NİRELERFİŞ ISAYNÜD

Arkadaşlarınızla şifreli haberleşmek çok eğlenceli olabilir. Sır gibi sakladığınız, başkalarından köşe bucak saklanarak konuştuğunuz şeyler mutlaka vardır. Bunları, yalnızca arkadaşlarınızın anlayabileceği biçimde şifreleyerek bir kâğıda yazdığınızı ve rahatça ortada bırakabildiğinizi düşünsenize! Bunu, herkesin kolayca anlayamayacağı şifre ya da kodlar kullanarak başarabilirsiniz. Haydi işe koyulalım ve birkaç numara öğrenelim.

"İnsanlar yazının icadından beri şifreli yazılar yazıyor" dersek yanlış olmaz. Tarih boyunca bir mesaj ne zaman gizli tutulmaya çalışılsa, şifreler ve kodlar kullanılmış. Devlet yöneticilerinin birbirlerine gönderdiği mektuplar, başkalarının okuyamaması için şifrelenmiş. Savaşların sonuçları, gizli mesajların sırrının çözülüp çözülemediğine göre değişmiş. Günümüzde de, özellikle hükümetler, silahlı kuvvetler, şirketler ve çeşitli kuruluşlar, gizli bilgileri korumak için şifreler ve kodları inceleyen bilim dalından, yani "kriptoloji"den yararlanıyor. Bu bilim dalında artık karmaşık matematiksel işlemler ve bilgisayarlar da kullanılıyor. Bu da, kullanılan şifre ve kodların çözümünü zorlaştırıyor.

Şifreler ve kodlar, biz farkında olmasak da, günlük yaşamımızın bir parçası durumunda. Otomatik para çekme makinelerinde, kredi kartlarında, e-postalarda, e-ticarette hep şifrelerden yararlanıyoruz. İnternet'ten hizmet veren çoğu kuruluş, kredi kartı numaralarımızı ve diğer özel bilgilerimizi içeren web sayfalarındaki gizli bilgilere ulaşılmasını engellemek için, şifreleme amaçlı özel bilgisayar yazılımları kullanıyor. İnternet'te hangi sayfaların korunduğunu siz de anlayabilirsiniz. Bunların adresi "http" yerine "https" ile başlıyor. Bu sayede, bankacılık işlemlerimizi ve önemli belgelerimizin istediğimiz kişilere iletilmesini, İnternet gibi aslında pek de güvenli olmayan bir ortamda gerçekleştirebiliyoruz. Bunu da, kriptoloji alanında son 30 yılda yapılan büyük buluşlara borçluyuz.

Şifre mi, Kod mu?

Şifreler ve kodlar, gizliliği sağlamanın olmazsa olmaz parçalarıdır. Bu iki terimi pek çok kişi aynı anlamda kullansa da, aralarında bazı farklılıklar var.

Sözcükler, cümlecikler, cümleler ya da sayılar yerine kullanılan simgelere, harflere, sözcüklere ya da sinyallere "kod" denir. Kodlar, iki

farklı amaçla kullanılabilir: mesajı kısa tutmak ve gizlemek. Şifrelerse, bir sözcük ya da cümledeki harflerin yerinin yeniden düzenlenmesiyle ya da her bir harfin yerine başka bir harfin ya da simgenin kullanılmasıyla oluşturulur.

Anahtarınız Var mı?

Bir şifre ya da kodun yararlı olabilmesi için mesajı gönderenin ve alıcının bazı bilgileri baştan paylaşmaları gerekir. Bunlardan biri, bir düz metni, şifreli metin haline getirmeye yarayan kurallar dizisi olan "algoritma" ya da "yöntem"dir. Ancak algoritmanın işe yaraması için "anahtar" bilgisinin de paylaşılması gerekir. Anahtar, algoritma kurallarının hangi düzene göre uygulanacağını belirtir. Anahtarın geçerli olacağı süreyi de her iki tarafın bilmesi gerekir. Algoritma, anahtar ve süre ilişkisini bir örnekle açıklayabiliriz.

