Hasan Ferdi Turgutlu Teknoloji Fakültesi

Yazılım Mühendisliği Bölümü

Araştırma Raporu

Sezar Şifrelemesi (Ceaser's Cipher)

YZM 4209 Bilgi Sistemleri Güvenliği

Orçun ÖZDİL – 172 80 30 65

Danışman: Öğr. Gör. Hüseyin TAŞ

ÖZGEÇMİŞ

Orçun ÖZDİL, 02/05/1978 tarihinde İzmir'de doğdu. 1999 yılında Ege Üniversitesi Eczacılık Fakültesi mezunudur ve halen serbest eczacılık yapmaktadır.

2017 yılı Dokuz Eylül Üniversitesi Bilgisayar Programcılığı mezunu olup, öğrenimini Manisa Celal Bayar Üniversitesi Hasan Ferdi Turgutlu Teknoloji Fakültesi – Yazılım Mühendisliği 4. sınıfta sürdürmektedir.

İngilizce ve Almanca bilmektedir. Evli ve bir çocuk babasıdır.

ÖNSÖZ / TEŞEKKÜR

Bu araştırmada, MCBÜ HFTTF YZM-4209 Bilgi Sistemleri Güvenliği Dersi kapsamında, Sezar Şifreleme Algoritması'nın (Caesar's Cipher) litratür araştırması ve bir örnek çalışma ile açıklanması amaçlanmıştır.

Araştırmam ve öğrenciliğim süresince tüm zorlukları benimle göğüsleyen ve hayatımın her evresinde bana destek olan ve sabır gösteren değerli eşim *ÖZGE ÖZDİL* ve biricik oğlum *EMİR ÖZDİL*'e sonsuz teşekkürlerimi sunarım.

ORÇUN ÖZDİL
İZMİR-2019

İÇİNDEKİLER

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. Bilginin korunması, güvenliğinin sağlanması gün geçtikçe büyüyen bir hızla önem kazanmaktadır. [4]

Bu nedenle bu çalışmada kriptoloji, kriptoanaliz, kriptografi, şifreleme algoritmaları tanım, tarihçe ve sınıflandırmaları ele alınmıştır. Şifreleme algoritmalarını en eski örneklerinden olan "Sezar Şifreleme Algoritması" açıklanmaya ve bir C# uygulaması ile görselleştirmeye çalışılmıştır,

ANAHTAR KELİMELER

Kriptoloji, kriptoanaliz, kriptografi, bilgi, bilgi güvenliği, siber savaş, şifreleme algoritmaları, Sezar Şifreleme

GİRİŞ

Kullanışa başlanması M.Ö.'ki yıllara dayanan kriptoloji biliminin tarihi insan hayatının özel bilgileri, harp sırları ve haberleşme gibi geniş alanda bilgilerin kötü amaçlı insanlardan saklanması, karşı tarafa güvenli şekilde ulaştırılması ve ulaştırılacağı kişi dışında kimseye sızmaması amacıyla kullanıldığı bilinmektedir. Tarih boyunca insan hayatı ve yaşam için önemli olan bilgilerin sürekli tehditlere maruz kalması, bu tehditlerle karşılaşmamak ve bilgi güvenliğini sağlamak amacıyla bilimin vazgeçilmezi olan kriptolojinin zaman zaman geliştirilmesini, yenilenmesini geliştirilmeye açık tutulmasını sağlamıştır. XX. yüzyılın başlarından başlayarak bilgilerin telsizler ortamında aktarılması, haberleşmenin makinalar ortamına geçmesi bilgileri büyük tehditler altında bırakmış ve bilginin tehditlerden korunması için artık makineler ortamında bilgi güvenliğini sağlamak amacıyla eski kriptoloji şifreleme sistemlerinin geliştirilmesi ve yeni kriptoloji sistemlerin hazırlanmasını zorunlu kılmıştır. Artık gelişen kriptolojide klasik tekniklerde kullanılan alfabeye göre yer değiştirme, kaydırma, mod alma ve diğer eski yöntemler kullanışsız hale gelmiştir. Makineler aracılığıyla bilgilerin, en küçük bilgi birimi olan bitleri arasında geliştirilen yeni kriptoloji şifreleme sistemleri ile şifreleme yaparak güvenliğinin sağlandığı yeni makineler dönemi başlamıştır.

Günümüzde büyük hacimde bilgilerin hayatımızın vazgeçilmezi olan elektronik ortamda ve ağlar üzerinden aktarılması, depolanması ve kullanışı bizi, bu bilgilerin çalınması, değiştirilmesi, bozulması ve özel bilgilerin ele geçirilmesi gibi büyük güvenlik sorunları ve tehditlerle karşı karşıya bırakıyor. Bu bilgilerin korunması sebebi ile kriptoloji bilimi sürekli geliştirilmekte ve geliştirilmeye açık olmaktadır. Ancak hala bilgiler tehditlere maruz kalmakta ve yeni kriptografi sistemlerin üretilmesine ihtiyaç duyulmaktadır. Yeni geliştirilen kriptoloji yöntemlerinin daha önceki yöntemlerin incelenerek ve değiştirilerek üretilmesi bu alanda üretimin kısıtlı olduğunun göstergesidir. Var olan sistemlerin incelenmesi ve değiştirilerek yeni kriptoloji sistemlerin geliştirilmesi ulusal açıdan olumlu olurken, dış kaynaklı bir kriptoloji sisteminin geliştirilerek ulusal bilgi güvenliği için kullanılması bu bilgilerin yüksek güvenliğini sağlamamaktadır. Bu nedenle bilgi güvenliğinin sağlanması için kriptoloji bilimine daha büyük önem verilmeli ve yeni kriptoloji sistemlerinin üretilmesi gerekmektedir.[3]

Şifreleme algoritmalaının anlaşılabilmesi için öncellikle bilgi, kriptoloji, kriptoanaliz ve kriptografi kavramlarının anlaşılması gerekmektedir.

1.1 Bilgi Nedir ?

En kısa tanımıyla bilgi, işlenmiş "veri"dir. Veri, olguların harf, sayı, renk gibi sembollerle ifade edilmesi iken, bilgi, herhangi bir konu ile ilgili verilerin bir araya gelmesi ile oluşan açıklayıcı ifadeler bütünüdür. [1]

Menşeyini Latince "informare" kelimesinden alan bilgi (information) kelimesi, her hangi bir şeyi şekillendirmek, şekil vermek anlamı gibi kabul edilmektedir (Vural, 2007).

Sözlük anlamıyla bilgi;

* Öğrenme, araştırma ve gözlem yoluyla elde edilen her türlü gerçek, malumat ve kavrayışın tümü,

* İnsan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bilim, malumat,

* İnsan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü, malumat, vukuf,

* Genel olarak ve ilk sezi durumunda zihnin kavradığı temel düşünceler ve

* Kurallardan yararlanarak kişinin veriye yönelttiği anlam olarak tanımlanmaktadır (TDK, 2016).

Literatürde bilgi farklı şekilde tanımlanmaktadır:

* Bilgi, insanın varlığı tanıma ve anlama isteği sonucunda oluşan, düşünebilen süje ile obje arasındaki ilişkidir. Suje; bilgiye yönelen, öğrenen, araştıran, bilen insandır. Obje; bilgiye konu olan, bilinen somut varlıkların tümüdür. İnsan başka bir varlığı düşündüğünde, araştırdığında, öğrendiğinde suje, başkası tarafından araştırıldığında ise objedir (Vural, 2007), (MEB, 2013). Türk Dil Kurumu bilgiyi şu şekilde tanımlamıştır: "İnsan zekâsının çalışması sonucunda ortaya çıkan düşünce ürünü, malumat, vukuf". (Muharremoğlu, 2013).

* Yaşamın varlığından beri bilgi, önemini hayatın çeşitli alanları üzerinde tutmakta ve zaman geçtikçe daha da artırmaktadır. Bilgi, geçmişlerden günümüze kadar çeşitli alanlarda hayatın süzgecinden geçerek, daha da gelişmiş, büyümüş ve çeşitli araçlarla günümüze kadar ulaşmıştır. Bilginin eski çağlardan günümüze ulaşmasında ve yaygınlaşmasında M.Ö' lere dayanan taş kitabeler, eserler, destanlar, masallar, XII yüzyıldan sonra ise medreseler, üniversiteler, kitaplar araç olarak en önemli role sahip olmuşlar. XX yüzyılın başlarından başlayarak ise artık bilginin saklanılması, korunması ve gelecek nesillere aktarılması yönünde hazırda devam eden çok büyük teknoloji gelişmeler sonucunda bilgi çağı adı verilen yeni dönemi yaşamaktayız. Yaşadığımız döneme adını kazıyan bilgi günümüzde insanların yaşam tarzına yön verdiği gibi, gelecekte de bu önemini koruyacak ve daha da ilerilere taşıyacaktır (Vural, 2007).

1.2 Bilgi Güvenliği Nedir ?

* Bilgi güvenliği; bilginin mevcut tehditlerden korunması, gereken teknolojinin doğru şekilde kullanılarak bilgiye mümkün tüm ortamlarda, istenmeyen kişiler tarafından ulaşılmasını önlemektir. Başka bir tanımla bilgi güvenliği; elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması zamanı bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür (Haklı, 2012).

* Bilgi, bir kurum için sunduğu ürünler kadar önem taşıdığından dolayı uygun bir ortamda korunmalıdır. Bilginin farklı kurumlar arasında paylaşılması arttıkca, bilgi paylaşımındakı çeşitli risklerin olma ihtimali ve bilgiyi korumaya yönelik gereksinimler de artmaktadır. Bilindiği gibi eskilerden beri tarih boyunca askeri alanda özel bilgilerin, harp sırlarının düşmandan korunması için, zamanla gelişerek günümüze kadar gelen çeşitli araçlar, yöntemler ve sistemler kullanılmıştır.

* Bilgi, baskılı olarak veya kağt dokümanları üzerinde yazılı, elektronik ortamlarda saklanan, posta ya da elektronik posta yolu ile aktarılabilen, insanlar arasında sözle ifade edilebilen birçok çeşitli biçimlerde bulunabilmektedir. Bilginin kullanıma yararlı olarak tutulabilmesi için mutlaka uygun bir ortamda korunması gereklidir. Aktif kullanımda olan bilgilerin büyük bir kısmı artık bilgisayarlar aracılığıyla elektronik olarak saklanmakta, korunmakta ve güvenli biçimde diğer bilgisayarlarla paylaşılabilmektedir.

* Bilgileri çeşitli risklerden ve tehlikelerden korumak ve güvenliğini sağlamak, bilginin iş risklerini azaltmak ve iş kazançlarını artırmak demektir. Örneğin bir firmanın veya şirketin özel işçi bilgileri, müşteri bilgileri, finansal ve yeni ürün bilgileri gibi özel bilgileri, iş kaybına ve iflasa götürebilecek güvenlik açığı sebebiyle rakip şirketlerin eline geçmemelidir.[3]

* Bilgi güvenliğinin sağlanması için kurumsal yapı, politika, süreç, yazılım ve donanımların bir arada işlevlerini içeren denetimler dizisi gerçekleştirilmektedir. Kurumun veya şirketin iş güvenliğinin sağlanması amacıyla, özel bir ortamda bahsetdiğimiz denetimlerin kurulması, uygulanması, izlenmesi, incelenmesi ve geliştirilmesi gerekmektedir. Tüm bu güvenlik yöntemlerinin diğer iş yönetimi süreçleri ile birlikde her hangi bir aksaklığa veya güvenlik açıklığına yol verilmeden yapılması gerekmektedir (Otgonjargal, 2013), (Akay, 2014).

2.1 Kriptoloji Nedir?

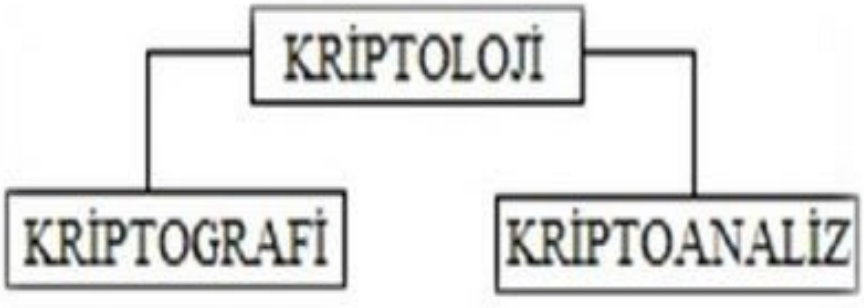
* “Kryptos Logos”,”gizli”+”dünya”.

* Haberleşen iki veya daha fazla tarafın bilgi alışverişini emniyetli olarak yapmasını sağlayani temeli matematiksel zor ifadelere dayanan tekniklerin ve uygulamaların bütünüdür.

