SDU International Journal of Technological Science
Vol. 10, No 2, August 2018
pp. 47-56

Computational Technologies

e-İMZA İLE DOSYA ŞİFRELEME UYGULAMASI

Ziya Dirlik *, Tuncay Aydoğan

Geliş Tarihi/ Received: 07.11.2018, Kabul tarihi/Accepted: 22.11.2018

Özet

Günümüz teknolojisinin hızlı şekilde gelişmesiyle ortaya çıkan güvenlik açıklarının ne kadar önemli olduğu görülmektedir. Kriptoloji, kişilerin veya kurumların bilgilerinin korunmasını sağlamaktadır. Kriptografik algoritmalar bilgi güvenliğinin sağlanması için yaygın olarak kullanılır. Gelişmeler ışığında önemli olan, kriptografik işlemlerinin günlük hayata nasıl uygulandığıdır. Bu çalışmada, geliştirilen uygulama ile dosyaların şifreleme işlemleri elektronik imza ile güçlendirilmiştir. Şifrelerin çözülmesi sırasında e-imza doğrulaması gerekmektedir. Böylelikle dosyayı şifreleyen ile şifreyi çözmeye çalışan kişinin aynı kişi olduğundan emin olunacaktır.

Anahtar Kelimeler: Elektronik İmza, Kriptografi, Bilgi Güvenliği, Bilgi gizleme, Elektronik Sertifika, SHA256

A FILE ENCRYPTION APPLICATION WITH e-SIGNATURE

Abstract

It has been seen that how important the security vulnerabilities emerging from the rapid development of today's technology are. Cryptology provides protection of information of persons or institutions. Cryptographic algorithms are widely used to provide information security. What is important in the light of developments is how cryptographic processes are applied to daily life. In this study, with the enhanced application, encryption process of files is strengthened by electronic signature. E-signature verification is required during decryption. It will ensure that the person encrypting the file and the person trying to decrypt the password are the same person.

Key Words: Electronic signature, Cryptography, Information security, Information hiding, Electronic certificate, SHA256

1. Giriş

İmza, bir yazının kimin tarafından yazıldığını veya içeriğinin tasdik edildiğini belli etmek amacıyla metnin altına konulan isim veya işarettir. İmza, bir yandan kişinin hüviyetini, diğer yandan da beyanda bulunma iradesini tespit eder. Böylece imzalayanın metni okuyup anladığı ya da belgeyi bizzat hazırlayan kişi olduğu ve bağlanma iradesinin varlığı anlaşılır [1].

Elektronik imza, dijital ortamdaki veriyi gönderenin ve alanın kim olduğunun kanıtlanmasına imkân tanır. Dolayısıyla imzalanmış bir belgeyi yollayan kişi onu yolladığını, alıcı da aldığını inkâr edemez. Elektronik imza, elle atılan imzanın elektronik ortamdaki karşılığını oluşturmaktadır. Elektronik imza, kapsamlı verilerde değişiklik yapılmasını önleyen veya verilerde değişiklik yapılması durumunda bu değişikliğin gerçekleştiğini anlamamızı sağlayan sistemdir. Elektronik imza , Adli Tıp incelemesinin ortaya koyduğu sonuçların yani verinin orijinalliğinin kanıtlanmasına, bir başka deyişle elektronik imzalı olarak veriyi kimin oluşturduğunun tespitine olanak verir [2].

* Süleyman Demirel Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 32000, Isparta
E-posta: ziyadirlik@sdu.edu.tr

Başka bir tanıma göre elektronik imza, ıslak imzanın fonksiyonlarını kapsayan ve bir veri mesajında bulunan veya ona eklenen mesaj ile mantıksal bağlantısı kurulabilen, bireyin kimliğini tanıtan ve bireyin, mesajın içeriğini onayladığını gösteren elektronik formattaki imzadır [3].

İmzanın geçerlilik kontrolü bilgisi için gerekli olan sertifika sahibinin açık anahtarı, imzalı veride bulunan "sertifikalar verisi" içerisinde yer almaktadır. Ayrıca, imza doğrulayıcı tarafından hesaplanan içerik özeti (Hash) ile imzada bulunan içerik özetinin birbiri ile uyumlu olması gerekmektedir. İmzanın hash'i hesaplanırken kriptografik algoritmalar kullanılır. Zamanla bu algoritmaların güvenilirliği azalmaktadır. Bu nedenle, elektronik imza verisi zamanla zayıflamakta ve kırılabilmesi mümkün olmaktadır [4].

