T.C

BEYKENT ÜNİVERSİTESİ

MÜHENDİSLİK MİMARLIK FAKÜLTESİ

LİSANS PROGRAMI

BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

ŞİFRELEME VE ÖZET ALGORİTMALARI

ENCODER UYGULAMASI

Siber Güvenlik ve Büyük Veri

Hazırlayan

BETÜL TUĞÇE DİKDOĞMUŞ

İstanbul, 2020

T.C

BEYKENT ÜNİVERSİTESİ

MÜHENDİSLİK MİMARLIK FAKÜLTESİ

LİSANS PROGRAMI

BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

ŞİFRELEME VE ÖZET ALGORİTMALARI

ENCODER UYGULAMASI

Siber Güvenlik ve Büyük Veri

Hazırlayan

BETÜL TUĞÇE DİKDOĞMUŞ

Danışman

DR. ÖĞR. ÜYESİ ATINÇ YILMAZ

İstanbul, 2020

ÖZET

ŞİFRELEME VE ÖZET ALGORİTMALARI

ENCODER UYGULAMASI

Betül Tuğçe Dikdoğmuş

Beykent Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği

Siber Güvenlik ve Büyük Veri

Aralık 2020

Teknolojinin gelişmesiyle beraber artık savaşlar ağır silahlarla değil elektronik ortamlarda gerçekleşmektedir. Bu savaştan zararlı çıkan ülkeler bilgi güvenliğinde zafiyet yaşayan ülkelerdir. Hem kişisel verilerin güvenliğini sağlamak hem de askeri sistemler, banka sistemleri ve benzeri alanlarda bilgi güvenliğini sağlamak için şifreleme ve özet algoritmaları kullanılmaktadır. Bu çalışmada şifreleme ve özet algoritmaları hakkında bilgiler verilmiştir. Sezar, ROT13, MD5 ve SHA1 gibi algoritmalar incelenerek geliştirilen encoder uygulamasında test edilmiştir.

Anahtar Kelimeler: Şifreleme, hash, anahtar.

GİRİŞ

Teknolojinin gelişmesi ve internet kullanımının yaygınlaşması bazı güvenlik sorunlarını da beraberinde getirmiştir. Bunun başlıca sebepleri, internetin açık bir sistem olması ve üzerinde dolaşan verinin gasp edilmeye uygun olmasıdır. Alınan ve gönderilen veri paketleri birçok halka açık ağlardan geçer, bu da bu paketlere erişimin herkes için mümkün olduğunu göstermektedir. Bu durum bilgi güvenliğinin sağlanması ihtiyacını doğurmuştur. Bilgi güvenliği bilginin gizlilik, bütünlük ve sürekliliğinin korunmasıyla sağlanır. Kriptoloji şifreleme bilimidir ve bilgi güvenliğini sağlamayı amaçlar. Bu amaç doğrultusunda birçok algoritma geliştirilmiştir. Bu algoritmalar bir siteye kayıt olurken, giriş çıkış işlemlerinde, dosya güvenliğini sağlamak için vb. birçok alanda kullanılmaktadır.

Bu çalışmanın amacı çeşitli algoritmaların mantıklarını kavrayarak uygulama güvenliği denetimlerinde ihtiyaç duyulabilecek en önemli araçlardan biri olan encoder geliştirmektir.

LİTERATÜR ÇALIŞMASI

KRİPTOLOJİ

Kriptoloji, Yunanca krypto's (saklı) ve lo'gos (kelime) kelimelerinin birleştirilmesinden oluşturulmuştur ve iletişimde gizlilik bilimi olarak değerlendirilmektedir [1].

Kriptoloji uzun yıllardır insanoğlu tarafından mahrem bilginin saklanması amacıyla kullanılmıştır. Bilişim teknolojilerinin ve dolayısıyla internet teknolojilerinin yaygınlaşmasıyla kriptoloji bilimi daha fazla önem kazanmıştır [3]. Şifre bilimi olan kriptoloji verilerin şifrelenmesi ve şifrelenmiş verilerin çözümlenmesi için tekniklerle ilgilenir [2].

