Ulusal Bilgi Güvenliğine Yönelik Bir Kriptografi Algoritması Geliştirilmesi ve Harf Frekans Analizine Karşı Güvenirlik Tespiti(Development of A Cryptographic Algorithm for National...

Article · June 2013

CITATIONS
5

READS
383

2 authors, including:

Aysun Coskun
Gazi University
8 PUBLICATIONS **17** CITATIONS

SEE PROFILE

Ulusal Bilgi Güvenliğine Yönelik Bir Kriptografi Algoritması Geliştirilmesi ve Harf Frekans Analizine Karşı Güvenirlik Tespiti

Ülkü ÜLKER

Bilgisayar Eğitimi Ana Bilim Dalı, Bilişim Enstitüsü, Gazi Üniversitesi, Ankara, Türkiye
ulkeruu@hotmail.com
(Geliş/Received: 06.02.2013; Kabul/Accepted: 21.06.2013)

Özet ─ Günümüzde savaşlar artık ağır silahlarla değil elektronik ortamlarda gerçekleşmektedir. Bu durum siber savaş olarak nitelendirilmektedir. Siber savaşın en etkili olduğu ülkeler bilgi güvenliğinde zafiyet yaşayan ülkelerdir. Bunun en büyük sebebi gelecekte ve hatta şimdinin en büyük tehlikesi olan siber savaşla ilgili bu ülkelerde yeterli farkındalık oluşturulamamasıdır. Dolayısıyla siber savaş, yeterli farkındalık sahibi olmayan ülkeler tarafından bir tehdit unsuru olarak görülmemekte ve bu nedenle bilgi güvenliği için gerekli tedbirler önemsenmemektedir. Bilginin korunması, güvenliğinin sağlanması gün geçtikçe büyüyen bir hızla önem kazanmaktadır. Bilgi güvenliğini sağlamanın yöntemlerinden birisi eldeki veriyi gizleyerek-şifreleyerek saklamak, iletmek ve paylaşmaktır. Bunun için geliştirilen bilim dalına kriptoloji denilmektedir. Kriptoloji, verinin şifrelenmesi ve şifrelenen verinin orijinal haline geri çevrilmesi ile ilgilenir. Bu makaledeki amaç; ülkenin siber savaşlara karşı milli güvenliği hususunda bilgi güvenliğine dikkat çekmek, bu alanda faydalı olacağına inanılan ulusal bir Kriptografi algoritması geliştirmek ve geliştirilen algoritmanın harf frekans analizine karşı güvenirlik incelemesini yaparak ulusal bilgi güvenliğinde güvenilir bir şifreleme algoritması üretebilmektir. Bu çalışmada diğerlerinden farklı olarak yeni bir algoritma geliştirilmiş ve saldırı tekniklerinden harf frekans analizine karşı güvenirliği incelenmiştir. Bu sayede ulusal bilgi güvenliği için gerekli olanın var olanları incelemenin yanı sıra yeni üretimler gerçekleştirmek olduğuna dikkat çekilmek istenmiştir.

Anahtar Kelimeler ─ Kriptoloji, kriptoanaliz, kriptografi, kriptosistemlere yapılan saldırılar, bilgi güvenliği, siber savaş, harf frekans analizi, Türkçe harf frekans dağılımı, şifreleme

Development of A Cryptographic Algorithm for National Information Security and Determination of Confidence Against Letter Frequency Analysis

Abstract ─ Today, wars take place in cyber world rather than heavy weapons. This recent situation is defined as "cyber war". The most affected countries by cyber wars are those suffering weakness in information security and, accordingly, one of the most important reasons is the failure of sufficient awareness in these countries regarding to cyber wars which stand the most dangerous hazard both in future and even now. Therefore, cyber wars are not considered as a threat by those countries who are lack of enough awareness resulted in ignoring the required measures related to information security. However, the protection of information and providing its security become increasingly more important. For achieving this, one method includes keeping the current information encrypted (i.e. hiding), transmission and sharing in this way, which is called "cryptology". Cryptology science deals with data encryption and decryption. The aim of this study is to draw attention to the information security in terms of national security against possible cyber wars, to develop a national cryptographic (encryption) algorithm considered to be highly profitable in this area, and produce a confident cryptological algorithm performing a confidence examination against letter frequency analysis. In this study, it has been developed a new and different algorithm and examined its confidence against letter-based analysis, a technique of attack. Thus, we intended to draw attention on the requirement of innovative productions as well as discussing the current ones required for national information security.

Key Words ─ Cryptology, cryptanalysis, cryptography, attacks to cryptosystems, information security, cyber war, letter frequency analysis, Turkish letter frequency distribution, and encryption

1.GİRİŞ (INTRODUCTION)

Bilgi bir değerdir. Geçmişten günümüze kadar geçen süreçte, toplumların sürekliliğini sağlamak için korunması gereken büyük bir güç olmuştur [1]. Roma imparatoru Sezar ve Spartalılar'dan bu yana bilginin korunması için geliştirilen teknikler oldukça gelişmiş, fakat bilginin gizlenmesi ya da farklı formlarda kullanılması temel yapı olarak kalmıştır. Bu sistem kriptoloji olarak adlandırılmaktadır [2,3].

Bilgi, içerisinde yönetme yeteneğini içerir. Bu nedenle toplumlar, birbirlerine üstünlük sağlayabilmek için ağır ve mekanik silahları kullanmak yerine 1990'lı yılların başlarında dünya literatürüne giren Bilgi Savaşı'nı tercih etmeye başlamıştır. Çok eskiden ağır silahlarla yapılan savaşların kazanılmasında yardımcı rolü oynayan bilgi casusluğu, günümüzde savaşların ana kahramanıdır [1,2].

Bilgi üzerindeki işlem zinciri bilgi savaşlarının temelini oluşturmaktadır. Bilgi elde edilir, gerekli düzeltmeler yapılarak kullanılabilir hale getirilir, daha sonra kullanılmak üzere saklanır ve gerektiğinde gözden geçirilerek kullanılır. Bu adımlar esnasında bilginin güvenliğini sağlamanın yollarından birisi bilgiyi başka bir formda saklamak ya da iletmektir. Kriptoloji biliminin alt dalı olan Kriptografi, bilginin olduğu şekilden daha farklı bir formda saklanması ya da iletilmesi ile ilgilenir [1,2].