Bilgi, kurumdaki diğer kaynaklar gibi, kurum için önem taşımakta ve bu nedenle de bilginin en iyi şekilde korunması gerekmektedir. Bilgiye yönelik olası saldırılar (tahrip edilmesi, silinmesi, gizliliğinin zarar görmesi), bilgi altyapısının bozulmasına ve beraberinde işlerin akmasına neden olmaktadır.

Günümüz teknolojisinin hızlı bir şekilde ilerlediği göz önüne alındığında güvenlik açıklarının ne kadar risk oluşturduğu görülmektedir. Kriptoloji, şahıslar veya devlet kurumları arasındaki haberleşmelerden, mesajlaşmalardan ve bunların oluşumlarının her aşamasındaki güvenlik boşluklarını dolduran önemli bir bilim dalıdır ve bu bilim dalı geçmişten bu yana farklı yöntemlerle kullanılmaktadır [5].

Bilgi güvenliği; kurumdaki işlerin sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması ve yatırımlardan gelecek faydanın artırılması için bilginin geniş çaplı tehditlerden korunmasını sağlamaktadır [6].

"Elektronik imza", "e-imza" ve "sayısal imza" anahtar kelime taramalarında e-imzanın finans sektörü, sigortacılık, hukuksal alandaki kullanımları, bilişim suçları, e-ticaret, kamu yönetimi açısından önemi ve bu alanlarda geliştirilen uygulamaların olduğu görülmektedir. Ayrıca e-imzayı güçlendirme amacıyla konum damgası sistemi, rol tabanlı kurumsal güvenli mesajlaşma sistemi, güvenli özet algoritması gibi modeller geliştirilmektedir.

Özlü'nün, "E-imza Güvenliğinin Artırılmasına Yönelik Konum Damgası Sistemi Önerisi ve Uygulaması" başlıklı çalışmasında, e-imzanın yetkisiz kişiler tarafından kullanımını önlemek amacıyla, elektronik olarak imzalanan belgelerin güvenliğini artıracak yeni bir sistem önerilmektedir. Küresel yer belirleme sisteminden de yararlanan bu sistem e-imzalı belgelerin nerede imzalandığının tespit edilmesine ve e-imza kullanımının konum açısından sınırlanabilmesine olanak sağlamaktadır. Çalışma kapsamında önerinin gerçekleşebilirliğini ortaya koymak için geliştirilen e-imza güvenliğinin artırılmasına yönelik konum damgası sistemi uygulamasında da başarılı sonuçlar elde etiiği görülmektedir [7].

Avaroğlu, "Elektronik İmza" çalışmasında, e-imza kullanımı hakkında ülkemizdeki bilinç ve bilgi birikimine katkı saglamak amacıyla bilgi ve bilgisayar sistemleri güvenliği, şifreleme bilimi, e-imza kavramı, e-imza teknik altyapısı (AAA) ve elektronik sertifikalar konusunda bir araştırma yapmıştır. Çalışmada, özellikle e-imzanın kişilere ne olduğunun tanıtılması, ne amaçla kullanıldığı, yararları, eksiklikleri, e-imza konusunda yaşanılan problemler ile e-imzada kullanılan altyapıdan bahsedilmektedir. E-imza sistemlerinin hayata geçirilmesinde dikkat edilmesi gereken hususlar ile e-imzanın yaygınlaşmasına yönelik öneriler de sunulmaktadır [8].

Budak'ın, "Güvenli Özet Algoritması" başlıklı çalışmasında, tek-yönlü özet fonksiyonlarının matematiksel temellerini, kripto analizini incelemiş ve güvenli özet algoritmasının simülasyonunu gerçekleştirmiştir. Günümüzde bir standart olarak kabul gören ve hemen hemen bütün yazılım ve donanım tabanlı kriptografik uygulamaların ayrılmaz bir parçası olarak yer alan özet fonksiyonlarının matematiksel temelleri ve yapıtaşları incelenmekte bu fonksiyonların kripto analizi yapılmaktadır. Özet fonksiyonlarından biri olan ve günümüzde bir standart olarak kabul gören güvenli özet algoritmasının işleyişini detaylı bir şekilde ele almakta ve kripto analizini yapmaktadır. Elektronik imza hakkında genel bilgi verilmekte, özet fonksiyonlarındaki zayıflıklar incelenerek elektronik imzaya etkisi ortaya konmaktadır [9].

