

# Ç tarihinden günümüze:

Haluk Oral\* / oralh@boun.edu.tr



## İlk Türkçe Şifreleme Kitapları

Matematiğin en heyecanlı konularından biri şifreleme ve şifre çözümdür. Eski Mısır'dan beri insanlık şifrelemeyle ilgilenmiştir. İnsanlar herkesin bilmesini istemediği konularda haberleştiği de bu ilgi sürecektir.

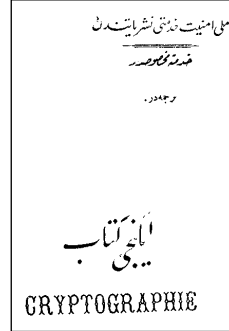
Pek çok kitapta ilk şifreleme örneği olarak Jül Sezar'a atfedilen yöntem verilir. Bu yöntemde her harf yerine alfabetik sıralamada kendisinden üç sonra gelen harf kullanılır; örneğin 'SİLAH' kelimesi 'ULOÇJ' olarak şifrelenir.

Önceleri, şifreleme yöntemlerinde matematiğin kullanıldığını pek söylenemez. Yapılan, birtakım kurnazlıklarla iletinin gizlenmesinden ibaretti; yani şifre analizi, şifrelerin kırılması için bir yöntem araştırması, başka bir deyişle, şifrenin ne kadar güvenilir olduğuna dair bir araştırma yapılmıyordu.

Şifrebilim (kriptoloji), şifreleme ve şifre analizinden oluşur. Bu tanıma göre, uzun yıllar şifrelemeyle uğraşılmasına karşın, şifrebilimin çok daha sonra, 800'lü yıllarda Araplar tarafından bulunduğunu söyleyebiliriz. İngilizce *cipher* ve bizim kullandığımız *şifre* ve *sıfır* sözcükleri de Arapçadan (جوفى, sat-fe-rı) gelir [1].

Bu kısa girişten sonra elimdeki bir iki kitaptan söz etmek istiyorum.

Önce, harf devriminden birkaç ay önce, 1928'de Arap harfleriyle basılmış bir kitap: "Milli Emniyet Hizmeti Neşriyatı"ndan bir tercüme:



Ankara  
15/Birinci Teşrin/ 928

آنقره  
928 / برنجی تشرین / 15

"Kriptografi" memleketimiz için pek yeni bir şeydir.

Milletler bir taraftan devletlerinin emniyetini ihlale müteveccih<sup>1</sup> her türlü tehlikelerden

korunmak, diğer taraftan diğerlerinin kendi haklarında düşüncüklerini ve muhaberatım<sup>2</sup> öğrenmek için var kuvvetleriyle çalışırlar.

Malum olduğu üzere bu gibi mahrem şeyler daima gizlenmekte ve rakam, gizli kelime, gizli yazı... ilb<sup>3</sup>. kapalı olarak ifade olunmaktadır. İşte bu gizli kapalı şeyler dahi ilim ve fen karşısında gizli kalamamaktadır. Bugün gizli kelime ve yazı ile yazılmış veya şifrelenmiş yazı ve şifre mütehasısların elinden kurtulamamaktadır. İlim ve fen bunda da muvaffak olmuş ve buna müteallik<sup>4</sup> ciltlerle eserler yazılmıştır.

Bu kitap söylenmesinde ve ifşasında mahzur olan mevâdir<sup>5</sup> ihtiva etmemekle beraber alakadarları tehlikeler hakkında cüzi dahi olsa tenvir edebileceği<sup>6</sup> kanaatiyle neşrolunmuştur.

Bunu takip edecek kitaplarda kriptografiye ait bazı malumat daha derç olunacaktır<sup>7</sup>.

[2]'nin önsözü

« قریبتوغرافی » مملکتتمز ایچون یب یکی بر شیدر . ملتله بر طرفدن دولتلرینک امنیتی اخلاله متوجه هر دولتهلکهلردن قوروتتیق ، دیگر طرفدن دیگرلرینک کندی حقلرته دوشو ندکلرینی و مخبراتی او کر تک ایچون وار قوتلریله چالیشیرلر . معلوم اولدنی اوزره بوکی محرم شیدر دائما کیزلنکده ورقم ، کیزی که ، کیزی یازی . . . الخ قبالی اولهرق افاده اولومقدهدر . ایشته بو کیزی قباللی شیدر دخی علم و فن قارشیسنده کیزی قالمقدهدر . بوکون کیزی که و یازی ایله یازلش و یا شیفره لئش یازی و شیفره ، متخصصلرک الندن قورتولمامقدهدر . علم و فن بوندده موفق اولش و بوکامتعلق جلدلرله اثرلر یازلشدر .

بو کتاب سویتمسندده وافشاسنده مخدور اولان موادی اجتوا ایجه مکله برابر علاقه دارلری تهلکهلر حقلنده جزئی دخی اولسه سنور ایده بیله چی قناعیتله نشر اولومشدر . بونی تمقیب ایده جک کتابلرده قریبتوغرافییه عائد بعض مالومات دهادر دوج اولونه جقدر .

\* Boğaziçi Üniversitesi Matematik Bölümü öğretim üyesi.

1 Yönelen.

2 Haberleşmeler.

3 vb.