Bir bilginin değerini, bilgiyi elinde tutan kişi ya da kurumların yaşamsal faaliyetlerine olan etkisi belirler. Örneğin devletler açısından düşünüldüğünde bir ulusun güvenliği ve devamı için, o ulusun elindeki milli istihbarat verilerini bilgiye dönüştürmesi ve elde ettiği bilgileri en iyi şekilde koruması gerekmektedir. Bunu sağlayabilmek, potansiyel tehdit unsurlarının farkında olmakla mümkündür. Bilgi güvenliğini tehdit eden unsurlar; bilgide kayıplar (güvenlik ihlali), bilgide değişiklik yapmak (bütünlük ihlali), başkası tarafından ele geçirilme (gizliliğin ihlali) gibi unsurlardır. Kriptoloji bilginin güvenliği, bütünlüğü ve gizliliği ile ilgilenir [3,4].

İnternet ağı genişledikçe bilgi güvenliğini tehdit eden unsurlar daha korkutucu hale gelmiştir. Bilgi güvenliği için yeni yöntem ve teknolojilerin geliştirilmesi ya da var olanların kendilerini daha iyi hale getirmeleri sürekli bir ihtiyaç döngüsü haline gelmiştir [5].

Bu sürekli ihtiyaç döngüsü incelendiğinde geçmişten günümüze kadar geçen süreçte kriptolojinin daha çok askeri ve diplomatik alanda kullanıldığı görülmüştür [6]. Günümüzde ise iletişim kanalları, bankamatik işlemleri, kredi kartı uygulamaları, internet ortamında gezinti, e-ticaret ve e-devlet uygulamaları, cep telefonları, fatura sistemleri, şehir şebekeleri, füze sistemleri, ulaşım araçları vb. gibi pek çok alanda kullanılır hale gelmiştir [7,8].

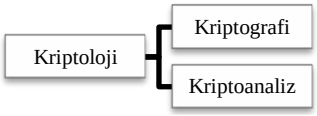
Kriptolojinin kullanım alanının bu kadar genişlemesinin sebebi bilgi güvenliğine karşı büyüyen ve farklılaşan tehdit unsurlarıdır. Bu durumu her geçen gün biraz daha büyüyen internet ağı tetiklemiştir. Bu tehdit unsurları kişileri, kurumları ve en önemlisi ulusları olumsuz etkilemektedir. Bir devlete ait milli istihbarat bilgilerinin kötü niyetli kişilerin eline geçmesi ve bu bilgileri devletin istemeyeceği şekilde kullanması devletin çöküş sürecini başlatabilir. Bu nedenle ulusal düzeydeki bilgilerin iyi korunması gereklidir [9].

Bu makalede ulusal bilgi güvenliğinin önemine dikkat çekilmek istenmiş ve bilgi güvenliğini sağlamanın bir yolu olan kriptoloji yani şifreleme bilimi üzerinde durulmuştur.

2. KRİPTOLOJİ (CRYPTOLOGY)

Kriptoloji, bilginin gizlenmesi ve ortaya çıkarılması ile ilgilenen matematiksel bir bilim dalıdır[10,11].

Kriptoloji bilimi iki alt sisteme ayrılmaktadır[10,12]:



Şekil 1. Kriptoloji bilimi alt dalları
(Sub-branches of Cryptology Science)

Bir şifreleme algoritmasının sağlaması gereken temel özelliklerden bazıları aşağıda tanımlanmıştır [13,14]:

- Gizlilik: Bilgi sadece istenen kişiler tarafından anlaşılmalıdır [13,14].
- Bütünlük: Bilgi yetkili kişiler dışında başka kimse tarafından değiştirilmemelidir [13,14].
- Reddedilemezlik: Bilgiyi üreten ya da ileten kişinin daha sonrasında bunu inkar edememesidir [3,14].
- Erişilebilirlik: Yetkili kişilerin ihtiyaç duyduğu anda gerekli bilgiye ulaşabilmesidir [3,13,14].
- Kimlik denetimi: Mesajı gönderen ve alan tarafların birbirlerinin kimliklerini doğrulamasıdır [3].

2.1 *Kriptografi (Cryptography)*

Verilerin açık halden kapalı yani gizli hale getirilmesi işlemidir. Verilerin gizliliğini, bütünlüğünü, güvenliğini sağlar. Bu işlemi yapan kişilere kriptograf denir. Eldeki metnin anlaşılabilir haline düz metin ya da açık metin denilmektedir. Düz metnin farklı işlemlerden geçirilerek anlaşılamayacak bir forma dönüştürülmesi sonucunda elde edilen yeni forma şifreli metin denilmektedir [10-12,15].

Örnek 2.1'de görülen şifreli metin, makalenin kapsamını oluşturan kriptografi algoritması ile elde edilmiştir:

Örnek 2.1 (Example 2.1) *Düz Metin :* MERHABA
*Şifreli Metin:*ĞKÖÖÖKĞ

Kriptografinin temel amacı bilginin gizliliğini sağlamaktır. Bu amaçla kullanılan üç temel yöntemden söz edilebilir [16]:

1. Yerine koyma yöntemleri
2. Yer değiştirme yöntemleri
3. Cebirsel yöntemler

2.1.1 Yerine koyma yöntemleri(Substitution Methods)

Düz metindeki harflerin yeri sabittir. Sayılar, semboller ya da başka bir alfabedeki harfler bu harflerin yerine yerleştirilerek şifreli metin elde edilir [16].

2.1.2 Yer değiştirme yöntemleri (Transposition Methods)

Düz metindeki harflerin yerleri değiştirilir. Başka bir alfabe ya da sembol kullanılmaz, düz metindeki harflerin kimlikleri sabittir; fakat yerleri değiştirilmiştir. Geçmişteki en güzel örneği Sezar şifreleme algoritmasıdır [16].

2.1.3 Cebirsel yöntemler (Algebraic Methods)

Matematiksel bazı fonksiyonların kullanımı, yerine koyma ve yer değiştirme işlemlerinin karışımı gibi karmaşık yapıda olan işlemleri kapsayan yöntemlerdir [16].

2.2 Kriptoanaliz (Cryptanalysis)

Kriptografların şifreli hale getirdiği metinlerin analizi ve şifrelerin çözümü ile ilgilenen kriptoloji alt bilim dalıdır. Bu işi yapan kişilere kriptoanalist denir. Şifreli metinden düz metni yani orijinal metni elde etme işlemidir [10].

Geçmişten günümüze kadar süregelen süreçte, kriptoanalistler ile kriptograflar arasındaki çekişme sonucunda hep daha iyi ve daha karmaşık sistemler geliştirilmiştir ve geliştirilmeye devam etmektedir.