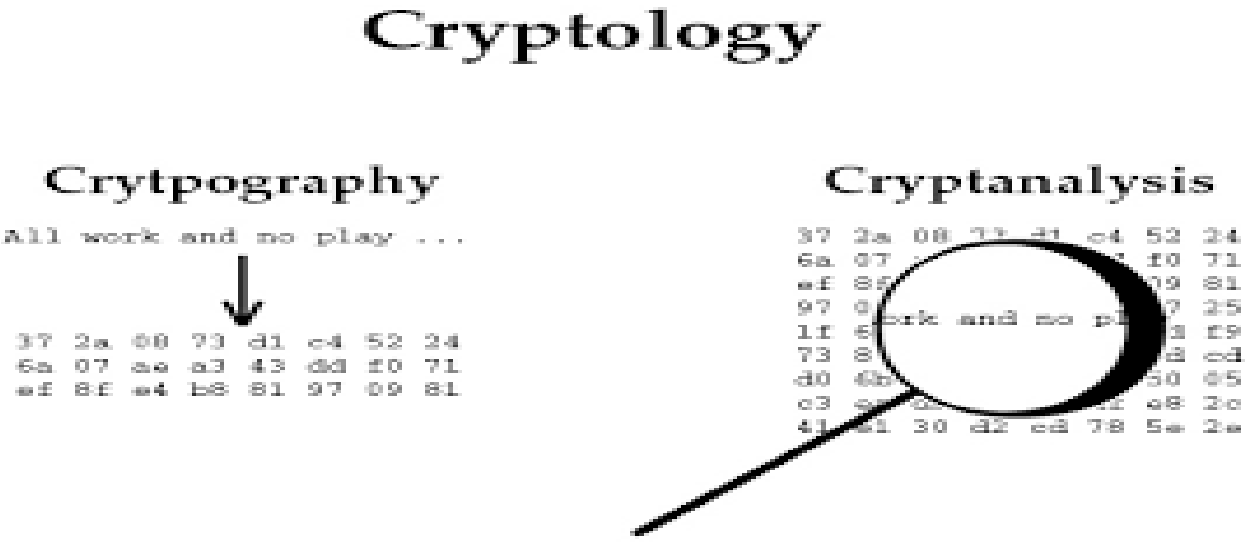
* Matematik, elektronik, optik, bilgisayar, sosyal mühendislik bilimleri gibi birçok disiplini kullanan özelleşmiş bir bilim dalıdır.

* Kriptoloji yunan kökenlidir, kyrtops (gizli, saklı) ‘κρυπτός’’ ve logos (bilim) ‘’λόγος’’ sözcüklerinin birleşiminden oluşmuştur, kısaca şifre bilimi demektir

* Kriptoloji, kriptografi ve kriptanaliz olarak iki alt bilim dalından oluşmaktadır.[1][3]



Şekil:1.1 [3]



Şekil:1.2

2.2 Kriptografi Nedir ?

* Gizli mesajlaşma, onaylama, dijital imzalar, elektronik para uygulamalarının tümüyle ilgili bilim dalıdır.

* Belgelerin şifrelenmesi ve şifrelerin çözülmesi için kullanılan yöntemlere verilen addır.

* Kriptografinin temel amacı bilginin gizliliğini sağlamaktır. Bu amaçla kullanılan üç temel yöntemden söz edilebilir [4]

1. Yerine koyma yöntemleri (Substitution Methods)

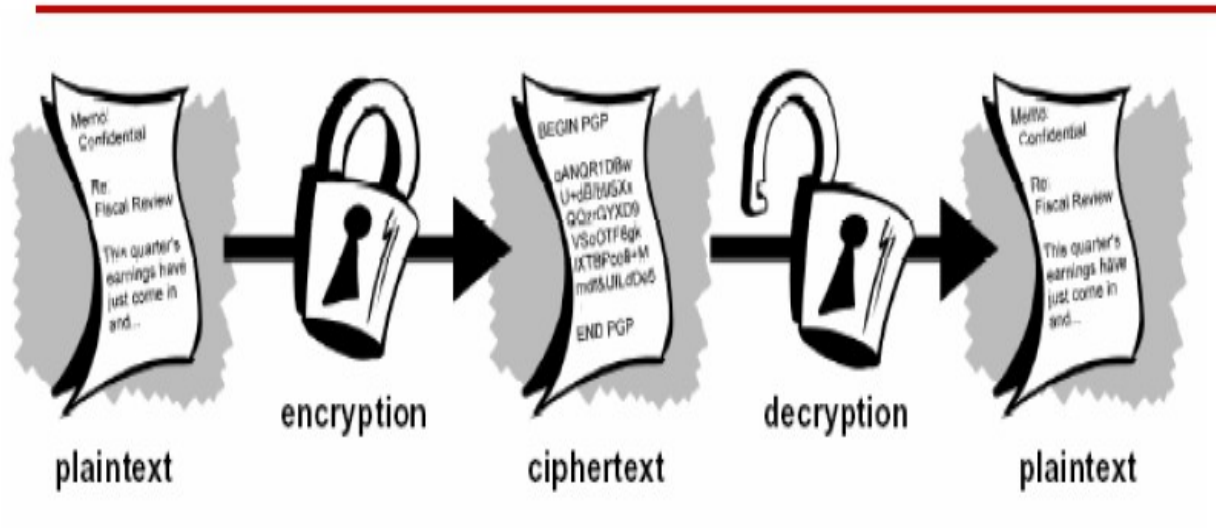
Düz metindeki harflerin yeri sabittir. Sayılar, semboller ya da başka bir alfabedeki harfler bu harflerin yerine yerleştirilerek şifreli metin elde edilir. Geçmişteki en güzel örneği Sezar şifreleme algoritmasıdır.[4]

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.[4]

3. Cebirsel yöntemler (Algebraic Methods)

Matematiksel bazı fonksiyonların kullanımı, yerine koyma ve yer değiştirme işlemlerinin karışımı gibi karmaşık yapıda olan işlemleri kapsayan yöntemlerdir .[4]



Şekil : 2.1 [5]

2.3 Kriptoanaliz Nedir ?

* Kriptografik algoritmaların açıklarını bulup ortaya çıkartmaya denir.
* Kriptografik sistemlerin kurduğu mekanizmaları inceler ve çözmeye çalışır.

BAZI KRİPTOANALİZ TEKNİKLERİ

Şifrelenen bilgilerin elde edilebilmesi için çeşitli kriptoanaliz teknikleri vardır. Bu teknikler kriptografi tekniklerine karşı kullanılan saldırı teknikleri olarak da bilinir.

Bunlardan bazıları :

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.[4]

2. 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.[4]

Frekans analizi, bir dile ait yapısal bazı özellikleri kullanarak şifreli metinden düz metni elde etmeyi amaçlar. 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. Örnek 3.1'de, verilen cümledeki A harfi için harf frekans hesaplaması görülmektedir:[4]

Frekans analizinin yapılabilmesi için uzun metinlere ihtiyaç duyulmaktadır. Uzun metinler, elde edilen verilerin güvenilir ve geçerli olmasını sağlamaktadır.[4]

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.[4]

3. 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.[4]

4. 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.[4]

5. 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 . [4]

2.4 Kriptolojinin tarihçesi

Kriptoloji yunancada gizli anlamına gelen κρυπτός (kriptos) ve yazı anlamında kullanılan γράφειν (grafein) sözcüklerinden oluşuyor (Konheim, 1981). Tarihini incelediğimizde çeşitli kaynaklardan edinilen bilgiler şifreleme işlemlerinin eskilere, miladdan önceki tarihe dayandığını gösteriyor. Önemli bilgilerin ortaya çıkması (askeri sırlar vs) ve bu bilgileri korumaya alma gereksinimi neticede kriptolojinin temel örneklerini ortaya çıkardı. O dönemlerde yalnızca askeri ve haberleşme alanında kullanılmasına rağmen teknoloji devriminin gelmesiyle büyük güvenlik sorunları ortaya çıktı ve bu da kriptografinin önemini çok fazla artırdı. Zamanımızda kriptoloji güvenlik acısından vazgeçilmeyecek şekilde kullanılmaktadır.

Eski zamanlarda kullanılan şifreleme sistemlerinin bir kısmı alfabedeki harfleri belli bir sayı ile ifade ederek oluşturuluyordu, örnek olarak en çok bilinenleri İbrani- Süryani, Grek ve Latin harf-sayı sistemidir. Daha sonra sözü geçen harf-sayı sistemi Arap alfabesine uygulanarak "Ebcet hesabı" adlandırılan bir sistem yapılmıştır. Ebcet hesabında, harflerin her birine 1'den 1000'e kadar sayısal değerler verilmiştir. İlk 9 harfe 1-9, ikinci harfe 10-90'a kadar onluk değerler, üçüncü 9 harfe 100-900'e kadar yüzlük değerler ve sonuncu harfe 1000 değeri verilmiştir. (Çimen, Akleylek, & Akyıldız, 2007).

Eski Yunan tarihçisi Heredotus'un yazdığına göre M.Ö. 480 yılında Yunanlar ve Persler arasındakı savaşta Stenografi (Yunanca "gizlenmiş yazı") adı verilen teknik kullanılmıştır. İranda yaşayan Yunanlı, kölelerinden birinin saçlarını kazıtarak yunanlara karşı düzenlenmiş Pers istilası planını onun kafası üzerine yazarak saçları uzadıktan sonra Atina'ya gönderiyor ve yunanlar kölenin saçlarını keserek haberi okuyorlar. Bu haber sayesinde İranlıların planına karşı hazırlanan Yunanlılar savaşı kazanıyorlar (Çimen, Akleylek, & Akyıldız, 2007), (Kahn, 1967).

M.Ö. 5. yüzyılın başlarında askeri amaçla kullanılan ilk şifreleme sistemi yunanlıların skytale adı verdikleri bir kriptografik cihaz olmuştur. Şifreleme işlemini yapmak için bir sopa ve uzun bir papirüs gerekmekte idi. Papirüsü silindirik sopanın üzerine sardıktan sonra şifrelenecek mesaj uzununa sopanın üzerine yazılıyordu. Papirüs açıldıktan sonar ise üzerinde şifrelenmiş anlamsız metin oluşuyordu. Şifreçözme işlemini yapmak için de aynı ölçüde bir sopa gerekiyordu. Sopanın azıcık farklı olması doğru mesaja ulaşmanı engelliyordu. Mesajı okumak isteyen kişi papirüsü aynı ölçütte sopanın üzerine sardıktan sonra anlamlı metine ulaşıyordu (Şen, 2006), (Nicholas, 2015), (Simon, 2001).

Skytaleden sonra Yunanlar tarafından (M.Ö. 205-123) tasarlanan şifreleme sistemi tarih sayfalarında yerini bulmuş Polybius'un dama tahtası şifrelemesi olmuştur. Polybius'un şifreleme sisteminde alfabe olarak Yunan ve Roma alfabesi kullanılıyordu. Sistem 5x5'lik matristen oluşuyordu ve her harfe iki sayı karşılık geliyordu. Sayılardan birincisi satırı, ikincisi sütunu göstermekteydi (Çimen, Akleylek, & Akyıldız, 2007).

Diğer önemli gelişmelerden biri M.Ö. 60-50 yılları arasında haberleşme amacıyla askeri alanda kullanılan Büyük Roma İmparatoru Julius Caesar (Sezar)'a ait şifreleme sistemidir. Sezar, komutanları ile iletişimi sağlamak için Sezar şifrelemesi olarak adlandırılan şifreleme sistemini kullanıyordu. Bu şifreleme sistemi ile her hangi bir metni şifrelemek için harf değiştirme işlemi yapılıyordu. (Sulak, Turan, & Demiröz, 2013), (Nicholas, 2015). Bu sistem ileride daha detaylı incelenecektir.

İlk şifre çözme işlemlerini Arap filozofu Al- Kindi yazdığı "Kriptografik Mesajların Deşifresi" (Risâle fi'stihrâci'l-mu'ammâ) isimli yazısında araştırmıştır. Al-Kindi araştırma

yaptığı bu yazıda kriptanaliz araştırmalarının temelini koymuş, frekans analizi kavramını ortaya atmıştır. Çalışması İstanbul'da, Süleymaniye Osmanlı Arşivi'nde bulunmaktadır. Al-Kindi'nin araştırdığı frekans analizine göre şifre metinin yazıldığı dil bilindikten sonra aynı dilde yazılmış yeteri kadar uzun bir metindeki harflerin kullanım sıklığına bakıldığında en çok kullanılan harf şifre metindeki en çok kullanılan harfe denk gelmekteydi. Bu araştırma tekniği ile Al-Kindi tek alfabeli şifreleme sistemlerini güvensiz hale getirmiştir ve şifreleme sistemleri için yeni dönem başlamıştır. Tek alfabeli sistemler güvensiz hale geldiğinden kriptograflar çok alfabeli şifreleme sistemleri geliştirmeyi düşünmeye başlamışlardır (Şen, 2006), (Ülkü, 2014), (Çimen, Akleylek, & Akyıldız, 2007).

İlk Çok alfabeli şifreleme sistemini Leon Alberti (1404-1472) 1466-1467 yıllarında harf kaydırma tekniğini kullanarak geliştirmiştir. Harf kaydırma işlemi Alberti diski ile yapılan bu sistemde harflerin kaydırılma miktarı kullanıcının isteğine göre belirlenmekteydi. Bu diskin iç çemberi sabit, dış çemberi ise hareket ettirilebilir ve harflerin değişik miktarda ötelenmiş hali görülebilirdi (Ülkü, 2014), (Nicholas, 2015).