Sağır, "Açık anahtar altyapısı ve elektronik imzanın mobil tabanlı uygulaması" başlıklı çalışmasında, Windows işletim sistemi üzerinde çalışan İmzager, İmzala-Gönder ve PDF İmzalama uygulamalarının yaptığı işlemlerden elektronik imzalama işleminin PFX dosyası formatıyla Android üzerinde gerçekleştirilmesini sağlayan bir uygulama gerçekleştirmiştir [10].

Bu çalışmada, Windows ortamında geliştirilen uygulamada elektronik imza ile dosya şifreleme işlemlerinin nasıl yapılacağı anlatılmaktadır. Özel bilgilerin olduğu dosyaların başkaları tarafından açılıp incelenmesini kimse istememektedir. Şifre konulup dosyaların şifrelenmesi durumunda ise şifreler bir şekilde tahmin edilebilmekte ya da kırılabilmektedir. Dosya şifreleme işlemler e-imza ile yapıldığında ise şifrenin tahmin edilme olasılığı ortadan kalkmaktadır. Şifrenin kırılma olasılığı ise daha da zorlaşmaktadır.

2. Materyal ve Metot

Bu bölümde elektronik imza ile dosya şifreleme uygulaması geliştirilirken kullanılan yöntemler anlatılmaktadır.

Kriptografi (Şifreleme)

Gizlilik, kimlik denetimi, bütünlük gibi bilgi güvenliği kavramlarını sağlayabilmek için uygulanan matematiksel yöntemlerin hepsine kriptografi denir. Bu matematiksel yöntemler, bilginin aktarımı esnasında olabilecek aktif ya da pasif saldırılardan bilgiyi ve bilgi ile birlikte bilginin göndericisi ve alıcı bilgisini de korumayı hedeflemektedir. Kısaca okunur olan bir verinin istenmeyen kişilerce okunamayacak duruma dönüştürülmesinde kullanılan yöntemlerin tamamı olarak tanımlanmaktadır.

Kriptografi, mesajların gizli tutulması sanatı veya bilimidir. Kriptanaliz şifrelerin kırılması sanatıdır. Doğru anahtarı bilmeden düz-metnin elde edilmesi şeklinde örneklendirilebilir. Kriptografi ile uğraşanlara kriptograf ve kriptanalizin uygulamacılarına kriptanalist denir.
Kriptografi gizli mesajlaşma, onaylama, dijital imzalar, elektronik para ve diğer uygulamaların tüm yönleriyle ilgilidir. Kriptoloji, kriptografik metotların matematiksel temelleriyle ilgilenen bir matematik dalıdır [15].

Kriptografi işlemi, veriyi anlamsız hale dönüştürme, veri üzerindeki saptanmayan değişimi engelleme ya da veriyi yetkisiz kişilerin kullanımından koruma amacıyla uygulanmaktadır. Kriptografi, verinin şifrelenmesi ve sonrasında ihtiyaç duyulduğunda tekrar orijinal haline dönüştürülmesi işlemleridir.

Elektronik İmza

Elektronik imza, başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan, kimlik doğrulamak amacıyla kullanılan elektronik veri şeklinde tanımlanmaktadır.

E-imza bir üst kavramdır. Her türlü elektronik ses, sembol veya uygulamayı kapsayan ve kullanılan teknolojiden bağımsız terim olduğu için üst kavram olarak kabul edilebilir. Ancak "sayısal imza" kavramı yerine kullanımına rastlamak da mümkündür.

Elektronik imza oluşturmak için tanımlanmış söz dizimi, Kriptografik Mesaj Söz Dizimi (Cryptographic Message Syntax - CMS)'dir. CMS; imza oluşturmanın yanında, özetleme, doğrulama ve isteğe bağlı mesaj içeriğinin şifrelenmesi gibi işlemler için de kullanılır [4].