Makale kapsamındaki çalışmada kriptografi algoritmasının kriptoanalizi cebirsel işlemler ile elde edilememiştir. Geliştirilen algoritmanın cebirsel işlemlerle kriptoanalizi gerçekleştirilemediği için biometrik yöntemlere başvurabileceği düşünülmüştür. Şifreli metinden düz metinin elde edilmesi için biometrik bir özellik olan ses kullanılmıştır. Çalışma donanımsal boyuta taşınabilir. Bu kısım geliştirilmeye açık bırakılmıştır.

3. BAZI KRİPTOANALİZ TEKNİKLERİ (SOME CRPTANALYSIS TECHNIQUES)

Gizlenen veriler her zaman insanoğlunun ilgisini çekmiştir. Geçmişten günümüze insanoğlu bu yapılara ulaşmak için çok çeşitli yöntemler denemiştir. Şifrelenen bilgilerin elde edilebilmesi için çeşitli kriptoanaliz teknikleri vardır. Bu teknikler kriptografi tekniklerine karşı kullanılan saldırı teknikleri olarak da bilinir. Bunlardan bazıları aşağıda tanımlanmıştır [11,12,17]:

3.1 Sadece Şifreli Metin Saldırısı (Chiphertext-Only Attack)

Metnin içeriği hiçbir şekilde bilinmediğinden şifreli metnin çözümlenmesi için tahminler yapılır. Tahmin sayısını en aza indirmek için harf frekans analizi kullanılır [11,12,17].

3.1.1 Harf frekans analizi (Letter Frequency Analysis)

Ünlü Arap bilgini Al-Kindi'nin "Kriptografik Mesajların Deşifresi" (Risâle fi'stihrâci'l-mu'ammâ) adlı eserinde anlattığı bir yöntemdir. Bu yöntem ile kriptoanaliz alanındaki ilk çalışmaların başladığı söylenebilir [6,18].

Frekans analizi, bir dile ait yapısal bazı özellikleri kullanarak şifreli metinden düz metni elde etmeyi amaçlar [19,20]. Şifreli metinde en sık kullanılan harf, metnin yazıldığı dilde en çok kullanılan harf ile eşleştirilir ve bu işlem tüm harfler için uygulanır. Her harfin kullanım sıklığı hesaplanır ve sırası ile harflerin yerleştirilmesi işlemi devam eder [11,17]. Örnek 3.1'de, verilen cümledeki A harfi için harf frekans hesaplaması görülmektedir:

Örnek 3.1. Ayşe pazara gitti ve elma aldı.
Toplam harf sayısı: 25
A harfinin sayısı : 6
A harfinin frekansı : 6/25 = 0,24

Frekans analizinin yapılabilmesi için uzun metinlere ihtiyaç duyulmaktadır. Uzun metinler, elde edilen verilerin güvenilir ve geçerli olmasını sağlamaktadır.

Frekans analizinde birebir eşleme dışında harf ikililerine, üçlülerine de bakılabilir. Bir dilde daha çok yan yana gelen sıralılar, şifreli metinde en çok yan yana gelen sıralıların yerine yerleştirilerek de çözümleme yapılabilir.

Bu çalışmada birebir eşleme yapılmıştır, harf sıralılarına bakılmamıştır. Ayrıca Türkçe için harf frekans analizi çalışmaları daha önceden yapılan bazı çalışmalarda bulunmaktadır. Bu nedenle dil üzerinde yeni bir araştırma yapılmamış ve şifreli metnin frekans analizi için bu veriler kullanılmıştır.

3.2 Bilinen Düz Metin Saldırısı (Known-plaintext Attack)

Şifreli metnin bazı kısımları tahmin edilir ve metin bölümlere ayrılır. Bu şekilde şifreli metin blokları çözümlenir. Şifreli metni oluşturmak için kullanılan anahtar (şifreleme işlemini gerçekleştirmek için kullanılan denklem, fonksiyon, tablo, kelime vb.) belirlenerek de çözümleme yapılabilir. Düz metin saldırısı olarak blok şifrelemeyi çözmek için kullanılan lineer kriptoanaliz örnek verilebilir [11,12,17].

3.3 Seçilmiş Düz Metin Saldırısı (Chosen-plaintext Attack)

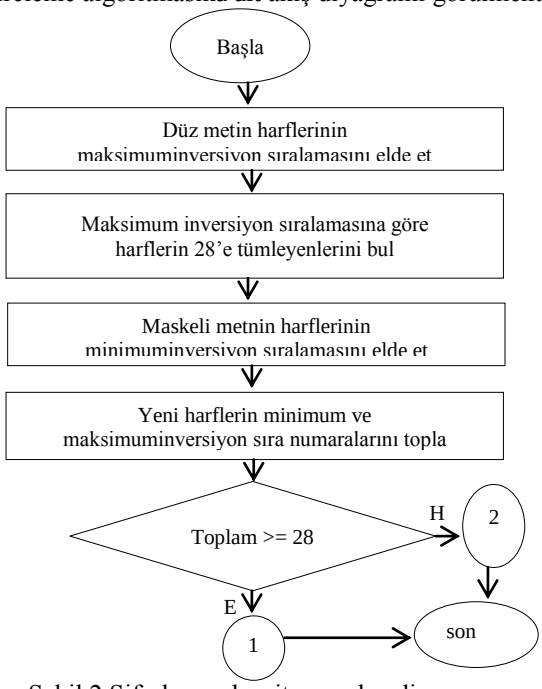
Bu saldırıda amaç şifreleme için kullanılan anahtar veriyi belirlemektir. Bu türe verilebilecek en uygun örnek diferansiyel kriptoanaliz saldırısıdır [11,12,17].

3.4 Ortadaki Adam Saldırısı (Man-in-the-middle Attack)

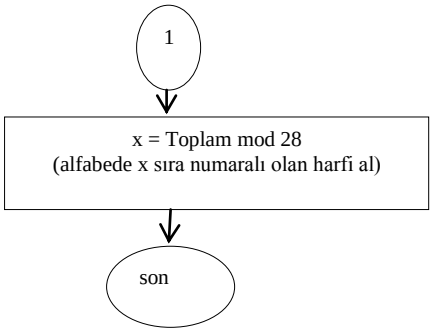
İki kişi arasında veri iletimi gerçekleştiği esnada üçüncü bir kişinin kendini gizleyerek veri iletimine müdahale etmesidir. Bu esnada verinin değiştirilmesi, saklanması, çalınması gibi durumlarla karşılaşılabilir [12].

