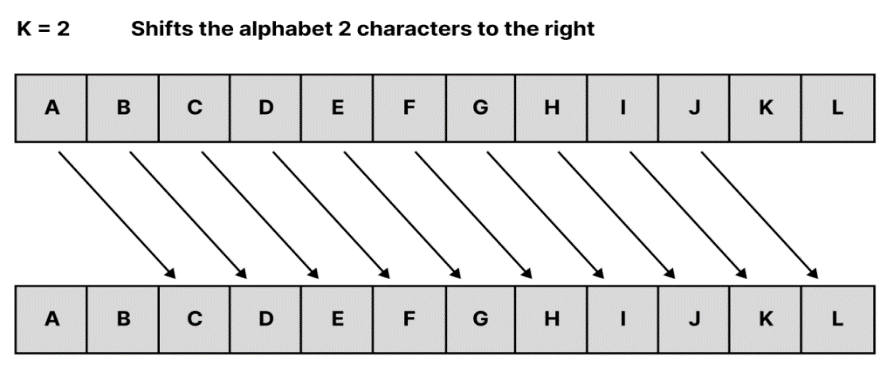
***KLASİK ŞİFRELEME YÖNTEMLERİ***

Klasik şifreleme metotları, modern kriptografi dönemine geçmeden önce daha ilkel ve basit mekanizmaların kullanıldığı şifreleme yöntemlerinden oluşmaktadır. Basit algoritmalarla ortaya çıkan bu metotlar modern çağda yetersiz kalmış ve şifreleme yöntemlerinin çok daha fazla karmaşık ve kırılamaz olması için pek çok teknolojik gelişmeden faydalanılmıştır. Klasik şifreleme algoritmalarına örnek olarak:

**Sezar Şifreleme**

Julius Sezar’ın askeri ve diplomatik mesajların gizliliğini korumak amacıyla bulduğu bir yöntemdir. En eski klasik şifreleme metotlarından biri olarak kabul edilir. Uygulama olarak basit mantıkta her harfin belirlenen adımda kaydırılmasıyla şifreli bir metin oluşturur.



Görseldeki gibi K=2 adım olarak belirlenmiş ve harfler iki adım kaydırılarak şifreli metin oluşturma amaçlanmıştır. Örn: K=5 olarak belirlenmiş bir Sezar şifreleme algoritması için

* **C A E S A R C I P H E R** 🡪 **H F J X F W H N U M J F**

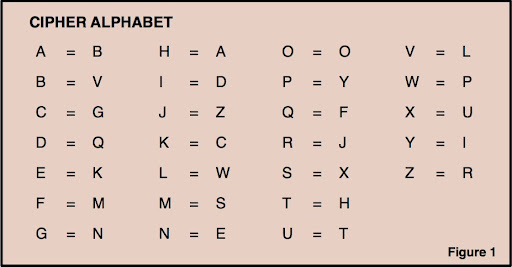
**!!!DİKKAT EDİLMESİ GEREKENLER:** Türk alfabesinde 29 harf bulunur fakat bazı harflerin İngiliz alfabesinde olmadığına dikkat edilmelidir 🡪 Ç, S, Ğ, İ , Ö, Ü harfleri dahil edilmemelidir.

* A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z harfleri ile kaydırma işlemi yapılmalı.
* Eğer Türkçe karakter kullanılmışsa text üzerinde, özel karakterlerde ve Türkçe harflerde kaydırma işlemi yapılmaz.

**Monoalfabetik Şifreleme**

Monoalfabetik şifreleme basit bir şekilde her harfin işaret ettiği başka bir harf kullanılarak şifreli mesaj oluşturmayı amaçlar. Basit ve kolay bir şifreleme olmasıyla birlikte çok kolay kırılabilmesi zamanla kullanılmamasına sebep olmuştur. Genellikle şifre kırma işlemi için harf frekanslarının şifreli metinde de değişmeyeceği fark edildiğinde, frekansı yüksek olan harflerin alfabede sık kullanılan harfler ile denenerek gizlenen metinin bulunabileceği fark edilmiştir.

* Örn: p harfinin frekansı en yüksek ise p harfi a, e, i gibi harfleri işaret ediyor olabilir. Bunun için p harfi yerine bu harfler denenerek şifresiz metine ulaşılabilir.

