ONDOKUZ MAYIS ÜNİVERSİTESİ

Bilgisayar Mühendisliği Bölümü

Yüksek Lisans

Kriptografi Mühendisliğine Giriş Dersi

Klasik şifreleme sistemlerinin (Sezar, Vigenere, Hill cipher, one time pad, foursquare, playfair, ADFGVX, ROT13) ve bunların istatistiksel analizlerini yapan görsel ve eğitici program oluşturma

Öğrenci: Ersin Enes ERYILMAZ, 13210488

Danışman: Yrd. Doç Dr. Sedat AKLEYLEK

04.06.2014

İÇİNDEKİLER

ÖZET

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.[1]

Tarih boyunca gizlilik her zaman insanoğlunun ilgisini çekmiştir. Yazının icadından itibaren insanlar yazıyla haberleşmeye başlamış, ancak insanoğlunun karşı koyamadığı merakı yüzünden gönderilen mesajların gizlenmesi ihtiyacı ortaya çıkmıştır. Mesajı kafa derisine kazıma, harfleri değiştirip anlamsız metinlere dönüştürme gibi türlü yöntemler denenmiş ve sonucunda şifreleme icad edilmiştir.[2]

Klasik şifreleme yöntemleri genellikle kağıt kalem kullanarak gerçekleştirilebilen, çok karışık matematik temellere dayanmayan sistemlerdir. En gelişmiş örnekleri mekanik cihazlar olan klasik şifreleme yöntemleri, elektronik cihazların kullanılmaya başlanmasıyla beraber ortadan kalkmıştır.

Bu projede klasik şifreleme yöntemleri analiz edilerek, eğitici ve öğretici bir program oluşturulacaktır.

Anahtar Kelimeler: kriptografi, klasik, şifreleme, analiz, program, Sezar, Vigenere, Hill cipher, one time pad, foursquare, playfair, ADFGVX, ROT13

1.Giriş

a. Problem Tanımı

Klasik şifreleme yöntemleri olan Sezar, Vigenere, Hill cipher, one time pad, foursquare, playfair, ADFGVX, ROT13 sistemleri nelerdir ve bu sistemler nasıl analiz edilir çalışması yapmak ana problemimizdir.

b. Amaç

Projenin amacı; Klasik şifreleme yöntemlerinin .NET programlama dillerinden olan C# İle programlanması, program için ekran tasarımlarının yapılması, istatiksel analizlerinin yapılarak öğretici bir program oluşturulmasıdır. Aynı zamanda bu program ile üniversitelerde kriptografi dersleri ve klasik şifreleme sistemleri hakkında öğrencilere ve eğitim görevlilerine kaynak oluşturacak, öğrencilerin kendi projelerine referans sağlayacak, şifreleme sistemlerine merak duyan kişilere basit bir şekilde klasik şifreleme yöntemlerini öğretecektir.

c. Kapsam

Bu program klasik şifreleme yöntemleri için yerli kaynak arayanlara, öğrenci ve eğitimcilere rehberlik edecek; üniversite ve şifreleme yöntemleri ile ilgilenenlere kullanım sağlayacaktır.

Projenin paydaşları eğitim-öğretim görevlileri, yazılımcı ve geliştiriciler, öğrenciler ve kriptografi ile uğraşan kriptanalist ve kriptograflardır. Eğitim ve öğretim görevlileri derslerde öğrencilere klasik şifreleme yöntemlerini anlatırken uygulamalı gösterim için bu programı kullanabilir Ayrıca geliştiriciler için yeni yazılımlar oluştururken bir örnek olacaktır.

2.İlişkili çalışmalar

Klasik şifreleme yöntemleri bir takım matematiksel işlemler gerektirdiği ve proje danışmanı öğretim üyesinin önerdiği;

http://www.sagemath.org/doc/reference/cryptography/sage/crypto/classical.html web adresindeki örneklerden yararlanılmıştır. Aynı zamanda ilgili akademik makaleler ve internetteki örnekler araştırılmıştır.

3.Tasarım

Bir yazılımın kullanılabilir ve uygulanabilir olması için tasarımlar düzenli sıralı ve programlı olması gerekmektedir. Tasarımlarla ilgili bilgiler aşağıdadır.

a.Sistem tasarımı

Sistemin genel mimari tasarımı ile klasik şifreleme yöntemlerinin nasıl işlediği çözülebilmesi sağlanacaktır. Kullanıcı dostu olacak proje ile, uygulamaya metinler kullanıcı tarafından girilecektir.

b.Veri tasarımı

Klasik şifreleme sistemleri programında veriler arayüz sayesinde kullanıcılar tarafından girilebilecektir. Bu sayede etkileşimli bir yazılım yazılmış olacaktır.