Evinize girmek için öncelikle sokak kapınızdaki kilide bir anahtar yerleştirmeniz gerekir. Burada anahtarın ve kilidin kullanılması yöntem, yani algoritmadır. Ancak bu yöntem, yalnızca doğru anahtarı kullandığınızda çalışır. Ayrıca, bu anahtar yalnızca bu evde oturduğunuz sürece çalışır. Çünkü siz bu evden taşındığınızda, evin yeni sahipleri, eski anahtarla kapının açılmaması için

Harf Yerine Sayı

Alfabedeki 29 harfin her biri sırasıyla 1'den 29'a kadar sayılarla gösterilir. A=1, B=2, ... Z=29 gibi. Bu biçimde hazırlayacağınız bir şifreyi hızla yazmak ya da hazırlanmış bir şifreyi hızla çözmek için alfabedeki harfleri sırasıyla yazıp bunların altına da, sayıları aşağıdaki gibi yerleştirebilirsiniz.

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
16	17	18	19	20	21	22	23	24	25	26	27	28	29

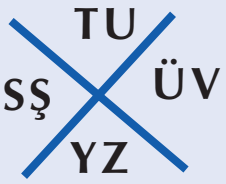
Bu şifreye göre "BİLİM ÇOCUK" "2 12 15 12 16 4 18 3 25 14" sayılarından oluşuyor.

İsterseniz, 1 sayısını "A" yerine başka bir harften başlatarak, şifreyi daha karmaşık hale getirebilirsiniz. Örneğin "A" yerine "M" harfine "1" dediğinizde, "Z" harfine "14" sayısı denk gelir. Buradan tekrar "A" ya döndüğünüzde, A=15, B=16..... L=29 olur.

Çerçeve

Bu şifre için ilk yapmanız gereken, alfabedeki tüm harfleri aşağıdaki biçimde bir kâğıda yazmak. Bu, sizin anahtarınız olacak.

AB	CÇ	DE
FGĞ	HI İ	JKL
MN	OÖ	PR



Bu şekle göre her harf kendini çevreleyen çerçeveyle gösteriliyor. Bu yüzden dikkatinizi harfleri çevreleyen çizgilere verin. Fark ettiyseniz çerçeve olarak adlandırdığımız her hücrede birden fazla harf var. Bu yüzden, soldan sağa ilk sırada yazılan harfler için yalnızca o iki ya da üç harfi çevreleyen çizgileri kullanacağız.

A= ⌟ , M= ⌝ , Y= ∧ gibi.

Çerçeve içinde ikinci sırada yazılan harfler için, çerçevenin içine bir nokta koyacağız.

B= ⌟· , G= ⌝· , Ş= > gibi.

Üçüncü sırada yazılan harfler için de, iki nokta koyacağız.

İ= ⊡ L= ⊏ gibi.

Buna göre "şifre" sözcüğünü

biçiminde yazıyoruz.

Bu sisteme göre adınızı yazmayı deneyebilirsiniz.

Sözlük Kodları

Sözlükler yüzyıllardır gizli haberleşme amacıyla kullanılır. Sistemi ve anahtar sözlüğün hangisi olduğunu bilmeyenlerin, bu işin işinden çıkması gerçekten çok zor. Bunun için haberleşmek istediğiniz kişilerde ve sizde aynı sözlüğün olması yeterli. Daha sonra iletmek istediğiniz mesajı bir yere yazın. İlk sözcüğünüzü sözlükten bulun. Sayfa numarasını, sütun numarasını ve bu sütunda yukardan aşağı kaçıncı satırda olduğunu yazın. Her sözcüğü ifade eden sayıların arasına nokta koymayı ve her bir sözcüğü simgeleyen kodlar arasına birer boşluk bırakmayı unutmayın!

Şimdi bir örnek yapalım. Bizim elimizde Türk Dil Kurumu'nun 1988 yılında basılmış sözlüğü var. Bu sözlükten yararlanarak, "Şifre çözmek kolay mı?" yazmak istiyoruz.