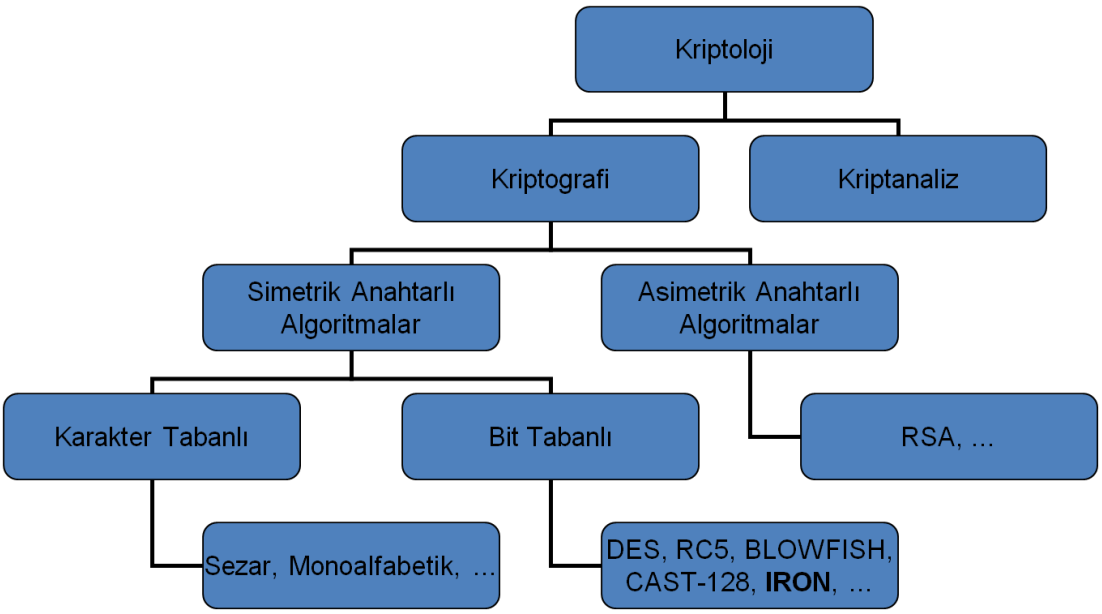
KRİPTOGRAFİ VE KRİPTOANALİZ

Kriptografi, verilerin açık halden kapalı yani gizli hale getirilmesi işlemidir. Verilerin gizliliğini, bütünlüğünü, güvenliğini sağlar. Bu işlemi yapan kişilere kriptograf denir. Eldeki metnin anlaşılabilir haline düz metin ya da açık metin denilmektedir. Düz metnin farklı işlemlerden geçirilerek anlaşılamayacak bir forma dönüştürülmesi sonucunda elde edilen yeni forma şifreli metin denilmektedir [5]. Şifreleme işlevinin güvenli bir şekilde gerçekleşmesi kriptolama sırasında kullanılan tüm yöntem ve bilgilerin gizliliğine dayanır [1]. Kriptografların şifreli hale getirdiği metinlerin analizi ve şifrelerin çözümü ile ilgilenen kriptoloji alt bilim dalıdır. Bu işi yapan kişilere kriptoanalist denir [5]. Kriptoanaliz, şifrelenmiş yani anlamsız bir metinden doğru metni bulma yöntemidir [4]. İyi bir kriptoanaliz için kriptografi de iyi bilinmelidir. Bu şifrelerin üretilme şekli bilindiği takdirde şifreleri çözmek mümkündür [2].