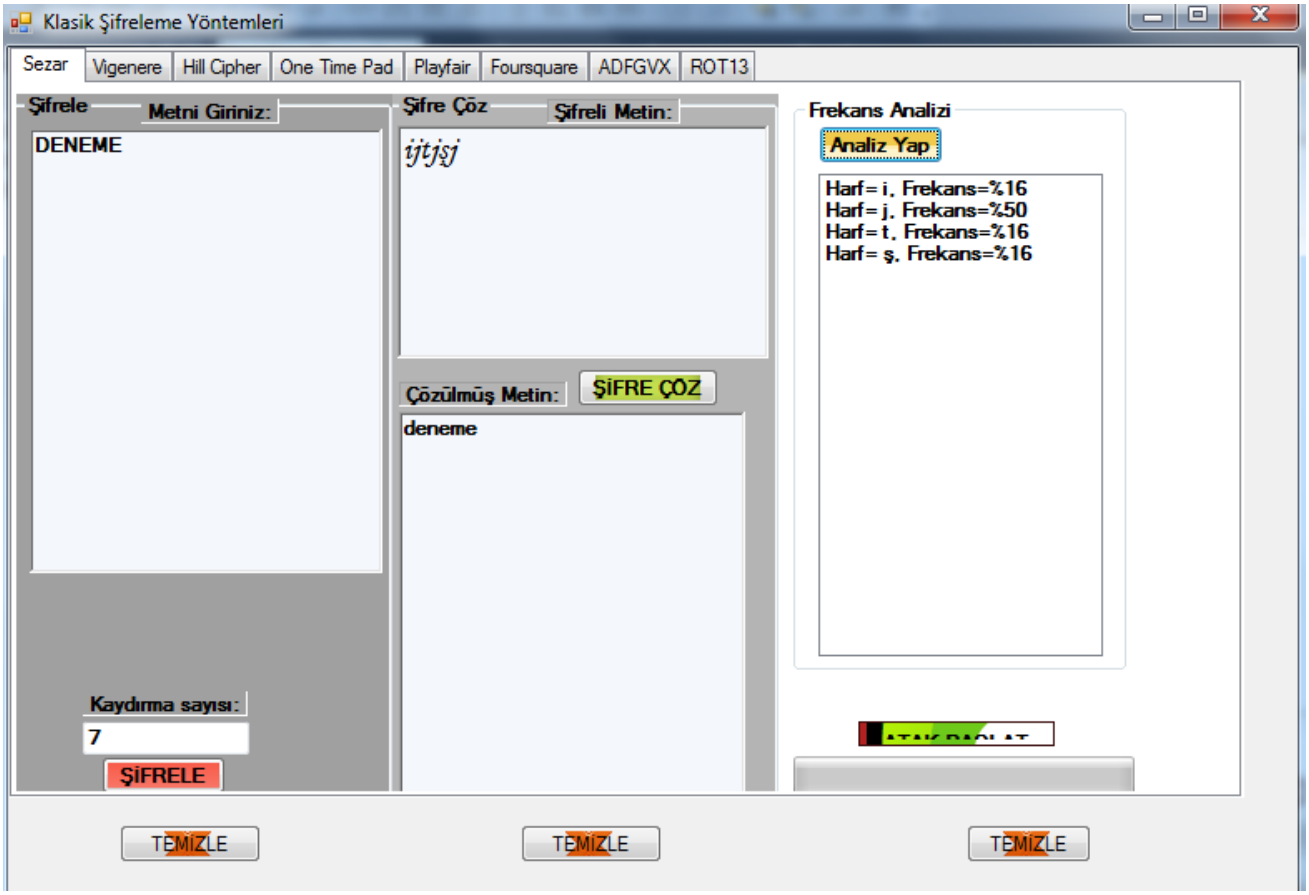
c.Arayüz tasarımı ve algoritmalar

Arayüz tasarımları ve algoritmalara hakkında bilgi aşağıdaki gibidir.

Sezar Algoritması

Algoritmanın orjinali metindeki her karakteri kendisinden sonra gelen n. harfle değiştirerek yeni bir metin oluşturmaktır. Burada n (kaydırma sayısı) harf ötelemeyi isteğinize göre değiştirebilirsiniz. [4]

Yeni oluşan metin şifrelenmiş metini oluşturur. Yöntem açık olduğundan şifrelenmiş metnin daha sonradan orjinaline çevirmek yani şifreyi çözmek mümkündür. Zamanında da dönemin savaşlarında mesajların güvenliği bu şekilde sağlanmıştır.

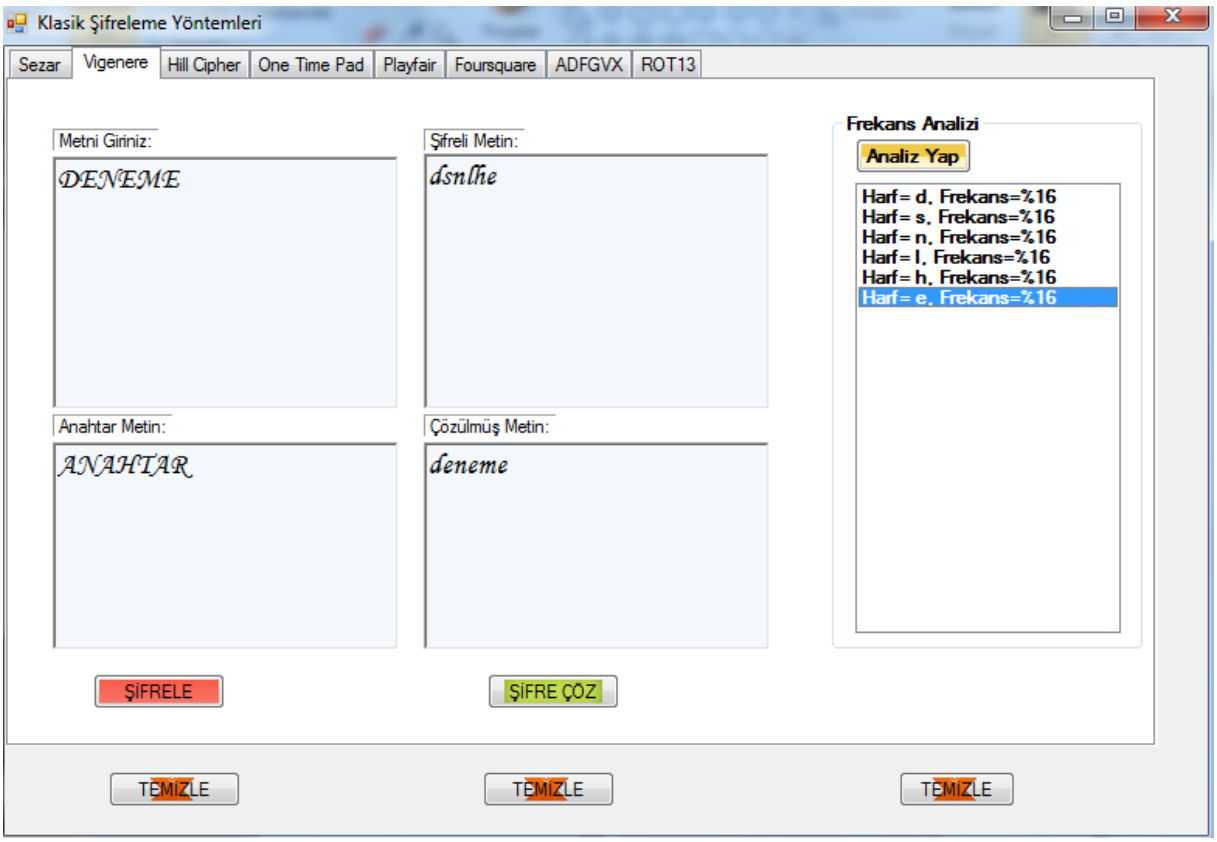


Sezar şifreleme yöntemi ile girilen metin istenilen kadar kaydırılabilir. Örnek metinde Düz metin olarak *Deneme* kelimesi girilmiştir. Kaydırma sayısı olarak 7 seçilmiştir. Ve şifrelimetin olarak *ijtjşj* elde edilmiştir. ŞİFREÇÖZ butonu ile algoritma tersten çalıştırılarak düzmetne ulaşılmıştır. Frekans analizi ile şifreli metinde bulunan harflerin kullanım sıklığı hesaplanmıştır. Sezar şifrelemede düzmetnin büyük veya küçük harf girilmesi fark etmemektedir. Rakam ve Noktalama işaretleri şifrelenmemektedir.