E-imzanın kullanımının dünya çapında kabul görmesinin ve gittikçe yaygınlaşmasının sebepleri; güvenilir, taklit edilemez, yeniden kullanılamaz, e-imzalı metin değiştirilemez ve e-imzanın inkâr edilemez olması şeklinde sıralanabilir.

E-imzaların sağladığı başlıca yararlar; veri bütünlüğü, kimlik doğrulama, inkâr edememe, gizlilik şeklinde sıralanabilir.

Veri bütünlüğü (Integrity), elektronik imza bilgisinin doğruluğunun onaylanmasıdır. Okunan mesajın yanlışlıkla ya da kasten değiştirilmediğini ispatlar. Teknik açıdan elektronik imza, imzalanmış doküman bir özet değeri içerir. İçerikte yapılacak herhangi bir değişiklik özet değerini de değiştireceği için imzanın geçerliliğini sona erdirmektedir.

Kimlik doğrulama (Authentication), basit olarak bir el sıkışma (hand-shake) işlemidir. Bu, bir kişinin (ya da ev sahibi firma, sunucu, müşteri) kimliğinin onaylanmasıdır. Bilgiyi imzalayanın yetkinliğini, işleme kimlerin katıldığını, bir başkası tarafından bilginin değiştirilmediğini garanti eder. Öne sürülen kimliğin doğruluğunu onaylayarak bir sisteme giriş yapmak isteyen kullanıcının doğru kimliğini belirler.
İnkâr edememe (Non-repudiation), elektronik ortamda mesajı gönderen ya da alan kullanıcının, mesajı aldığını ya da gönderdiğini inkâr edememesidir. Karşılıklı haberleşmede tarafların birbirinden gelen mesajları aldığını, gönderdiğini teyit etmesi veya bunu inkâr etmemesi gereklidir. Bunu sağlamak için, mesajı gönderen veya alan kişilerin kayıtları güvenilir bir makam tarafından tutulur. Güvenli haberleşmenin yapılabilmesi için uygulanan yaklaşımlar ile inkâr edilemezlik sağlanmaktadır [12].

Elektronik imza altyapısı (Açık Anahtar Altyapısı-AAA)

Elektronik ortamda iletilen bilginin dönüştürülmesi işlemlerine şifreleme denilmektedir. Bu yöntemde bilgi, alıcı dışında başka bir kişi tarafından okunamaması ya da değiştirilememesi için kodlanır. Şifreleme ile gönderilen herhangi bir bilginin gizliliği korunmuş ve bütünlüğü bozulmamış olur [13].

Elektronik imza, Açık Anahtar Altyapısını kullanmaktadır. AAA kullanılarak oluşturulan elektronik imza verisi imzacıya ve imzalanan dokümana özel oluşturulmaktadır. Bu nedenle başkaları tarafından taklit edilemez ve imzalı belge üzerinde değişiklik yapılamaz. İstenildiğinde elektronik imzanın doğruluğu kontrol edilebilir.

Elektronik imza, imza sahibinin kimliğinin doğruluğunu kanıtlar. İmzalanmış olan verinin içeriğinin başka kişi tarafından değiştirilip değiştirilmediğini (bütünlüğünün bozulup bozulmadığını) kanıtlar [14].

Özel anahtar (private key), imza sahibine ait olan, imza sahibi tarafından elektronik imzayı oluşturmak için kullanılan ve benzersiz, kriptografik, gizli anahtar gibi verilerdir. E-imzayı oluşturmak için kullanılır. Sadece kişinin kendisinde bulunur ve güvenli elektronik imza oluşturma aracı içinde saklanır.

Bu çalışmadaki uygulama kişinin özel anahtar bilgisi ile şifreleme işlemi gerçekleştirmektedir. Windows ortamında, yazılan uygulama ile imza sahibinin özel anahtar bilgisi ile şifreleme ve şifre çözme işlemleri gerçekleştirilmektedir.

Nitelikli Elektronik Sertifikalar

Elektronik sertifika, günlük hayatta kullanmış olduğumuz nüfus cüzdanı, ehliyet, pasaport vb. kimlik kartlarının elektronik ortamdaki karşılığıdır. Elektronik sertifikalar, kişi için üretilen anahtar çiftlerinden açık anahtarı, kişinin kimlik bilgisine bağlayan elektronik kayıtlardır. Başka bir ifadeyle elektronik sertifikalar kişinin sanal ortamdaki kimlik kartı olarak ifade edilmektedir.

