

Polybius Şifresi

Ali Eskici / alieskici@mynet.com

Eski Yunan'da savaşlar ve ticaret yoğunluğunda. Aynı bugün bütün dünyada olduğu gibi... Bu nedenle askeri ve ticari bilginin güvenilir şekilde iletilmesini sağlamak için Yunanlılar bazı şifreleme sistemleri geliştirdiler.



Yunanlı tarihçi, general ve devlet adamı Polybius (M.Ö. 200-118), bugün Polybius damatahtası denen bir cihaz kullanarak metin şifrelemenin temellerini ortaya koydu. Ayrıca, Yunanlılar benzer konularda, diğer ulusların ve Romalıların kullandığı ilkel şifreleme tekniklerini de kullanıyorlardı.

Polybius damatahtası alfabenin tüm harflerini içeren beş beşlik bir ızgaradan oluşuyordu.

Her harf, ilk harfin bulunduğu satır ve ikincisi de sütun olmak üzere iki sayıya dönüştürülüyordu. Şu halde A için 11, B harfi için 12 ve sonrakiler için ilgili sayılar eşleşirdi.

	1	2	3	4	5
1	A	B			
2					
3					
4					
5					

Polybius şifrelemesinde kullanılan ızgara yukarıda ifade edildiği gibi 5×5 birimlik değil, kullanılan alfabe hatta şifrelenecek metnin içerdiği harf sayısına bağlı olarak istenen $n \times m$ boyutta tasarlanabilir.

Polybius şifrelemesinde her sayı (ya da simge) tek bir harfe tekabül ettiğinden, dilin yapısından hareketle böyle bir şifreyi çözmek zor değildir, hele şifrelenmiş metin yeterince uzunsa. Örneğin Türkçede sık kullanılan iki harfli kelimelerden çok yoktur. Bunların ve, ya, de, da gibi sözcüklerin olabileceği

hemen çıkar. Türkçenin -ler, -lar, -yorum, -yorsun, -cekler gibi ekleri de bize ipucu verir.

Polybius şifreleme yöntemi sayesinde her harfe tekabül eden sayı kolaylıkla bulunabilir, hangi harfin hangi harfe tekabül ettiğini ezberlemeye gerek yok. Hatta daha büyük damatahtaları kullanarak ve alfabe bittiğinde alfabeyi yeni baştan yazarak, aynı harfi birkaç sayıyla da gösterebiliriz, o zaman şifreyi çözmek daha zor olur.

Dilbilim kurallarına uymayan ya da çok sık şifreleme hatası yapan birinin şifresini çözmek zaman alabilir elbet, ama gene de metin uzunsa bu bile çok zor değildir.

Aşağıda MD Yayın Kurulu tarafından bize yol gösteren gizli şifreyle şifrelenmiş metni bulacaksınız.

16 11 21 - 56 36 21 41 36 21 24 36 61 - 16 11
 21 - 98 55 73 38 61 - 16 36 61 11 - 57 36 56 21
 36 52 52 11 72 11 - 24 31 56 98 31 57 31 61
 23 - 99 23 17 19 41 24 19 72 19 29 24 23 - 55
 61 14 36 - 17 36 99 - 52 36 41 23 39 41 23 61
 29 23 24 19 29. 23 73 - 55 61 14 36 - 48 11 73
 11 39 52 11 21 24 11 72 11 29 - 56 23 73 19
 56 41 23 - 11 41 98 11 41 11 - 16 11 21 - 56 23
 61 19 41 57 23 29 23 - 24 31 56 98 31 57 31 -
 75 41 29 23 41 19 - 16 31, 24 11 56 75 21 24
 31 29, 48 38 61 99 38 - 57 23 61 24 19 72 19
 29 - 98 11 16 11 - 61 36 - 24 23 21 - 57 75 99
 23 72 23 - 57 23 21 99 23 61 - 48 23 21 17 19
 99 - 14 31 29 16 23 61 19 61 - 56 23 61 - 17 36
 61 14 36 21 36 57 11 61 24 36, 61 36 - 24 36 -
 16 75 39 - 23 21 57 23 24 23 99 11 - 99 23 21
 23 61 41 19 72 19 61 - 11 48 11 61 24 36 - 16
 36 61 11 - 98 55 73 36 52 41 36 56 36 61 - 16
 11 21 - 98 55 73 - 67 23 21 24 19.

Şifreyi Nasıl Çözdüm?

Şifre metnin Türkçe bir metni ifade ettiği Türkçe'nin kendine has yapısından hemen anlaşılıyor: uzun ve ek almış kelimeler aynı sayı gruplarıyla bitiyor.

MD'nin şifre sisteminde, Polybius şifresinde olduğu gibi her harfe tek bir sayı tekabül ettiğini

1									
2									
3									
4									
5									
6									
7									
8									
9									

varsaydım. Bunun böyle olduğuna dair ipucu, harflerin ifade edildiği sayıların 99'a kadar olan sayılarla temsil edilmesinden geliyordu. Noktalama işaretleri şifrelemede ayrıca gösterildiğinden ve şifrelemede 0 ifadesi olmadığından

Türkçenin 29 harfi için 11'den 99'a kadar gösterimli bir yerine koyma metodu kullanıldığını anladım. İçine şifresini keşfettiğim harfleri yerleştirmek amacıyla, yandaki gibi, 9 x 9 birimlik bir harf ızgarası hazırladım.