şifre: 1385. sayfanın, 2. sütununda, yukardan aşağıya 35. satırda;

çözmek: 323. sayfanın, 1. sütununda, 7. satırda;

kolay: 886. sayfanın 1. sütununda, 19. satırda;

mı: 1021. sayfanın 2. sütununda 6. satırda açıklanıyor.

Buna göre cümlemizin kodlanmış hali

"1385.2.35 323.1.7 886.1.19 1021.2.6"

biçiminde yazılıyor.

Sözcüklerin başına ya da sonuna bir ek geldiğinde ve sözcük bu haliyle sözlükte geçmediğinde, bu ekleri kodlanmış sözcüklere düz yazıyla ekleyebilirsiniz. Örneğin sözlüğünüzde –mı eki tanımlanmamışsa "kolay mı" sözcüğünü "886.1.19mı" biçiminde yazabilirsiniz.

Bu tür bir kodlama için sözlük yerine herhangi bir kitabı da kullanabilirsiniz. Bu durumda, istediğiniz sözcüğe işaret edebilmek için, sayfa numarasından sonra, paragraf numarasını ve bu paragrafta kaçıncı sözcük olduğunu yazmanız gerekecek.

Tablo

İlk yapmanız gereken kendinize aşağıdaki gibi bir tablo hazırlamak. Bu, sizin anahtarınız olacak. Daha sonra bu tabloya bakarak kullanmak istediğiniz harfin yerini belirten sütun ve satır adlarını not etmeniz gerekiyor. Önce sütun adını, sonra da satır adını yazın. Örneğin, aşağıdaki tabloya göre A=A1, B=A2, ... ve Z=E4. Ama siz harflerin yerini istediğiniz gibi değiştirebilirsiniz. Alfabetik bir sıralama olması gerekmiyor. Ayrıca, sütun ve satırlara da başka adlar verebilir, hatta buralarda istediğiniz simgeleri kullanabilirsiniz.

	1	2	3	4	5
A	A	B	C	Ç	D
B	E	F	G	Ğ	H
C	I	İ	J	K	L
Ç	M	N	O	Ö	P
D	R	S	Ş	T	U
E	Ü	V	Y	Z	*

Peki, bu tabloya göre aşağıda ne yazdığını bulabilecek misiniz?

C4 D1 C2 Ç5 D4 Ç3 C5 Ç3 C3 C2 Ç2 B1 C4 A1 A5 A1 D1 A5 A1 B1 B4 C5 B1 Ç2 A3 B1 C5 C2

o kilidi değiştirir. Bu durumda, algoritmayı bilseniz de elinizdeki anahtar artık işinize yaramaz.

Algoritma, anahtar ve süre seçimi gereksinimlerinize bağlıdır. Örneğin, şifreli metinlerin kısa sürede çözülmesi sizin için önemliyse, hızla çözebileceğiniz kolay algoritmalar seçebilirsiniz. Ama bu durumda, anahtarları sık sık değiştirmeniz gerekir. Çünkü, şifrelerin dünyasında en önemli nokta, algoritmanın nasıl çalıştığını gösteren anahtarın çok iyi gizlenmesidir.

Bu yazımızdaki örneklerden yola çıkarak, siz de kendi algoritmanızı yaratabilirsiniz. Sözcüklerdeki sesli harfleri kullanmamayı, sözcükleri tersten yazmayı, her harf için özel simgeler geliştirmeyi, her sözcüğün ilk harfini başka bir harfle değiştirme-

Blok Şifresi

Blok şifresi oluşturmak için, iletmek istediğiniz mesajı sözcükler arasında boşluk bırakmadan bir kenara yazın. “bugünsaatbeştebuluşalım” gibi. Sonra, mesajınızı harflerin sırasını bozmadan ve harfler tam birbirinin altına gelerek, düzgün bir kare ya da dikdörtgen blok oluşacak biçimde bölerek yazın. Örneğin, “Bugün saat beşte buluşalım.” cümlesini

B	U	G	Ü
N	S	A	A
T	B	E	Ş
T	E	B	U
L	U	Ş	A
L	I	M	.