4. GELİŞTİRİLEN KRİPTOGRAFİ ALGORİTMASI (DEVELOPED CRYPTOGRAPHY ALGORITHM)

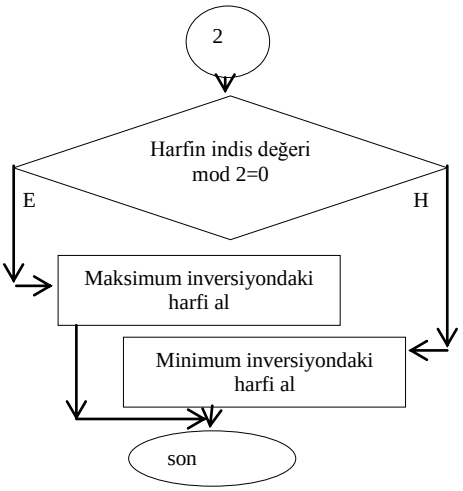
Algoritma Türkçe Alfabe kullanılarak geliştirilmiştir. Şifreleme işlemi için farklı bir alfabe kullanılmamıştır. Harflerin sıra numarasını gösteren sayısal verilerle bazı matematiksel işlemler yapılmış ve harfler üzerinde yer değiştirme işlemi uygulanmıştır. Girilen metindeki boşluklar atılarak metin bir bütün olarak algılanmakta ve şifreleme işlemi bütün metni tek bir kelime gibi algılayarak yapılmaktadır. Bir metin içerisinde geçen bir kelimenin şifrelenmiş hali ile o kelimenin tek başına şifrelenmiş hali birbirinden farklıdır. Düz metin şifreli hale getirildiğinde düz metindeki birbirinden farklı harfler şifreli metinde aynı harfle temsil edilebilmektedir. Bu durum harf frekans analizi incelemesi bölümünde açıklanacaktır. Bu durum algoritmanın geri işlerliğini etkilemiş ve dolayısıyla şifreleme işlemi için uygulanan adımlar geri çevrilememiştir. Bu nedenle algoritma simetrik anahtarlı bir yapıda değildir. Bu durum biyometrik sistemlerden yararlanılabileceği fikrinin oluşmasına yol açmıştır. Şifreli metinin çözümü için sesli komutlar kullanılmıştır. Şekil 2.'de döngü sayısı bir olan şifreleme algoritmasına ait akış diyagramı görülmektedir:



Şekil 2.Şifreleme algoritması akış diyagramı (Flow-chart of the encryption algorithm)



Şekil 3.Şifreleme algoritması akış diyagramı 1 numaralı if bloğu değerlendirmesi (Estimate of first if condition on the flow-chart of the encryption algorithm)



Şekil 4.Şifreleme algoritması akış diyagramı 2 numaralı if bloğu değerlendirmesi (Estimate of second if condition on the flow-chart of the encryption algorithm)

4.1 Algoritma İçin Geliştirme Önerisi (Suggestion for developing of the algorithm)

Deşifreleme işlemi için biyometrik bir özellik olan ses, retina tarama ya da parmak izi, şifreli metnin çözüm anahtarı olarak kullanılabilir [21]. Çalışma kapsamında ses özelliği tercih edilmiştir. Bu şekilde bir donanım biriminin geliştirilebilir olduğu düşünülmektedir. Yapılan çalışma kapsamında donanımsal boyuta yer verilmemiştir. Dolayısıyla çalışma bu yönde geliştirilmeye açıktır.

Tablo 1'de algoritmanın adım adım uygulandığı örnek bir veri görülmektedir:

Çizelge 1. Geliştirilen algoritma kullanılarak şifrelenen veri örneği (Encrypted data sample using developed algorithm)

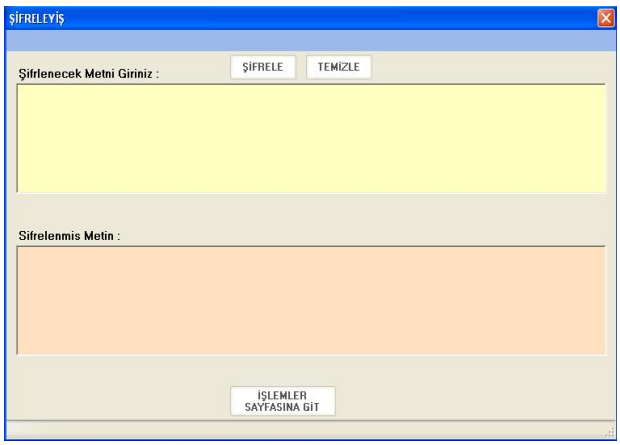
Düz Metindeki Kelime	B	İ	L	İ	Ş	İ	M
Maksimum İnversiyon	Ş(22)	M(15)	L(14)	İ(11)	İ(11)	İ(11)	B(1)
Mod 28'e göre Harfler	F	K	L	O	O	O	Y
Harflerin indisleri	0	1	2	3	4	5	6
FKLOOOY Minimum inversiyon	6	13	14	17	17	17	27
FKLOOOY maksimum inversiyon	27	17	17	17	14	13	6
Toplam	33	30	31	34	31	30	33
If Bloğu	33>28	30>28	31>28	34>28	31>28	30>28	33>28
	33 mod 28=5 düz alfabedeki 5 numaralı harf	30 mod 28=2 düz alfabedeki 2 numaralı harf	31 mod 28=3 düz alfabedeki 3 numaralı harf	34 mod 28=6 düz alfabedeki 6 numaralı harf	31mod28= 3 düz alfabedeki 5 numaralı harf	30 mod 28=2 düz alfabedeki 2 numaralı harf	33 mod 28=5 düz alfabedeki 5 numaralı harf
Şifreli Hali	E	C	Ç	F	Ç	C	E

5. GELİŞTİRİLEN PROGRAMIN TANITIMI
(PRESENTATION OF THE PROGRAM DEVELOPED)

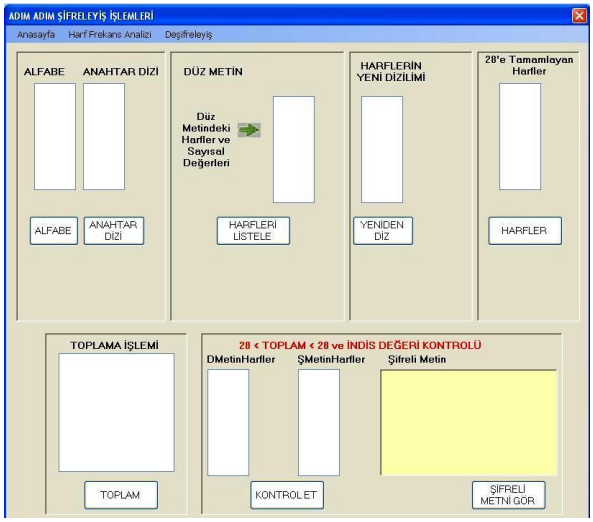
Uygulamanın similasyonu için, donanımsal olarak Windows XP SP3 işletim sistemine sahip Dell Inspiron 6000 dizüstü bilgisayar ve bir adet mikrofon, yazılımsal olarak Microsoft Visual Studio 2010 programı C# dili ve DikteApi demo programı kullanılmıştır.