Önce 16 11 21 sayılarıyla başladım. Bu sayı grubunun belirttiği ifadeler, "bir, iki, çok, yok, boş, dur, bak, gör" gibi kelimeler olabilirdi. Sonra "61 36, 24 36, 16 31" gibi ikili grupları inceledim. Bunlar da "de, ki, bu, ne" gibi Türkçe'de az sayıda bulunan iki harfli kelimeler olabilirdi.

İkili sayı gruplarından 61 36 - 24 36 kelimele-
rinin ne olabileceğini düşündüm. Türkçede bu şekilde yanyana gelebilecek iki harfli kelimeler "ve de", "ne de", "ne ki", "ve bu", "bu ne", "ne bu" şekillerinde olabiliyor. Bunları sırayla deneyerek elde ettiğim sayı-harf karşılıklarını diğer sayı gruplarının belirttiği kelimelerin olabilirlikleri üzerinde test ederek yerleştirme işlemlerini yaptım. Kısa sü-

1	İ			C		B	P		I
2	R		A	D					M
3	U					E		Ü	Ş
4	L						Z	Ç	
5		T			Ö	Y	S		
6	N						V		
7		Ğ	Z		O				
8									
9							G	K	

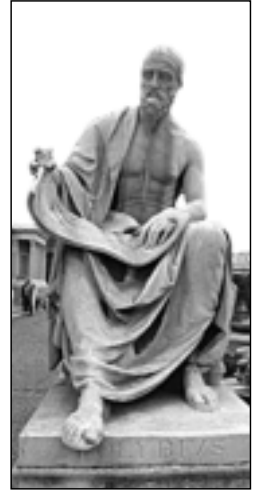
rede bulduğum (deşifre ettiğim) harfler kelimelerin parçaları olmaya başlayınca bu defa deneme-yanılma yolunu bırakıp kimi harfleri çıkmış olan kelimeleri doldurarak aradaki boş harflerin hangi sayıları temsil ettiğini tahmin ederek buldum. Bulduklarımı diğer sayı gruplarında yerleştirince o kelimeler de parçacıkları tamamlamaya başladı. Harfler bu şekilde birbirlerini adeta besleyince, açık metnin bulunması ışık hızına yaklaştı. Sonunda tabloyu yukardaki gibi tamamladım.

Tablo tamamlandığında deşifreleme işlemi de bitmiş oluyordu. Böylece, elde ettiğim açık metin şu oldu:

BİR YERLERDEN BİR GÖZÜN BENİ SEYRETTİĞİ DUYGUSUNA KAPILDĞIMDA ÖNCE PEK TELAŞLANMADIM. AZ ÖNCE ÇİZİŞTİRDİĞİM YAZIYLA İLGİLİ BİR YANILSAMA DUYGUSU OLMALI BU, DİYORDUM, ÇÜNKÜ SANDIĞIM GİBİ NE DAR SOKAĞA SARKAN ÇARPIK CUMBANIN YAN PENCERESİNDE, NE DE BOŞ ARSADAKİ KARANLIĞIN İÇİNDE BENİ GÖZETLEYEN BİR GÖZ VARDI.

Bazı ı'ların üstüne noktalar konmuş... Herhalde bizi şaşırtmak için olmalı, yoksa MD'nin böyle bir hata yapacağını sanmıyorum!

Şimdi de okurun deşifrelemesi için aynı yöntemle şifrelenmiş bir metni sunuyorum:



58 85 37 85 48 77 17 - 64 85 73 14 21 14 - 73 46
68 13 48 - 32 63 55 48 - 85 44 85 64 77 17 73 85
45 84 - 46 63 85 58 63 85 44 73 85 17 - 84 12 85
44 14 71 - 46 63 48 85 64 77 17 77 17 - 12 84 44
14 58 - 84 11 84 17 - 71 14 45 - 26 14 - 54 14 11
14 44 63 84 - 85 17 63 85 48 - 46 63 48 85 64 77
- 58 55 65 14 58 64 14 63 - 12 85 45 77 37 - 85 11
77 63 85 44 77 - 84 11 84 17 - 45 85 12 13 63 - 14
73 84 63 14 12 84 63 84 44. 85 17 21 85 45 - 12
14 17 21 14 - 58 55 65 14 58 64 14 63 - 12 85 45
77 37 - 85 11 77 63 85 44 77 - 84 17 64 85 17 85
- 38 84 11 12 84 44 - 37 14 58 - 45 85 65 85 17 73
77 44 48 85 65. 85 58 44 77 21 85 - 58 85 37 85
48 77 17 - 12 13 17 73 85 17 - 11 46 45 - 73 85 38
85 - 36 85 65 63 85 64 77 - 46 63 73 13 68 13 17
13 - 54 32 44 55 62 - 73 14 - 73 55 37 55 17 48 14
48 14 45, 54 85 63 85 45 64 84 48 84 65 84 17 -
48 14 44 45 14 65 84 17 73 14 45 84 - 84 45 64 -
26 14 - 48 46 44 32 71 14 64 84 - 77 37 77 17 - 77
65 54 85 44 85 64 77 17 73 85 - 12 84 36 71 14
45 - 45 77 65 85 44 71 48 85 45 - 84 11 84 17 - 46
44 85 58 85 - 54 84 71 48 14 45 71 14 17 - 73 85
38 85 - 45 46 63 85 58 - 26 14 - 85 17 63 85 48 63
77 - 73 14 68 84 63 ♥