Vigenere

Vigenère şifrelemesi uzun zaman güvenilir bir şifreleme algoritması olarak biliniyordu („Le Chiffre indéchiffrable“, Türkçede: „deşifre edilemeyen şifre“).[5] Seçilen bir anahtar kelime şifreleme için kullanılacak alfabe sayısını belirliyor. Her kullanılan alfabede harfler Sezar şifrelemesinde olduğu gibi alfabedeki sırasından bir sonraki harf ile değiştiriliyor.

İlk olarak 1854 yılında İngiliz matematikçi Charles Babbage Vigenère şifrelemesi çözmeyi başardı. Bu buluşunu hiç açıklamaması üzerine Prus albay Friedrich Kasiski 1863 yılında kendi deşifreleme yöntemini açıklayarak bu yöntemin tanınmasını sağladı.



Vigenere şifreleme yöntemi ile girilen metin anahtar metin kadar kaydırılabilir. Örnek metinde Düz metin olarak *Deneme* kelimesi girilmiştir. Anahtar metin olarak *ANAHTAR* kelimesi seçilmiştir. Ve şifrelimetin olarak *dsnlhe* elde edilmiştir. ŞİFREÇÖZ butonu ile algoritma tersten çalıştırılarak düzmetne ulaşılmıştır. Frekans analizi ile şifreli metinde bulunan harflerin kullanım sıklığı hesaplanmıştır. Vigenere şifrelemede düzmetnin büyük veya küçük harf girilmesi fark etmemektedir. Rakam ve Noktalama işaretleri şifrelenmemektedir.

Hill Cipher

Hill şifreleme yöntemi bir blok şifreleme örneğidir. Blok şifrelemeyi de şöyle ifade edebiliriz. Düz metni bitişik ve aynı uzunluktaki bloklara bölme, her bloğu şifreleyerek şifreli metin bloklarına dönüştürme ve bu şifreli blokları şifreli metin çıktısı olarak gruplamaktır. Hill şifreleme yöntemi Lester Hill tarafından bulunmuş ve 1929 yılında yayınlanmıştır.[6]

Örnek:

Bir mesajı Hill yöntemi ile belli bir düzen içinde şifrelememiz gerekir. Öncelikle mesajın göndericisi ve alıcısı bir anahtar nxn lik A matrisi üzerinde anlaşmış olmalılardır. Bu A matrisini seçerken dikkat etmemiz gereken bir özellik ise MOD26 ya göre terslenebilen bir matris olmasıdır. Düz metin n uzunluğundaki bloklar şeklinde şifrelenir. Aşağıdaki örnekte A 2x2 lik bir matris ve mesajımız 2 karakterli bloklar halinde şifrelenecektir.

Anahtar Matrisimiz: $A= \begin{bmatrix} 3 & 25 \\ 24 & 17 \end{bmatrix}$

Mesajımız: MISSISIPI

Öncelikle bloklara bölelim. Bu sayede mesajımız MI-SS-IS-SI-PP-I halini alır.

İlk bloğumuz MI dir. Bu seferde bloğumuzdaki karakterlerin harf tablosundaki yerine göre aldığı değerlerden oluşan matrisimizi oluşturalım. M->12, I->8 olduğundan

$\begin{bmatrix} 12 \\ 8 \end{bmatrix}$dir

Gönderenin hesaplaması gereken ise

$$A\begin{bmatrix} 12 \\ 8 \end{bmatrix} = \begin{bmatrix} 2 \\ 8 \end{bmatrix} \text{(mod26) dir}$$

Bu işlem yapıldığında ilk iki karakterin şifreli karşılığı 2 ile 8 olacaktır. Bu değerlerin alfabetik karşılığınada bakıldığında CI çıktısını elde etmiş oluruz.

Bu işlemi düz metnimizdeki her bloğa uygularsak

Düz Metin: MI-SS-IS-SI-PP-IK

Şifreli Metin: CI-KK-GE-UW-ER-OY

Düz metnimizde son bloğa K eklememizin sebebi. Son bloğun uzunluğunu da 2 yapmaktır.

Hill yönteminin en önemli özelliğini de burada görmüş oluruz. S veya P nin yan yana kullanımında S->K olmuş sonradan ise S->E ve S->U olmuştur. Dolayısıyla Hill yöntemi ile düz metindeki karakterleri maskeleyebiliriz.

Şifre Çözümü (Deşifrelenmesi) :

Mesajın deşifrelenmesi için öncelikle anahtar matrisimiz olan A matrisinin tersi hesaplanmalıdır.

$$\mathbf{A^{-1} = det(A)^{-1}} \begin{bmatrix} \mathbf{d} & \mathbf{-b} \\ \mathbf{-c} & \mathbf{a} \end{bmatrix} \text{(mod 26)}$$

Anahtar matrisin tersi ile şifreli karakter çiftlerinin çarpımı bize düz metni verir.

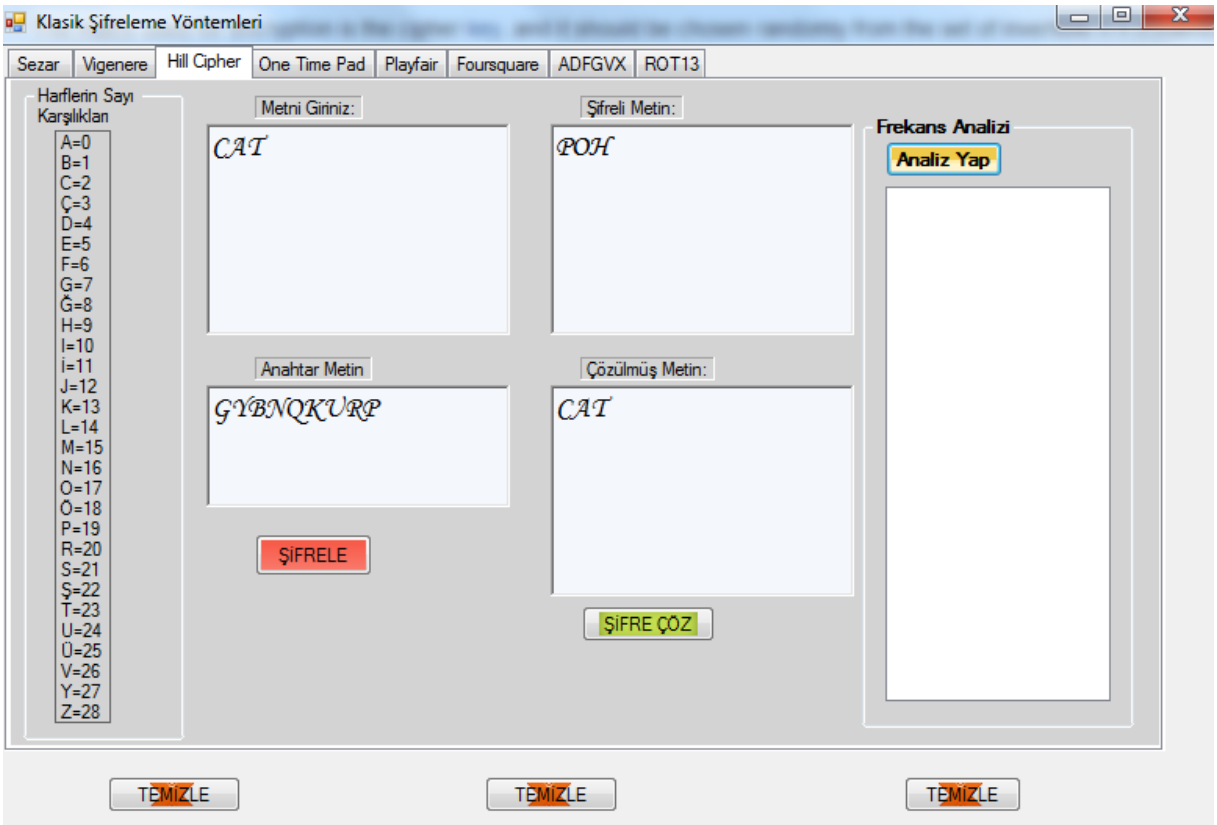
Anahtar Matrisimiz: A= $\begin{bmatrix} 3 & 17 \\ 8 & 25 \end{bmatrix}$