Demo olarak hazırlanan program için Windows Form Application proje tipi seçilmiştir. Şifreleme işlemi bir önceki bölümde anlatılan akış diyagramına uygun bir şekilde gerçekleştirilmiştir.

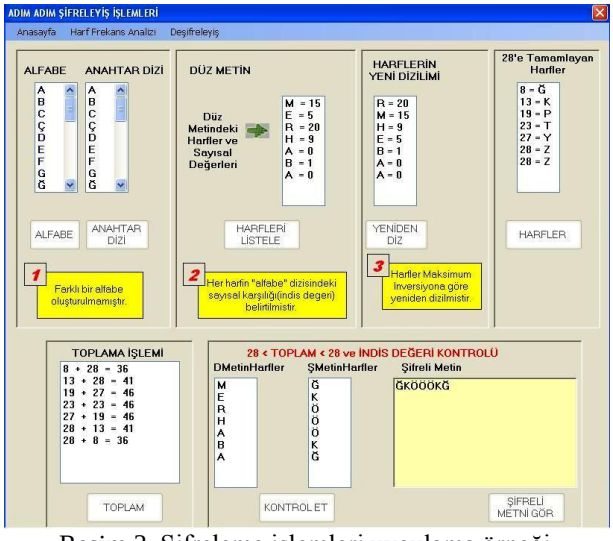
Program tanıtım amaçlı olduğu için dört arayüze sahiptir. Birinci arayüzde girilen düz metnin şifrelenmesi işlemi gerçekleştirilmiştir. İkinci arayüzde şifreleme işlemi adım adım yaptırılarak açıklanmıştır. Üçüncü arayüzde harf frekans analizi incelemeleri yapılmıştır. Dördüncü arayüzde konuşma tanıma özelliklerinin kullanımına imkan sağlayan Dikte Api demo programı ile şifrelenmiş bilgi ya da verinin açık hale getirilmesi sağlanmıştır.



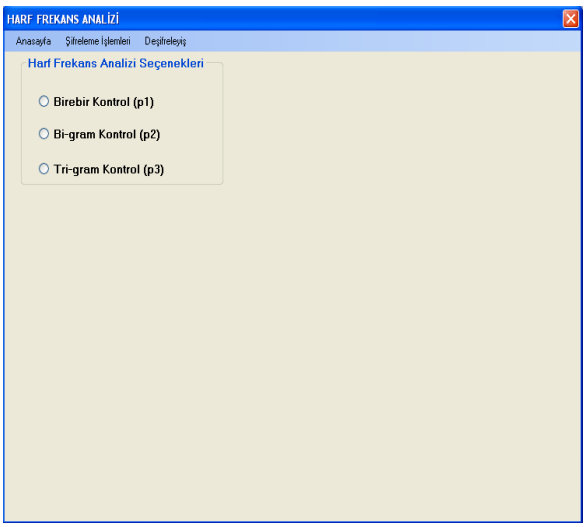
Resim 1. Şifreleme Ekranı (Screenshot for encryption)



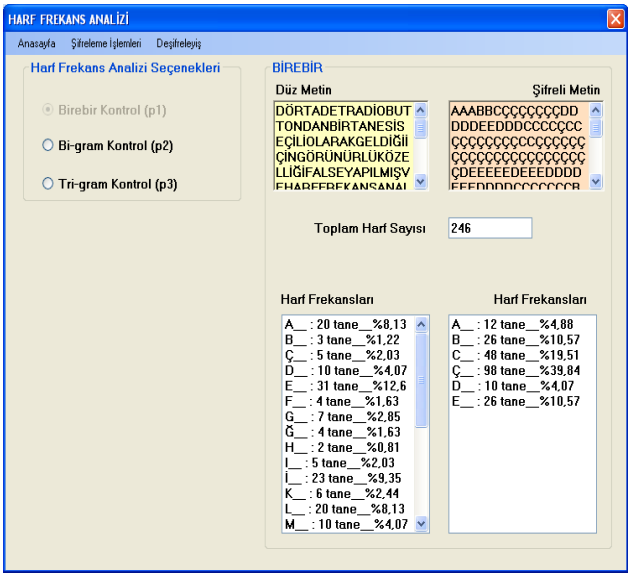
Resim 2. Şifreleme işlemlerinin adım adım gerçekleştirilmesi (A step by step encryption process)



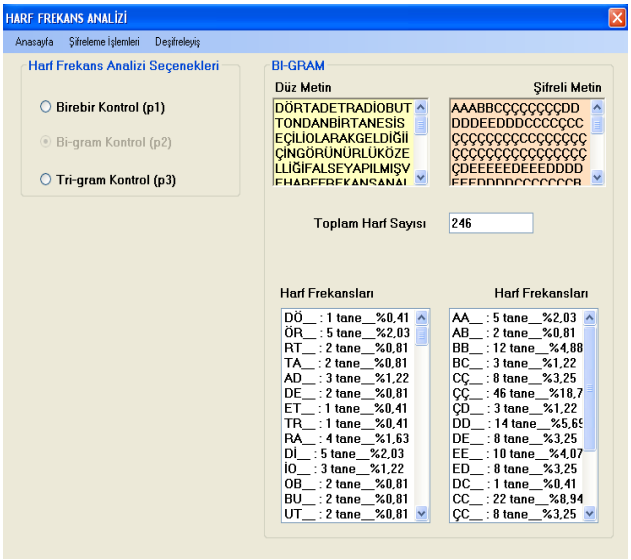
Resim 3. Şifreleme işlemleri uygulama örneği (A sample application for encryption)



