GİZLİ HABERLEŞME ARACI: ŞİFRE

BERLOQUIN

Bir yazıyı başlıca iki yolla şifreliyebiliriz: 1 - Basit metod, 2 — Polialfabetik (çok alfabeli) metod. Basit metodda her harfin yerine bir başka değişmez harf konur. Bir örnek verelim: B = Ü, A = Z, S = K, İ = H, T = Y vs. ise BASİT kelimesi ÜZKHY şeklini alır. Aynı şifre ile İSBAT yazmak istersek HKÜZY yazmamız gerekir. Burada kısa kesmek için yalnızca beş harfin karşılıklarını verdik, tabii aslında alfabenin bütün harfleri için bir diğer harf bulunur, hangi harfin hangi harfe karşılık olacağı istendiği gibi, gelişigüzel olarak seçilir. Her harfin hangi harfe karşılık olduğunu bir liste halinde yazarsak ŞİFRE ANAHTARI elde etmiş oluruz, şifre anahtarı istenince değiştirilebilir. Basit şifre metodu bazı sakıncaları nedeni ile terkedilmiş gibidir. Bir kere böyle uzun bir şifre anahtarını hatırda tutmak çok zordur. Anahtarı yazılı olarak taşımak ise ele geçmesine yol açabilir. Basit şifrenin ikinci ve en büyük mahzuru ise şudur: anahtar ele geçmese bile şifre nisbeten kolay olarak çözülür. Bunun için iki teknik kullanılır: 1 — Şifreli yazıda bir kelimenin tanınması ihtimali, 2 — Şifreli yazıda her harfin ne kadar sık kullanıldığını (frekansını) bulmak.

Basit şifreli bir yazıda bir kelime tahmin yolu ile çözülebilir, bunun için merkezi etrafında simetrik beş harflik kelimeler aranır. Örneğin KAÇAK kelimesi Ç merkezi etrafında simetrikdir, K = S, A = O, Ç = Y ise kaçak SOYOS olarak yazılacaktır, elde merkezi etrafında simetrik beş harfli kelimelerin listesi varsa bunlar bir bir denenerek sonunda SOYOS = KAÇAK olduğu bulunur, böylece anahtarın üç harfi çözülmüştür, diğer beş harfli simetrik kelimeler diğer harfleri çözdürür. Başka türlü de kelime tahmin edilebilir, örneğin ANANAS, ANANE, ANA kelimeleri A = B, N = E, S = O, E = K olarak şifrelenmiş olsun, şifreli kelimeler BEBEBO, BEBEK, BEB olacaktır, görülüyor ki böyle bir şifrede, özellikle şifre uzmanları için, kelimeleri yapılarından tanıma ihtimali kuvvetlidir.

Yine basit şifrede her harfin tekrarlanma sıklığına bakarak onun hangi harf olduğu tahmin edilebilir. Burada şu esastan gidilir: belli bir dilde hangi kelimelerin ne derece sık kullanıldığı kesinlikle bellidir, o halde şifreli yazıda tekrarlayan kelimelerin tekrarlanma sıklığına bakılarak o kelimelerin ne olduğu tahmin edilebilir. Belli bir dilde hangi harflerin ne derece sık kullanıldığı ise daha da kesinlikle bellidir. Örneğin Fransızcada her 100 harfde 18 E, 8 S, 8 A, 8 N, 7 T, 7 I, 7 R, 6 U vs. vardır. O halde şifreli bir yazıda bir harf % 18, diğer bazıları % 8 civarında tekrarlanmışsa o yazı basit şifre ile yazılmış demektir ve % 18 sıklıkla tekrarlayan harf E'dir. Ne yazık ki S, A, N, T, I, R harflerinin sıklıkları birbirine çok yakındır, örneğin % 8 sıklığı olan bir harf, S, A veya N olabilir ve her üç ihtimalin de denenmesi gerekir.