YÖNTEM

ŞİFRELEME ALGORİTMALARI

Verilerin güvenliğini sağlayabilmek için çeşitli şifreleme ve şifre çözme teknikleri oluşturulmuştur. Şekil 1'de görüldüğü üzere bu tekniklerin çeşitli ihtiyaç ve yöntemlere göre sınıflandırılması yapılmıştır. Simetrik algoritmalarda şifreleme ve şifre çözme işlemlerinde aynı anahtar kullanılmaktadır. Eğer anahtar kötü niyetli kişinin eline geçerse şifreli metinler kolaylıkla çözülür. Bu durum simetrik algoritmanın zayıf bir yönüdür ancak basit ve kullanışlı olmalarından ötürü tercih edilmektedir. Şekil 1'deki gibi simetrik algoritmalara DES, RC5 veya Sezar algoritmaları örnek gösterilebilir. Simetrik algoritmalardaki anahtar dağıtımı ve güvenlik problemlerine çözüm getirmek amacıyla asimetrik algoritmalar oluşturulmuştur. Asimetrik algoritmalar şifreleme ve şifre çözme işlemlerini farklı anahtarlar kullanarak yapmaktadırlar. Şifreleme açık anahtar ile yapılırken deşifreleme işlemleri için gizli anahtar kullanılmaktadır. Yani açık anahtar haberleşme yapacak olan kişilere dağıtılır ancak gizli anahtar sadece alıcıda bulunur. Şekil 1'deki gibi RSA algoritması en yaygın kullanılan asimetrik şifreleme algoritmasıdır.



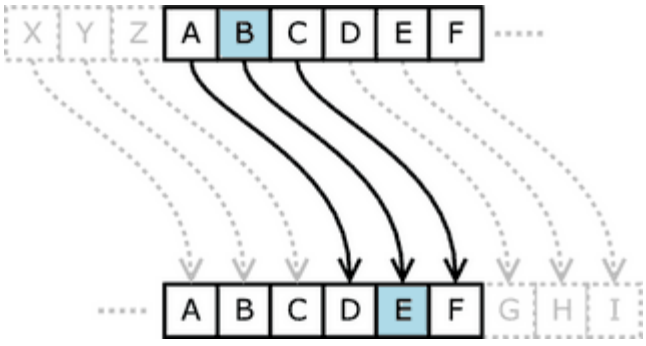
Şekil 1. Şifreleme Algoritmalarının Sınıflandırılması

ÖZET ALGORİTMALARI

Hash algoritmaları olarak da bilinirler. Girilen bir metni alıp sabit uzunlukta çıktılara dönüştürürler. Yani girdi bir şiir de olsa basit bir kelime de olsa hep aynı uzunlukta çıktılar verir. Girdinin uzunluğundan bağımsız olarak hep aynı uzunlukta çıktı ürettiği için mesaj özeti olarak saklanabilmektedirler. Üretilen çıktılar girdilere özeldir ve aynı girdi her zaman aynı sonucu verir. Hashlenmiş bir veri tekrar orijinal haline çevrilemez. Çünkü hash fonksiyonları tek yönlüdürler. Hash algoritmaları parolaların saklanması, sayısal imzalama, mesajın değiştirilmediğinin kontrolü gibi birçok alanda kullanılmaktadırlar. Hash algoritmalarına örnek olarak MD5 ve SHA ailesi verilebilir.

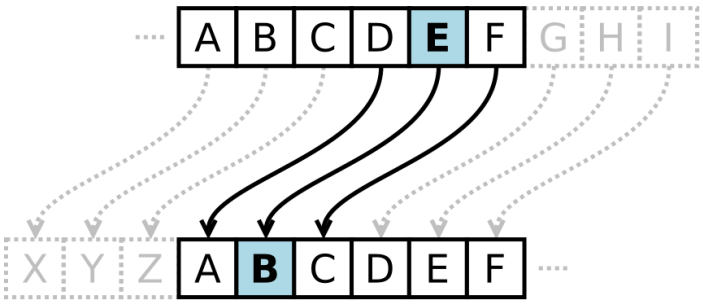
SEZAR

İlk kez Julius Caesar tarafından kullanılmış şifreleme tekniğidir. Orijinal metnin harflerinin belirlenen anahtar sayısı kadar ileri ötelenmesi sonucu denk düşen harflerle şifreleme yapılmaktadır. Şekil 2'de görüldüğü üzere anahtar 3 olarak belirlenmiş ve A harfi kendinden sonra gelen 3.harfe ötelenmiş ve D harfiyle yer değiştirmiştir. Aynı şekilde B ve C harfleri de 3 harf ötelenerek E ve F harfleriyle yer değişmişlerdir.



