

BELTEK C++BUILDER EĞİTİMİ BİTİRME PROJESİ

# Dosya Şifreleme Programı

PROJE RAPORU

Halil Kemal TAŞKIN

ANKARA 2012 TEMMUZ

- **Projenin Adı**

“Dosya Şifreleme Programı”

- **Projenin Amacı**

Bu proje, bilgisayar üzerinde saklanan dosyaların, gizli bir şifre ve belirli bir algoritma ile karıştırılarak yetkisiz kişiler tarafından erişilmesini engellemek için C++Builder kullanarak bir şifreleme programı oluşturmayı amaçlar.

- **Projenin Açıklaması**

Günümüzde teknolojinin hayatımızın her alanında kullanıma geçmesi ile birlikte gerek özel bilgilerimiz gerekse herkes ile paylaşmak istemediğimiz bilgiler istemeden de olsa başkalarının eline geçebilmekte. Bu bağlamda, bilgisayar ortamında tutulan bilgilerin güvenli bir şekilde saklanması için çözümlerden birisi de şifreleme yazılımlarıdır. Şifreleme yazılımları temelde matematiksel modeller üzerine kurulmuş modern kriptografik yöntemleri kullanarak sayısal bilgileri gizleyebilmektedir.

Bilgisayar üzerinde tutulan her dosya aslında 1’ler ve 0’lardan oluşan ‘binary’ diziler olarak görülebilir. Modern kriptografi bilimi de 1’ler ve 0’lardan oluşan dizileri şifrelemek için yöntemler sunar. Bunun için dünyada standart olmuş birçok modern sistem vardır. Bunlardan bir kaç RSA, ECC, DSA, 3DES, AES, RC4, MD5, SHA1 vb. Bu sistemler uzun yıllardan beri Internet bankacılığı, online alışveriş vb. sistemlerde kredi kartı bilgileri gibi önemli bilgilerin çalınmasına ve yanlış ellere geçmesine engel olmak için kullanılmakta olup, güvenilirlikleri doğrulanmıştır.

Bu projede bilgisayar üzerinde bulunan dosyaların şifrlenmesi RC4 algoritması ile yapılmıştır. RC4 algoritması, bilim adamı Ron Rivest tarafından 1987 yılında tasarlanmış olup günümüzde de aktif olarak güvenlik sistemlerinde kullanılmaktadır. Projede RC4 algoritmasının tercih edilmesinin sebebi hem hızlı hem de güvenli olmasıdır. RC4 dizi şifreleme algoritması olarak tasarlandığı için dosyalar üzerine uygulanması daha kolay olmaktadır.

Proje kapsamında yazılan şifreleme programında 4 temel özellik vardır. Bunlar;

1. Dosya Şifreleme
2. Şifrelenmiş Dosyayı Çözme
3. BMP Resim Dosyası Şifreleme
4. Şifrelenmiş BMP Resim Dosyasını Çözme

Ayrıca, güvenli şifre seçimine yardımcı olmak için, rastgele şifre üreten bir yardımcı ekran hazırlanmıştır.

### **Teknik Detaylar:**

RC4 algoritması iki aşamalı çalışmaktadır. İlk olarak yazılan şifrenin algoritma için uygun biçime getirilmesi gereklidir. Algoritmanın tasarımından dolayı kullanıcılar 256 karakterden büyük şifre kullanamazlar. İkinci aşama ise verilen şifreyi kullanarak rastgele byte oluşturma (dizi çıktısı oluşturma) aşamasıdır. RC4 temel olarak, her çalıştırıldığında 1 byte’lık rastgele veri üretmektedir. Oluşan 1 byte’lık rastgele veri, şifrelenecek olan dosyanın sıradaki 1 byte’ı ile XOR işlemine tutulur. XOR işlemi 2 tabanında modüler toplama işlemi demektir.

XOR işlemine özgü olan bir özellik ise aynı değerin kendisi ile XOR işlemine tabi tutulması sonucunda 0 çıkmasıdır. Bu özellik sayesinde RC4 ile şifrelenmiş bir dosyayı çözmek için şifrelenmiş dosyayı aynı şifre ile tekrar şifrelemek yeterli olacaktır.

RC4'ün bilinen bazı zayıflıkları vardır. Ancak bunları aşmak için basit yöntemler vardır. Projedeki RC4 algoritmasında, ilk 3072 byte çıktı ihmal edilerek şifrelemeye 3073. byte'tan başlanmıştır. Bunun sebebi yukarıda da belirtildiği üzere bilinen bazı zayıflıkları aşmak içindir. Bu sayede sistem daha güvenli hale gelmiştir.