Yeni çok alfabeli şifrelerin geliştirilmesine bakılmaksızın onlar uzun yıllar güvenliği koruyamıyordu ve güvensiz hale geliyordu. İlk uzun zaman kırılmayan çok alfabeli şifreleme sistemi 1553 yılında Giovan Batista Belaso adlı bir İtalyan kriptograf tarafından geliştirilmiştir. 1586 yılında Blaise De Vigenere bu sistemi biraz daha geliştirerek uzun zaman kırılmayan ve Vigenére Şifresi adlandırılan yeni bir şifreleme sistemi geliştirdi. Bu şifreleme sistemi tek alfabeli şifreleme sistemlerinden çok farklı idi ve bu sisteme frekans analizini uygulamak mümkün değildi. Bu sistemle düz metindeki her harf için farklı alfabe oluşturularak şifreleme işlemi yapılıyordu. Şifre alfabeler anahtar kelimeye göre seçildiğinden düz metindeki aynı sözler için şifre metinde farklı sözler karşılık geliyordu ve böylece frekans analizi ile bu sorunu çözmek mümkün olmuyordu. Vigenere bu şifreyi keşfetmekle çok güvenilir ve uzun yıllar kırılmayan bir şifreleme sistemi geliştirmişti. Bu sistem iki yüz yıldan fazla kırılmaz bir sistem olarak kaldı. 18. yüzyılın sonlarında Vigenre şifresi Babbage ve Kasiski tarafından kırıldı ve güvenilirliğini yitirdi. Bu analizislerin dikkatini çeken belirli bir döngüden (anahtar kelimedeki harf sayı) sonra aynı şifre alfabenin kullanılması olmuştur (Ülkü, 2014), (Nicholas, 2015), (Kahn, 1967).

1790.yılda Tomas Jefferson “Jefferson Diski” adı verilen yeni bir şifreleme sistemi oluşturdu. İngiliz alfabesi 26 harften oluştuğundan dolayı Jefforson Diski harflerin rastgele yer alıdığı 26 diskten ibaret idi. Disk üzerinde anahtar kelime ve şifremetin yazıldıkdan sonra disk karıştırılıyordu ve çok anlamsız hale gelen şifremetin oluşmuş oluyordu. Düzmetine ulaşmak isteğen kişi diskin aynısı üzerinde anahtar kelimeni oluşturduktan sonra düzmetine ulaşıyordu. Şifremetin ve anahtar kelme düşman eline geçtiğinde de düzmetine ulaşmak için şifreleme yapılan diskin aynısını kullanması gerekmeyteydi. Böylece her disk diğerinden farklı olduğu için gönderilen haber alıcıya güvenli şekilde ulaştırılıyordu (Nicholas, 2015), (Çimen, Akleylek, & Akyıldız, 2007).

1854 yılında Charles Wheatstone ve Baron Lyon Playfair 5x5 lik bir matris kullanarak Wheatstone-Playfair şifresi’ni tasarlıyorlar. İngiliz alfabesi için tasarlanan bu sistemde 25 hücre olduğu için İ ve J harfleri bir arada ve her hücreye bir harf gelmekle alfabenin tüm harfleri hücrelere giriliyor. İngilizlerin askeri alanda kullandıkları Playfair şifreleme sistemi 1900’lü yılların başlarına kadar güvenliğini sağlasa da sonrasında harf ikililerinin frekans dağılımı kullanılarak deşifre edilmiştir (Çimen, Akleylek, & Akyıldız, 2007).

Tarihte şifreleme sistemlerinin güvenliğinden ve praktikliğinden ilk defe Hollandali kriptograf Auguste Kerskhoffs 1883 yılında yayınladığı “La Cryptographie Militarie” makalesinde bahs etmiştir. Yazısında bir şifreleme sisteminin anahtar sözcüğünden başka her şeyi bilinse bile güvenilirliğini sağlaması gerektiğini belirtmiştir. Bu makale yayınlandıktan sonra tasarlanan şifreleme sistemleri için aşağıda gösterilen Kerskhoff

Prensipleri ortaya konmuştur (Çimen, Akleylek, & Akyıldız, 2007).

* Sistem pratik ve matematiksel bir gerçekliğe dayanmalıdır.

* Sistemde kullanılan anahtarlar taraflar arasında kolayca, üçüncü kişinin değiştirmesine izin verilmeden değiştirilebilmelidir.

* Sistem telegraf uygulamasında kullanılabilmelidir.

* Sistemin kullanılabilmesi için fazla sayıda insana ihtiyaç duyulmamalıdır.

* Sistemin uygulaması ve anlaşılması kolay olmalıdır.

* Şifreleme sisteminin güvenliği, şifreleme algoritmasını gizli tutmaya dayanmamalıdır. Yani sistem hakkındaki her şey herkes tarafından bilinse bile güvenilirliğini korumalıdır. Güvenlik; yalnızca anahtarı gizli tutmaya dayanmalıdır (Çimen, Akleylek, & Akyıldız, 2007).

1800'lü yılların sonlarına doğru teknolojinin gelişmesi kriptolojinin önemini daha da artırmakta idi. O dönem teknolojisi için çok önemli bir gelişme olan İtalyan fizikçi Markoni'nin keşfettiği telsiz cihazı kablo kullanılmadan iller arası haberleşme imkânını sağlıyordu. Bu aletin keşfi askeri alan için savaşlarda haberleşmeyi kolaylaştırması bakımından çok önemli idi. Ancak bu alet haberleşmeyi kolaylaştırmasıyla beraber büyük güvenlik sorunları da getirdi. Telsizin her yana yayılma özelliği olduğundan düşmanın da mesaja ulaşma olasılığı ortaya çıkıyordu.

Telsizin bu zayıflığı bilginin güvenli bir sistemle şifrelenmesi ihtiyacını ortaya çıkardı. Yeni yöntemler arama ihtiyacı kriptografinin gelişimine de katkıda bulunmuştur (Ülkü, 2014), (Çimen, Akleylek, & Akyıldız, 2007).

Birinci dünya savaşında telsizle güvenli haberleşmeyi sağlamak için kriptografların birçok yeni şifreleme sistemi geliştirmesine rağmen, bunların hepsi güvenliğini koruyamadı ve kırıldı. O dönemlerde almanlar tarafından kullanılan ve daha güvenli sayılan şifreleme sistemlerinden biri 1918 yılında tasarlanan ADFGVX sistemi idi. Buna karşılık Fransızların en ünlü kriptanalistlerinin almanların kırılmaz saydığı şifreleme sistemini çözmek için büyük çabaları vardı. Onlardan en ünlüsü sayılan George Painvin durmadan çalışarak kırılmaz sayılan bu şifreleme sistemini çözdü ve almanların telsizle haberleşdikleri büyük miktarda şifreli mesajları ele geçirip deşifre etti. Kriptanalistlerin bu önemli çalışmaları almanların yenilgisine sebep oldu (Simon, 2001).

1917'de İngiltereli kriptanalistlerin Almanya Dışişleri Bakanı Arthur Zimmermann'ın Meksika Başkanı'na çekmiş olduğu telgrafı deşifre etmesi Birinci Dünya Savaşını değiştiren bir kriptanaliz oldu. Almanların Avrupa güçlerini ele geçirerek savaşı kazanma planları vardı. Savaş zamanı almanların gizli planından habersiz olan ve ingilizlerin müttefiki sayılan Amerka savaşa katılmayacaktı. Ama almanların İngiltere üzerinden gönderdiği mesajları deşifre eden ingiliz kriptanalistler haberi Amerikanın o zamanki başkanı Woodrow Wilson'a duyurdular ve Amerika savaşa katılma kararı aldı. Tarihe "Zimmermann Telegrafı" ismiyle giren bu olay Birinci Dünya Savaşının seyrini değiştirdi (Nicholas, 2015), (Simon, 2001), (Çimen, Akleylek, & Akyıldız, 2007).

Birinci Dünya Savaşı zamanı kriptanalistler kriptograflardan daha etkili olduklarını gösterdiler ve savaşı kazandılar. O sırada ünlü kriptograflar yeni kırılmaz ve dayanıklı bir güvenlik sistemi geliştirmek için çok çaba harcıyorlardı. 1917 yılında Amerikalı mühendis Gilbert Vernam, Vernam şifrelemesi adıyla tanınan yeni bir şifreleme tekniği geliştirdi. Vernam şifreleme sisteminde şifreleme adımları Vigenere şifrelemesine benzemekteydi. Vernam şifrelemesinin avantajı anahtarın düzmetinle aynı uzunlukda olması idi. Vigenere şifresinde yapılan Kriptanaliz işlemleri bu sistem için geçerli olmamaktaydı. Vernam

Şifresine Kriptanaliz yapmak için önce şifrelemede kullanılan anahtardaki harfleri doğru bulmak gerekiyordu. Anahtar uzun olduğundan dolayı zor bir anahtar seçildiği takdirde bu şifreleme sistemi kırılmaz bir güvenliğe sahip oluyordu (Nicholas, 2015), (Çimen, Akleylek, & Akyıldız, 2007).

Kağıt-kalemle yapılan şifreleme sistemlerinin Birinci Dünya Savaşı zamanı güvenilirliğini sağlayamamasının ardından bir çok devlet şifrelemenin artık makinalarla yapılması gerektiğini düşündüler. 1918 yılında alman mühendis Arthur Scherbius makinalarla şifrelemenin temelini koydu ve şifresinin kırılmayacağını düşündüğü Enigma adlı makinayı tasarladı. O dönem için makina fiyatının çok yüsek olduğundan alıcılar tarafından iyi karşılanmadı.

Makinasının beklenen ilgiyi görmemesinin ardından Scherbius Alman ordusuyla anlaşma kararı aldı. İngilizlere ait bir belgeyi Alman ordusuna sunduktan sonra 1926 yılında makinalarını onlara satmaya başladı. 1943 yılında ingilizler ilk elektron bilgisayar sayılan Colossus adı verdikleri şifre çözme makinasıyla Enigmayı çözmeyi başardılar. Daha sonra Enigmanın şifrelediği mesajları çözmek için şu anda kullanılan bilgisayarların temeli sayılan Eniac'ı yaptılar (Simon, 2001), (Çimen, Akleylek, & Akyıldız, 2007).

1929 yılında Leste Hill çok alfabeli şifreleme sisteminin daha pratik hali olan Hill şifresini tasarladı. Bu sistemde, Claude Shannon'un 1949 yılında öne sürdüğü "güvenli bir şifreleme sistemi karıştırma işlemini iyi yapmalıdır" fikri sağlanmıştır. Bu sistemde her harfin bir sayı karşılığı vardır ve şifrelenecek metin alt gruplara bölünerek seçilmiş anahtar matrisleriyle şifreleniyor. Sonradan Leste Hill ortağıyla beraber 6x6'lık bloklarla Hill şifresini uygulayabilen yeni bir makine geliştirmiştir, ancak bu makine ilgiyle karşılanmamış ve çok fazla talep görmemiştir (Ülkü, 2014), (Çimen, Akleylek, & Akyıldız, 2007).

Harflerin bitlerle ifade edildiği ilk modern kriptografi 1970 yılında IBM labaratuvarında önceler Demon adı verilen, sonraki zamanlarda Lucifer adı verilen 64 bitlik anahtarlı yeni şifreleme sistemi geliştirildi. Bu sistem 1975 yılında Amerika'da Birleşik Bilgi İşleme Standardı olarak seçilmiştir (Ülkü, 2014), (Çimen, Akleylek, & Akyıldız, 2007).

1973 yılında elektronik haberleşmenin yaygınlaşması ile Amerika Milli Standartlar Bürosu Herkes tarafından kullanabilecek bir şifreleme sistemine ihtiyaç duyulduğunu ilan etmiştir. Yeni tasarlanacak algoritmanın adı da büro tarafından "Veri Şifreleme Standardı (Data Encrypt System(DES))" olarak belirlenmişti (Ülkü, 2014), (Çimen, Akleylek, & Akyıldız, 2007).

1975 yılında yayınlanan DES algoritması, 1976 yılında Veri Şifreleme Standardı olarak kabul edildi. DES algoritması Feistel yapısı aracılığıyla Shannon'un karıştırma önerisinin özelliklerini sağlamaktadır. Vernam şifresinden başlayarak tasarlanan yeni modern şifreleme sistemlerinde bilgisayar aracılığıyla harflerin bitlerle şifrelenmesi işlemi kullanılmaya başlandı. DES algoritması ikilik tabandakı bir düzmetni 64 bitlik bloklar halinde parçalayıp 56 bitlik anahtarla şifreleme yapıyor. Anahtarın gizliliği ve rastgele seçilmesi bu sistemin güvenilirliğini sağlıyor. Şifreleme anahtarını elde edebilen kişi rahatlıkla şifre çözme anahtarını da elde ederek düzmetine ulaşması mümkündür. DES algoritmasının Shannon'un yayılma ve karıştırma özelliğini sağlaması onun en önemli tarafıdır. Karıştırma işlemi her anahtar için düzmetin ve şifremetin arasında istatistiksel bağlantı olmamasını sağlar. DES için bu özellikler güvenlik açısından çok önemlidir (Ülkü, 2014), (Simon, 2001).

