ŞİFRELEME TEKNİKLERİ

Giriş

Neden Şifreleme bu kadar önemli ve sürekli daha güvenli şifreleme teknikleri geliştirilmektedir ? Bu sorunun cevabı aslında biz insan oğlunun içinde mevcut olan güvenememe ve güvensizlik korkusudur.Bilgiyi altın olarak gören biz insanoğlu her zaman kendi bilgilerini korumaya ve saklamaya çalışmıştır.Şifreleme ise insan mahremiyetini koruyan ve koruyacak bir tabu olarak görülmüştür.Ve biz insanlar sürekli kırılamaz ve çok çok güvenli şifreleme teknikleri geliştirmeye çalışmaktayız.Bu bölümde sizlere mevcut kullanılan şifreleme tekniklerine göz atacağız ve zayıf taraflarını tartışacağız.

Şifreleme yani ***CRYPTOGRAPHY*** Türkçe olarak ***kripto*** olarak kullandığımız şifreli veriden veya bilgiden ileri gelmektedir.Dilimize de giren bu ifade ilerleyen bölümlerde de göreceğiniz gibi ileri düzeyde matematik gerektiren ve bunun değişik şekillerde uygulanarak hali hazırda kullandığımız bir çok şifreleme teknikliğine dönüşmüştür.

Daha İlk çağlarda *Sezar* şifreli bilgileri seçtiği askerlerinin kafa tasına işlemekte ve saçlarını uzatıp bilgilerini güvenlik altına almaktaydı.Yani insan oğlunun ilk çağlarından beri gizlilik ve bilgi her zaman ön plandaydı.

Almanlar bilgilerini saklamak için ***ENİGMA*** dedikleri ilk mekanik olarak çalışan makineyi icat etmiştirler.Bilinen klavyeye benzeyen bu makine basılan her harf için farklı bir harf çıktısı vermekteydi.

Günümüzde ise ileri teknoloji ürünü bilgisayarlar sayesinde daha güvenli şifreleme teknikleri geliştirildi.MD5,AES,RSA,DES,Blowfish ve bunların karışık olarak kullanılan tekniklerinden oluşmaktadır.

Şifrelemede amaç kırılamaz şifreleme teknikleri geliştirmedir.Ama hiçbir zaman kırılamayacak şifreleme teknikleri geliştirilemeyecektir.Sadece daha güvenli olarak tabir ettiğimiz teknikler geliştirilmektedir.***Unutulmamalıdır ki şifreleme bir süreç değil tamamen bir proses olmalıdır.***

İskender atasoy

KLASİK ŞİFRELEME TEKNİKLERİ

1-) Modüler Şifreleme(*Shift Chipper*):

Modüler şifreleme Beklide en basit şifreleme tekniği diyebiliriz.Temel Aldığı yapı ise matematikte kullandığımız modüler aritmetik mantığıdır.

Tanımlamalar : X ve Y tam sayı olmak üzere ve M pozitif tam sayı olduğunu farz edersek; X ≡ Y (mod M) eğer X-Y M değerine bölünebiliyorsa bu matematikte kullandığımız modüler aritmetik kurallarından biri.Örnek vermek gerekiyorsa 27'nin 13'e göre mod'u 1 dir.

27 ≡ 1 (mod 13) 'tür.

Y değeri 0≤ Y≤ X arasında bir değer alacaktır.

Aynı zamanda negatif sayılarında modu alınabilir.Örneğin -131'in 9'a göre modu -5 pozitif olarak 4 olacaktır.Bizim çalışma alanımız yani alfabemiz pozitif sayılardan oluşan bir matris olarak düşünmekteyiz.

Şifreleme Yapısı : Modüler Şifreleme(*Shift Chipper*)

Kullandığımız alfabe 'ye göre M yani bölme değerimiz artacaktır.Latin alfabesi örneğin 26 harf Türkçe ise 28 harf mevcuttur.

K sabiti dediğimiz sabit değeri

0 ≤ K ≤ M ve M değeri Alfabenin uzunluğundan bir eksiktir.Yani Türkçe alfabesi 28 harftir. M =28-1=27 olarak belirlenecektir.Şifrelemek E(x) Şifreyi çözme fonksiyonumuz ise D(y) olarak kabul edersek.

$$E(x) = (x + K) \bmod 27$$

$$D(y) = (y - K) \bmod 27$$

A=0 ,B=1,C=2,……..,Z=27 olarak bir tablo oluştururuz.Örnek Tablo:

A	**B**	**C**	**Ç**	**D**	**E**	**F**	**G**	**H**	**I**	**İ**	**J**	**K**	**L**
0	1	2	3	4	5	6	7	8	9	10	11	12	13

M	**N**	**O**	**Ö**	**P**	**R**	**S**	**Ş**	**T**	**U**	**Ü**	**V**	**Y**	**Z**
14	15	16	17	18	19	20	21	22	23	24	25	26	27

Bu tabloda dikkatinizi belki çekmiştir.Sadece büyük harflerin bir tablosu bulunmaktadır.Aynı zamanda noktalama işaretleri ve boşlukta ekstra olarak bizim tablomuzda bulunması gerekmektedir.Biz basit olarak boşlukları almıyacağız.

Örnek: K=14 olarak aşağıdaki metnin şifreleyelim :

“ ***şifreleme zevklidir*** ”

Metnin tablomuzdaki karşılığı(Boşluklar ve nokta göz ardı edilmiştir.)

şifrelemezevklidir

	ş	i	…….	e	z	……	r
E(x)	21	10 6 19 5	13 5 14 5		27 5 25 12	13 10 4 10 19	

K=14 olarak

D(y) 7 24 20 5 19 27 19 0 19 13 19 11 26 27 24 18 24 5
Şifreli metin

“ ***GÜSERZRARLRJYZÜPÜE*** ”