Polialfabetik şifrelerde harflerin tekrarlanma sıklığına bakarak şifre çözmek önlenmek istenmiştir. İlk bakışta böyle bir şifreyi çözme olanağı yok gibidir. Polialfabetik şifreyi birlikte adım adım öğrenelim:

1 — A'dan Z'ye kadar olan harfleri sırasıyla yazıp A'dan başlıyarak sıra numarası verelim:

A	B	C	Ç	D	E	F
1	2	3	4	5	6	7
G	Ğ	H	I	İ	J	K
8	9	10	11	12	13	14
L	M	N	O	Ö	P	R
15	16	17	18	19	20	21
S	Ş	T	U	Ü	V	Y	Z
22	23	24	25	26	27	28	29

2 — Şifrelemek istediğimiz bir cümle yazalım:

BUGÜN GELİYORUM

3 — Bu cümlenin altına yalnız bizim bileceğimiz bir anahtar kelimeyi, örneğin ARTIK kelimesini tekrar tekrar yazalım:

B U G Ü N G E L İ Y O R U M
A R T I K A R T I K A R T I

4 — Şimdi oldukça karmaşık bir noktayı anlamamız gerekiyor:

a) Üst satırdaki her harfin kodlanması altındaki harfe göre yapılacaktır, B'nin kodlanmasını A, U'nun kodlanmasını, R, G'nin kodlanmasını T vs. tayin edecektir.

b) Her harf için değişik bir alfabe kullanılacaktır, öyle ki B'nin alfabesi A ile, U'nun alfabesi R ile, G'nin alfabesi T ile, Ü'nün alfabesi I ile, N'nin alfabesi K ile başlıyacaktır vs.

c) Örneğin R ile başlıyan alfabeyi yazalım:

RSŞTUÜVYZABCÇDEFGĞHIİJKLMNOÖP

Gürüldüğü gibi bu da 29 harflik bir alfabedir, harfler sırası ile yazılmıştır (Z'den sonra A, B... diye devam ederek), yani diyebiliriz ki alfabemiz A ile değil de R ile başlasaydı böyle olacaktı.

Bir diğer örnek olarak T ile başlayan alfabeyi yazalım:

TUÜVYZABCÇDEFGĞHIİJKLMNOÖPRSŞ

Kolaylık olmak üzere A ile başlayan alfabeye A alfabesi, R ile başlayan alfabeye R alfabesi, T ile başlayan alfabeye T alfabesi vs. diyelim.

d) Üst satırdaki her harf kendi altına gelen harfin alfabesindeki sırasına konacaktır: Örneğin U normal alfabenin 25. harfidir, U harfi R alfabesindeki yerine konacak, yani R alfabesinin 25. harfi olarak yazılacaktır, R alfabesini yukarda yazmıştık, bunun 25. harfini sayarak bulalım: M harfi. Demek ki U harfi M olarak kodlanacaktır. G normal alfabenin 8. harfidir, G'nin altında T vardır, o halde G, T alfabesinin 8. harfi olarak yazılacaktır, yukarda verdiğimiz T alfabesinin 8. harfi B'dir, demek ki G yerine B yazılacaktır. Benzer mantık yürüterek Ü yerine, F, N yerine A yazmamız gerektiği hemen anlaşılır. B harfinin altında A harfi vardır, yani B harfi A alfabesine, bir diğer deyişle normal alfabeye göre kodlanacaktır, bu demektir ki aynen alınacaktır, anahtar kelimenin A'ları üzerindeki harfler aynen alınır. Bu kodlamaya göre BUGÜN kelimesi BMBFA şeklini almıştır.

5 — Bütün bunları formüllerin nasıl çıkarıldığını anlamanız için yazdık. Gerçekte polialfabetik şifreleme formüller sayesinde çok basitleştirilmiştir. Şifresi yazılacak kelimedeki (örneğin BUGÜN'deki) harflerin alfabetik sıra numaralarına (2, 25, 8, 26, 17) "a" diyelim. Anahtar kelimedeki (ARTIK) harflerin sıra numarasına "b" diyelim (1, 21, 24, 11, 14). Şifrenin kendisindeki (BMBFA) harflerin sıra numarası da "x" olsun (2, 16, 2, 7, 1).