Şifreli Metnimiz: CIKKGEUWEROY

Deşifre için ilk bloğumuzu seçelim CI

$A^{-1}\begin{bmatrix} 2 \\ 8 \end{bmatrix} = \begin{bmatrix} 12 \\ 8 \end{bmatrix} (\text{mod}26)$ dir

Mesaj deşifrelendiğinde ilk iki karakterin sayısal değeri olan 12 ve 8 sayıları bulunur. Bunlarda CI -> MI demektir. Mesajı alan kişi elinde bulunan şifreli metindeki her bir karakter bloğu için bu işlemi uygular.



Hill Cipher şifreleme yöntemi ile girilen metin anahtar metin ile sayı değerlerinin matris çarpımı yapılarak şifreli metin elde edilir. Örnek metinde Düz metin olarak *CAT* kelimesi girilmiştir. Anahtar metin olarak *GYBNQKURP* kelimesi seçilmiştir. Ve şifrelimetin olarak *POH* elde edilmiştir. ŞİFREÇÖZ butonu ile algoritma tersten çalıştırılarak düzmetne ulaşılmıştır. Frekans analizi ile şifreli metinde bulunan harflerin kullanım sıklığı hesaplanmıştır. Hill Cipher şifrelemede düzmetnin büyük veya küçük harf girilmesi fark etmemektedir. Rakam ve Noktalama işaretleri şifrelenmemektedir.

One Time Pad

One-time pad belirli usullerle karıştırılmış harflerden oluşturulan tek kullanımlık şifreleme yöntemidir. Bir diğer adı ise Vernam şifreleme yöntemidir.

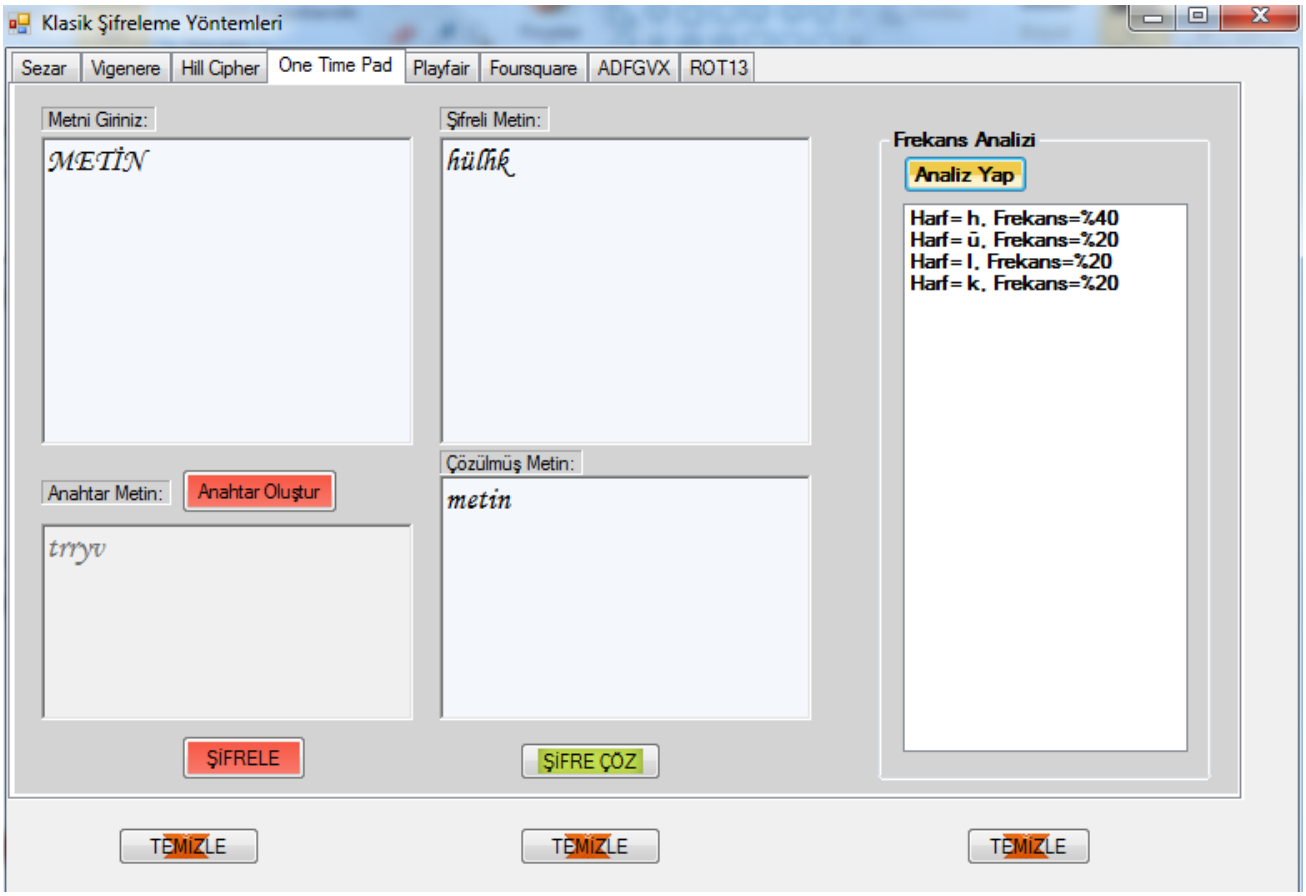
Tarihi:

Gilbert Sandford Vernam (1890-7 Şubat 1960) AT & T Bell Labs da çalışan bir mühendisti. 1917 de 1. Dünya Savaşı sırasında Gilbert Vernam 'a Almanların çözemeyeceği bir şifreleme metodu icat etmekle görevlendirilmişti ve bunun sonucu olarak önce akış şifrelemeyi icat etmiş ve sonrasında Joseph Mauborgne ile mükemmel şifreleme tekniği olan one-time pad (tek kullanımlık bloknot) şifreleme metodunu bulmuşlardır. Akabininde teletype makinasıyla beraber kullanılmaya başlamıştır.