Nitelikli elektronik sertifikalar, geçerlilik süresinin sona ermesinden önce sertifika sahibinin veya sertifika sahibinin onayını almak koşuluyla kurumsal başvuru sahibinin talebi doğrultusunda Elektronik Sertifika Hizmet Sağlayıcısı (ESHS) tarafından yenilenir. ESHS, nitelikli elektronik sertifikayı, sertifika sahibine ait bilgilerin geçerliliğini doğrulayarak yeniler. Sertifikada yer alan bilgilerin değişmesi halinde de yenilenmesi gerekir [3].

Ülkemizde şu anda hizmet veren beş tane ESHS vardır (Çizelge 2.1). 5070 Sayılı Elektronik imza Kanunu'nun kabulü ile ilk kurulan ESHS'lerden biri TUBITAK-UEKAE'dir. TUBITAK-UEKAE devlet desteği ile kurulan bir kamu ESHS'dir. Yapılan yasal düzenlemeler ile TUBITAK-UEKAE sadece kamu kurumu çalışanlarına nitelikli elektronik sertifika vermektedir.

Çizelge 2.1. Türkiye'de elektronik sertifika hizmet sağlayıcıları

Elektronik Sertifika Hizmet Sağlayıcı -TÜRKİYE-
Elektronik Bilgi Güvenliği A.Ş. (E-Güven)
TUBİTAK-UEKAE (Kamu Sertifikasyon Merkezi)
E-İmza Bilgi Güvenliği Hizmetleri A.Ş.(E-İmzaTR)
EBG Bilişim Teknolojileri ve Hizmetleri A.Ş. (E-Tuğra)
TürkTrust Bilgi, İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.

Elektronik sertifikaların temel görevi, kişinin sanal ortamda kimliğini belirlemek ve yapılan işlemin inkâr edilmemesini sağlamaktır. Elektronik sertifikaların oluşturulması ve yayımlanması, kişinin kendi talebi üzerine oluşturulmaktadır.

Elektronik sertifikalar talep üzerine oluşturulmakta ve yayımlanmaktadır. Resim 2.1'de bir elektronik sertifika örneği gösterilmektedir. ESHS tarafından, nitelikli elektronik sertifika başvurusundan sonra sertifika oluşturulur ve sertifika sahibine teslim edilir. Sertifikanın geçerlilik süresi sözleşmeyle belirlenir. Sertifika, teslim edilmeden önce sertifikayı talep eden kullanıcının, elektronik imza kullanımına ilişkin aydınlatma yükümlülüğünü yerine getirmesi ve sertifikanın sigortalandıktan sonra kullanıcıya teslim edilmesi gerekmektedir [15].

Sertifika Seri Numarası	**59014325431**
Sertifika Sahibinin Kimlik Bilgileri	**Ziya DİRLİK**
Sertifika Geçerlilik Başlangıç Tarihi	**10 Subat 2008 14.00**
Sertifika Geçerlilik Bitiş Tarihi	**10Eylül 2009 14.00**
Sertifikanın Kullanım Amacı	**Test Kullanımı**
Kullanılacak Algoritma	**Sha1RSA**
Sertifika Sahibinin Açık Anahtar Bilgisi	**65 94 73 58 59 ef 8e 6f 1e 95 22 a7 c9 67 2e a5 d4 ee 2c 1c**
Yayınlayan ESHS	**XXXX Kurumu**
ESHS Elektronik İmzası	**4t 4a 31 e8 9y 3d fa 3e 0a b7 dd 70 71 c7 51 7c 45 83 4f 11**