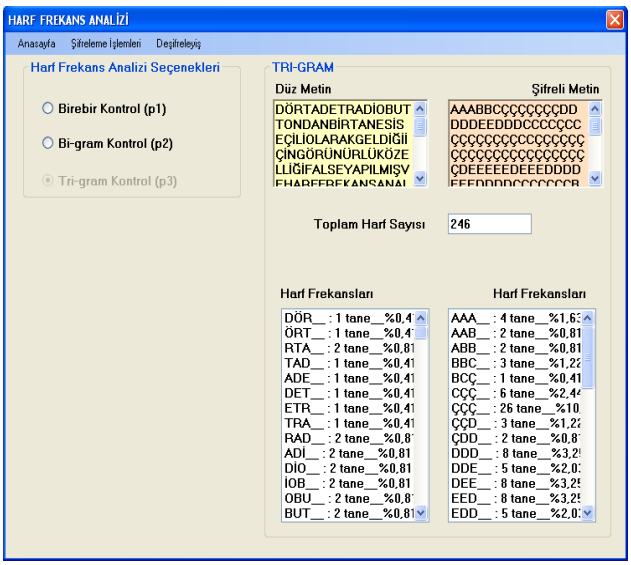
Resim 4. Harf frekans analizi ekranı
(Screenshot for letter frequency analysis)



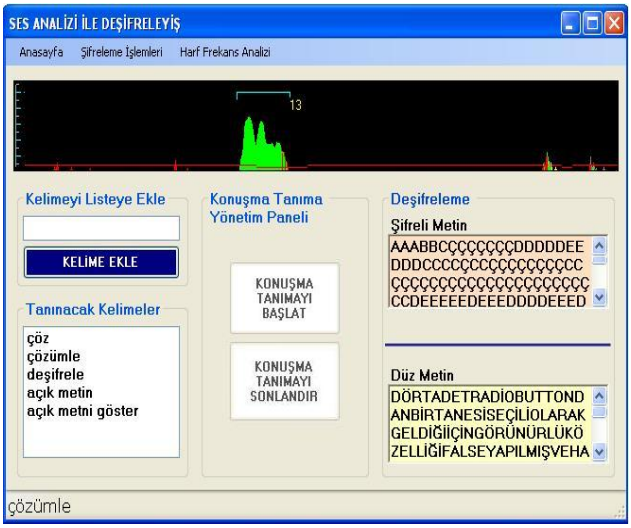
Resim 5. Harf frekans analizi bire-bir uygulama örneği
(A one-to-one sample application for letter frequency analysis)



Resim 6. Harf frekans analizi bi-gram uygulama örneği
(A bi-gram sample application for letter frequency analysis)



Resim 7. Harf frekans analizi tri-gram uygulama örneği
(A tri-gram sample application for letter frequency analysis)



Resim 8. Şifrelenmiş metinin ses komutu ile açık hale getirilmesi (Decryption of the cipher text by voice command)

6. HARF FREKANS ANALİZİNDEN ELDE EDİLEN BULGULAR (CONSEQUENT FINDINGS FROM LETTER FREQUENCY ANALYSIS)

Şifrelenmiş metin üzerinde harf frekans analizinden sağlıklı veriler elde edebilmek için uzun metinler üzerinde çalışmak gereklidir. Bu kısımda yapılan çalışma için küçük bir örnek üzerinde frekans analiz değerlendirmesi yapılmıştır.

Harf Frekans Analizinde ilk aşamada kullanılması gereken en önemli bilgi her dilin kendi özelliklerine göre en çok kullanılan harflerinin olduğu bilgisidir. Türkçe'de en çok kullanılan harflerden ilki A harfidir. Onu sırası ile E, İ, N ve R izlemektedir [13].

Tablo 2 ve Tablo 3'te örnek 6.1'de verilmiş olan küçük metin üzerinde yapılan incelemeler görülmektedir:

Örnek 6.1 (Example 6.1)

Düz metin :"*Bilişim teknolojilerinin bizlere sağladığı kolaylıklar arttıkça, elektronik ortamların kullanımı yaygınlaşmakta, bilginin işlendiği, taşındığı, saklandığı ortamlara erişimler zamandan, mekandan bağımsız hale gelmektedir*[2]."

Toplam harf sayısı : 194

Çizelge 2. Düz metin harf frekansları
(The letter frequencies of the plain text)

Harf	Harf Sayısı	Kullanım%'si
a	26	13,40
b	4	2,06
c	_	_
ç	1	0,51
d	7	3,60
e	14	7,21
f	_	_
g	3	1,54
ğ	5	2,57
h	1	0,51
ı	15	7,73
i	17	8,76
j	1	0,51
k	11	5,67
l	20	10,63
m	10	5,15
n	15	7,73
o	6	3,09
ö	_	_
p	_	_
r	11	5,67
s	3	1,54
ş	5	2,57
t	9	4,63
u	1	0,51
ü	_	_
v	_	_
y	3	1,54
z	3	1,54

Örneklem olarak kullanılan düz metindeki harflerin frekans analizine göre en çok kullanılandan en az kullanılana doğru sıralaması;

A, L, İ, I=N, E, K=R, M, T, D, O, Ğ=Ş, B, G=S=Y=Z, Ç=H=J=U

Paragraf olarak şifrelenmiş şifreli metin; "aabbbdeeeeeeeeeffffffggğğğğgggeddddddggfffffgggggggggeeeedddeeedççççççddddddddddççççççççççddddddçccccçddddddçççççççççççddddddddddçççççdeeedddeeeggggggggggffffggddddddeggggğğğggfffffeeeeeeeeedbbbaaa" şeklindedir.

Paragraf olarak şifrelenmiş şifreli metindeki harf tekrarlarının çok fazla olmasından dolayı daha sağlıklı veriler elde edebilmek için harf frerkans analizi incelemeleri kelime kelime şifrelenmiş şifreli metin üzerinde yapılmıştır.

Kelime kelime şifrelenmiş şifreli metin ; "ecçfçceaçfabbabbbabbafçayçhfhçaglllilillgbğbbbbbbbğbeeemmeeeaçajamaçaeğöimmiöğedcçbbbçcdbbeffçbbçffebbieçffçeicgfffffgcecdğğğdcegjıgğğgıjgeğğiklğğebçcacğçbajjhhjjajjhııhjjafeğğefallllbçğhğfğhğçb" şeklindedir.