Programı kullanarak şifreli dosyayı çözmeye çalışan bir kişi, şifreli dosyayı seçip çözmeye çalıştığında şifreyi bilmiyorsa bile dosyayı herhangi bir şifre ile açmaya çalışabilir. Program bu durumda şifrenin hatalı olduğuna dair herhangi bir uyarı vermeyecektir. Ancak çözülen dosya tamamen anlamsız bir hal alacaktır. Bu da programın güvenlik seviyesini artırmaktadır.

Program da sıradan herhangi bir dosyayı şifrelemenin yanında BMP uzantılı resim dosyalarını şifrelemek için özel bölüm mevcuttur. BMP dosyaları basit yapıda dosyalardır. Bilindiği gibi resim dosyaları piksel denilen renk noktaları hakkında bilgiler içerir ve bunları yan yana koyarak resim oluşturulur. BMP yapısı gereği dosyanın başında başlık denilen ve resmin piksel sayısı vb. bilgilerini içeren bir kısım bulundurulur. Buranın ardından piksel bilgileri depolanır. Eğer (Windows'un dosyayı tanıyabilmesi için) başlık kısmını şifrelemeyip sadece piksel bilgilerini şifrelersek, şifrelenen veri yine geçerli bir BMP resmi oluşturacaktır. Ancak piksel bilgisi şifrelendiği için anlamsız bir resim çıkacaktır. Bir dosyanın şifrelendiğini anlamak ve görmek adına BMP şifrelemesi güzel bir örnektir.

Proje, C++Builder'ın son sürümü olan "Embarcadero RAD Studio C++Builder XE2 Update 4" kullanılarak yazılmıştır. Programa görsellik katmak adına, bu sürümde dâhili olarak gelen görsel temalar programa uygulanmıştır. Programın çalışması için 6 adet ek dosyaya ihtiyaç vardır. Bu dosyalar program ile aynı klasöre yerleştirilmiştir. Proje, Windows XP, Vista ve 7 sürümlerinin 32-bit mimarilerinde çalışması için derlenmiştir.

- **Programın Kullanımı**

Programı çalıştırdığımızda karşımıza aşağıdaki gibi bir ekran gelecektir:

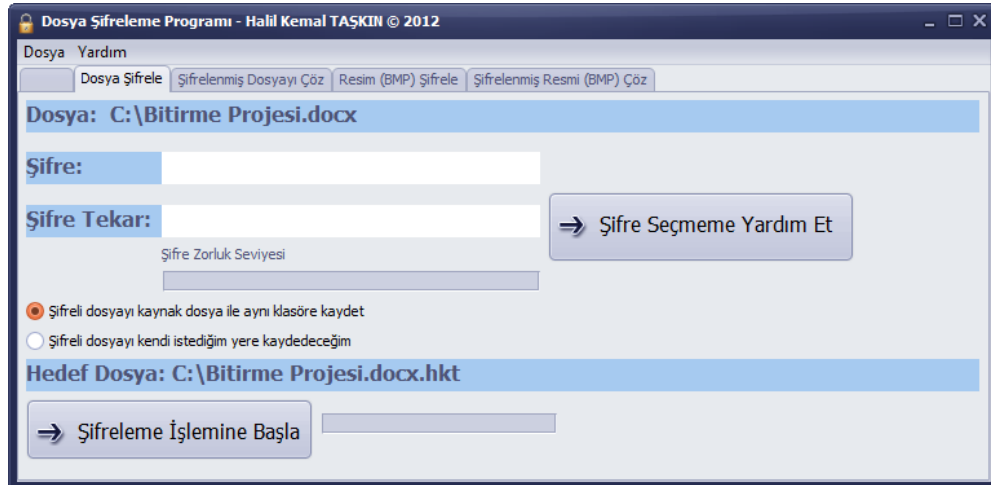


Giriş ekranında uygulama simgesi ve kısa bir açıklama mevcuttur. Açıklamada da belirtildiği üzere programın bütün işlemleri sol üstteki “Dosya” menüsü üzerinden yapılmaktadır.

