ORTAOKUL DÜZEYİNDE MATEMATİK PROJESİ

Proje Adı: KORAY'IN ŞİFRELEME YÖNTEMİ

Projenin Dalı: Matematik

Öğrenci Adı Soyadı : K. KAPLAN

Sınıfı : 7. sınıf

Danışman Öğretmen : Halil TERECİ

Proje amacı: Kriptolojinin temel mantığını kavratmak için modüler aritmetiğin kullanılması.

Giriş: Kriptoloji, şifre bilimidir. Çeşitli iletilerin, yazıların belli bir sisteme göre şifrelenmesi, bu mesajların güvenlikli bir ortamda alıcıya iletilmesi ve iletilmiş mesajın deşifre edilmesidir. Kriptoloji algoritmaları tamamen matematiksel fonksiyonlardan oluşur. Örneğin Sezar şifresinde A harfi yerine D, B harfi yerine E kullanılmıştır... ve bu şekilde devam etmektedir.(1)

Kullanılan yöntem:

$$y=(ax+b)(\text{mod}M)$$

fonksiyonunu kullandım.
Burada;

x , düz metindeki harflerin sayısal karşılığı.

m, düz metinde kullanılan alfabenin karakter sayısı.

a ve b gizli sayılarımız

y de fonksiyonumuzun işlem sonucunda aldığı değerdir .

Y nin X'e geri dönüşümü ise;

$$x=\text{ters}(a)(y-b)(\text{mod}M)$$

formülü yardımıyla hesaplanır.
Ters (a) , a ile çarpımının modülü m e göre sonucu 1 olan sayıdır .Bunu kısaca şöyle ifade edebiliriz :

$$a.\text{ters}(a)(\text{mod}m)=1.$$

Aşağıdaki örnekte gördüğümüz gibi

$$y=(7x+5)(\text{mod}29)$$

fonksiyonunu kullandığımızda O ve K harfleri Ğ ve H şeklinde şifreli hallerini alır .Hesap modülü 29 aritmetiğini içerdiğinden , eğer çarpan 29 ile en büyük ortak bölene sahip ise bazı karakterler beklenen sonucu vermeyebilir. Bu yüzden m ve a nın en büyük ortak böleni '1' olmalıdır.

'Yani aralarında asal olacak şekilde seçmeliyiz.'

Bulgular

Farz edelim ki mesaj;

y=(7x+5)MOD29

şifreleme fonksiyonu ile şifrelensin . Şifreli metnimiz *SAMSUN* olsun . Öncelikle düz metinimizdeki her bir karakterin aşağıda verilen tablodaki gibi 0 ile 29 arasındaki sayısal değerini bulmalıyız.

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ
0	1	2	3	4	5	6	7	8	9	10	11
J	K	L	M	N	O	Ö	P	R	S	Ş	T
12	13	14	15	16	17	18	19	20	21	22	23
U	Ü	V	Y	Z	(ALFABEMİZDEKİ HARFLERİN						
24	25	26	27	28	SAYISAL DEĞERLERİ)						

Böylece *SAMSUN* metnimizin uygun sayısal değerleri 21, 0, 15, 21, 24, 16 dir.Buradaki her bir değer için daha önce belirlediğimiz y=(7x+5)MOD30 fonksiyonunu kullanırsak .(2)

S = y=(7. 21+5) (mod29) = 7 ----------> G
A = y=(7. 0+5) (mod29) = 5 ----------> E
M = y=(7. 15+5) (mod29) = 23 ----------> T
S = y=(7. 21+5) (mod29) = 7 ----------> G
U = y=(7. 24+5) (mod29) = 28 ----------> Z
N = y=(7. 16+5) (mod29) = 1 ----------> B

Böylece şifreli metnimiz " G E T G Z B " olur. (3)

DEŞİFRELEME:

Deşifreleme (şifre çözümü) için y fonksiyonunu aşağıdaki gibi değiştirelim.
x=ters(a) (y-5) (mod29) deşifreleme fonksiyonumuz

a=7 ve b=5 demiştik.

Böylelikle x=ters(7) (mod29) 13

bu şekilde deşifreleme fonksiyonumuz

X=25(y-5) (mod29) olur.

Şimdi şifreli metnimiz olan SAMSUN daki her bir karakterin karşılığı olan sayısal değeri tablomuzdan bulalım.

7, 5, 23, 7, 28, 1 dir.

G:X=25(y-5)(mod29) =22 = S
E :X=25(y-5)(mod29) =0 = A
T :X=25(y-5)(mod29)=16 = M
G :X=25(y-5)(mod29) =22 = S
Z :X=25(y-5)(mod29) =25 = U
B :X=25(y-5)(mod29) =17 = N

Bu sayede düz metinimize ulaşırız *SAMSUN*

Sonuçlar, Sonuçların Değerlendirilmesi

Bu şifreleme yöntemi biraz daha genelleştirilmiştir ve güvenlik azda olsa simetrik şifreleme yöntemine göre daha güçlüdür. Tabi bu kağıt kalem kriptolojisinin bir örneği olduğundan bunu günümüz koşullarına göre düşünürsek, çok zayıf bir yöntem olduğunu görürüz. Fakat bu bize kriptolojinin temel mantığını kavratmak için güzel bir örnek teşkil etmektedir.

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ
0	1	2	3	4	5	6	7	8	9	10	11
J	K	L	M	N	O	Ö	P	R	S	Ş	T
12	13	14	15	16	17	18	19	20	21	22	23
U	Ü	V	Y	Z	(ALFABEMİZDEKİ HARFLERİN						
24	25	26	27	28	SAYISAL DEĞERLERİ)						

Kaynakça

1. http://tr.wikipedia.org/wiki/Kriptoloji

2. www.sanal okulumuz.com

3. kriptoloji.net/basit-sifreleme-teknikleri