1976 yılında alıcı ve gönderici arasında anahtar paylaşımı işleminin daha kolay bir şekilde yapılması için Whitfield Diffie ve Martin Hellman yeni bir algoritma yaptılar. Diffie-Hellman anahtar değişim algoritması, sayılar teorisi yardımıyla şifrelemede açık anahtarın

kullanılabileceğini kanıtlamış ve böylece açık anahtarlı kriptografinin temelini koymuşlar. Bununla da anahtar paylaşımı zorunluğu ortadan kalkmış ve bu algoritmayla şifreleme yapan kişiler kendilerine ait özel anahtarlarını kullanmışlar (Ülkü, 2014), (Nicholas, 2015), (Simon, 2001).

Diffie-Hellman anahtar değişim algoritmasının tasarlanmasından sonra artık şifrelemede herkes kendi özel anahtarını kullana bilicekti. Bu gelişme kriptografları daha da çok çalışmaya ve yeni açık anahtarlı bir şifreleme algoritması tasarlamaya sevk ediyordu. 1977 yılında Ronald Rivest, Adi Shamir ve Leonard Adleman, RSA (Rivest-Shamir-Adleman) adı verdikleri açık anahtarlı bir şifreleme algoritması tasarladılar. RSA algoritması Diffie-Hellman anahtar değişimini içeren ilk şifreleme sistemi oldu. Bu algoritma matematikte zor problemlerden sayılan çarpanlara ayırma problemine dayanarak tasarlanmıştır (Nicholas, 2015), (Çimen, Akleylek, & Akyıldız, 2007).

Günümüzde de kullanılan RSA şifreleme sistemi kullanılmaya başladığı dönemlerde uygulanması kolay ve kırılması zor olmasına bakılmaksızın güvenlik açısından daha da karmaşıklaştırılıyordu. Bit uzunluğunun 128 bitten 512 bite çıkması büyük bir matematiksel hesaplama işlemi gerektiriyordu. RSA'nın bu zayıf yönlerini göze alan kriptograflar yeni açık anahtarlı şifreleme sistemi tasarlamağı düşünüyorlardı. 1985 yılında Neal Koblitz ve Victor S. Miller tarafından tasarlanan Elliptik Eğri algoritması RSA'ya göre daha az bit kullandığından hızlıydı ve en az RSA kadar güvenliğe sahipti (Çimen, Akleylek, & Akyıldız, 2007).

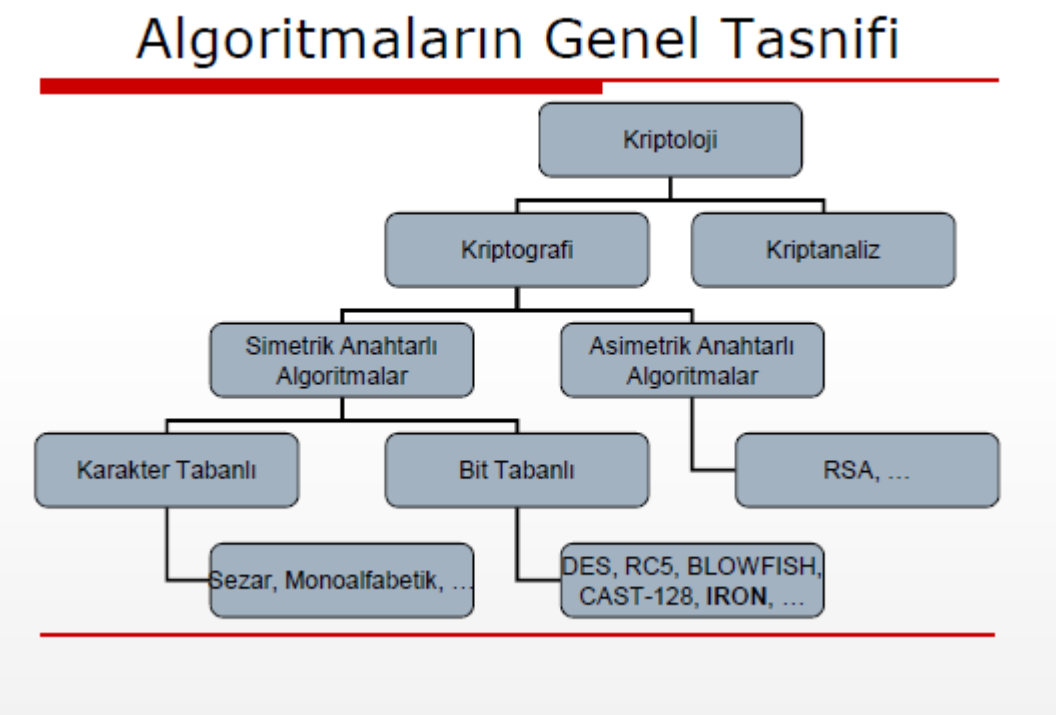
1990 yıllarında DES ve ona benzer yapıdakı şifreleme sistemlerinin güvenliği sona ermiştir. Kriptanalistlerin yeni geliştirdikleri Linear ve Differensial Kriptanaliz yapıları bu sistemlerin bazı anahtarların kullanımında güvensiz olduklarını kanıtlamıştır (Çimen, Akleylek, & Akyıldız, 2007).

1997 tarihinde Amerka Ulusal Standardlar ve Teknoloji Enstititüsü yeni bir Gelişmiş Şifreleme Standartı (AES) yarışması ile DES'in yerini alacak yeni şifreleme sistemi seçeceğini duyurmuştur. 2000 yılında yapılan başvurular arasından diğerlerinden daha güvenilir ve hızlı olan, iki Belçikalı kriptograf Joan Daemen ve Vincent Rijmen'in tasarladığı AES algoritması seçilmiştir. AES algoritması şimdiye kadar güvenliğini korumakta ve kullanılmaktadır (Çimen, Akleylek, & Akyıldız, 2007).

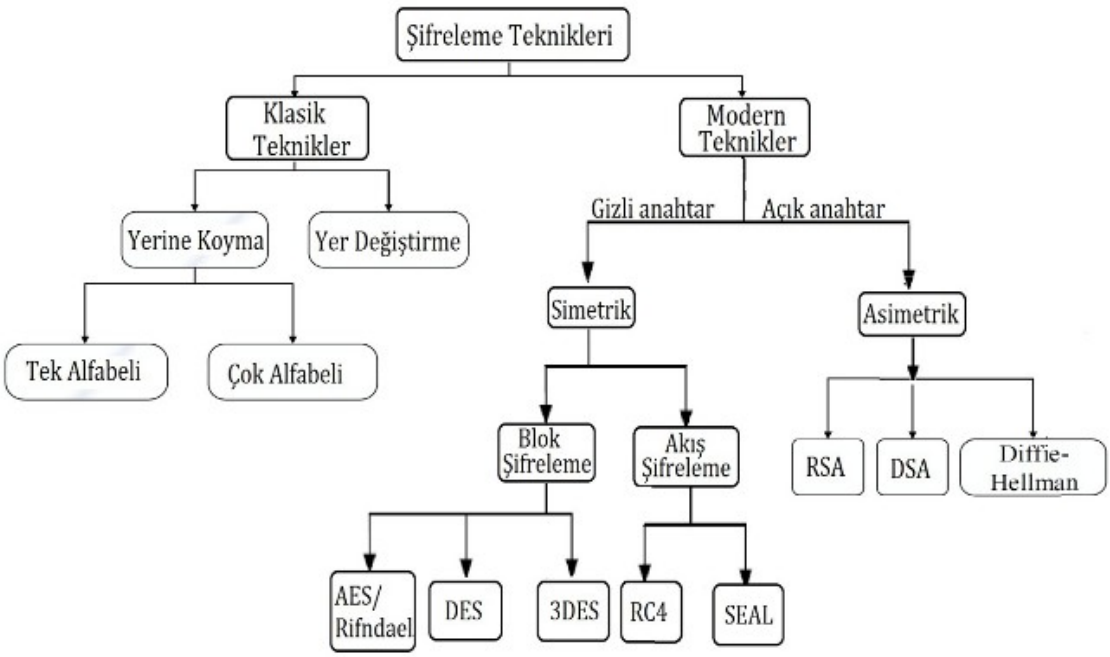
Kriptolojiyle ilgili yapılan ilk konfrans bilim adamları tarafından 1981 yılında California Santa Barbara Üniversitesi'nde CRYPTO 81 adı altında gerçekleşmiştir. Bu konfransla beraber ilk defa 1982 yılında Almanya'da düzenlenen EUROCRYPT, ilk defa 1990 yılında Avusturalya'da düzenlenen ASIACRYPT, ilk defa 2000 yılında Hindistan'da düzenlenen INDOCRYPT isimli konferanslarda her sene gerçekleştirilmektedir. Bunlardan başka 2005 yılında ODTÜ Uygulamalı Matematik Enstitüsünde düzenlenmesine başlanılmış Ulusal Kriptoloji Sempozyumu da her yıl gerçekleştirilmektedir (Çimen, Akleylek, & Akyıldız, 2007).

Dünyada kriptografi alanında eğitim ve araştırmaya yönelik ilk ders kitapları 1987 yılında çıkmıştır (Ülkü, 2014).[3]

3.1 Şifreleme Algoritmalarının Genel Sınıflandırması



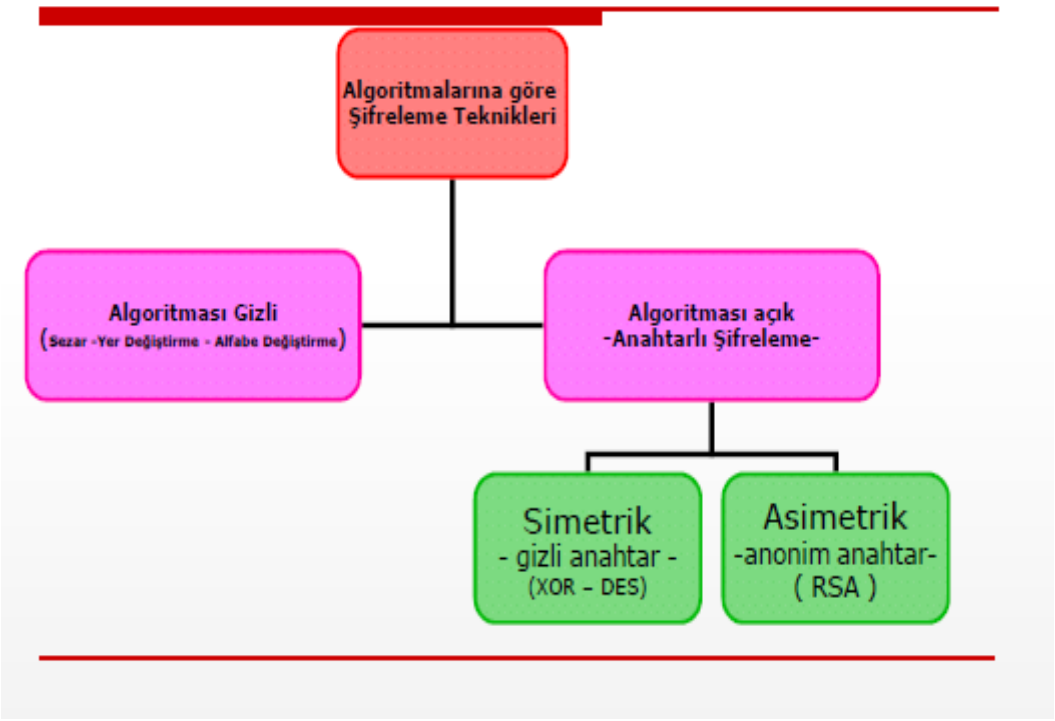
Şekil 3.1 [5]



Şekil : 3.2 [3]

3.2 Şifreleme Algoritmalarının Sınıflandırma kriterleri

1. Algoritmanın gizliliği/açıklığı



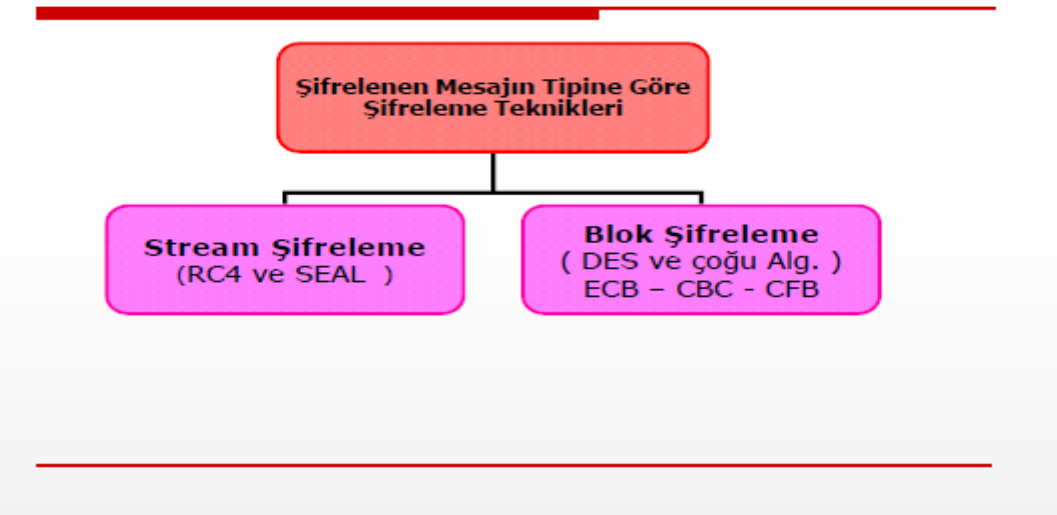
Şekil 3.3 [5]