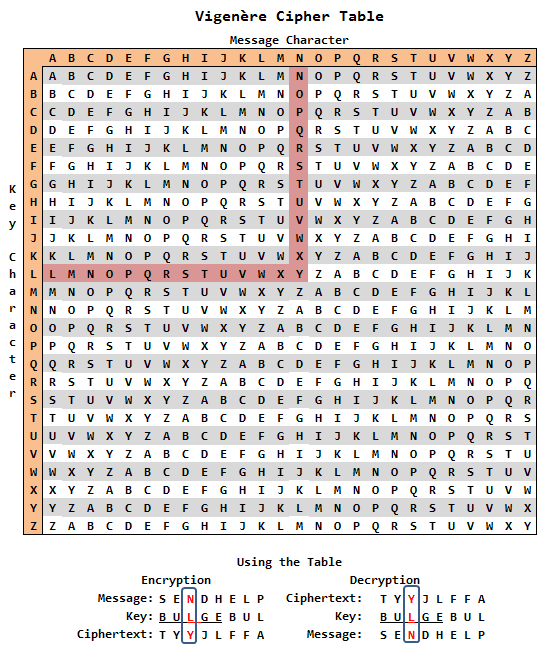


Yandaki resimde de görüldüğü gibi her harf başka bir harfe eşdeğerdir. Örneğin:

* ”alfabe” kelimesinin karşılığı 🡪 “bwmbvn”

**Polialfabetik Şifreleme**

Polialfabetik şifreleme monoalfabetik şifrelemenin tersine alfabedeki her harfin birden fazla harfe işaret etmesi söz konusudur. Yani bir harf her zaman tek bir harfi işaret etmez değişkenlik gösterir. Bu şifreleme yönteminin uygulama kısmında ise en çok kullanılan “Viegenere Tablosu” adı verilen tablo ile harflerin karşılıkları hesaplanarak şifreli metinler oluşturulmaktadır.

Uygulanışı:

* Yandaki resimde karakter tablosunda belli bir dizilime göre harfler verilmiştir.
* Bu dizilimlere bakmadan önce kendimize bir anahtar değer belirleriz. Burada “BULGE” olarak belirlenmiş.
* Şimdi bu anahtar değere göre tablodan mesajın harfleriyle anahtar ifadenin harfleri tablodan kesiştirilerek bulunan karşılık, şifreli metinin oluşturur.
* S+B🡪T , E+U🡪Y, N+L🡪Y şeklinde tek tek harfleri yazarız ve şifreli metini oluştururuz.

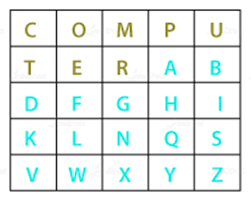


Burada da tablo olmadan harflerin 0 ile 28 arası index değerlerini kullanıyoruz. Bu index değerleri toplayıp sonrasında mod aldığımız zaman (mod 29) yeni harfin index değerine ulaşmış oluyoruz.

🡪Burada da görebileceğimiz gibi monoalfabetik şifrelemeye göre daha komplex bir şifreleme yöntemi çıkarımını yapabiliriz.

**PlayFair Şifreleme**

Playfair ve hill şifrelemleri blok şifreleme kullanılarak yapılan ve üzerinde matematiksel işlemler ile şifreli metinler oluşturulan tekniklerdir. Playfair şifreleme polialfabetik şifrelemelerde olduğu gibi harf çiftleriyle çalışır. Çalışma mantığına daha detaylı değinecek olursak:

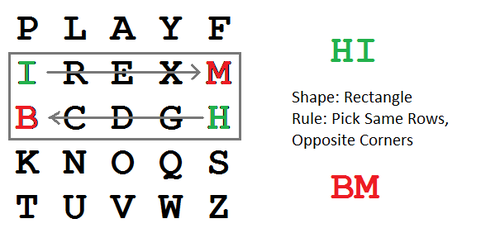
* Anahtar kelime “COMPUTER” olarak belirlendi
* Önce anahtar kelime sırasıyla 5x5’lik matrise yerleştirilir. Sonrasına alfabede geriye kalan harfler sırasıyla matrise yerleştirilerek matris tamamlanır.
* Sonrasında gizlenecek metin seçilir, örneğin “ATTACK” olsun.
* ATTACK kelimesi ikili gruplara ayrılır🡪 AT, TA, CK
* Herkes kendi grubundakiyle karşılaştırırılır. Örn:

A ve T harflerini içine alan en küçük dikdörtgeni çizersek

C:\Users\hp\OneDrive\Masaüstü\images.png

Bu şekilde bir dikdörtgen oluşur ve tabloya tekrar baktığımızda A ve T harflerinin bir sağındaki karakteri seçeriz. Buradan da E ve B harflerini buluruz.

C:\Users\hp\OneDrive\Masaüstü\images.png

T ve A harfleri içinde aynı dikdörtgeni kullandığımızda 🡪 B ve E harflerini buluruz.

C ve K harflerinin oluşturduğu dikdörtgen içinde bu sefer C ve K harflerinin bir altındaki harfler seçillir. Bu harflere tablodan bakarsak T ve V harflerini elde ederiz 🡪 EBBETV kelimesi oluşur

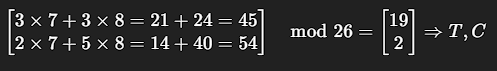
NOT: Eğer oluşan dikdörtgen aynı satır ve sütun içirisinde değilde yandaki gibiyse görseldeki kural uygulanır.