biçiminde yazabilirsiniz. Şimdi yapmanız gereken, birinci sütundan başlayarak, alt alta duran harfleri yan yana yazmak. Her bir sütundan sonra bir boşluk bırakmayı da unutmayın. Bu durumda örnek cümlemizin şifreli hali “BNTTLL USBEUI GAEBŞM ÜAŞUA.” Bu biçimde şifrelenmiş bir metinle karşılaştığınızda yapmanız gereken, şifreli kod sözcükleri tekrar yukardan aşağıya blok halinde yazmak ve bu kez sütunları değil satırları okumak.

Paragraf - Sözcük - Harf

Sözlük kodlarında olduğu gibi bunda da belli bir metinden yararlanmanız gerekiyor. Seçeceğiniz metin, sizin anahtarınız olacak. Buna göre, mesajınızdaki kelimeleri oluşturan her harf için, 3 ayrı sayıdan oluşan bir şifre oluşturacaksınız. İlk sayı, o harfin hangi paragrafta olduğunu belirtecek. İkinci sayı, paragraftaki kaçıncı sözcüğe bakılması gerektiğini gösterecek. Üçüncü sayı da, bu sözcüğün kaçıncı harfinin aradığımız harf olduğunu söyleyecek. Örneğin, 2 3 5 yazdığınızda anahtar metnin 2. paragrafının, 3. sözcüğünün, 5. harfini belirtmiş olacaksınız. Ancak, şifrenizi yazarken, tek bir harfi simgeleyen sayılar arasına bir boşluk bırakmayı unutmamanız gerekiyor. Farklı harfleri simgeleyen şifreli rakamların arasına da daha fazla boşluk bırakabilir ya da sırayla bir harfin şifresini kırmızı, bir harfin şifresini siyah kalemle yazabilirsiniz.

Şimdi yukarıdaki paragraftan yararlanarak “kod” yazalım.

“1 2 1 1 16 1 1 5 4”

yi de deneyebilirsiniz. Kim bilir, belki tümüyle yeni, belki de bizim örneklerimizden iki ya da üçünü birleştirerek yeni bir algoritma geliştirirsiniz. Ancak, bunların şifreler dünyasının en basit örnekleri olduğunu unutmayın. Gerçekteyse durum çok farklı. Biliminsanlarının bile yıllardır çözemediği şifreler var.

Şifre Çözmek Kolay mı?

Gelelim elinize geçen şifreli bir metni nasıl çözeceğinize. Bu, elinizde anahtar olmadığı sürece çok zor olabilir. Ayrıca, birden fazla anahtar kullanılmışsa, işiniz daha da zorlaşır. Ancak şifre çözmek için mesajla ilgili bir şeyler bilmek yardımcı olur. Kimin yazdığı, kime gönderildiği, hangi dilde yazıldığı ve şifreli metnin içinde anahtar bir sözcüğün olup olmadığı gibi. Bu soruları yanıtladıktan sonra, mesajda kullanılan harflerin kaç kez tekrarlandığını sayabilirsiniz. Buna, “sıklık sayımı” denir. Harflerin ne kadar sık kullanıldığını bilmek, her şifreli harfin hangi düz metin harfine denk geldiğini tahmin etmeye yardımcı olur. Bundan sonra, kullanılan dilin kurallarına göre diğer tahminlerde bulunabilirsiniz. Örneğin, metnin Türkçe yazıldığını biliyorsanız, sözcüklerin ilk harfinin “ğ” olamayacağını bilirsiniz. Bu arada, bu yazımızın başlığının tersten okunması gerektiğini anlamışsınızdır sanıyoruz. Bunu, bu notu okumadan bildiyseniz ilk şifrenizi çözdünüz bile demektir.

Meltem Yenal Coşkun

Kaynaklar:
http://www.nsa.gov/kids/
http://www.pbs.org/wgbh/nova/decoding/
http://www.cs.unibo.it/babaoglu/courses/security/documents/intro-to-crypto.pdf
http://www.scouting.org.za/codes/