2. Anahtar Uzunluğu / Sayısı

Anahtar Uzunluğu	Sayı Değeri	10^6 şifre/s	10^9 şifre/s	10^{12}şifre/s
32 bit	~$4x10^9$	36 dak	2.16 s	2.16 ms
40 bit	~10^{12}	6 gün	9 dak	1 s
56 bit	~$7.2x10^{16}$	1142 yıl	1 yıl 2 ay	10 saat
64 bit	$1.8x10^{19}$	292 000 yıl	292 yıl	3.5 ay
128 bit	$1.7x10^{38}$	$5.4x10^{24}$ yıl	$5.4x10^{21}$ yıl	$5.4x10^{18}$ yıl

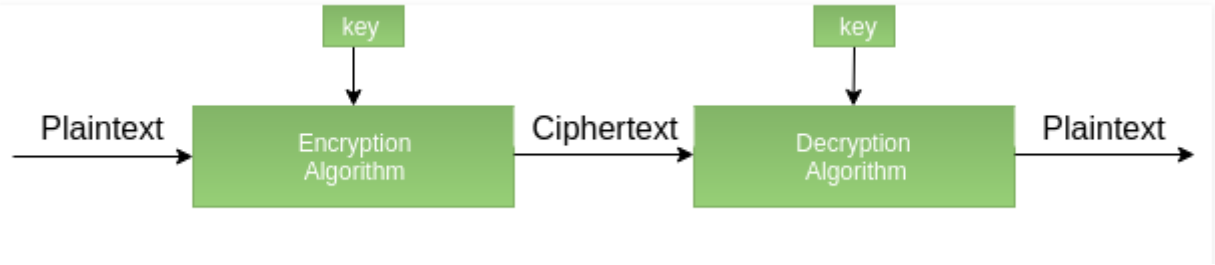
Şekil : 3.4 [5]

3. Şifrelenen mesajın tipi



Şekil 3.5 [5]

4.1 Temel Kriptoloji Terimleri ve Şifreleme Akış Diyagramı



Şekil : 4.1 [5]

Plain Text (Düz Metin) **:** Şifrelenecek mesaj

Encryption (Şifreleme) **:** Veriyi, alıcının dışında kimsenin anlamayacağı şekilde kodlamaktır.

Chipher Text (Şifreli Metin) : Şifrelenmiş mesaja denir.

Decryption (Şifre Çözme) **:** Şifreli metinin düz metine dönüştürülmesi işlemidir.

Şifreleme Algoritması **:** Veriyi şifrelerken ya da çözerken kullanılan matematiksel metodtur.

Key (Anahtar) **:** Şifreleme-çözme işleminde kullanılan değeridir. [5]

5.1 Sezar Şifreleme (Caesar's cipher) Nedir ?

M.Ö. 60-50 yılları arasında haberleşme amacıyla askeri alanda kullanılan Büyük Roma İmparatoru Julius Caesar (Sezar)'a ait şifreleme sistemidir.

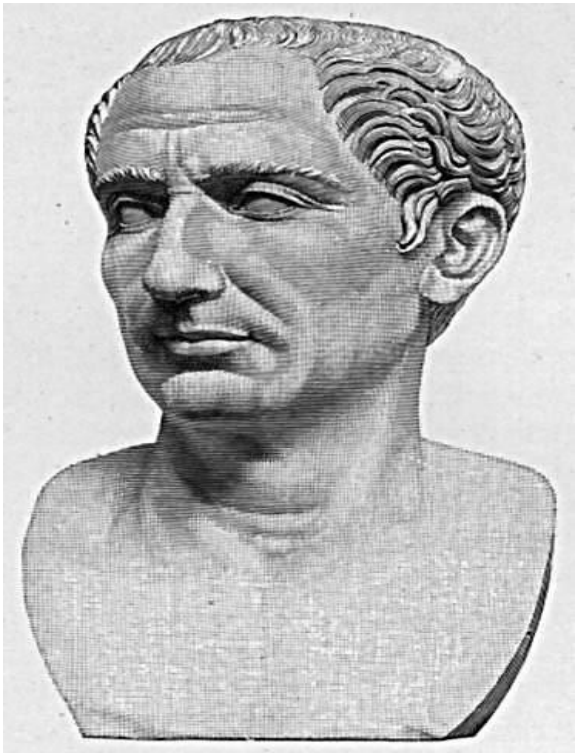
Sezar, komutanları ile iletişimi sağlamak için Sezar şifrelemesi olarak adlandırılan şifreleme sistemini kullanıyordu. Bu şifreleme sistemi ile her hangi bir metni şifrelemek için harf değiştirme işlemi yapılıyordu.

Her harf düz alfabenin üç harf sola kaydırılmasından oluşan şifre alfabedeki karşılığıyla, yani kendisinden sonrakı üçüncü harfle değiştiriliyordu. Şifrelenmiş metni alan kişi şifre çözme işlemini yapmak için şifre metindeki her harfi alfabe sayının üç eksiği kadar sola kaydırdıktan sonra düz alfabedeki aynı yerde duran harfi almaktaydı. Böylece şifre çözme işlemi de kolaylıkla yapılabiliyordu (Sulak, Turan, & Demiröz, 2013), (Nicholas, 2015).

Bunun dışında,

* 19. yüzyılda bazı gazetelerde kişisel reklamlar bölümü , bu yöntemle şifrelenmiş mesajların alışverişinde kullanılmıştır. Kahn (1967),

* The Times'daki Caesar şifresiyle şifrelenmiş gizli mesajlar, aşıkların iletişimi için kullanılmıştır. * 1915 gibi yakın bir tarihte bile, Sezar şifresi kullanımdaydı: Rus ordusu, askerlerine için çok zor ve karmaşık şifrelerin öğretecek zaman bulamadığında bu yöntem onların yerine geçti; Alman ve Avusturyalı kriptanalistler mesajlarının şifresini çözmede çok zorlanmadılar. ([1])



Sezar şifresi, adını Devlet adamı ve general **Gaius Julius Caesar** (M.Ö. 100-44))' dan almaktadır. [1]

Kodu şifrelemek veya şifresini çözmek için bir Caesar şifresiyle dönen iki disk kullanılabilir. [1]

5.2 Sezar Şifreleme (Caesar's cipher) Algoritması

Sezar şifreleme tekniğinde, alfabedeki harflerin sıra numaraları, bir anahtar oranında karakter sola kaydırılarak yeni alfabe oluşturulur. Bu teknik tek alfabeli şifreleme tekniğidir ve ötelenme şifreleme tekniği olarak da bilinmektedir (Ülkü, 2014) (Başar, 2004).

Matematiksel olarak şifreleme (Encryption);

$$E_n(x) = (x + n) \mod 26.$$

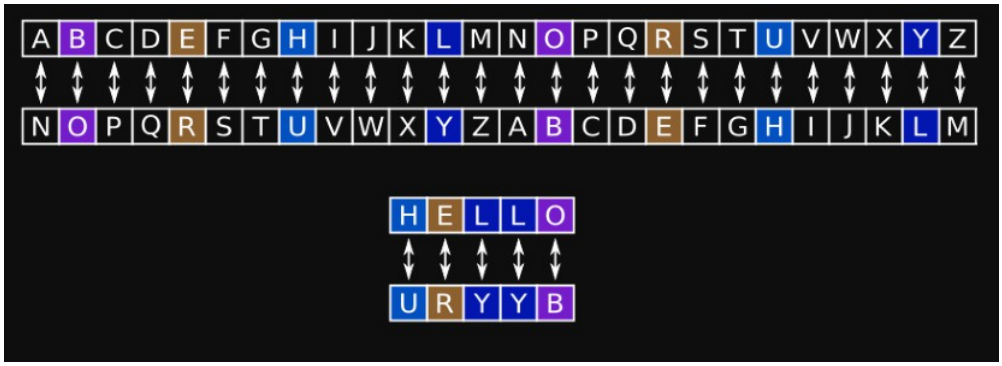
Şekil : 5.1 [1]

Matematiksel olarak Şifre Çözme (Decryption);

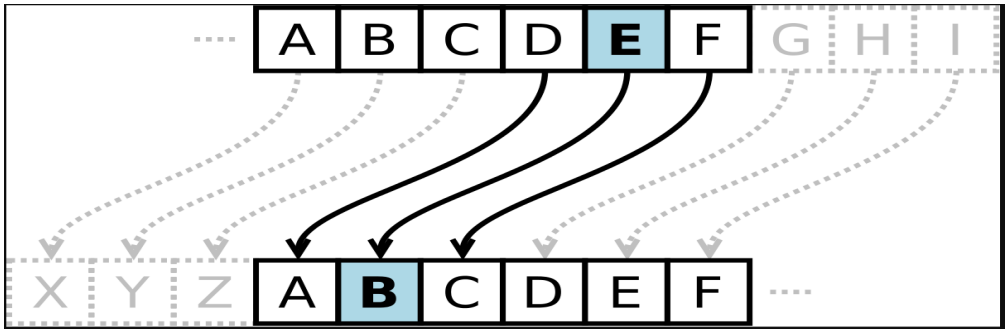
$$D_n(x) = (x - n) \mod 26.$$

Şekil : 5.2 [1]

şeklindedir. Burada x, düz metindeki harfin düz alfabedeki sıra numarasıdır. n harflerin kaydırılma miktarıdır. Ek: (Şifrelenmiş metindeki harflerin düz alfabedeki sıra numarasıdır. 26 ise İngiliz alfabesindeki toplam harf sayısından gelmektedir. Türkçe alfabe için uygulanırsa bu sayı 29 olarak kullanılmalıdır (Ülkü, 2014)).

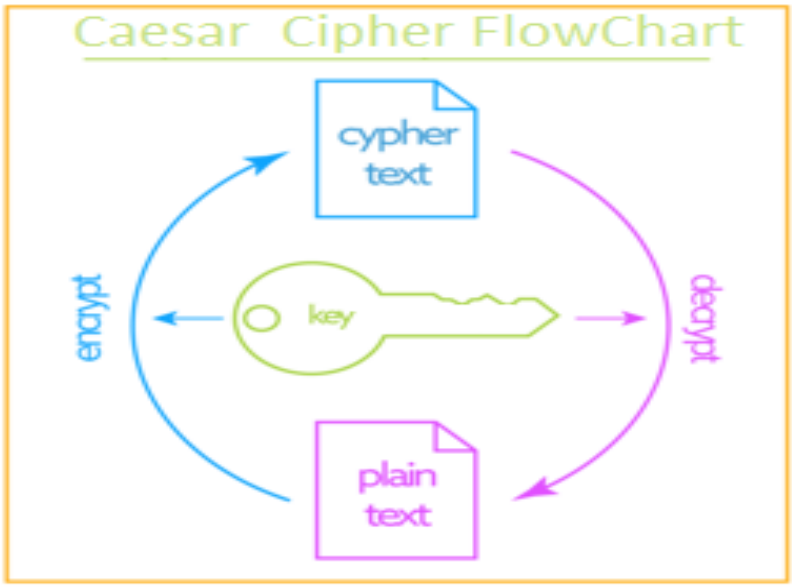


Şekil : 5.3

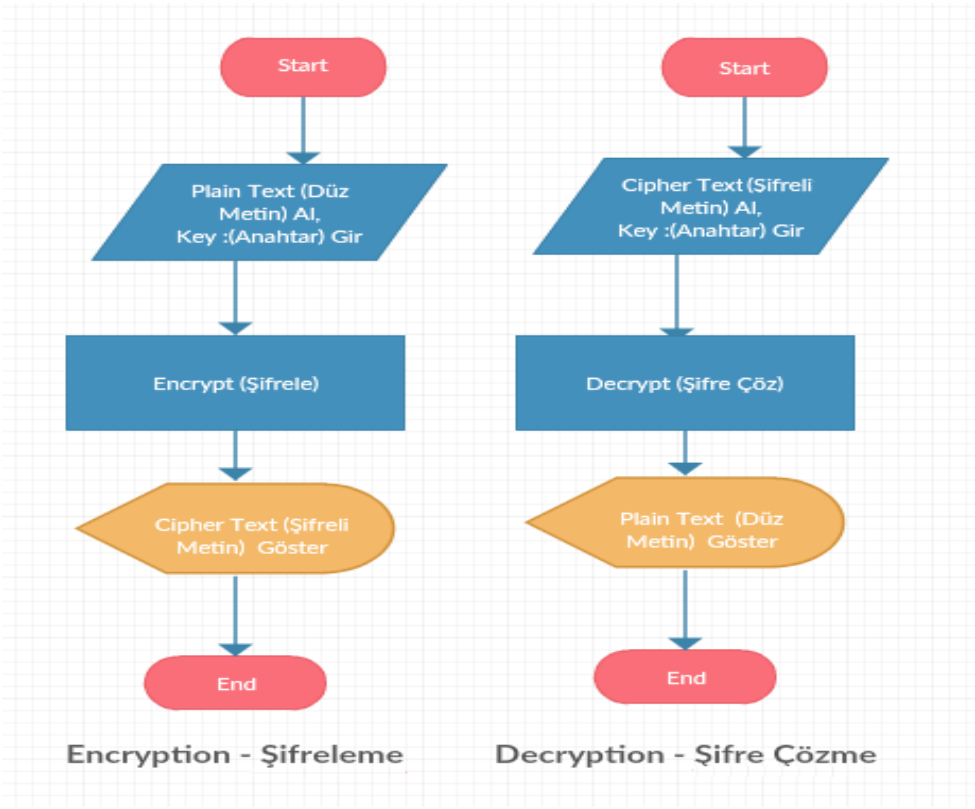


Şekil : 5.4 [1]