Şekil 2. Sezar Algoritması ile Şifreleme

Şifreli metnin çözümü ise şifreli metindeki harflerin anahtar sayısına göre geriye ötelenmesi sonucu denk düşen harflerle yer değiştirmesiyle yapılır. Anahtar 3 olarak belirlenmişti. Şekil 3'e bakıldığında sırasıyla her harf 3 harf geriye ötelenerek orjinal mesaja dönüş yapılmıştır.

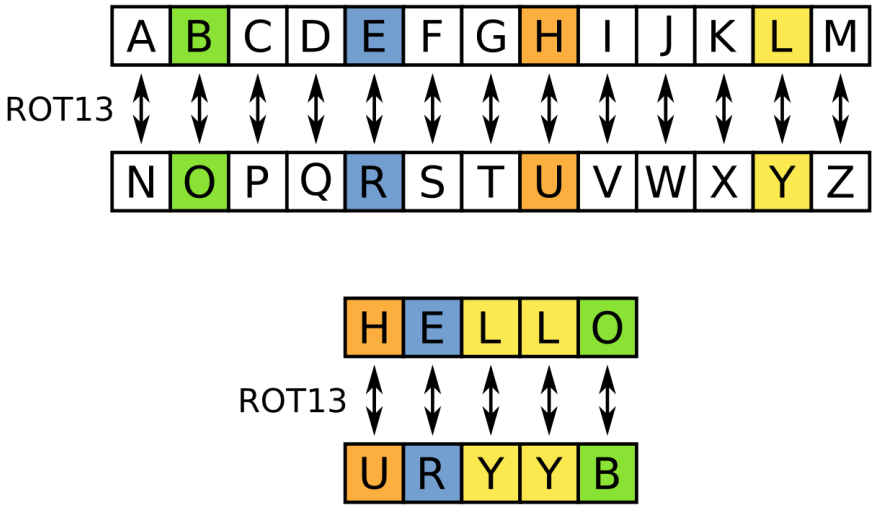


Şekil 3. Sezar Algoritması ile Şifre Çözme

Zamanında güvenli bir yol olsa da şifreleme türü biliniyor ise en fazla 25 deneme ile şifreyi kırmak mümkündür. Dolayısıyla brute-force dediğimiz kaba kuvvet saldırıları ile şifreler kolayca çözülmektedirler.

ROT13

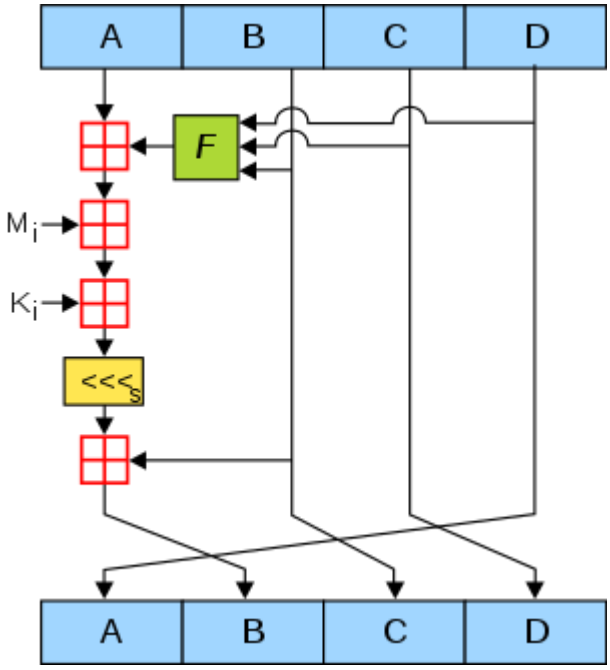
İngilizcedeki her harfin kendisinden sonra gelen 13.harf ile yer değiştirmesiyle şifreleme ve şifre çözme işlemleri yapılır. Şekil 4'e bakıldığında "HELLO" kelimesinin her harfi kendinden sonraki 13.harf ile yer değiştirmiş ve şifreli mesaj olarak "URYYB" üretilmiştir. Şifreyi çözerken de aynı işlem uygulanarak tekrar "HELLO" elde edilir.