Resim 2.1. Elektronik sertifika örneği

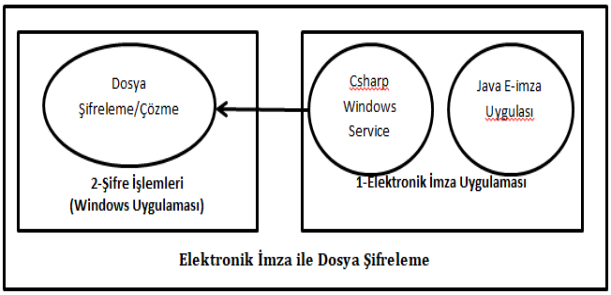
3. Bulgular

Günümüzde teknolojinin ilerlemesi ile bilginin, verilerin şifrelenmesi önemli bir unsur haline gelmektedir. Şahsi ya da kurum tarafından ortak kullanılan bilgisayarlardaki dosyalar saklanmak istenilmektedir. Saklama işlemleri basit bir şifreleme işlemi ile yapıldığında, şifrelerin kırılması ya da tahmin edilmesi kolaylaşmaktadır. Konulan şifreler akılda kalması için basit şifreler olmaktadır.

Bu çalışmada, Windows işletim sistemi ortamındaki dosyaların şifrelerinin kırılmasını zorlaştırmak amacıyla bir uygulama geliştirilmiştir. Uygulama sayesinde, şifreleme işlemleri elektronik imza ile gerçekleştirilmektedir. Elektronik Sertifika Hizmet Sağlayıcısı (ESHS) tarafından elektronik imzanın içerisine yerleştirilmiş, her e-imza için benzersiz olan hexadecimal seri numarası ile şifreleme ve şifre çözme işlemleri gerçekleştirilmektedir.

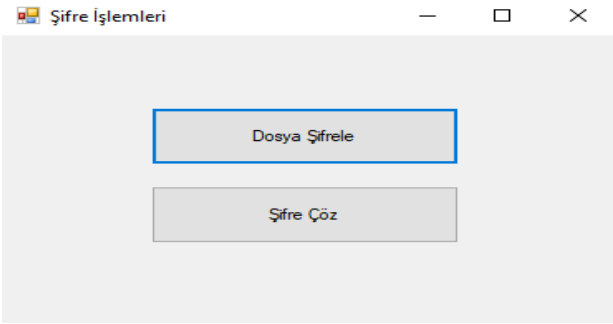
ESH sağlayıcıları tarafından gönderilen akıllı kartın okunması için gerekli programlar bilgisayara yüklenmelidir. Yüklenmesi gereken programlar "http://www.kamusm.gov.tr/" adresinde anlatılmaktadır. Şifreleme işlemlerinin gerçekleşebilmesi için programların bilgisayara kurulu olması ve çalışır olması gerekmektedir. Aksi durumda geliştirilen elektronik imza uygulaması karta erişim sağlayamayacağı için şifreleme işlemleri gerçekleştirilmemektedir.

Resim 3.1'de tasarlanan sistemin yapısal şeması görülmektedir. Elektronik imza uygulaması, Java programlama dilinde geliştirilmiştir. Kamu Sertifikasyon Merkezi tarafından elektronik imza geliştiricileri için yayımlanan kütüphaneler kullanılarak Netbeans ortamında yazılmıştır.



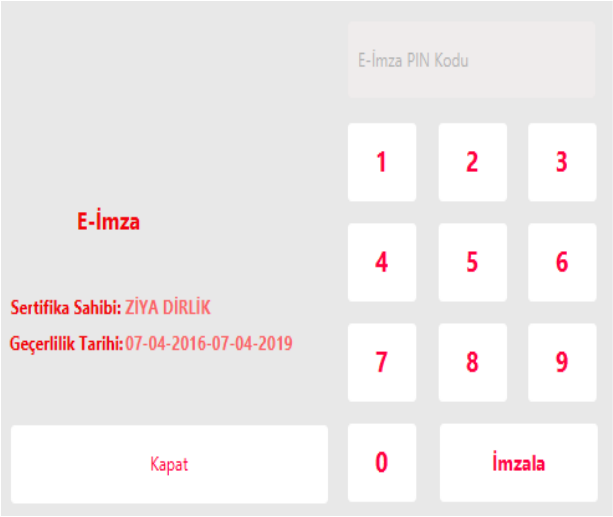
Resim 3.1. Tasarlanan sistemin yapısal şeması

Windows uygulaması, C# programlama dilinde geliştirilmiştir. Geliştirilen uygulamada, e-imza uygulamasında kimlik doğrulaması başarılı şekilde gerçekleştirildikten sonra şifreleme ve şifre çözme işlemlerine izin verilmektedir. Aksi durumda şifreleme ve şifre çözme işlemlerine izin verilmemektedir. Geliştirilen Windows uygulamasının ara yüzü Resim 3.2'de gösterilmektedir.