5.3 Sezar Şifreleme (Caesar's cipher) Akış Diyagramı - FlowChart



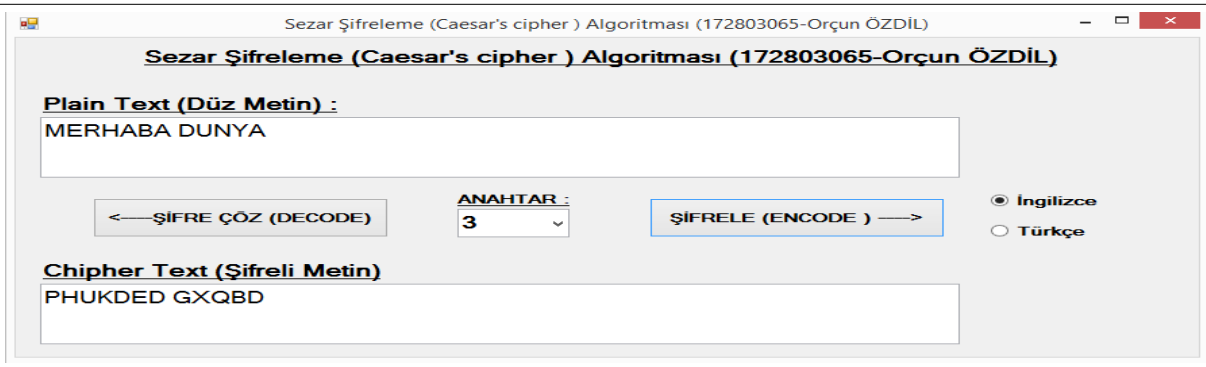
Şekil : 5.5



Şekil : 5.6

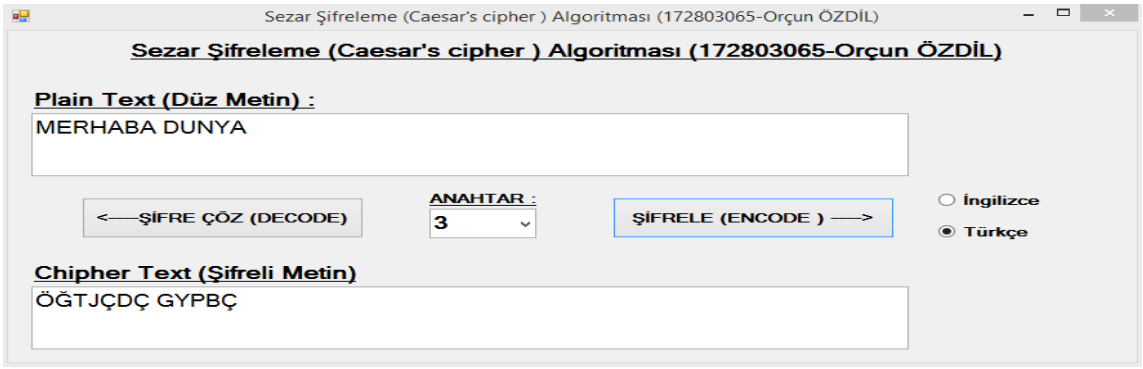
6.1 C# ile Sezar Şifreleme (Caesar's cipher) Uygulaması

6.1.1. Encryption – Şifreleme



Şekil : 6.1 İngiliz alfabesi ile bir şifreleme örneği (x=26):

MERHABA DUNYA --> PHUKDED GXQBD
ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC



Şekil : 6.2 Türk alfabesi ile bir şifreleme örneği (x=29) :

MERHABA DUNYA --> ÖĞTJÇDÇ GYPBÇ
ABCÇDEFGĞHIİJKLMNOÖPRSŞTUÜVYZ
ÇDEFGĞHIİJKLMNOÖPRSŞTUÜVYZABC

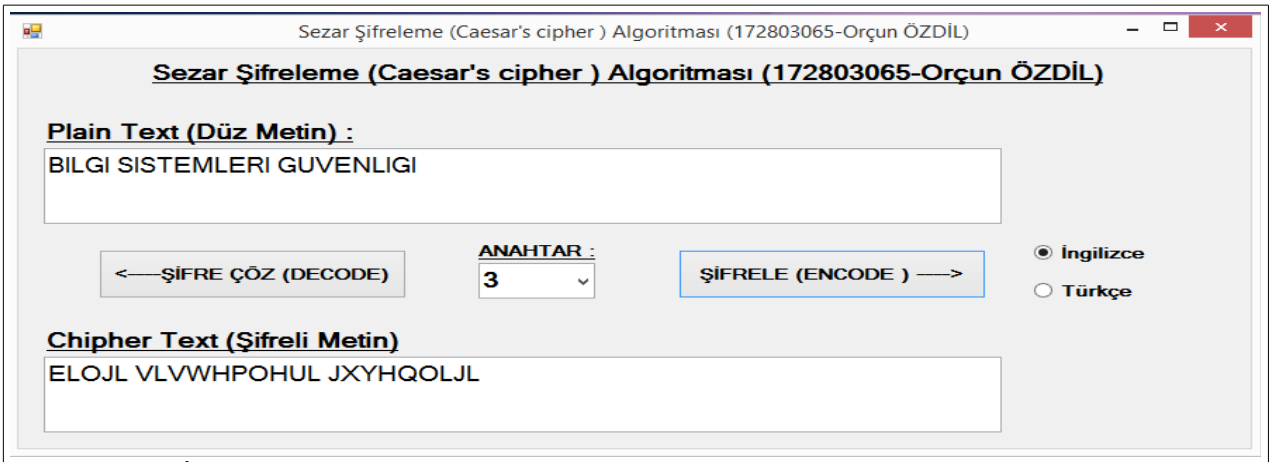
```
private string EncodeCeasar(string plainText)
{

    string chipherText = "";//Şifreli metin
    foreach (char c in plainText)//Düz metin içinde dolaşıyoruz
    {
        int index = alphabet.IndexOf(c);
        if (index >= 0)
        {
            int newindex = (index + Key) % alphabetLen;
            chipherText += alphabet[newindex];//harfin yeni değerini atıyoruz
        }
        else
        {
            chipherText += c;
        }
    }
    return chipherText;
}
```

Şekil : 6.3

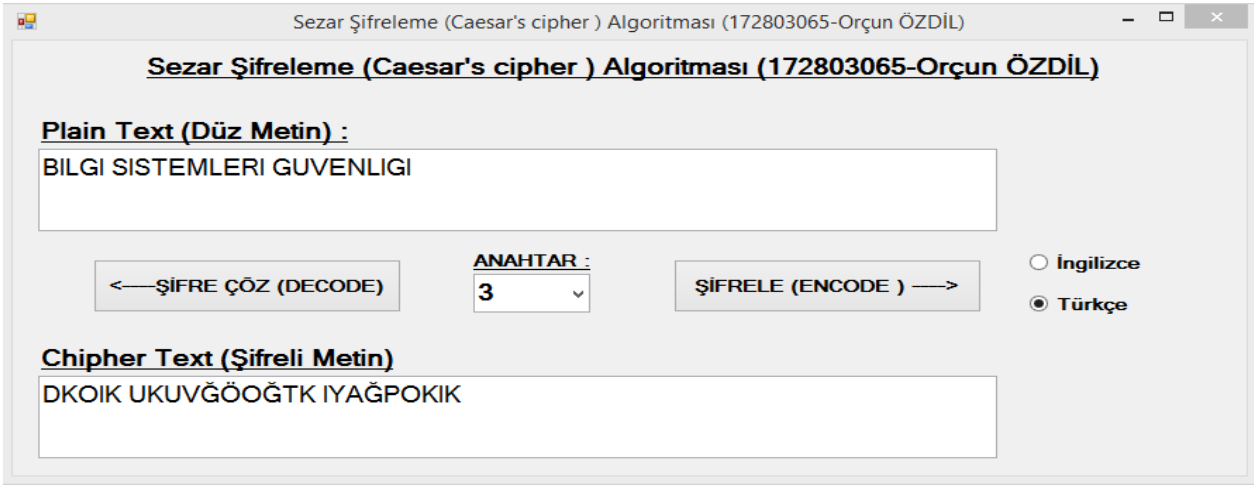
C# Kodu

6.1.2. Decryption – Şifre Çözme



Şekil : 6.4 İngiliz alfabesi ile bir şifre çözme örneği (x=26):

ELOJL VLVWHPOHUL JXYHQOLJL --> BILGI SISTEMLERI GUVENLIGI



Şekil : 6.5 Türk alfabesi ile bir şifre çözme örneği (x=29) :

DKOIK UKUVĞÖOĞTK IYAĞPOKIK --> BILGI SISTEMLERI GUVENLIGI

```
private string DecodeCeasar(string chipherText)
{
    string plainText = ""; //Düz metin
    foreach (char c in chipherText)//Şifreli metin içinde dolaşıyoruz
    {
        int index = alphabet.IndexOf(c);
        if (index >= 0)
        {
            int newindex = (index - Key + alphabetLen) % alphabetLen;
            plainText += alphabet[newindex];//harfin yeni değerini atıyoruz
        }
        else
        {
            plainText += c;
        }

    }
    return plainText;
}
```

Şekil : 6.6

C# Kodu

7.1 Sezar Şifreleme (Caesar's cipher) Uygulamasına Kriptoanaliz Yöntemlerinin Uygulanması

7.1.1. BruteForce:

Elimizdeki Şifreli metine, Sezar Şifrelenmesi uygulandığı bildiğimiz bir durumda, şifreli metine brute force uyguluyoruz. Yani alfabedeki tüm harf olasılıklarını deniyoruz.

1. Önce bir şifreli metin oluşturalım:

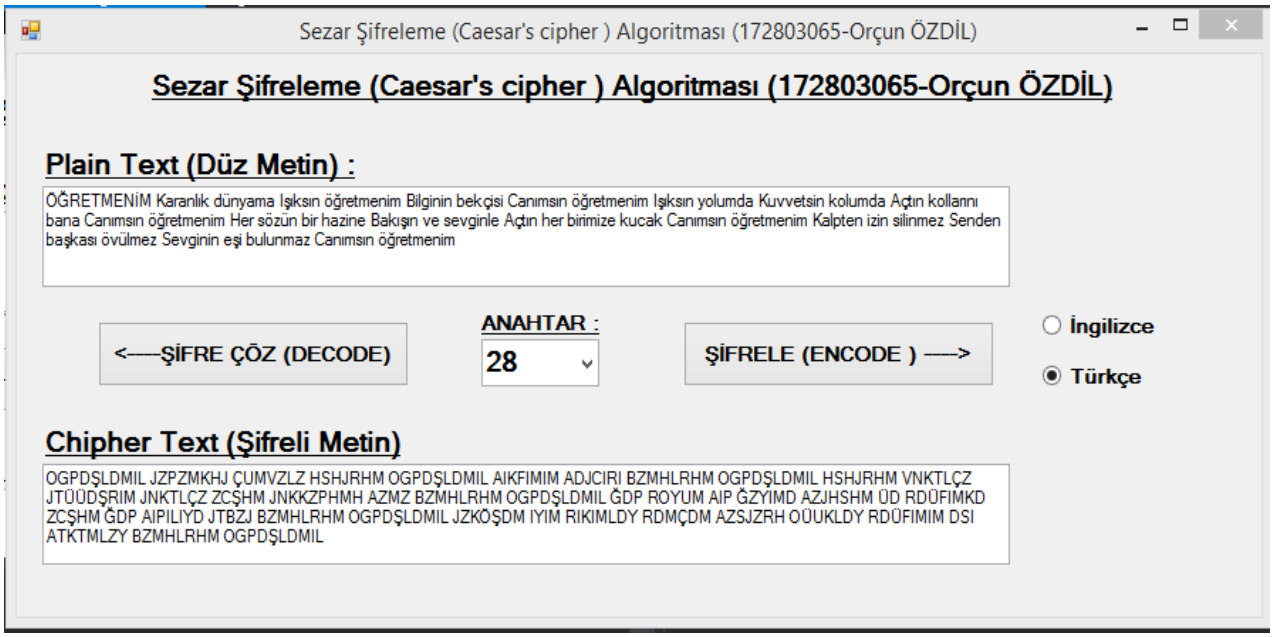
"Öğretmenim" adlı şiiri **anahtar=28** olacak şekilde şifreliyoruz:

Orjinal Metin:

ÖĞRETMENİM Karanlık dünyama Işıksın öğretmenim Bilginin bekçisi Canımsın öğretmenim Işıksın yolumda Kuvvetsin kolumda Açtın kollarını bana Canımsın öğretmenim Her sözün bir hazine Bakışın ve sevginle Açtın her birimize kucak Canımsın öğretmenim Kalpten izin silinmez Senden başkası övülmez Sevginin eşi bulunmaz Canımsın öğretmenim

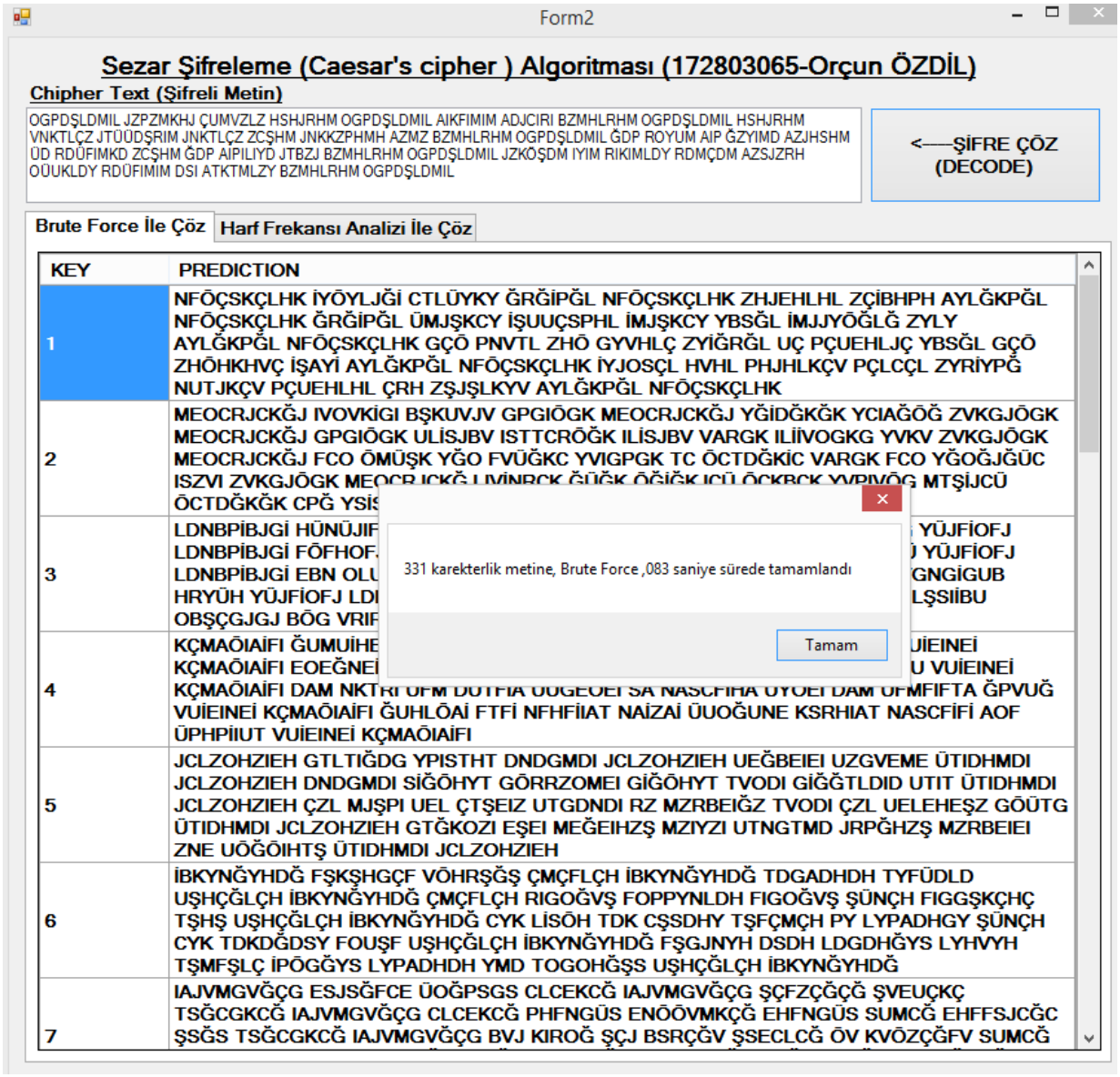
Şifreli Metin:

OGPDŞLDMIL JZPZMKHJ ÇUMVZLZ HSHJRHM OGPDŞLDMIL AIKFIMIM ADJCIRI BZMHLRHM OGPDŞLDMIL HSHJRHM VNKTLÇZ JTÜÜDŞRIM JNKTLÇZ ZCŞHM JNKKZPHMH AZMZ BZMHLRHM OGPDŞLDMIL ĞDP ROYUM AIP ĞZYIMD AZJHSHM ÜD RDÜFIMKD ZCŞHM ĞDP AIPILIYD JTBZJ BZMHLRHM OGPDŞLDMIL JZKÖŞDM IYIM RIKIMLDY RDMÇDM AZSJZRH OÜUKLDY RDÜFIMIM DSI ATKTMLZY BZMHLRHM OGPDŞLDMIL



Şekil : 7.1

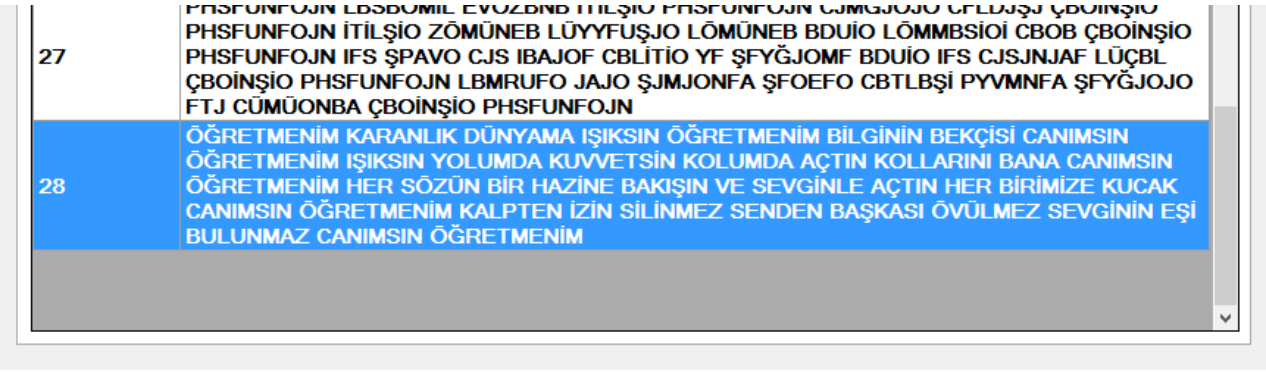
2. Şifreli Metine Brute Force uygulayalım:



Şekil : 7.2

Örnek Metine Brute Force uyguladık ve ortalama bir bilgisayar ile 331 karekterlik metin, 0,083 saniyede çözüldü. Tüm Olasılıkları bir grid üzerinde görüntüledik.

Şimdi sonuçlara bakarak anahtarımızın ne olduğunu bulalım.



Şekil : 7.3

28. satır bize doğru sonucu verdi. Buradan Anahtarın =28 olduğunu buluyoruz.

7.1.2 Harf frekans analizi (Letter Frequency Analysis) ile Tahmin:

Türk alfabesindeki harflerin kullanım sıklıkları:

en yüksek dereceye sahip olan yani en sık kullanılan harfler **A, E, I, N, R,**

üst-orta derecede olanlar **L, İ, D, K,**

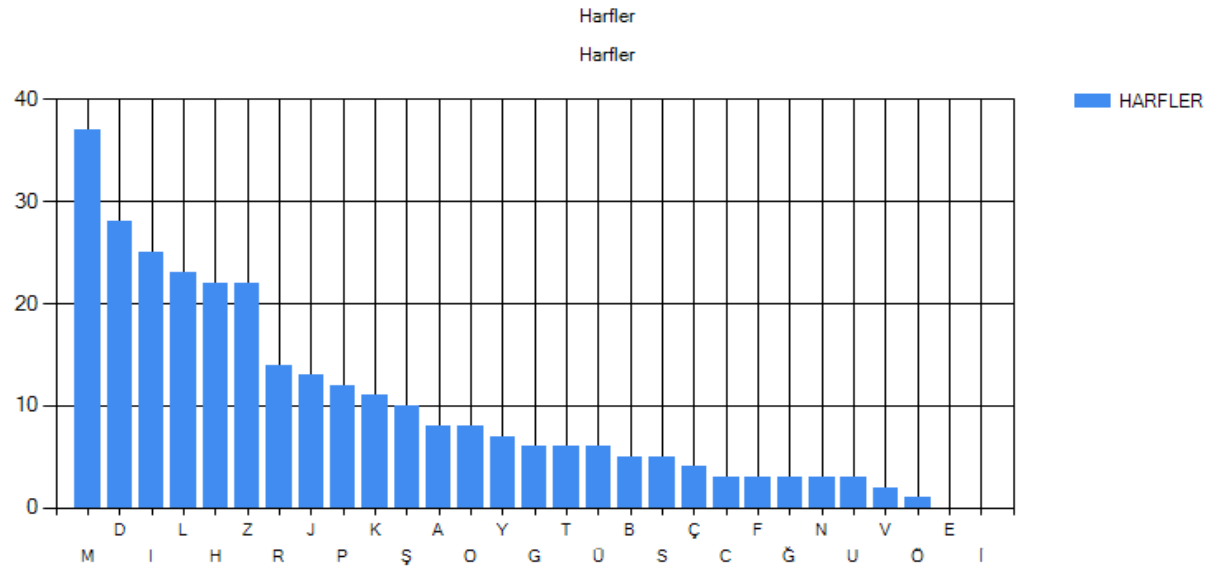
alt-orta derecede olanlar **M, U, Y, T, B, S,**

düşük dereceli olanlar **O, Ü, Ş, Z, G, Ç, H, Ğ, V, C, Ö, P, F, J`**dir.

Harf || Olasılık (%)	Harf || Olasılık (%)
A ~ 11,68	N ~ 7,23
B ~ 2,95	O ~ 2,45
C ~ 0,97	Ö > 0,87
Ç ~ 1,26	P ~ 0,79
D ~ 4,87	R ~ 6,95
E ~ 9,01	S ~ 2,95
F ~ 0,44	Ş ~ 1,94
G ~ 1,34	T ~ 3,09
Ğ ~ 1,13	U ~ 3,43
H ~ 1,14	Ü ~ 1,99
I ~ 8,27	V ~ 0,98
İ ~ 5,20	Y ~ 3,37
J ~ 0,01	Z ~ 1,50
K ~ 4,71	
L ~ 5,75	
M ~ 3,74	

Şekil : 7.4 (https://www.turkcebilgi.com/turk_alfabesindeki_harflerin_kullanim_sikliklari)

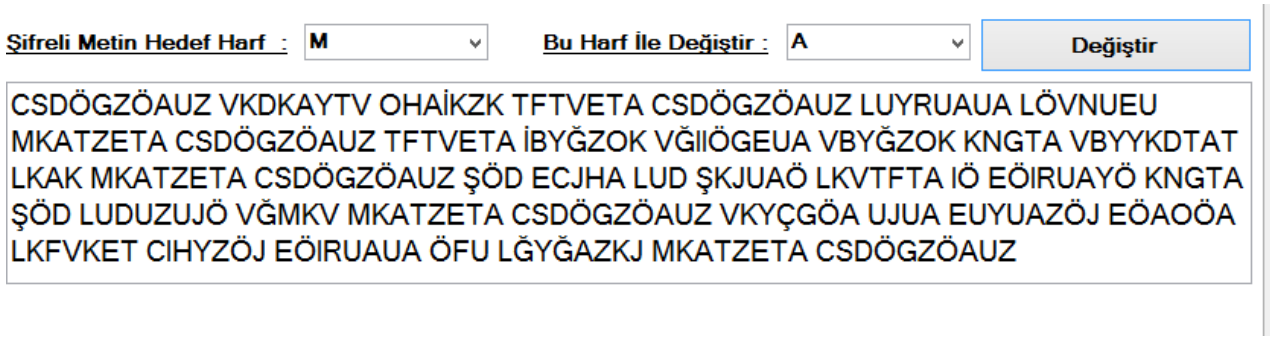
Örnek şifreli metinimizdeki harf dağılımını inceliyoruz:



Şekil : 7.5

Sonuç: En çok kullanılan ilk 3 harfimiz: M – D – I

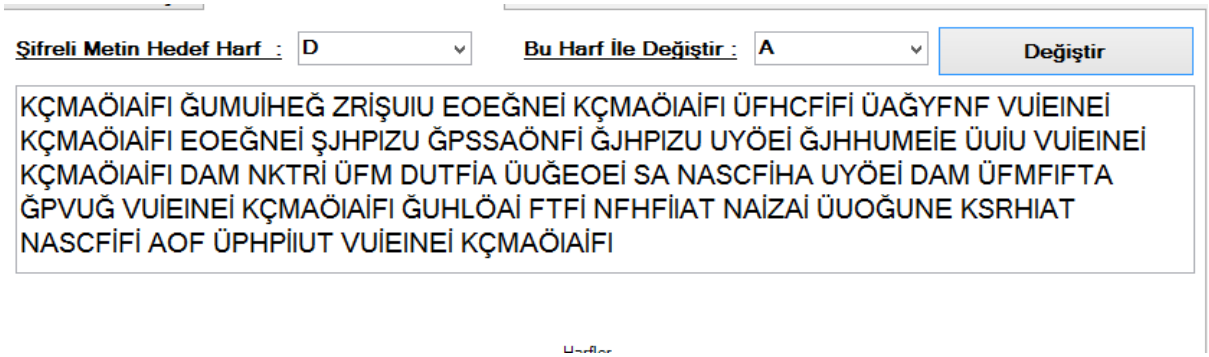
1.Harf olan “M” 'nin “A” olduğunu var sayarak deniyoruz.



