**YAZILIM MUHENDISLIGI GUNCEL KONULAR GUVENLİ DİJİTAL HAYAT UYGULAMASI**

**Mücahit Bozkurt**

**16541036**

**Proje Konusu:** 1Milyon Bit Üreteci Hashing ve 3DES Şifreleme Algoritması

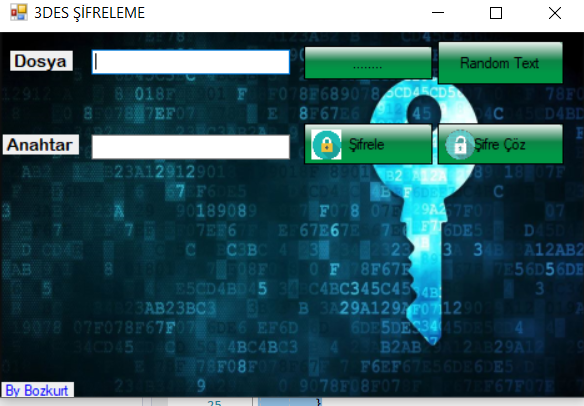
**Github:** <https://github.com/mucahit1/3DES_SIFRELEME>

**Mail:**16541036@firat.edu.tr,bmcahit1456@gmail.com

**Proje Tanıtımı ve Gereksinimler**

Projede hedef öncelikle bir milyon bit üretecek ve bunu text dosyasına kaydedecek bir ardından bu dosya üzerinde hash ve 3DES şifreleme işlemleri yapacak bir form ortaya koymak.Verilerin şifrelenmesi için güvenli bir algoritma ortaya koymak ve kullanıma sunmak hedeflendi.Farklı formatlardaki dosyaları şifrelemek için kullanılabilecek bir ürüm ortaya koymak amaçlandı.

**Tasarım**



C# NET.Framework ile bir form uygulaması oluşturdum.

Bir milyon bit üreteci olarak

using (StreamWriter writer = new StreamWriter(filename, false, Encoding.UTF8))

{

for (int i = 0; i < 1000000; i++)

{

number = r.Next(lowerRange, upperRange);

writer.Write(number + " ");

}

writer.Flush();

writer.Close();

MessageBox.Show("Text Dosyanız Oluşturuldu.Dosya Yolunuz:" + filename);

For döngösü içerisinde random olarak 0-2 aralıgındaki değerleri 1 mılyon kez yazdıran metodu bır butona atadım.

Ardından bu butona bir openfilediaolog yardımcı metodu atadım.Dosyaların kaydedileceği dosya yolunu seçtikten sonra buraya 1 miyon kez 0 1 yazdırırak.Txt Dosyasının içeriğini tamamlamış oldum.

Ardından 3Des için bir class oluşturdum ve bu class içerisinde

c# UTF ve 3des kodlama kutuphanelerinden de faydalanarak şifreleme şifre çözme metodlarını yazdım.

public void Sifrele(string filepath)

{

byte[] Bytes = File.ReadAllBytes(filepath);

byte[] eBytes = des.CreateEncryptor().TransformFinalBlock(Bytes, 0, Bytes.Length);

File.WriteAllBytes(filepath, eBytes);

}

3DES algoritması çift taraflı çalışır yani şifrelenen veri, bir anahtar yardımıyla tekrar çözülebilir. Anahtar 24 byte uzunluğundadır. Hesaplarsak 24×8 =192 bit eder, her byte’in 1 biti eşlik biti olarak kullanıldığından 192-24=168 bit elde edilir. Yani DES’teki 56 bitlik anahtarın tam tamına 3 katı bir anahtar uzunluğu elde edilmiş olur. Bu algoritmanın dezavantajı ise, Des işlemi 3 kez yapıldığı için üç kat daha yavaş çalışmasıdır. Günümüzde halen bankacılık, elektronik ödeme sistemi, yazılım anahtarı oluşturma gibi yerlerde kullanım alanı bulmaktadır.

Veri, 3DES anahtarının ilk 8 baytı ile şifrelenir. Sonra veri anahtarın ortadaki 8 baytı ile çözülür. Son olarak anahtarın son 8 baytı ile şifrelenerek 8 bayt bir blok elde edilir.

**Kodlama yapılırken**

System.Security.Cryptography kütüphanesi kullanıldı.

TripleDESCryptoServiceProvider sınıfı kullanıldı.

Diğer winform companentleri ise standart olarak kullanıldı.( Label button textbox form)

**Sonuç**

3DES,AES ve şifreleme algoritmaları hakkında teknik bilgi birikimi pekiştirildi.

Hashing işlemleri ve türevlerinin sql veri kayıtlarında nasıl kullanılabileceği araştırıldı ve gerekliliği kavrandı.