### **Dosya menüsü altındaki seçenekler:**

#### **1. Dosya Şifrele:**

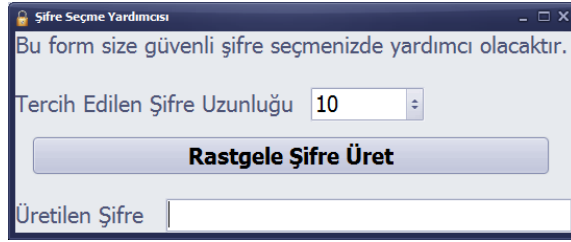
Bu butonun seçilmesi halinde sizden şifrelemek istediğiniz dosyayı seçmeniz istenecektir. Dosyayı seçtiğinizde otomatik olarak ilgili sekmeye yönlendirilecek ve şifre vb. ek bilgileri girmeniz istenecektir. Aşağıda örnek bir ekran görüntüsü verilmiştir:



En üstteki TLabel nesnesinde seçilen dosyanın tam yolu görünmektedir. Altta şifre ve tekrar şifre TEdit nesnelerine dosyaları şifrelerken kullanacağınız şifreyi yazmanız gereklidir. “Şifre” satırında şifrenizi yazarken aynı anda TEdit nesnesinin sağ

tarafında, yazılan şifrenin uzunluğunu ve Şifre Zorluk Seviyesi kısmında ise yazdığınız şifrenin güvenlik seviyesini çizgisel olarak görebilirsiniz.

“Şifre Seçmeme Yardım Et” butonuna tıklayınca aşağıda ekran görüntüsü verilen bir form açılacaktır.



Form üzerinde üretmek istediğiniz şifre uzunluğunu 8-255 arasında seçerek “Rastgele Şifre Üret” butonuna bastığınızda TEdit nesnesine üretilen şifre yazdırılacaktır. Butona her tıklamada farklı bir şifre üretilecektir. Üretilen şifreyi seçerek kopyalayıp diğer form üzerinde kullanabilirsiniz.

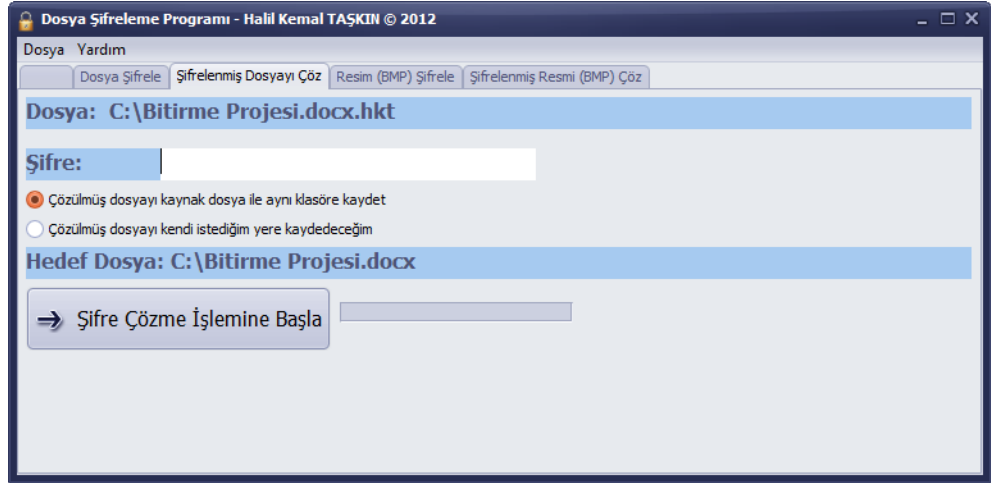
Şifrelenmiş dosyanın kaydedileceği dosya “Hedef Dosya” satırında gösterilmiştir. Varsayılanda şifrelenmiş dosya otomatik olarak esas dosya ile aynı klasörde aynı isimde ancak sonuna “.hkt” eklenmiş olarak tanımlanmıştır. “.hkt” uzantısının herhangi bir özel seçimi olmayıp sadece bu programa özgü olması adına isminin baş harfleri alınarak oluşturulan bir uzantı olmuştur. Eğer hedef (şifrelenmiş) dosya farklı bir konuma kaydedilmek istenirse “Şifreli dosyayı kendi istediğim yere kaydedeceğim” seçeneği seçilerek görünür hale gelen “Kaydet” butonu seçilir ve hedef dosyanın konumu SaveDialog nesnesi aracılığıyla seçilir.