Şekil 4. ROT13 Algoritması ile Şifreleme

MD5 (Message-Digest Algorithm 5)

Ron Rivest tarafından geliştirilmiş tek yönlü özet algoritmalarından biridir. Girdi uzunluğu ne olursa olsun her zaman 128 bit uzunluğunda 32 karakterli 16'lık sayı sisteminde bir çıktı üretir. Girdideki en ufak bir değişiklik çıktının tamamen değişmesiyle sonuçlanır.



Şekil 5. MD5 Algoritması Diyagramı

MD5 mesajı önce 128 bitlik bloklara parçalar. Eğer 128 bit olmuyorsa tamamlamak için sona 1 ekleyip geri kalanı 128 bite tamamlayana kadar 0 koyar. Daha sonrasında bu 128 bitlik inputları her biri 32 bit olacak şekilde 4 parçaya böler. Şekil 5'te görüldüğü üzere bu 4 parçaya sırasıyla A, B, C ve D diyoruz. M mesajın farklı bir noktasından bilgi alıp onu kullanmaktadır. K ise MD5'in içinde sabit olarak tutulan bir tablosu var, o tablodan okunuyor. Her zaman ilk 32 biti yani A'yı işleme koyarak sonuçtaki B'ye yazıyor ve bu işleyiş diğerleri kaydırılarak devam ediyor. B, C, D input olarak F fonksiyonuna girip A'ya beraber XOR fonksiyonundan geçiriliyor. Daha sonra M ve K ile de XOR'lanarak kaydırma yapılıyor ve B ile de XOR'lanıp B'ye yazılıyor. Daha sonra yukarıda da anlatıldığı üzere B C'ye, C D'ye, D ise A'ya kaydırılıyor. Bu işlemler toplamda 64 kez tekrar ediliyor. Her 16'lık tekrarda F fonksiyonu değişiyor.

MD5 algoritması, üzerinde işlem yapılan dosyada oynanma yapılıp yapılmadığının kontrolü gibi işlemler için kullanılmaktadır. Aynı zamanda SHA ailesi gibi veritabanına şifre kayıtları yapılırken de MD5 algoritması kullanılarak şifre hashlenir. Sisteme her giriş işlemi yapılırken şifre hash fonksiyonundan geçirilerek veritabanındaki hashlenmiş değer ile karşılaştırılır ve hash değerleri uyuşuyorsa sisteme giriş izni verilir. Şifrelenmiş metinden geri dönüşüm yapılamadığı için güvenlidir. Ancak bazı tablolarda sık kullanılan değerlerin MD5 kayıtları tutulmaktadır. Elde edilen hashli değerler tablolarla karşılaştırılarak şifrenin orjinali elde edilebilmektedir.

SHA1 (Secure Hash Algorithm)

Amerika'nın ulusal güvenlik kurumu NSA tarafından tasarlanmış güvenli özetleme algoritmasıdır. MD5 algoritması ile çok benzerdir ancak birbirlerinden farkı oluşturdukları özet boyutlarıdır. Girdinin uzunluğundan bağımsız olarak her zaman 160 bit uzunluğunda 40 karakterli 16'lık sayı sisteminde bir çıktı üretir. 2017 yılında Google, SHA1'e çakışma saldırısında bulunduklarını ve 2 farklı PDF dosyasından aynı mesaj özetini aldıklarını açıkladılar. Bu da SHA1'in dijital imzalama gibi çakışma direncine bağımlı uygulamalar için yeterince güvenilir olmadığını ispatlamıştır.