Güvenliği:

Pad'lar rastgele üretilmelidir. Eğer belli bir sisteme göre gidilirse saldırgan tarafından kırılma riski yüksektir.

Pad'lar tek seferlik kullanılmalıdır.[7]

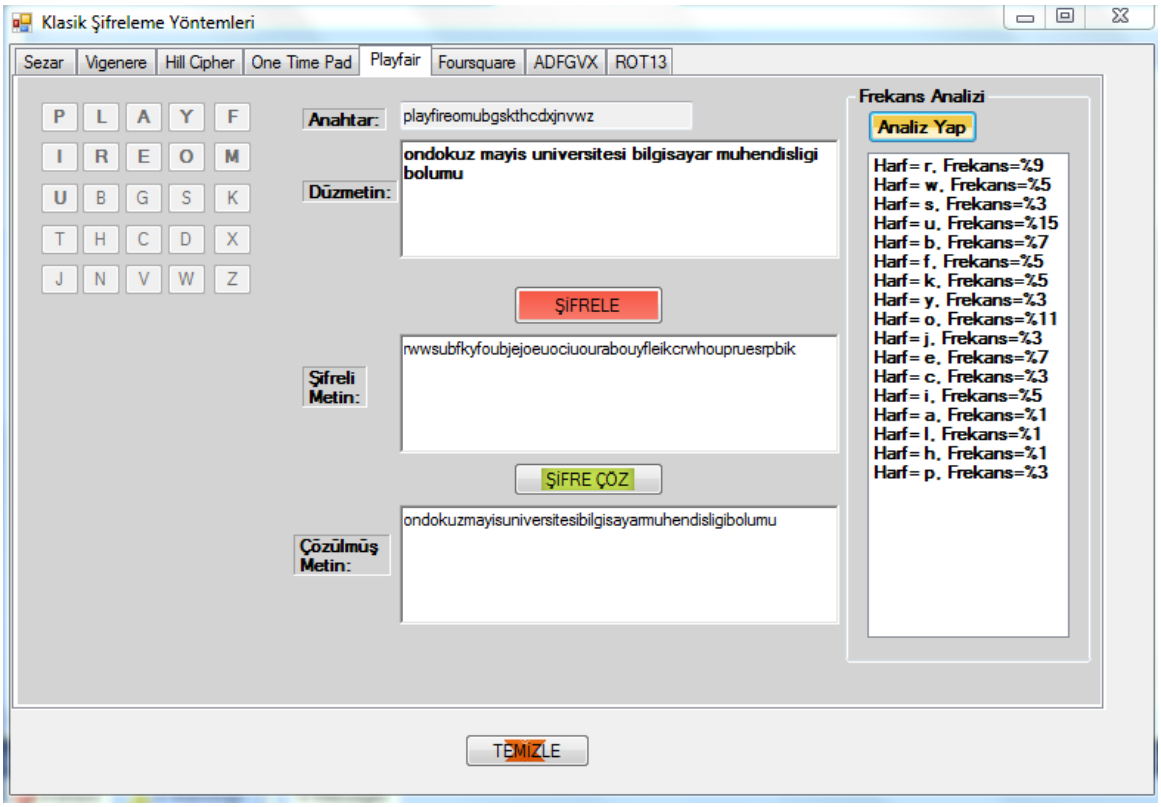


One Time Pad şifreleme yöntemi ile girilen metin anahtar metin kadar kaydırılabilir. Anahtar metin rastgele oluşturulmuştur. Örnek metinde Düz metin olarak *Metin* kelimesi girilmiştir. Anahtar metin olarak *trryv* kelimesi seçilmiştir. Ve şifrelimetin olarak *hülhk* elde edilmiştir. ŞİFREÇÖZ butonu ile algoritma tersten çalıştırılarak düzmetne ulaşılmıştır. Frekans analizi ile şifreli metinde bulunan harflerin kullanım sıklığı hesaplanmıştır. One Time Pad şifrelemede düzmetnin büyük veya küçük harf girilmesi fark etmemektedir. Rakam ve Noktalama işaretleri şifrelenmemektedir.

Playfair

Playfair şifre veya Playfair kare manuel simetrik şifreleme tekniği ve literatüre giren ilk değiştirme şifrelemesidir. Şeması Charles Wheatstone tarafından 1854 yılında icat edildi, ancak şifrenin kullanımını teşvik edildiğinden Rab Playfair adını taşır oldu.

