KLASİK ŞİFRELEME YÖNTEMLERİ UYGULAMASI

05130000248 Tolgahan AKGÜN

İÇİNDEKİLER

* Uygulamanın Amacı
* Kullanılan Teknolojiler
* Kullanılan Sınıflar ve Metodları
* Uygulama Kullanım Kılavuzu
* Uygulama ile İlgili Notlar

Uygulamanın Amacı

Uygulamadaki amaç klasik şifreleme yöntemlerini tanımak ve gerçekleştirmektir. Bu amaçla Shift Cipher, Ceaser Cipher, Vigenére Cipher, Steganography ve Hill Cipher şifreleme yöntemleri için birer uygulama yazılmıştır.

Kullanılan Teknolojiler

Uygulama .NET Framework 4 Client ortamında Visual Studio 2010’da form uygulaması olarak gerçekleştirilmiştir.

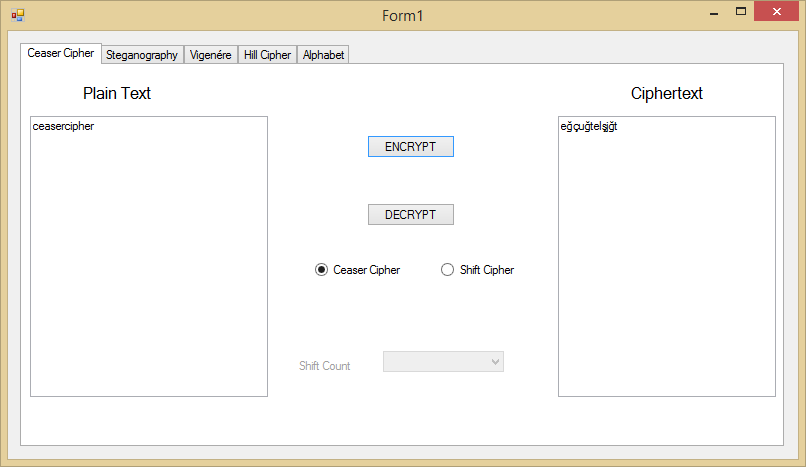
Kullanılan Sınıflar ve Metodları

* Alphabet.cs: Uygulamada önceden tanımlı olan dillerdeki alfabeleri static olarak tutan sınıftır.
* ControlText.cs: Girilen metinin uygulamada tanımlanmış olan alfabeye uygun olup olmadığını kontrol eden sınıftır.
* bool suitsAlphabet(char[] alphabet, char[] text) : Parametre olarak verilen metinin alfabeyi uyup uymadığını kontrol eder ve sonucuna göre true ya da false değeri döndürür.
* HillCipher.cs: Hill Cipher methoduyla şifreleme ve deşifreleme yapan sınıftır.
* string Encrypt(Matrix<double> matrix, char[] alphabet, String stream): Parametre olarak verilen matrix yani anahtar ile istenilen alfabe üzerinde şifreleme işlemi yapar ve sonucu string olarak döndürür.
* string Decrypt(Matrix<double> matrix, char[] alphabet, String stream):

Parametre olarak verilen matrix yani anahtar ile istenilen alfabe üzerinde deşifreleme işlemi yapar ve sonucu string olarak döndürür.