Şifreleme formülü son derece basittir:

x = a + b — 30 (a + b 30'dan büyükse)
x = a + b — 1 (a + b 30'dan küçükse)

BUGÜN, ARTIK, BMBFA harflerinin sıra numarası arasındaki ilişki bu formüle dayanmaktadır: 2 + 1 — 1 = 2, 25 + 21 — 30 = 16, 8 + 24 — 30 = 2, 26 + 11 — 30 = 7, 17 + 14 — 30 = 1.

Bu formüle göre GELİYORUM'u kodlayalım:

GELİYORUM	a'lar:	8	6	15	12	28	18	21	25	16
ARTIKARTI	b'ler:	1	21	24	11	14	1	21	24	11
	x'ler:	8	26	9	22	12	18	12	19	26
		G	Ü	Ğ	S	İ	O	İ	Ö	Ü

GELİYORUM'un kodlanmış şekli GÜĞSİOİÖÜ oldu.

Polialfabetik şifreyi çözmek için bu işlemin tersi yapılacaktır. Elimizde şifreli bir yazı varsa ve anahtar kelimeyi de biliyorsak (ki hatırlanması kolaydır) x ve b belli demektir, o zaman a'yı bulabiliriz. Bunun için formülleri a'ya göre çözelim:

a = x — b + 30 (x, b'den küçükse)
a = x — b + 1 (x, b'den büyükse)

Örneğin GÜĞSİOİÖÜ şifreli kelimesi elimize geçti, anahtar ARTIK'ı da biliyoruz, bu şifreyi çözelim:

GÜĞSİOİÖÜ	x'ler:	8	26	9	22	12	18	12	19	26
ARTIKARTI	b'ler:	1	21	24	11	14	1	21	24	11
	a'lar:	8	6	15	12	28	18	21	25	16
		G	E	L	İ	Y	O	R	U	M

Son olarak elimizde yazının aslı ile şifrelenmiş şeklinin bulunduğunu düşünelim ve anahtar kelimeyi bulmaya çalışalım: Bunun için formülleri b'ye göre çözelim:

b = x — a + 30
b = x — a + 1

GÜĞSİOİÖÜ	x'ler:	8	26	9	22	12	18	12	19	26
GELİYORUM	a'lar:	8	6	15	12	28	18	21	25	16
	b'ler:	1	21	24	11	14	1	21	24	11
		A	R	T	I	K	A	R	T	I

Anahtar kelime kısa olduğundan asıl yazının küçük bir kısmı bile anahtarı bulmaya yeter. Anahtar kelime bulunduktan sonra şifreli yazının satırları altında kaydırılır, ta ki anahtara göre çözülen şifreli yazı anlamlı bir kelime versin, o zaman anahtar kelime şifreli yazı altında oturması gerekli pozisyona oturmuş demektir ve yapılacak iş bu durumdan itibaren anahtar kelimeyi tekrar tekrar yazmak ve formüle göre şifreyi çözmektir. Burada anlatmak istediğimiz şudur: anahtar kelimenin bilinmesi şifreyi çözmeye yetmez, çünkü anahtar kelime şifreli yazı satırları altına yazılırken herhangi bir yere yazılırsa anahtar doğru olmasına rağmen şifrenin çözülmesi anlamsız bir metin verir. Anahtar kelime tek ve ancak bir tek pozisyonda anlamlı kelimeler vermeye başlıyacaktır.

Başta polialfabetik şifrelerde harflerin tekrarlama sıklığının görünüşde önemini yitirdiğine değinmiştik. Aslında bunun da çaresi bulunmuştur:

BUGÜN GELİ YORUM...
ARTI K ARTI KARTI ...
BMBFA GÜĞSİ Oİ ÖÜ...

Üçüncü satırdaki harfleri beş gruba ayıralım: üstünde A olanlar, R olanlar, T olanlar, I olanlar ve K olanlar. Bu beş grupdan herbiri içinde basit şifreler için geçerli olan harflerin belli sıklıkla tekrarlanması kuralı geçerlidir. O halde gerekli olan anahtar kelimenin kendisinin değil uzunluğunun, yani kaç harfli olduğunun bilinmesidir, o zaman polialfabetik şifre basit şifre metodları ile çözülebilecektir.

