φ tarihinden günümüze:

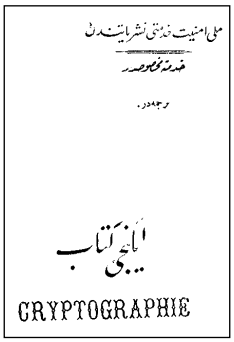
Haluk Oral* / *oralh@boun.edu.tr*

İlk Türkçe Şifreleme Kitapları

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

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 (j°u, sat-fe-rı) gelir [1].



Bu kısa girişten sonra elimdeki bir iki kitaptan sözetmek 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
15 / برنجی تشرین / 928

"Kriptografi" memleketimiz için pek yeni bir şeydir. Milletler bir taraftan devletlerinin emniyetini ihlale müteveccih[1] her türlü tehlikelerden korunmak, diğer taraftan diğerlerinin kendi haklarında düşündüklerini ve muhaberatını[2] öğrenmek için var kuvvetleriyle çalışırlar. Malum olduğu üzre bu gibi mahrem şeyler daima gizlenmekte ve rakam, gizli kelime, gizli yazı... ilh[3]. 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 mütehassısların elinden kurtulamamaktadır. İlim ve fen bunda da muvaffak olmuş ve buna müteallik[4] ciltlerle eserler yazılmıştır.
Bu kitap söylenmesinde ve ifşasında mahzur olan mevâddı[5] ihtiva etmemekle beraber alakadarları tehlikeler hakkında cüzi dahi olsa tenvir edebileceği[6] kanaatiyle neşrolunmuştur.
Bunu takip edecek kitaplarda kriptografiye ait bazı malumat daha derç olunacaktır[7].

« قريپتوغرافی » مملکتمز ایچون یپ یکی بر شیدر . ملتلر بر طرفدن دولتلرینك امنیتنی اخلاله متوجه هر درلو تهلکه لردن قورومق ، دیکر طرفدن دیکرلرینك کندی حقلرنده دوشو ندکلرینی و مخابراتی اوکرنمك ایچون وار قوتلریله چالیشیرلر .
معلوم اولدیغی اوزره بوکبی محرم شیلر دائما کیزلنمکده و رقم ، کیزلی کلمه ، کیزلی یازی . . . . الخ قبیلی اولهرق افاده اولونمقده‌در . ایشته بوکیزلی قپاقلی شیلر دخی علم و فن قارشیسنده کیزلی قاله‌ماعقده‌در . بوکون کیزلی کلمه و یازی ایله یازلمش ویا شیفره‌لنمش یازی و شیفره ، متخصصلرك الندن قورتولهاعقده‌در . علم و فن بونده‌ده موفق اولمش وبوکا متعلق جلدلرله اثرلر یازلمشدر .
بو کتاب سویلنمسنده وافشاسنده محذور اولان موادی احتوا ایتمکله برابر علاقه‌دارلری تهلکه‌لر حقنده جزئی دخی اولسه تنویر ایده‌بیله‌جکی قناعتیله نشر اولونمشدر . بونی تعقیب ایده‌جك کتابلرده قریپتوغرافی‌یه عائد بعض معلومات دها درج اولونه‌جقدر .

[2]'nin önsözü

* Boğaziçi Üniversitesi Matematik Bölümü öğretim üyesi.

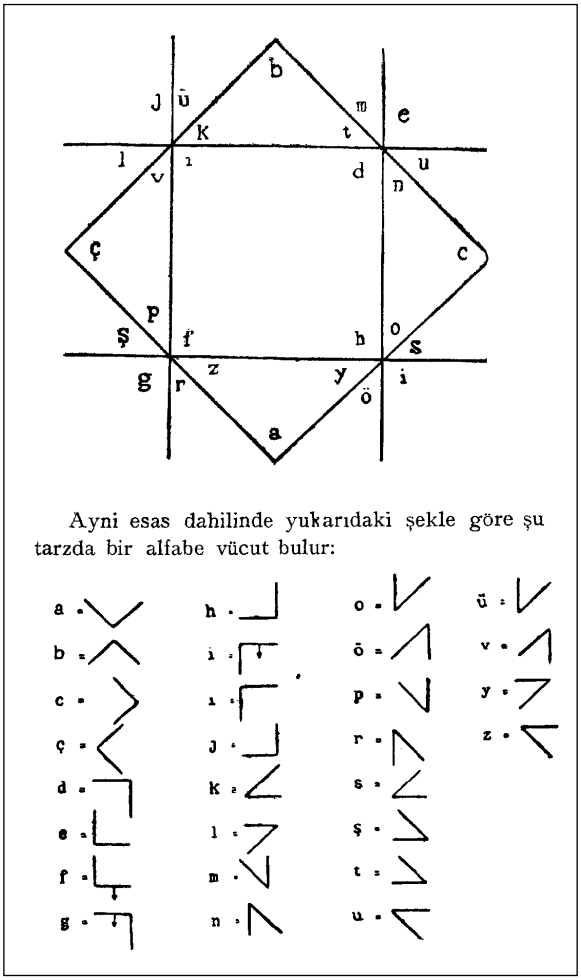
1 Yönelen.
2 Haberleşmeler.
3 vb.
4 Bağlı, ilişiği olan.
5 Maddeler.
6 Aydınlatabileceği.
7 Gazeteye yazma, basma.

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

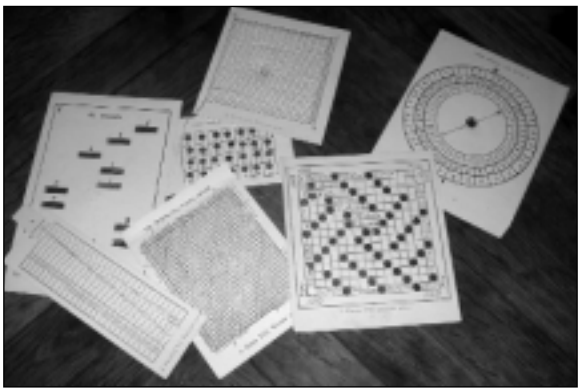
Nerdeyse kelime kelime yabancı dilden çevrilen bu kitap yanlışlarla dolu. Sanırım Cumhuriyet döneminde basılmış ilk şifrebilim kitabıdır. Bazı tarihi bilgiler yanında şifre kırma örnekleri de verilmiştir, tabii hep Fransızca.

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 uyarlama olabilir çünkü örnekler bu sefer Türkçe. Birçok şifreleme yöntemi verilmekle beraber şifre kırma yöntemlerinden sözedilmez.

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



Burada yapılan, en yukarıdaki birinci şekilden her harfe tekabül eden açıyı bularak, harf yerine mesajda o 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 başlayacak her satırdan geçecek şekilde tek parça bir iplik çekilir (iplik kartonun arkasından zigzag yapmaktadır.) Şifrelenecek mesajın ilk harfi birinci satırdaki iplikte işaretlenir, ikinci harfi 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. ♣

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.

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.