4 Bağlı, ilişkisi olan.

5 Maddeler.

6 Aydınlatılabileceği.

7 Gazeteye yazma, basma.

Cryptographie [2]. Başlığında da belli ki kitap Fransızcadan çevrilmiş, ancak ne yazarı ne de çevirmeni belirtilmemiş.

Nerdeyse kelime kelime yabancı dilden çevrilen bu kitap yanlışlarla dolu. Sanırım Cumhuriyet döneminde basılmış ilk şifrebilim kitabıdır. Bazı tarihi bilgiler yanında şifre kırma örnekleri de verilmiştir, tabii hep Fransızca.

İkinci kitap bir yıl sonrasına ait. Harf devrimi 1928'de yapıldığından, bu kitap Latin harfleriyle basılmış. Yine "Milli Emniyet Hizmeti Neşriyatı"ndan: Gizli Anlaşmalar. Yine yazarı belli değil. Çeviri ya da uyarılama olabilir çünkü örnekler bu sefer Türkçe. Birçok şifreleme yöntemi verilmekle beraber şifre kırma yöntemlerinden söz edilmez.

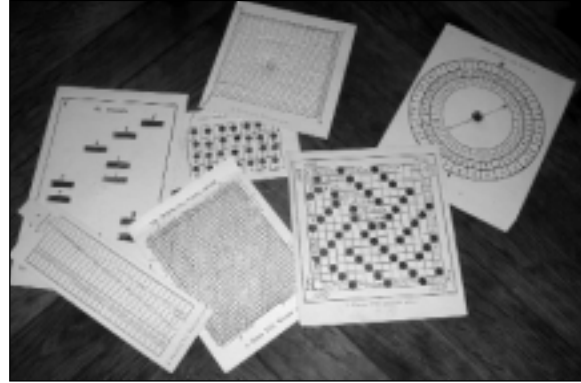
Kitapta açıklanan çok basit ve çözmesi çok kolay bir şifreleme örneği:

Aynı esas dahilinde yukarıdaki şekle göre şu tarzda bir alfabe vücut bulur:

a .	h .	o .	ü .
b .	i .	ö .	v .
c .	j .	p .	y .
ç .	k .	r .	z .
d .	l .	ş .	
e .	m .	t .	
f .	n .	u .	
g .			

Burada yapılan, en yukarıdaki birinci şekilden her harfe tekabül eden açıyı bularak, harf yerine mesaja da açıyı kullanmak. Her harfe tekabül eden şekil sağ tarafta gösterilmiş. Ama bunu yapmakla, her harf yerine bir sayı kullanmak arasında hiçbir fark

yok, çünkü ne de olsa birebir bir şifreleme sözkonusu. Bu tür şifrelemeleri çözmek çok kolaydır. İstatistiksel yöntemlerle, dilin yapısına göre, en çok kullanılan harfler göz önüne alınarak kolayca çözülür.



Bugün, çağdışı olarak nitelendirebileceğimiz birkaç şifreleme araç gereci.

Kitapta, başka hiçbir yerde görmediğim ilginç bir şifreleme yöntemi var: İplik şifresi... Bir kartonu yatay ve dikey doğrularla karelere bölelim. En üst sıraya alfabenin harflerini yazalım. Her ne kadar kitapta harfler alfabetik sıralanmışsa da, harfler herhangi bir sırayla dizilebilir. Kartonun sağ ve sol sütunları bir iplik geçecek büyüklükte delinir.

Sonra, kartona, en üst satırdan başlayarak her satırdan geçecek şekilde tek parça bir iplik çekilir (iplik kartonun arkasından zigzag yapmaktadır.) Şifrelenecek mesajın ikinci satırdaki iplikte işaretlenir, ikinci harfi

Papalık 1555'te şifre sekreterliğini kurdu. Bu bölümde nerdeyse tüm Avrupa devletlerinin şifreli haberleşmeleri izleniyor ve şifreler kırılıyordu. Şifrebilim Müslümanlar tarafından kurulmuştu ama Osmanlıların bu konuda fazla bilgili olduğunu söyleyemeyiz. 1567'de "the Great Vicar of St. Peter" tek kelimesini bile bilmediği Türkçe yazılmış şifreli bir metni altı saatten az bir zamanda çözmüştü. Bu asırlarda şifrebilimle ilgili nerdeyse bütün gelişmeler şifre sekreterliği aracılığıyla oldu diyebiliriz.

ikinci satırdaki iplikte şifrelenir ve bu böylece devam eder. Şifreleme işi bittiğinde iplik çıkarılıp öbür kişiye yollanır. Öbür kişide de aynı kartondan olduğundan, o kişi ipliği kartona tekrar geçirerek şifreyi rahatlıkla çözer. Yalnız en ufak bir kayma yanlış anlamalara neden olabilir. ♣

#### Kaynakça

- [1] Sevan Nişanyan, *Sözlerin Soyağacı, Çağdaş Türkçenin Etimolojik Sözlüğü*, Adam Yayıncılık, 2. basım, Şubat 2003.
- [2] Cryptographie, "Milli Emniyet Hizmeti Neşriyatından. Hizmete Mahsustur. Tercümedir. İkinci Kitap." 1928.
- [3] Gizli Anlaşmalar, "Milli Emniyet Hizmeti Neşriyatından. Hizmete Mahsustur. Beşinci Kitap." 1929.