Toplam harf sayısı : 194

Çizelge 3. Şifreli metin harf frekansları
(The letter frequencies of the cipher text)

Harf	Harf Sayısı	Kullanım%'si
a	16	8,24
b	29	14,94
c	10	5,15
ç	18	9,27
d	4	2,06
e	19	9,79
f	18	9,27
g	8	4,12
ğ	20	10,63
h	8	4,12
ı	4	2,06
i	7	3,60
j	11	5,67
k	1	0,51
l	10	5,15
m	5	2,57
n	_	_
o	_	_
ö	2	1,03
p	_	_
r	_	_
s	_	_
ş	_	_
t	_	_
u	_	_
ü	_	_
v	_	_
y	1	0,51
z	_	_

Şifreli metnin harf frekans analizine karşı güvenirliği incelenerek geliştirilen algoritmanın güvenirliği bu kısımda tespit edilmeye çalışılmıştır.

Düz metin için oluşturulan harf frekans tablosunda da en çok kullanılan harfin %13,40 oranıyla "A" harfi olduğu görülmektedir. Şifreli metinde de en çok geçen harf "B" olduğuna göre şifreli metindeki B harfleri yerine A harfi yazılmalıdır. Şifreli metindeki "Ğ" harfi yerine "E" harfi, "E" harfi yerine "K" harfi yazılmalıdır. "Ç" ve "F" harflerinin dağılımları aynı oranda çıktığı için deneme yanılma yapılmalıdır. Öncelikle "Ç" harfi yerine "İ" yazılmalı eğer anlamsız olduysa "F" harfi yerine "İ" yazılmalıdır. Bu işleme tüm harfler için yerleştirme işlemi uygulanana kadar devam edilmelidir.

Örnek 6.2'de görülen metin, şifreli metni çözmek için yapılan bazı harf değişikliklerini göstermektedir:

Örnek 6.2 (Example 6.2)

KCÇFÇCKAÇFAAAAAAAAAAAFÇAYÇHFHÇAGLL
İLİLLGAEAAAAAAAAKAKKKMMKKKAÇAJAMAÇ
AKEÖİMMİÖEKDCÇAAAÇCDAAKFFÇAAÇFFKAA
İKÇFFÇKİCGFFFFFGCKCDEEEDCKGJIGEEGIJGKE
EİKLEEKAÇCACEÇAAJJHHJJAJJHIIHJJAFKEEKFA
LLLLAÇEHEFEHEÇA

Örnek 6.2'de aynı harfin pek çok kez arka arkaya gelmiş olması bu metin üzerinde harf frekans analizinin etkili olmayacağını göstermektedir, çünkü Türkçe'nin yapısal özelliklerine göre en çok tekrarlanan harf "A" olmasına rağmen şifreli metinde en çok kullanılan harf(B) yerine "A" yazıldığında birbirinden farklı birçok harf "A" ile temsil edilmiş olur ve bu tekrarların çözülmesi harf frekans analizi ile mümkün değildir. "A" harfi birden fazla harfi temsil etmiştir, oysaki harf frekans analizinde bir harf sadece bir harfi temsil ettiği zaman doğru ya da doğruya yakın sonuç elde edilebilir. Tek bir harfin birden fazla harfi şifrelemiş olması geliştirilen kriptografi algoritmasının en önemli avantajıdır.

7. SONUÇ VE ÖNERİLER (CONCLUSION AND SUGGESTIONS)

Daha önce yapılmış olan çalışmalar incelendiğinde makalenin kapsamını oluşturan alana yönelik yeni üretimlerin çok az sayıda kalmış olması bu alana dikkat çekilmesinin önemini ortaya koymuştur. Alandaki çalışmalar yoğun olarak daha önce yapılan çalışmaların incelenmesi, iyileştirilmesi ya da karşılaştırılması boyutundadır. Bu çalışmalar var olanlardan daha iyi seçenekler oluşturabilmek için oldukça önemlidir, fakat çalışmacılar yeni üretimlere de yöneltilmelidir. Sanal ortamın oldukça geniş bir kitleye ulaşmış olması ülkelerin güvenliklerini büyük bir tehdit altına almıştır. Ağır silahlarla mücadele durumu artık yerini siber savaşa bırakmaktadır. Ulusal bilgilerin güvenli bir şekilde korunabilmesi ve her türlü siber saldırıya hazırlıklı olunması gerekmektedir. Sistemlerin sürekli olarak güncellenmesi gerekliliği açık bir şekilde görülmektedir, çünkü bilgiyi elde etme ve koruma süreci sonu hiç gelmeyen kısır bir döngüdür.

Yapılan çalışma sembolik olmakla birlikte bilgi güvenliğinin hassas bir konu olduğunu ve gün geçtikçe daha çok önem kazandığını vurgulamak amaçlıdır. Bu alanda yapılabilecek pek çok çalışmadan biri olan kriptografi, gelebilecek saldırıları engellemek ya da zaman kazanmak açısından önemlidir. Yetkisiz kişiler verilere bir şekilde ulaşsa da verilerin şifreli bir şekilde saklanmış olması hem zaman kazanmak hem de yeni çözümler üretebilmek için önemlidir.

Kriptografi yani şifreleme bilimi günümüzde güncel hayatın pek çok alanında kullanılmaktadır. Örneğin bankamatikler, rezervasyon sistemleri, e-posta iletileri, telefon bankacılığı, normal bankacılık işlemleri, cep telefonları, uydu sistemleri, füze sistemleri, savaş uçakları, sağlık sistemleri, mimari projeler, fatura sistemleri gibi daha pek çok alanda kullanılabilmektedir. Bilgi ve veri güvenliğinin taşıdığı önem günümüzde giderek hayati hale gelmiştir. Sanal dünya ülkeler ve bölgeler arasındaki sınırın ortadan kalkmasını sağlamıştır. Sanal dünyada yer almayan harita sınırları, gerçek dünyada aşılamasa da elektronik ortamda rahatlıkla aşılabilmektedir. Vatandaşlara ve kurumlara kolaylık sağlamak için tüm güncel faaliyetlerin de elektronik ortama aktarıldığı düşünülürse yaklaşan tehlikelerin giderek büyüdüğü de görülecektir. Son dönemde yaşanan kurumsal web sitelerinin ve sayfalarının yetkisiz(izinsiz) erişimi sonucu açığa çıkmaması gereken pek çok doküman herkesin ulaşabileceği şekilde açığa çıkarılmıştır. Bu durum ülkelerin milli güvenliği için akıl almaz bir tehlikenin her an gelebileceğini göstermektedir.