Resim 3.2. Şifreleme işlemleri için geliştirilen uygulamanın ara yüzü

Şifreleme işlemleri, uygulamanın ara yüzünden dosya şifrele butonuna tıklandığında dosya "Gözat" penceresi açılmaktadır. "Dosya Gözat" penceresinden şifrelenmek istenilen dosya seçildikten sonra, Resim 3.3'deki e-imza uygulaması çalışmaktadır.



Resim 3.3. Elektronik imza uygulaması

E-imza uygulamasında PIN kodu doğru şekilde girildikten sonra dosyanın şifrelenme işlemi başarılı şekilde yapılmaktadır.

Şifre çözme işlemleri için Resim 3.2'deki ara yüzden "Şifre Çöz" butonuna tıklanması gerekmektedir. Butona tıklandıktan sonra, şifreli dosyanın seçilmesi için "Dosya Gözat" penceresi açılmaktadır. Dosya seçildikten sonra kimlik doğrulama işlemleri için e-imza uygulaması çalışmaktadır. E-imza kimlik doğrulama işlemi başarılı şekilde sağlandıktan sonra dosyanın şifre çözme işlemi başarılı şekilde yapılmaktadır.

Şifreleme İşlemlerinin Altyapısı

ESH tarafından kişi adına oluşturulan Akıllı kartın içerisinde, her kişi için özel oluşturulan hexadecimal seri numarası verilmektedir. E-imza uygulamasında kimlik doğrulama işlemi başarılı şekilde sağlandıktan sonra, geliştirilen uygulama ile karttaki hexadecimal numaraya erişim sağlanmaktadır. Bu numara ile şifreleme işlemleri SHA256 algoritmasına göre gerçekleştirilmektedir. Bu sayede şifrelenen dosyaların başkası tarafından açılması zorlaşmaktadır.

SHA256, girilen mesajın uzunluğundan bağımsız, 256-bit (32 byte) mesaj özeti oluşturur ve bu kriptografik olarak en güvenilir özetleme fonksiyonlarından biridir. Bir çok kripto ağı altyapısında SHA256 isimli özet fonksiyonu kullanılmaktadır [16].

SHA256 özet algoritma yapısı, üç farklı işleme bölünebilir. Bunlar aşağıda sırasıyla şu şekildedir.

- **Ön işleme:** Özet algoritması tarafından beklenen 512 bitlik bloğun eksik kısımları 0 ile genişletilmekte ve 512 bitten daha uzun olan mesajlar, 512 bitlik bloklara bölünerek fonksiyona beslenmektedir.
- **Mesaj planlayıcı:** 16 kelimelik giriş mesaj bloğundan altmış dört adet kelime üreten fonksiyondur.
- **Sıkıştırma fonksiyonu:** Her döngüde mesaj planlayıcıdan gelen mesaj bağımlı kelimenin gerçek özet işlevinin yapıldığı fonksiyondur [17].

Şekil 3.4 de SHA256 algoritmasının "EncryptFile()" ismindeki method ile uygulamaya eklendiği komut satırları görülmektedir. Method dosya yolu ve kartın haxedecimal kodunu parametre alarak, "CoreEncryption.AES_Encrypt()" methodu ile dosya şifrelenerek şifreli bir dosya oluşturulmaktadır. Sonraki kod satırlarında eski dosya ile yeni oluşturulan şifreli dosya yer değiştirilmektedir. Bu şekilde şifreli dosya oluşturulmaktadır.

```
public void EncryptFile(string filePath, string haxedecimalkod)
      {
         byte[] bytesToBeEncrypted = File.ReadAllBytes(filePath);
         byte[] passwordBytes = Encoding.UTF8.GetBytes(haxedecimalkod);
         // Hash the password with SHA256
         passwordBytes = SHA256.Create().ComputeHash(passwordBytes);
         byte[] bytesEncrypted = CoreEncryption.AES_Encrypt(bytesToBeEncrypted,
            passwordBytes);
         string fileEncrypted = filePath;
         File.WriteAllBytes(fileEncrypted, bytesEncrypted);
      }
```

