PROJE ÖZETİ

PROJE ADI: E-Günce: Şifreli Günlük Yazılımı

İnsanlar uzun yıllardır günlük yazmaktadırlar. Günlüklerde kişisel ve özel bilgiler de bulunabilmektedir. Bu nedenle günlüğün sahibinin günlüğünü koruması gerekmektedir. Bu projede de, güvenliğini Advanced Encryption Standard isimli algoritma (*Rijndael*) ile sağlayan bir günlük yazılımı geliştirilmiştir. Hızlı ve kolay kullanılabilir olmasından dolayı proje, C# dili kullanılarak geliştirilmiştir.

Projenin şifreleme adımları şu şekildedir:

1) Kullanıcı şifrelenmesini istediği günlük metnini Windows form içerisinde bulunan ilgili alana yazar,
2) Güvenliğin sağlanması için kullanılacak olan anahtarı da (*bu anahtar çok önemlidir zira şifreli içerik yalnızca aynı anahtar ile çözülebilir.*) ilgili alana yazar,
3) Şifreli dosyanın bulunacağı konumu seçer,
4) Şifrele butonuna basar.
5) Dosya AES algoritması ile şifrelenir.

Eğer herhangi bir hata oluşmazsa, kullanıcının seçtiği konumda günlüğün şifrelendiği tarihin de yazılı olduğu şifreli bir dosya oluşturulur.

Şifre çözme adımlarını da şu şekilde sıralayabiliriz:

1) Kullanıcı şifreli dosyayı Windows formda bulunan “Aç” butonu ile seçer,
2) Şifrelemede kullanılan *aynı* anahtarı da anahtar kısmına yazar,
3) Şifre çöz butonuna basar.
4) Dosya AES algoritması ile geri-şifrelenir. (Şifresi çözülür.)

Eğer dosya hasar almamışsa ve anahtar da doğruysa, şifre çözülür ve şifresiz metin Windows formdaki ilgili bölümde otomatik olarak yazılır.

Gelecekte, halen üzerinde çalıştığımız kendi güvenlik standardımızı da uygulama kapsamında kullanabilmek, ülkemize özgü kriptoloji çalışmalarına katkıda bulunmak, gelecek planlarımız dahilindedir.

Anahtar Kelimeler: Şifreleme, AES, Rijndael, günlük, kriptoloji, kriptografi, yazıbilim, şifrebilim, C#, C Sharp, Advanced Encryption Standard, E-Günce