerini kaybetmiş ve tek tek tanınamaz hale gelmiştir. Bu nedenle normal tek alfabeli istatistiksel analiz yöntemleri uygulanamamaktadır. İkinci olarak *digraphic* kodlama istatistik uygulanabilecek mesaj uzunluğunu yarıya indirmektedir. Üçüncü ve en önemli özellikse *digraph*'ların sayısının alfabedeki harf sayısına oranla çok büyük olmasıdır. Bu nedenle dile bağlı karakteristik özellikler çok daha büyük bir sahaya yayılmıştır ve tanınamaz hale gelmiştir. 26 harf yerine 676 *digraph* vardır ve İngilizce'de en çok kullanılan harfler olan *e* ve *t*'nin kullanım oranları sırasıyla yüzde 12 ve 9 olmasına karşılık en çok kullanılan *digraph*'lar olan *th* ve *he*'nin kullanım oranları sırasıyla yüzde 3 ve 2,5'e düşmektedir. Bu özelliklerinden ötürü sistem, zamanında kırılamaz olarak nitelendirilmişti.

Playfair'den sonra kriptoloji biliminde devrim yapmış ve kriptolojiyle matematiğin yakın ilgisini ortaya koymuş bir diğer sistemse Lester Hill'in geliştirdiği Hill sistemidir. Hill, bu sistemin ilkelerini *The American Mathematical Monthly* dergisinin 1929 Haziran-Temmuz sayısında yayımlanan "Cryptography in an Algebraic Alphabet" (Bir Cebirsel Alfabe ile Kriptografi) başlıklı makalesinde ortaya koydu. Hill sistemi, ABD ordusunda sadece üç harf gruplu radyo çağrı sinyallerinin şifrelenmesi amacıyla kullanılmıştır. Ancak, yukarıda da belirtildiği gibi kriptolojinin matematikle olan yakın ilgisinin ortaya konması ve *polygraphic* (birden fazla sayıda açık metin karakterinin şifrelenirken birlikte işleme tabi tutulması) kriptografiyi ilk defa mümkün kılması açısından kriptoloji tarihinde ayrı bir yere ve öneme sahiptir.

Hill, sisteminde anahtar ve açık metin harflerinin sayısal değerlerinin olduğu eşitlikler kullandı. Bu sistemde şifreleme işlemi, denklemlerin çözümlerinin bulunmasından ibarettir. Denklem sayısı, *polygraph*'taki harf sayısına, yani şifrelenirken birlikte işlem gören harf sayısına eşittir. İngiliz alfabesinde 26 harf bulunduğundan ve şifrelerin de çözülebilmesi gerektiğinden Hill tüm işlemlerini MOD-26 üzerinden yaptı. Bu sistem, yalnızca 0'dan 25'e kadar olan sayıların kullanıldığı ve 26'dan büyük her sayıdan, sonuçta 26'dan küçük bir sayı kalana kadar 26'nın çıkartıldığı bir sayı sistemidir.

Hill'in sistemi çok fazla kullanım alanı bulamamış olmasına karşın kriptoloji konusunda çalışanlar üzerinde büyük bir etki bırakır. Çalışmanın güzelliği matematikçileri konuya eğilmeye zorlar. Şifreleme sistemlerinin matematiksel bir biçimde formüle edilmesi, bu sistemlerin zayıflıklarını ve kriptologların sistem tasarımındaki hatalarını ortaya koymaktadır. Daha da önemlisi, kriptoanalistler artık istatistiksel yöntemlerin dışında matematiksel yöntemler de kullanabileceklerini görmüşlerdir.

Bugünkü kriptoloji matematiksel işlemler, matematiksel yöntemler ve matematiksel düşünceyle doyuma ulaşmış bulunuyor. Kriptoloji, uygulamada artık matematiğin bir kolu haline geldi. Bu noktaya gelinmesinde Lester Hill'in katkısı yadsınamaz.

I. Dünya Savaşı sırasında kriptografinin çok yoğun kullanımı ve savaşın haberleşme teknolojisinin ilerlemesine katkısı, savaş sonrasında kriptografinin gelişen teknolojiden daha fazla yararlanmasına neden oldu. Radyo icat edilmişti ve telsiz haberleşmelerini dinlemek artık çok daha kolaydı. Üstelik I. Dünya Savaşı sırasında kriptoanaliz teknikleri de oldukça gelişmişti. Bu nedenle daha güçlü şifreleme sistemlerine gereksinim doğdu. Sonuçta dünyada en çok kullanılacak kriptografik yöntem ortaya çıkacaktı ve bu yöntemle çalışan cihazlar bir sonraki dünya savaşında gizli haberleşmeye yön verecekti: Rotorlu elektromekanik cihazlar...

wikimedia

Jefferson cihazı

Kaynaklar:
Bone, J. V., *A Brief History of Cryptology*, 2005.
Cipher A. D. ve Louis K., *Cryptology: Machines, History, & Methods*, Artech House Cryptology Series, 1989.
Kahn, D., *The Codebreakers: The Story of Secret Writing*, Scribner, 1996.
Menezes, A. J., Oorschot, P. C. ve Vanston, S. A., *Handbook of Applied Cryptography*, CRC, 1997.
Hill, Lester S., "Cryptography in an Algebraic Alphabet," *The American Mathematical Monthly*, Cilt 36, Sayı 6, (Haziran-Temmuz 1929).