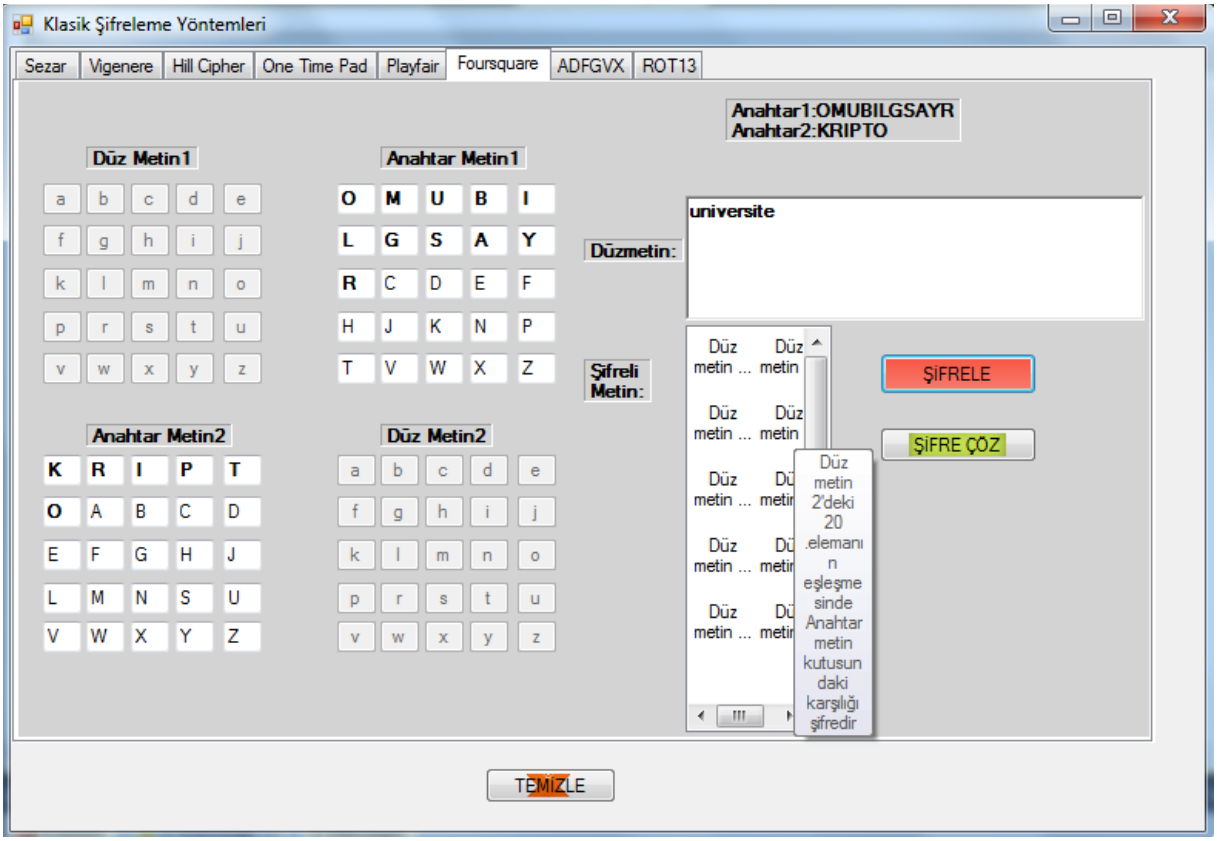
Teknik basit kaydırma şifreleme yöntemleri ve daha karmaşık vigenere şifre sisteminin, tek harf kullanımının yerine, harf çiftleri şifreler. Playfair böylece basit kaydırma şifreleri kırmak için kullanılan frekans analizi onunla kullanmak zordur. Frekans analizleri gerçekleştirilebilir, ama 26 olası monografları yerine 600 olası digraphs(çiftli harf) üzerinde çalışır. Digraphs sıklığı analizi mümkün, ama çok daha zordur[8]



Playfair şifreleme yöntemi için anahtar olarak playfireomubgskthcdxjnvwz seçilmiştir.
Düzmetin olarak: ondokuz mayis universitesi bilgisayar muhendisligi bolumu seçilmiştir. Anahtar ile düzmetin Playfair ile şifrelendiğinde; rwwsubfkyfoubjejoeuociuourabouyfleikcrwhoupruesrpbik metni oluşmuştur.

Foursquare

Foursquare şifreleme yönteminde 5*5 kutulu, ikisi düzmetin için ikisi de şifre metinler için olmak üzere 4 adet kare kutu vardır. Girilen metin ve anahtar ile foursquare işleme tabi tutularak Şifreli metin elde edilecektir. Düzmetindeki ilk harf ile düzmetindeki ikinci harfin anahtar kutularındaki kesiştiği yerler bize şifreleri verecektir. [9]



Foursquare şifreleme yöntemi ile girilen metin ve anahtar ile foursquare işleme tabi tutularak Şifreli metin elde edilecektir. Foursquare rastgele doldurulacaktır. Frekans analizi ile şifreli metinde bulunan harflerin kullanım sıklığı hesaplanmıştır. Foursquare şifrelemede düzmetnin büyük veya küçük harf girilmesi fark etmemektedir. Rakam ve Noktalama işaretleri şifrelenmemektedir.

ADFGVX

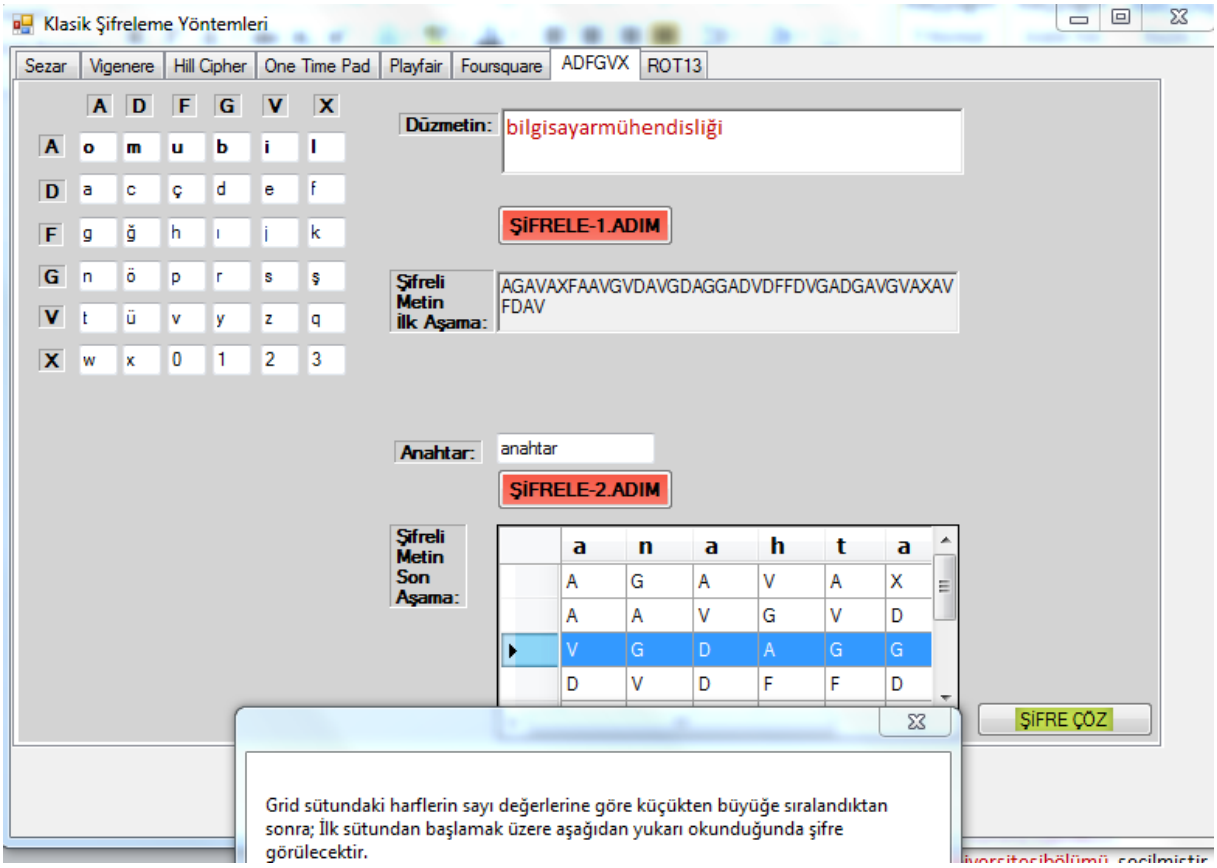
Şifrelemede, ADFGVX şifre I. Dünya Savaşı sırasında Batı Cephesi Alman Ordusu tarafından kullanılan bir alan şifrelemeydi, aslında ADFGX denilen bir önceki şifrenin bir uzantısı idi.