C:\Users\hp\Pictures\images.png

**Hill Şifreleme**

Playfair şifreleme de olduğu gibi blok şifreleme yaparak oluşturulur. Fakat bu bloklarda harfler yerine harflere karşılık gelen index sayılar kullanılır. (A=0, B=1,…,Z=25)

* Şifreli blok= (anahtar matris x şifrelenecek metin) şeklinde formulize edebiliriz. Burada aslında sayılarla yapılan bir matris çarpımı işlemi temel alınır. Bu sayılar karşılığında da harfler vardır.
* Örneğin 2x2’lik anahtar matris ve 2x1’ lik matris oluşturan “HI” matrisi için

Anahtar metin

Metin= “HI”

(H=7,I=8)

**Permütasyon Şifreleri**

Permütasyon şifreleri, permütasyonun kendi mantığında da olduğu gibi harfleri farklı şekillerde sıralama yöntemine dayanır. Şifrelenecek metnin karakterleri için herhangi bir oynama yapılmadan sadece konumları değiştirilerek şifreli metinler oluşturulur.

* MERHABA 🡪 HAMREBA şeklinde harflerin yerleri değiştirilebilir.
* 1.harf 3.sıraya, 2.harf 5.sıraya, 3.harf 1.sıraya şeklinde gitmiş ve buradan yeni sıralama (1,2,3,4,5,6,) iken (4,5,1,3,2,6,7=anahtar sıra ) oluşmuş.

Yani bu şifreleme de sıralamayı belirleyen anahtar sıradır. Anahtar sırada verilen sayılar her harfin hangi konuma gittiğini belirtir ve ortaya şifreli metin çıkar. Tersine çevrilerek de şifre çözülebilir. Ayrıca harf frekansı değişmeyeceği için frekans analizi saldırılarına karşı dayanıksız bir yöntemdir.

**Şifrelerin Kırılma Yöntemleri**

Klasik şifreleme metotları daha basit ve ilkel algoritmaları sebebiyle bazı bilinen çözümlerle kırılabilmektedir. Buna örnek olarak frekans analizi, Bruteforce saldırısı, matematiksel analizler, düz metin şifreli metin karşılaştırmaları vb. yöntemler bulunmaktadır.

* *FREKANS ANALİZİ:* Monoalfabetik şifrelemelerde yani harflerin bazı sabit harfler ile yer değiştirdiği şifrelerde çok kullanılır. Özellikle Sezar şifrelemede kullanılırken permütasyon şifrelerinde de kullanılabildiğini görebiliriz. Yani kısaca harfin ya da harfe karşılık gelen sabit ifadelerin sıklığı değişmiyorsa frekans analizi yöntemi ile şifre kırılabilir. Frekans analizi uygulamada frekansı yüksek olan harflerin o dilde sık kullanılan harfler ile de deneme yaparak tahmini çözümler üretebilir ki eğer anlamlı metin oluşturulabiliyorsa bu yöntemin işe yaradığı görülebilir.
* *BRUTE FORCE:* Brute force yöntemi deneme yanılma yoluyla tahminler arasından doğru olanı seçmeyi amaçlar. Olabilecek bütün şifreler denenmeye çalışılır bu yüzden büyük wordlistler kullanılır. Dolayısıyla anahtar ifade büyüdükçe tahmin etmek zorlaşacaktır. Hala aktif olarak kullanılan bir şifre kırma tekniği olmasıyla birlikte Sezar şifreleme, Viegenere ve buna benzer anahtar alanı küçük olan şifrelemeler için ideal bir yöntemdir.
* *MATEMATİKSEL ANALİZ:* Hill şifrelemesinde kullanılan matris işlemleri gibi işlemler için sayısal analiz yöntemleriyle şifre kırma işlemleri gerçekleştirilebilir. Burada lineer cebirden yardım alınarak matrislerin tersine çevirilmesi ile şifre çözümlemeleri yapılabilmektedir.
* *ANAHTAR UZUNLUĞU TESPİTİ:* Özellikle polialfabetik şifrelerde anahtarın uzunluğu şifrenin kırılması için fikir verebilir. Anahtar uzunluğu tespit edildiği zaman frekans analizi yapılabilir. Örneğin şifrelenen metinde tekrar eden harf ve harf grupları tespit edilirse aradaki karakter mesafeleri ile ortak bölenler bulunup tahmini anahtar uzunluğu yakalanabilir. Örneğin tekrar eden harf grubu “xyz” ise bu tekrarlamalar arasındaki mesafeler de 15 karakterde bir oluşuyor ise muhtemel anahtar uzunluğu 15 karakter olabilir. Özellikle Viegenere yöntemi için kullanışlı olabilir.