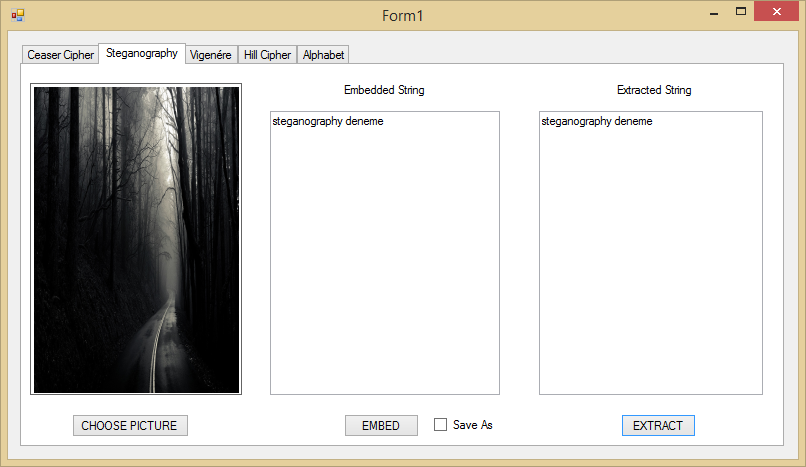
* Modulo.cs: Negatif sayıların modunu almak için oluşturulmuş sınıftır.
* int mod(int a, int b): A sayısının b tabanına göre modunu hesaplar.
* ShiftCipher.cs: Parametre olarak verilen kaydırma değeri kadar istenilen alfabe üzerinde Shift Cipher methoduyla şifreleme ve deşifreleme yapar. Ceaser Cipher için de bu sınıf kullanılır ve kaydırma değeri olarak da 3 değeri static parametre olarak gönderilir.
* string encrypt(char[] alphabet, string plainText, int shiftCount): Parametre olarak gönderilen alfabe, metin ve kaydırma sayısını kullanarak Shiift Cipher methoduyla şifreleme yapar.
* string decrypt(char[] alphabet, string plainText, int shiftCount): Parametre olarak gönderilen alfabe, metin ve kaydırma sayısını kullanarak Shiift Cipher methoduyla deşifreleme yapar.
* Steganography.cs: Resimler içine metin gizleme ve resimlere gizlenmiş metinlerin resimlerden tekrar elde edilmesi için oluşturlumuş sınıftır.
* Bitmap embedText(string text, Bitmap bmp): Parametre olarak verilen metni, parametre olarak verilen Bitmap resim nesnesinin içine saklar ve resim nesnesini döndürür.
* string extractText(Bitmap bmp): Parametre olarak verilen resim nesnesinin içinde saklı olan metni resimden çıkartır ve geri döndürür.
* VigenéreCipher.cs: Vigenére Cipher metoduyla şifreleme ve şifreleme yapan sınıftır.
* string Encrypt(char[] alphabet, string password, string text): Parametre olarak verilen anahtar değeriyle ve metin ile istenilen alfabe üzerinde şifreleme işlemi yapar ve sonucunda oluşan metni döndürür.
* string Decrypt(char[] alphabet, string password, string text) : Parametre olarak verilen anahtar değeriyle ve metin ile istenilen alfabe üzerinde deşifreleme işlemi yapar ve sonucunda oluşan metni döndürür.

Uygulama Kullanım Kılavuzu

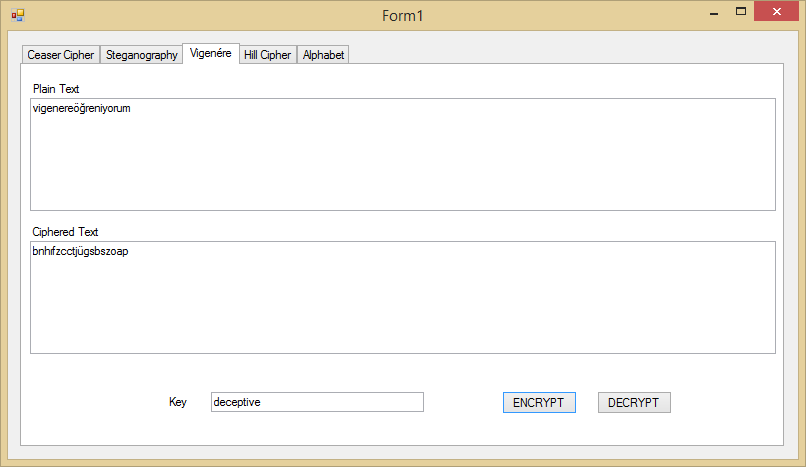


Uygulamayı çalıştırdığımıza karşımıza yukarı gösterilen ekran gelecektir. Varsayılan değer olarak Ceaser Cİpher ya daShift Cipher işlemlerini yapabileceğimiz ekran gelecektir. Buradan Plain Text bölümüne şifrelenmesini isteğimiz metni girip “ENCRYPT” tuşuna basarak girilen metini şifreleyebiliriz ve sonucunu da Cipher Text bölümünde görebiliriz. Aynı şekilde deşifrelenmesini istediğimiz metni Cipher Text bölümüne girip “DECRYPT” tuşuna basarak da Cease Cipher yoluyla deşifreleme yapabilir ve sonucunu da Plain Text bölümünde görebiliriz.