Tüm bu sebeplerle bu çalışma kapsamında bilgi güvenliği için bir kriptografi algoritması geliştirilmeye çalışılmıştır. Geliştirilen algoritma üzerinde harf frekans analizi incelemeleri yapılmış ve bu saldırıya karşı güvenilir bir algoritma olduğu tespit edilmiştir. Ancak farklı saldırı türleri için herhangi bir inceleme yapılmamıştır.

Geliştirilen kriptografi algoritmaları her an kırılabileceği için her zaman geliştirilmeye açıktır. Algoritma sadece harf frekans analizi ile incelenmiştir, algoritmanın güvenirliğini tespit etmek için başka yöntemlere de başvurulabilir. Proje donanımsal boyuta taşınabilir. Yeni bir kripto cihazı üretilebilir. Şifreleme işleminin deşifreleme anahtarı olarak biyometrik özellikler kullanılabilir.

Günlük hayatın pek çok alanına giren kriptografinin en önemli boyutu ulusal bilgi güvenliğini sağlaması, siber saldırılarda bilgi hırsızlığı girişimlerini boşa çıkarmasıdır. Bu nedenle bu alandaki çalışmalar daha yoğun hale getirilmeli ve ulusal kriptografi algoritmaları geliştirilmelidir. En güvenli sistemler bile çözüldüğü için farklı algoritmalar geliştirilmeli ve var olanların güvenirlik derecesi arttırılmalıdır. Ulusal bilgilerin ulusal olmayan bir şifreleme algoritması ile şifrelenmesi ülkenin ve milletin kaderini şifrelemeyi geliştiren devletin eline bırakmaktır. Ülke ve millet açısından ulusal çalışmalara daha çok önem verilmeli ve var olan sistemler üzerinde oynama yapmaktansa sıfırdan yeni üretimler gerçekleştirilmelidir.

KAYNAKLAR (REFERENCES)

[1]A.Jones, "Information Warfare-what has beenhappining?", ***ComputerFraud& Security***, 4-7(November 2005).
[2] G.Canbek, Ş.Sağıroğlu, **Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri**, Ankara, 2006.
[3] Ş.Sağıroğlu, M.Alkan, "Bilgi Güvenliği Bilimi(Kriptoloji)", **Her Yönüyle Elektronik İmza**, Grafiker Yayınları, Ankara, 21-50, 2005.
[4] İnternet: Tübitak Bilgem Ulusal Bilgi Güvenliği Kapısı, "BGYS-0001 Bilgi Güvenliği Yönetim Sistemi Kurulum Kılavuzu", www.bilgiguvenligi.gov.tr/bilgi-guvenligi-yonetimi-dokumanlari/uekae-bgys-0001-bilgi-guvenligi-yonetim-sistemi-kurulum-kilavuzu.htm (2013).

[5] M. Tekerek, "Bilgi Güvenliği Yönetimi", ***KSU Fen ve Mühendislik Dergisi***, 11(1): 132-137 , 2008.
[6] M.Ü. Çeşmeci, "Kriptoloji Tarihi" , ***UEKAE Dergisi***, 2009.
[7] A. Jones, "Cyber Terrorism:Fact or Fiction", ***Computer Fraud & Security***, 4-7, June 2005.
[8] İnternet: Konferans Sonuç Bildirgesi", V**.** ***Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı***, "www.iscturkey.org/ISCTURKEY2012/index.html, 2013.
[9] V.Vural, Ş.Sağıroğlu, "Ülke Bilgi Güvenliği", ***3.Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı***, Ankara, Aralık 2008.
[10]İnternet: Kriptoloji, http://tr.wikipedia.org/wiki/Kriptoloji , 04.02.2013.
[11] S.Soyalıç, "KriptografikHash Fonksiyonları ve Uygulamaları", Yüksek Lisans Tezi, ***Erciyes Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı***, Kayseri 2005.
[12] R. Yılmaz, "Kriptolojik Uygulamalarda Bazı İstatistik Testler", Yüksek Lisans Tezi, ***Selçuk Üniversitesi Fen Bilimleri Enstitüsü İstatistik Anabilim Dalı***, Konya 2010.
[13] K.Aslandağ, "Bilgi Güvenliği Kavramı ve Bilgi Güvenliği Yönetim Sistemleri ile Şirket Performansı İlişkisine Dair Bir Uygulama", Yüksek Lisans Tezi, ***Gebze Yüksek Teknoloji Estitüsü, Sosyal Bilimler Enstitüsü Strateji Anabilim Dalı***, Gebze 2010.
[14] A.Uğur, "Uzaktan Erişimli Kriptografik Güvenli Haberleşme Protokolü", Yüksek Lisans Tezi, ***Pamukkale Üniversitesi Fen Bilimleri Enstitüsü***, Denizli 2005.
[15] S. Akyelek, H.M. Yıldırım, Z.Y. Tok, "Kriptoloji ve Uygulama Alanları: Açık Anahtar Altyapısı ve Kayıtlı Elektronik Posta", ***Akademik Bilişim 2011***, İnönü Üniversitesi, Malatya, 713-718, 2011.
[16] V.Nabiyev, "**Yapay Zeka**" , 3.baskı, Ankara, 2010.
[17]H.N. Buluş, "Temel Şifreleme Algoritmaları ve Kriptanalizlerinin incelenmesi", Yüksek Lisans Tezi, ***Trakya Üniversitesi Fen Bilimleri Enstitüsü***, Edirne 2006.
[18] C. Çimen, S. Akleylek ve E. Akyıldız, "**Şifrelerin Matematiği Kriptografi**", ODTÜ Yayıncılık, 2008.
[19] D.Arda, E. Buluş, "Türk Alfabesi ve Yapısal Özellikleri Kullanılarak Tek Alfabeli Yerine Koymada Şifreleme ve Kriptanaliz", ***20. Türkiye Bilişim Kurultayı***, İstanbul, 2003.
[20] D. Arda, E. Buluş, T. Yerlikaya, "Türkiye Türkçesi' nin Bazı Dil Karakteristik Ölçütlerini Kullanarak Vigenere Şifresi ile Şifreleme ve Kriptanaliz", ***ELECO'2004 Elektrik-Elektronik-Bilgisayar Mühendisliği Sempozyumu ve Fuarı***, Bursa, 2004.
[21] A.K. Jain, A. Ross, , S.Pankanti, "Biometrics:AToolFor Information Security**",** ***IEEE Transactions On Information ForensicsAnd Security***, Vol.1 , No.2, Haziran 2006.