Şekil : 7.6

Sonuç: Anlamlı bir sonuç elde edemedik

2.Harf olan “D” 'nin “A” olduğunu var sayarak deniyoruz.

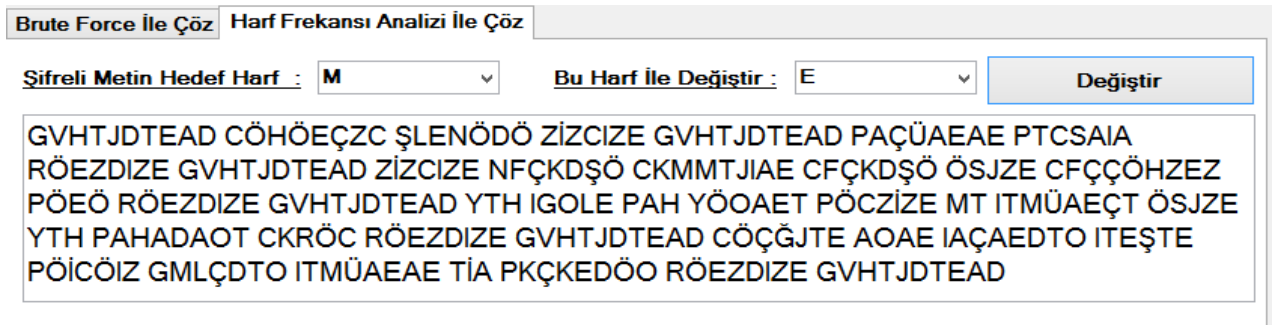


Şekil : 7.7

Sonuç: Anlamlı bir sonuç elde edemedik

---

1. Harf olan “M” 'nin “E” olduğunu var sayarak deniyoruz.

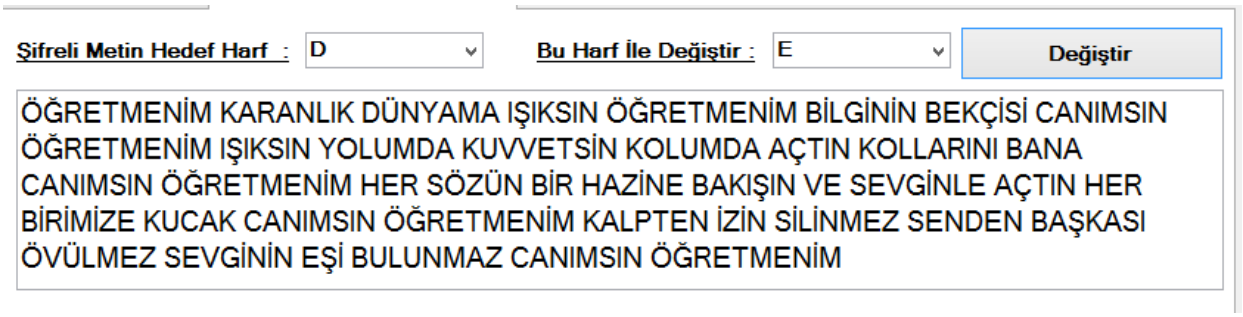


Şekil : 7.8

Sonuç: Anlamlı bir sonuç elde edemedik

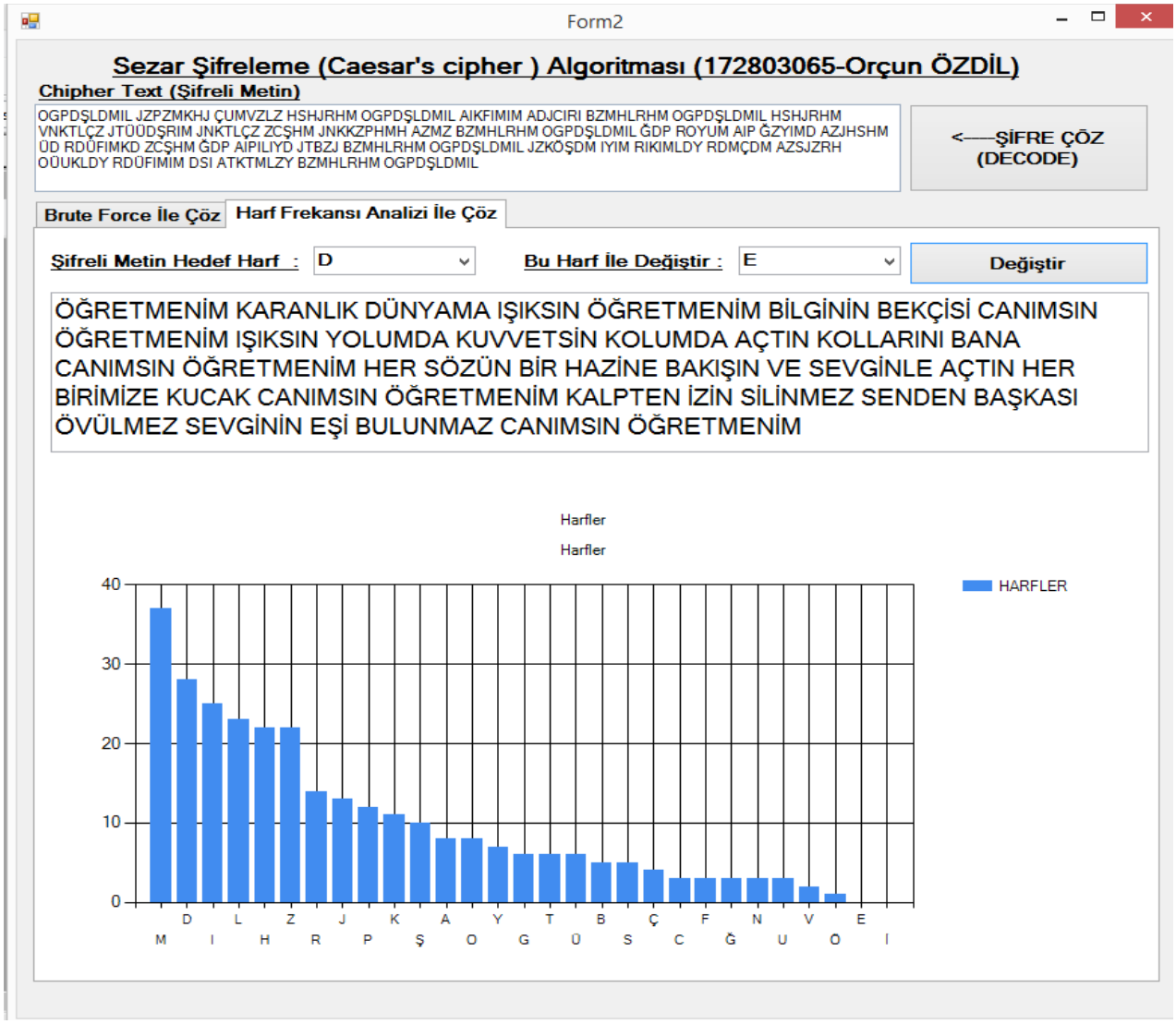
---

2. Harf olan “D” 'nin “E” olduğunu var sayarak deniyoruz.



Şekil : 7.9

Sonuç: 4. denemede sonuca ulaşıyoruz. Örneğimizde frekansı en yüksek ikinci harf olan “D”, dilimizdeki frekansı en yüksek ikini harf olan “E” ile eşleşti. Yani Orijinal metinde, E harfi D'ye donüşmüş. Anahtar=28.


Form2
Sezar Şifreleme (Caesar's cipher) Algoritması (172803065-Orçun ÖZDİL)
Chipher Text (Şifreli Metin)
OGPDŞLDMIL JZPZMKHJ ÇUMVZLZ HSHJRHM OGPDŞLDMIL AIKFIMIM ADJCIRI BZMHLRHM OGPDŞLDMIL HSHJRHM VNKTLÇZ JTÜÜDŞRIM JNKTLÇZ ZCŞHM JNKKZPHMH AZMZ BZMHLRHM OGPDŞLDMIL ĞDP ROYUM AIP ĞZYIMD AZJHSHM ÜD RDÜFIMKD ZCŞHM ĞDP AIPILIYD JTBZJ BZMHLRHM OGPDŞLDMIL JZKÖŞDM IYIM RIKIMLDY RDMÇDM AZSJZRH OÜUKLDY RDÜFIMIM DSI ATKTMLZY BZMHLRHM OGPDŞLDMIL
<—–ŞİFRE ÇÖZ (DECODE)
Brute Force İle Çöz
Harf Frekansı Analizi İle Çöz
Şifreli Metin Hedef Harf :
D
Bu Harf İle Değiştir :
E
Değiştir
ÖĞRETMENİM KARANLIK DÜNYAMA IŞIKSIN ÖĞRETMENİM BİLGİNİN BEKÇİSİ CANIMSIN ÖĞRETMENİM IŞIKSIN YOLUMDA KUVVETSİN KOLUMDA AÇTIN KOLLARINI BANA CANIMSIN ÖĞRETMENİM HER SÖZÜN BİR HAZİNE BAKIŞIN VE SEVGİNLE AÇTIN HER BİRİMİZE KUCAK CANIMSIN ÖĞRETMENİM KALPTEN İZİN SİLİNMEZ SENDEN BAŞKASI ÖVÜLMEZ SEVGİNİN EŞİ BULUNMAZ CANIMSIN ÖĞRETMENİM
Harfler
Harfler
HARFLER
40
30
20
10
0
D L Z J K A Y T B Ç F N V E
M I H R P Ş O G Ü S C Ğ U Ö I

Şekil : 7.10

SONUÇ

- Sezar Şifrelemesi ya da Sezar Kaydırma algoritmasının (Caesar Cipher-Shifter) zorluk derecesi, en fazla kullanılan alfabedeki harf sayısı kadar olmaktadır. Harf sayısının modu alındığından, daha yüksek rakamlar anlam ifade etmemektedir. (Örn: İngilizce alfabe için, anahtar=25 ile anahtar=129 aynı anlama gelmektedir. 129 Mod 26 ==25)

- Kullanılacak alfabeye küçük-büyük harf, boşluk ve noktalama işaretleri eklenerek, ihtimaller arttırılsa bile, ortalama bir bilgisayar ile saniyeler içerisinde kırılabilmektedir.

- Bu algoritma ile şifreli metine tekrar tekrar şifreleme uygulansa bile, ilave bir güvenlik veya çözülme zorluğu katmamaktadır. Sadece yeni bir anahtar-kayma oluşturmaktadır. (Örn: anahtar=2 ile şifrelenmiş bir metin, tekrar anahtar=3 ile şifrelenirse, 2+3=5 ,sadece anahtar=5 şifrelemesi- kayması uygulanmış olur.)

- Günümüz teknoloji ile oldukça basit çözülebilir, belki de ilkel görünse bile, kullanıldığı dönem için oldukça zekice ve kullanışlı bir algoritma olmuştur. Aynı zamanda daha sonra ortaya çıkan başka kaydırma algoritmalarına da (Örn:Vigenere Şifreleme) öncülük etmiştir.

- Araştırma Raporu Github Adresi : https://github.com/Oozdil/BilgiSistemleriGuvenligi

REFERANSLAR

[1] https://everipedia.org/wiki/lang_en/Caesar_cipher

[2] http://iibf.erciyes.edu.tr/guven/veri/bilgi_nedir.pdf

[3] SES ALGILAMA YÖNTEMİ İLE TEK KULLANIMLIK ANAHTAR (ONE TIME PAD) ÜRETİMİ YÜKSEK LİSANS TEZİ JABRAYİL HASANOV 2016

[4] Ulusal Bilgi Güvenliğine Yönelik Bir Kriptografi Algoritması Geliştirilmesi ve Harf Frekans Analizine Karşı Güvenirlik Tespiti - Aysun COŞKUN, Ülkü ÜLKER- 2016

[5] Şifreleme Algoritmalarının sınıflandırılması Dr.Mehmet Tektaş

[6] Bilgi Güvenliği ve Teknoloji - Dr.Hamdi Murat Yıldırım 2014

[7] Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication - International Journal of Computer Applications - Atish Jain- November 2015

[8] Multiple Ceaser Cipher Encryption Algorithm- Abdullateef Balogun -Abacus - December 2017