ALGORİTMALAR

# *Doğrusal-Afin Şifreleme Ödev Raporu*

ALİ TAYYİP AYDIN

348409

**KRİPTOGRAFİ NEDİR?**  
  
Kriptografi, gizlilik, kimlik denetimi, bütünlük gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemler bütünüdür. Bu yöntemler, bir bilginin iletimi esnasında karşılaşılabilecek aktif ya da pasif ataklardan bilgiyi -dolayısıyla bilgi ile beraber bilginin göndericisi ve alıcısını da- koruma amacı güderler.  
Bir başka deyişle kriptografi, okunabilir durumdaki bir bilginin istenmeyen taraflarca okunamayacak bir hale dönüştürülmesinde kullanılan tekniklerin tümü olarak da gösterilir.

**Kriptoloji nedir?**  
  
Kriptoloji, şifre bilimidir. Çeşitli iletilerin, yazıların belli bir sisteme göre şifrelenmesi, bu mesajların güvenlikli bir ortamda alıcıya iletilmesi ve iletilmiş mesajın deşifre edilmesidir.

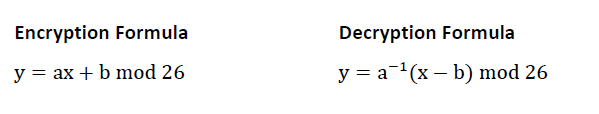
**Doğrusal şifreleme:**

Bu şifreleme yöntemindeki amaç geometride doğrunun denklemi olarak bilinen y=ax+b [doğrusal fonksiyonunu](http://www.bilgisayarkavramlari.com/2008/11/03/dogrusal-fonksiyon-linear-function/) şifreleme işleminde kullanmaktır. Buna göre x, şifrelenecek mesajı , y şifrelenmiş mesajı (cipher text) ifade etmekte olup a ve b ikilisi anahtarı oluşturmaktadır.

Örnek mesaj: “baba dede”  
Anahtar: (3,2) yani a=3, b=2 olarak verilmiş  
Şifreli mesajın oluşturulması: b harfi için 2. harf olduğu kabul edilirse, 3×2 + 2 = 8 olarak bulunur yani karşılığı alfabenin 8. harfidir. Bu harf ‘h’ harfidir. Diğer harflerde benzer şekilde hesaplanır. Örneğin ‘e’ harfine karşılık gelen harf için 3×5 +2 = 17 yani ‘q’ harfi bulunur.  
Şifreli mesaj: “hehe nqnq”

Bu şifreleme yönteminin aslında bir [yerine koyma şifrelemesi (substitution cipher)](http://bilgisayarkavramlari.com/2008/02/21/yerine-koyma-sifrelemesi-substitution-cipher/) olduğu söylenebilir. Buna göre sadece hangi karakterin hangi karakter yerine konulacağı bir formüle bağlanmıştır.

**Doğrusal şifrelemede metinler şifrelerken ve şifrelenmiş metin çözülürken kullanılacak formüller:**



**Yapmış bulunduğum program şu 3 işlemi yapmaktadır.**

1- Anahtar değerlerini alarak şifreleme işlemi,

2- Anahtar değerleri belli olan metni deşifre etmek,

3- Brute Force yöntemi kullanarak şifrelenmiş metnin olası çözümünü kullanıcıya sunmak.

**1- Anahtar değerlerini alarak şifreleme işlemi algoritması:**

1.1- Şifrelenecek metin, A ve B anahtarları kullanıcıdan alınır,

1.2- A anahtarının kullanılan klavyedeki harf sayısıyla aralarında asallığı kontrol edilir ve gerekli işlemler yapılır.

1.3- Şifrelenecek metindeki her bir karakter y= (ax + b) mod26 formülüne tabi tutularak şifreli metin elde edilir.

**2- Anahtar değerleri belli olan metni deşifre etme algoritması**

2.1- Deşifrelenecek metin, A ve B anahtarları kullanıcıdan alınır

2.2- a^-1 yani A anahtarının modüler tersi bulunur.

2.3- Deşifrelenecek metindeki her bir karakter y= a^-1 ( x - b )mod26 formülüne tabi tutularak gizlenmiş metin elde edilir.

**3- Brute Force yöntemi kullanarak şifrelenmiş metnin çözme algoritması**

3.1- Deşifrelenecek metin ve içinde denenecek kelimeleri içeren bir sözlük kullanıcıdan alınır

3.2- A ve B anahtarlarının alfabedeki harf sayısı kadar oluşturabilecekleri tüm ikilileri alınır. (ör alfabe 30 harf ise 30\*30 = 900 adet 2'li vardır (0,0)(0,1)..(30,30))

3.3- 2. adım sıra ile yapılır. Bu sırada her bir turda A anahtarı için a^-1 yani A anahtarının modüler tersi bulunur.

3.4- Deşifrelenecek metindeki her bir karakter y= a^-1 ( x - b )mod26 formülüne tabi tutularak gizlenmiş metin elde edilir.

3.5- Gizlenmiş metin elde edilirken her bir boşluk geldiğinde cümlenin boşluk gelmeden bir önceki kelimesi sözlükle karşılaştırmaya tabi tutulur. Bu karşılaştırma sonucu her bir a,b anahtarının temsil ettiği metinin(ki bu 30 harflik bir alfabe için 900 metin demektir) puan değerine bu karşılaştırmada eşleşen harf sayısı eklenir.

3.6- 5. adım tüm a,b değerleri için tekrarlandıktan sonra oluşan tüm metinlerin puan durumları karşılaştırılır ve en yüksek puan almış olan kelime olası sonuç olarak kullanıcıya verilir.