Albay Fritz Nebel tarafından icat edilen ve Mart 1918 tanıtılan, şifre tek sütunlu transpozisyonlu değiştirilmiş Polybius kare kombine kesirlenmiş transpozisyon şifreydi. [10]

Bu yöntemin avantajı alfa ve sayısal karakterler birarada içeriyor olmasıdır.[11]

ADFGVX Fransız Ordusu Teğmen ve kriptanalist Georges Painvin tarafından Haziran 1918'de kırıldı. Şifreyi kırmak için ilk önce kullanılan anahtarın boyutu sütun sayısı tahmin dilmeye çalışılır. Daha sonra istatiksel analiz kullanılmaya çalışılır. Fakat şifreyi çözmek kolay değildir. Kullanılan anahtarı bulmak için şifrenin yinelenen yerleri kullanıldı.

ADFGX ve ADFGVX şifreleri artık güvensiz olarak kabul edilmektedir.



ADFGVX şifreleme yöntemi ile girilen metin ve anahtar ADFGVX ile işleme tabi tutularak Şifreli metin elde edilecektir. ADFGVX: `omubilacçdefgğhıijknöprsştüvyzqwx0123`
Olarak seçilmiştir. Düzmetin olarak bilgisayarmühendisliği seçilmiştir. Anahtar metin olarak anahtar seçilmiştir. ŞİFREÇÖZ butonu ile algoritma tersten çalıştırılarak düzmetne ulaşılacaktır. Frekans analizi ile şifreli metinde bulunan harflerin kullanım sıklığı hesaplanmıştır. ADFGVX şifrelemede düzmetnin büyük veya küçük harf girilmesi fark etmemektedir.

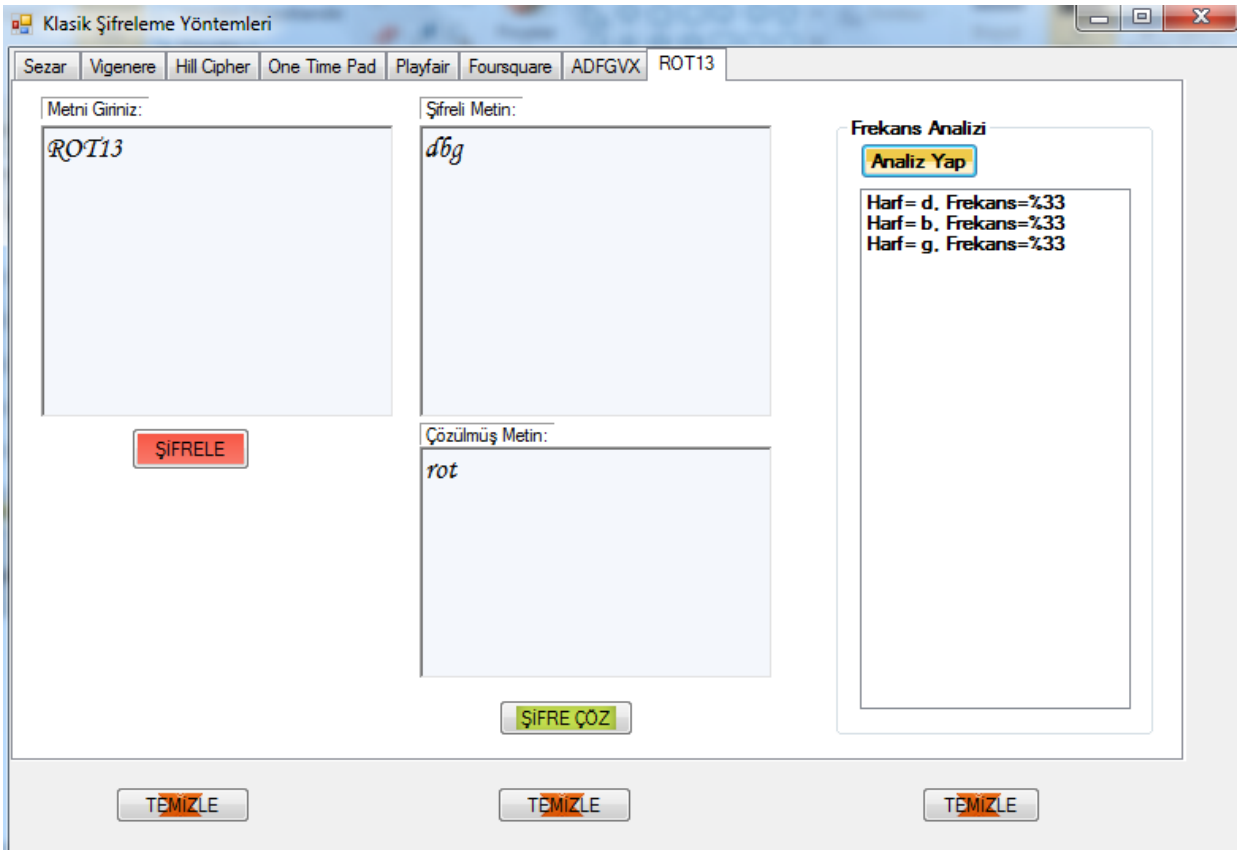
ROT13

ROT13 (Rotate13) forumlarda ve web proxy sayfalarında sıkça görülen ayrıca, çeşitli puzzle, riddle, bulmaca türlerinde karşımıza çıkan bir şifreleme türüdür.

*ROT13 (Rotate13) yer değiştirme yöntemi kullanan bir Caesar(Sezar) şifreleme türüdür.

*Mantık olarak İngiliz alfabesindeki bir harfin 13 harf sonraki harf ile eşleşmesidir.[12]

-Bu projede Türkçe alfabeye göre ROT13 kodlanmıştır.



ROT13 şifreleme yöntemi ile girilen metin 13 ileri kaydırılabilir. Örnek metinde Düz metin olarak *ROT13* kelimesi girilmiştir. Şifrelimetin olarak *dbg* elde edilmiştir. ŞİFREÇÖZ butonu ile algoritma tersten çalıştırılarak düzmetne ulaşılmıştır. Frekans analizi ile şifreli metinde bulunan harflerin kullanım sıklığı hesaplanmıştır. ROT13 şifrelemede düzmetnin büyük veya küçük harf girilmesi fark etmemektedir. Rakam ve Noktalama işaretleri şifrelenmemektedir.