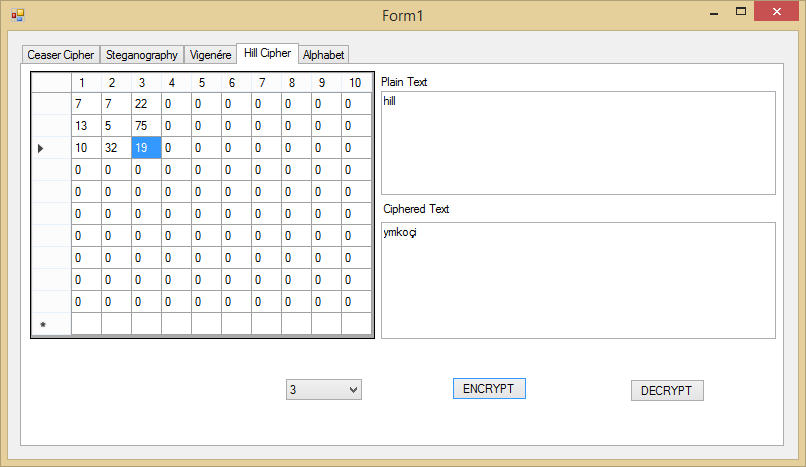
Ceaser Shift uygulamasına benzer bir mantıkla bulunduğumuz sayfada Shift Cipher işlemini yapabiliriz. Shift Cipher Radio Button tuşuna tıklayarak Shift Cİpher seçeneğini aktifleştiriyoruz ve daha sonra Shift Count Combo Box’u aracılığıyla kaydırma sayısını giriyoruz. Son olarak da Encrypt tuşuna basarak şifreleme işlemini gerçekleştirip sonucunu Cipher Text bölümünde görebiliriz. Aynı şekilde deşifrelenmesini istediğimiz metni Cipher Text bölümüne girip daha sonra da Shift Count sayısını girerek “DECRYPT” tuşuna basarak da Shift Cipher yoluyla deşifreleme yapabilir ve sonucunu da Plain Text bölümünde görebiliriz.



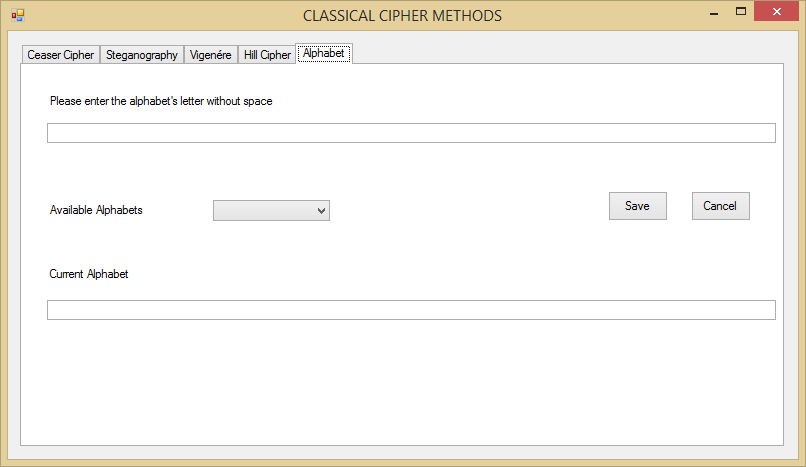
Yukarıdaki ekrandan “CHOOSE PICTURE” tuşuna basarak resim seçiyoruz. Daha sonra resmin içine saklanmasını istediğimiz metni Embedded String sahasına girip “EMBED” tuşuna basıyoruz ve metnimiz resmin içine saklanıyor. Eğer resmin içine saklanmış olan metinin tekrar çıkarılmasını istersek de “EXTRACT” tuşuna basarak resimden çıkarılmış metni Extracted String sahasında görebiliriz.



Yukarıdaki ekranda Vigenére Cipher methoduyla şifreleme ve deşifreleme yapabiliyoruz. Plain Text kısmına şifrelenecek metinimizi giriyoruz ve key kısmına da anahtarımızı girip “ENCRYPT” tuşuna basıyoruz ve şifrelenmiş metinimiz Ciphered Text sahasında görülüyor. Aynı şekilde Ciphered Text sahasına girdiğimiz metini de key “DECRYPT” tuşuna basarak deşifreleyebiliyoruz.



Yukarıdaki ekranda Hill Cipher metoduyla şifreleme ve deşifreleme yapılmaktadır. Data Grid View Controller’i aracılığıyla anahtar matrisimizi giriyoruz ve altındaki Combo Box aracılığıyla da matrisimizin kenar uzunluğunu giriyoruz. Daha sonra da şifrelenmesini istediğimiz metni Plain Text sahasına girip “ECNRYPT” tuşuna basıyoruz ve şifrelenmiş metin Ciphered Text sahasında görülebiliyor. Aynı şekilde anahtarımızı girip Ciphered Text sahasına da deşifrelenecek metini girip “DECRYPT” tuşuna basarak da deşifrelenmiş metinimizi Plain Text sahasında görebiliyoruz.



Yukarıdaki ekrandan farklı diller için alfabe girişi yapılabilmektedir.

Uygulama ile İlgili Notlar

Uygulamada açık kaynak kodlu kütüphaneler ve birtakım hazır kodlardan yararlanılmıştır. Matrislerdeki işlemler için MATHNET isimli kütüphane kullanılmıştır. Ayrıca Steganography isimli sınıfın bazı metodlarında da [www.codeproject.com](http://www.codeproject.com) adlı siteden alınmış birtakım kodlar kullanılmıştır. Kullanılan kütüphaneler ve kodlar ile ilgili lisanslar uygulamanın kaynak kodunda açıkça belirtilmiştir.