Şekil 3.4 Şifreleme işlemlerinin yapıldığı method

4. Tartışma ve Sonuç

Geliştirilen uygulama ile kişisel ya da ortak kullanılan bilgisayarlardaki, dosyaları şifrelemek elektronik imza ile daha güvenli olmaktadır. Dosyaların şifrelenmesi ve şifrelerin çözülmesi için mutlaka e-imza doğrulaması gerekmektedir. Bu sayede verilerimize ulaşmak artık, e-imza'yı elinde bulunduran kişi ile mümkün olmaktadır. Kendimizin belirlemiş olduğu bir şifre olmadığı için ortada şifrelerin çalınma, ele geçirilme durumu da olmamaktadır. E-imza doğrulaması sayesinde dosyayı şifreleyen kullanıcı ile şifreyi çözen kullanıcının aynı kişi olduğu doğrulanmaktadır.

E-imza ile dosya şifreleme dosyaların korunmasını yeni bir yaklaşımla güçlendirmiştir. Her nekadar litaratürde SHA256 algoritmasının üst düzey özel yazılımlar ile kırılabileceğine yönelik yayınlar olsa da SHA256 yaygın olarak kullanılmaktadır.

Geliştirilen uygulama windows platformunda çalışan bir uygulamadır. İlerleyen çalışmalarda linux, macos gibi platformlar için ve başka şifreleme algoritmaları ile uygulama geliştirilebilir.

Kaynakça

[1] Reed, C., 2003. 'What is a Signature?', The Journal of Information, Law and Technology

[2] Yalçınkaya, B., 2008. Elektronik İmzalı Belgelerin Yönetimi ve Arşivlenmesi, Marmara Üniversitesi, Türkiyat Araştırmaları Enstitüsü, Yüksek Lisans Tezi, 160s, İstanbul

[3] Orta, M., 2007. Türkiye'de Elektronik İmza Uygulaması, Elektrik Mühendisliği

[4] Selçuk, G. H., 2016. E-devlet Uygulamaları için Elektronik imza formatları, TÜBİTAK – UEKAE Kamu Sertifikasyon Merkezi

[5] Aydoğan, M., 2014. Adli Bilişimde Görüntü Üzerine Kriptografi Uygulamaları, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 88s

[6] Özlü, M., 2011. E-imza Güvenliğinin Arttırılmasına Yönelik Konum Damgası Sistemi Önerisi ve Uygulaması, Selçuk Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 78s, Konya

[7] Avaroğlu, E., 2007. Elektronik İmza, İnönü Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 170s, Malatya

[8] Budak, B. (2010).Güvenli özet algoritması, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 110s, Ankara

[9] Sağır, M., 2014. Açık anahtar altyapısı ve elektronik imzanın mobil tabanlı uygulaması, Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 73s, Kocaeli

[10] Aslandağ, K., 2010. Bilgi Güvenliği Kavramı ve Bilgi Güvenliği Yönetim Sistemleri ile Şirket Performansı İlişkisine Dair Bir Uygulama, Gebze İleri teknoloji Enstitüsü, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, 106s

[11] Özduran, V., 2008. Birleşik Şifreleme ve Turbo Kodlama Sistemleri, İstanbul Üniversitesi, Fen Bilimeri Enstitüsü, Yüksek Lisans Tezi, 127s

[12] Özler, İ., 2007., Bilgi Güvenliği ve Elektronik İmza Kavramları, Ekonomik Boyutlarının İncelenmesi ve Elektronik İmza Uygulamaları, Dicle Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, 125s, Diyarbakır

[13] Çak, M., 2002. Elektronik Ticaret ve Vergilendirilmesi, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, 158s, İstanbul

[14] Başbakanlık, 2005. E-dönüşüm Türkiye projesi birlikte çalışabilirlik esasları rehberi

[15] EİK, 2004. 25355 Sayılı 5070 numaralı, Elektronik İmza Kanunu

[16] YILDIRIM, H., 2018. Açık ve uzaktan öğrenmede blokzincir teknolojisinin kullanımı

[17] BALCISOY, E., 2017. Yüksek performanslı bitcoin madenciliği için sha256 özet algoritmasının eniyilenmesi