4.Gerçekleştirim

Klasik şifreleme sistemleri (Sezar, Vigenere, Hill cipher, one time pad, foursquare, playfair, ADFGVX, ROT13) .NET programlama dili ve görsel öğeleri ile programlanarak kullanıma hazır hale getirilmiştir.

5.Konfigürasyon

Klasik Şifreleme Sistemi geliştirilirken kullanılan geliştirme aracı Microsoft Visual Studio ve C# programlama dilidir. Microsoft Visual Studio ile ekran tasarımları yapıldıktan sonra C# ile programlanmıştır.

6.Proje takvimi

Projenin geliştirme takviminde; 1. Gelişim raporu teslim tarihi 28.04.2014, 2. Gelişim raporu (daha çok yazılım tasarım raporu) teslim tarihi 21.05.2014, final raporu teslim tarihi 06.06.2014 ve düzeltilmiş son rapor teslim tarihi 16.06.2014 tarihleridir.

7.Değerlendirme

Kriptografi: gizlilik, kimlik denetimi, bütünlük gibi bilgi denetimi kavramlarını sağlamak için çalışan matematiksel yöntemler bütünüdür. Bu yöntemler, bir bilginin iletimi esnasında karşılaşılabilecek aktif veya pasif ataklardan bilgiyi, dolayısıyla bilgi ile beraber bilginin göndericisi ve alıcısını da koruma amacı güderler. Kriptografik bir programın, içindeki bilgileri görme yetkisi olanlar dışındaki herkesten gizli tutması, kimlik denetimi yapması, tek bir veri parçası için dahi gönderilen bu verinin üzerinde hiçbir değişiklik, ekleme, yeniden düzenleme yapılmadığını garanti etmesi, izinsiz kişi ya da uygulamaların erişmemeleri gereken kaynaklara erişemeyecekleri garantisi vermesi beklenir. Bir başka deyişle kriptografi, okunabilir durumdaki bir bilginin istenmeyen taraflarca okunamayacak bir hale dönüştürülmesinde kullanılan tekniklerin tümüdür.[3]

Klasik şifreleme yöntemlerinin programlanarak kullanıma sunulması ile Türkçe kaynak eksiklikleri bir nebze olsun giderilmiş olacak. Böylelikle araştırmalar için yabancı kaynaklardan önce algoritmaların değerlendirmelerinde bu program ve kodlar kullanılabilecektir.

8.Sonuçlar

Yüzyıllardır insanoğlu bir mesajı bir yerden başka bir yere ulaştırmak ve bu mesajın yolda başkalarının eline geçmemesi için uğraşmış ve bunun sonucunda şifreleme sistemlerini icat etmiştir. Klasik şifreleme yöntemleri de bu ihtiyaçtan doğarak üretilmiştir.

Klasik şifreleme sistemleri yabancı kaynaklı şifreleme sistemleri olduğundan, ülkemizde birçok insan ve konu ile alakalı öğretim görevlileri ve öğrenciler için, sistemlerin içyüzü tam olarak bilinememektedir.

9.Projenin özgünlüğü

.

a.Yenilikçilik

Bu projede bahsedilen klasik şifreleme sistemleri yabancı kaynaklı şifreleme sistemleri olup, ülkemizde birçok insan için hala nasıl yöntemler kullanıldığı bilinmemektedir. İşte bu proje ile klasik

şifreleme sistemleri hepsi bir arada Türkçe olarak programlanacak ve kullanıma sunulacaktır. Bu bağlamda ülkemizdeki öğrenci, eğitimci ve araştırmacılar için yerli bir kaynak ve örnek olacaktır.

b.Etki

Klasik şifreleme yöntemlerinin programlanması ve Türkçe olarak kullanıma sunulması ile başka çalışmalara da öncülük ederek diğer çalışmaları etkileyecektir.

c.Uygulanabilirlik

Yazılım programlandıktan sonra Kriptografi ve ilgili derslerde dersi veren öğretim görevlilerine kaynaklık ederek öğrencilerin sistemler hakkında bilgi sahibi olmasını ve klasik şifreleme yöntemleri hakkında bilgi sahibi olmak isteyen araştırmacılara örnek olacaktır.

d.Kullanışlılık

Klasik şifreleme sistemleri yabancı kaynaklı şifreleme sistemleri olduğundan, ülkemizde birçok insan ve konu ile alakalı öğretim görevlileri ve öğrenciler için, sistemlerin içyüzü tam olarak bilinememektedir.

10. Referanslar

[1]http://tr.wikipedia.org/wiki/Kriptografi
[2] Şifrelerin Matematiği: Kriptografi- Canan Çimen, Ersan Akyıldız, Sedat Akleylek
[3] http://e-bergi.com/y/Kriptografi-Algoritmalari-ve-Kullanimlari-
http://www.sagemath.org/doc/reference/cryptography/sage/crypto/classical.html
[4] http://blog.burakkutbay.com/sezar-sifreleme-algoritmasi-nedir-rot13-nedir.html
[5] Jörn Müller-Quade: Hieroglyphen, Enigma, RSA - Eine Geschichte der Kryptographie. Fakultät für Informatik der Universität Karlsruhe, S. 36. 28 Mayıs 2008.

[6] http://www.mutasyon.net/makaleoku.asp?id=781

[7] http://kriptoloji.net/one-time-pad-vernam-cipher

[8] http://en.wikipedia.org/wiki/Playfair_cipher

[9] http://geocachingtoolbox.com/index.php?page=fourSquareCipher

[10] http://en.wikipedia.org/wiki/ADFGVX_cipher

[11] http://www.dickason.com/caching/OHMIKY-ADFGVX.html

[12]http://www.millikuvvetler.net/rot13-sifreleme-teknigi-
t2248.html?s=3983deb8425cafc8f402a7f17f44d001&t=2248

11.Ekler

1-Klasik Şifreleme Yöntemlerinin .NET ortamında yazılan program ile ilgili kodlar buradan indirilebilir: https://drive.google.com/file/d/0BxKbwQavpp3wMS1jYnZpNDAwZTg/edit?usp=sharing

2-Klasik Şifreleme Yöntemlerinin kullanımı ve yöntemlerle ilgili örnekler buradaki video ile anlatılmıştır: https://drive.google.com/file/d/0BxKbwQavpp3wdXBfcXpJaDFGdEU/edit?usp=sharing

3-Bilgisayarlar için kurulum dosyası buradan indirilebilir: https://drive.google.com/file/d/0BxKbwQavpp3wRXVyR2lwYnZEeGs/edit?usp=sharing