Tüm bu işlemlerden sonra “Şifreleme İşlemine Başla” butonu ile dosya şifrelemesine başlanır. Butona tıkladığınızda eğer bilgiler hatalı ya da eksik ise düzeltmeniz için program sizi uyaracaktır. Şifreleme süreci başlayınca butonun yanındaki ilerleme çubuğu aktif olur. Şifreleme bitince ilerleme çubuğunun sağındaki TLabel nesnesinde işlemin bittiğine dair mesaj yazdırılır.

Farklı bir işlem için yeniden Dosya menüsünden ilgili buton seçilebilir.

## 2. Şifrelenmiş Dosyayı Çöz:

Bu butonu, 1. Kısımda anlatıldığı gibi şifrelediğiniz bir dosyayı tekrar eski haline getirmek (şifresini çözmek) için kullanabilirsiniz. Butona tıkladığınızda şifreli dosyayı seçmeniz istenecektir. Bu ekranda sadece “.hkt” uzantılı dosyalar görüntülenmektedir. Dosya seçiminden sonra otomatik olarak aşağıda ekran görüntüsü verilen sekmeye yönlendirilirsiniz.



İlk sekmeye benzer şekilde kaynak dosya konumu ve hedef dosya konumu gösterilmektedir. Hedef dosya konumunu değiştirmek isterseniz 1. Kısımda anlatılan işlemlerin aynısını burada da uygulayabilirsiniz. Hedef dosya adı varsayılanda otomatik olarak kaynak dosya adından “.hkt” uzantısı silinmiş olarak oluşturulur. Bu sayede gerçek dosya uzantısı da korunmuş olur. “Şifre Çözme İşlemine Başla” butonu ile süreci başlatabilirsiniz. Eğer bilgilerde eksiklik ya da hata varsa çözme işlemi başlamadan önce program sizi uyaracaktır.

### 3. Resim (BMP) Şifrele:

Butona tıkladığınızda sizden şifrelemeyi istediğiniz “.bmp” uzantılı dosyayı seçmeniz istenecektir. Bu ekranda sadece “.bmp” uzantılı dosyalar görüntülenir. Dosyayı seçtikten sonra otomatik olarak ilgili sekmeye yönlendirilirsiniz. Örnek bir ekran görüntüsü aşağıda verilmiştir.



“Dosya” satırında açılan dosyanın tam yolu görünmektedir. “Şifre” satırına dosya şifrelenirken kullanılacak şifreyi yazıp “Şifrele” butonu ile işlemi başlatabilirsiniz. Seçtiğiniz resim otomatik olarak Resim Önizleme kısmında görüntülenecektir. Şifrele butonuna tıklayınca bilgilerde eksik ya da hata varsa program sizi uyaracaktır, aksi takdirde resmin şifreli halinin nereye kaydedileceğini soran bir ekran gelecektir. Dosya adı otomatik olarak kaynak dosyanın sonuna, uzantısından önce “Şifreli” ibaresi eklenerek oluşturulacaktır. Hedef dosyayı seçmenizle birlikte şifreleme işlemi

başlar ve bitince “Şifrelenmiş Resim” kısmında şifreli BMP dosyasının ön izlemesi görünür.

#### 4. Şifrelenmiş Resmi (BMP) Çöz

3. kısımda anlatıldığı gibi şifrelenen resimleri çözmek için bu buton kullanılabilir. Butona tıklanınca şifreli BMP dosyasının yerini soran bir ekran gelir. Dosya seçilince ilgili sekmeye otomatik olarak yönlendirilirsiniz ve şifrelenmiş resmin ön izlemesi görünür. Aşağıda örnek bir ekran görüntüsü mevcuttur:



3. kısımda anlatılana benzer şekilde “Şifre” satırına çözülmesi istenen dosyanın şifresini yazıp “Çöz” butonuna basıldığında bilgilerde eksik ya da hata yoksa çözülmüş dosyanın nereye kaydedileceği sorulacaktır aksi takdirde program sizi uyaracaktır. Hedef dosya seçildiğinde çözme işlemi otomatik olarak başlayacaktır. Çözme işlemi bitince “Çözülmüş Resim” kısmında otomatik olarak ön izlemesi görüntülenecektir.

#### 5. Çıkış

Programı kapatır.

Yardım menüsü altında ise sadece “Hakkında” butonu mevcuttur. Program hakkında kısa bilgi verir. Örnek ekran görüntüsü aşağıdaki gibidir.