Anahtarın kendisini bilmeden uzunluğunu nasıl bulabiliriz? Zor gözüken bu husus Alman binbaşısı F. W. Kasiski'nin 1863'de yaptığı keşifle mümkün olmuştur: anahtar kelimedeki benzer harf grupları asıl yazıdaki benzer harf gruplarının altına gelmişse elde edilen şifrede de benzer harf grupları ortaya çıkar. Bir örnekle açıklayalım:

GECE GELİN
AKIŞ AKIŞA
GÖJ Y GÖUDN

Burada açıkca görülüyor ki 1. satırdaki GE tekrarları anahtardaki AK tekrarları tarafından şifreye GÖ tekrarları olarak nakledilmişlerdir. Kasiski kuralı gereğince GÖ tekrarları arasında anahtar kelimenin 1, 2, 3... tam katları bulunması gerekmektedir, bu örnekde iki GÖ arasındaki uzaklığa bakarak anahtarın 2 veya 4 harfli olması gerektiğini söyliyebiliriz. GÖ'lerin tekrarı 15 harflik bir ara ile olsaydı anahtar ya 3, ya da 5 harfli olmak zorundaydı (tam kat olma zorunluğu nedeni ile). Anahtarın kaç harfli olduğunu böylece bulduktan sonra (2 ve 4 ihtimallerinin ayrı ayrı denenmesi gerekir, 4 ihtimalini denediğimizi düşünelim) yapacağımız şey şifreli yazının harfleri altına sırasıyla 1, 2, 3, 4 yazmak, sonra da altında aynı sayı olan harfleri bir araya toplamaktır, bu dört grup harfin her birinde basit şifrelerin harf tekrarlama sıklığı kuralı geçerlidir ve şifre artık basit bir şifre gibi çözülebilir.

Anahtar kelime FEDA olduğuna göre aşağıdaki polialfabetik şifreyi çözmeye çalışın bakalım:

DIREĞIOLİÜMNİ NRAŞERLFÜ CEŞIULİÜ

NOT: *formüller orijinal yazıda bulunmayıp Çevirenin buluşudur.*

SCIENCE ET VIE'den
Çeviren: Dr. Selçuk ALSAN

Geleceğin Uçağı:

CONCORDE'DAN YENİ HABERLER

Walter BAIER

Bazıları onu hava ulaşımında şimdiye kadar erişilenin en üstünü sayarken, bazıları da İngiliz - Fransız işbirliğinin bu yapıtını ölü doğmuş bir çocuğa benzetmektedirler. İki hükümet arasında Concorde'un yapımının durdurulup durdurulmaması üzerinde görüşmeler yapılırken, ilk Concorde uçakları tarifeli seferlerine devam etmektedirler. Bütün tartışmaların ve görüşmelerin sonucu ne olursa olsun, Concorde Avrupa uçak endüstrisinin üstün teknik bir başarısıdır.

Alfa Alfa, hava alanının sorularına tamamiyle doğru cevap vermişti: Uçuş yüzeyi 506, okunan hız 530 mil'di. Arap kule görevlisi verilen bilginin tekrarını istedi. Alfa Alfa tekrarladı: Uçuş yüzeyi 506, okunan hız 530 mil. Sonra telsiz sustu.

Kaptan pilot gülümsedi: "Concorde'un gelişinin herhalde birden farkında olamadı, ilk önce arkadaşlarına anlatacak". Gerçekten Arap görevlinin yeniden sesi işitilinceye kadar bir kaç dakika geçti. Bu arada da o ve arkadaşları, Londra ile Basra Körfezindeki Bahreyn arasında işleyen Concorde'un ses hızı üstündeki hızına alışmış olacaklardır, bu, uçağın Avustralya'ya giderken, yolunun ilk aşamasıydı. Bahreyn hava alanındaki görevlilerin şaşırması doğaldı: Uçuş yüzeyi 506,