SHA2 AİLESİ

SHA1 gibi tasarımcıları NSA'dır. Kriptografik özet fonksiyonları kümesidir. SHA1'le benzerlikleri olsa da SHA1'den daha güvenilirdir. Yaygın olarak bazı güvenlik uygulamaları ve protokollerde kullanılmaktadırlar. 6 tane algoritması vardır. Bunlar SHA224, SHA256, SHA384, SHA512, SHA512/224 ve SHA512/256. Farklı kaydırma miktarları ve toplama sabitleri kullansalar da yapıları aynı sayılır.

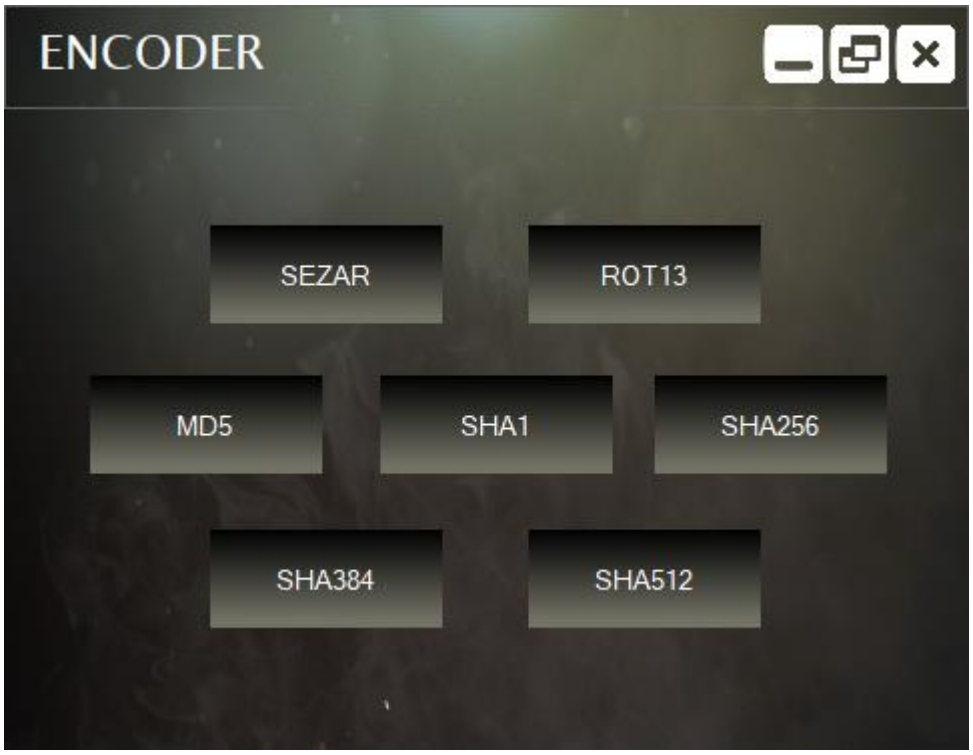
SHA256 girdinin uzunluğundan bağımsız olarak her zaman 256 bit uzunluğunda 64 karakterli 16'lık sayı sisteminde bir çıktı üretir. SHA384 ise 384 bit uzunluğunda 96 karakterli16'lık sayı sisteminde bir çıktı üretmektedir. SHA512 algoritması ise 512 bit uzunluğunda 128 karakterli 16'lık sayı sisteminde bir çıktı üretmektedir.

KULLANILAN TEKNOLOJİLER

Proje Visual Studio'nun C# Windows Form uygulaması üzerinden hazırlanmıştır. Görselliği zenginleştirmek amacıyla Bunifu Framework kullanılmıştır.

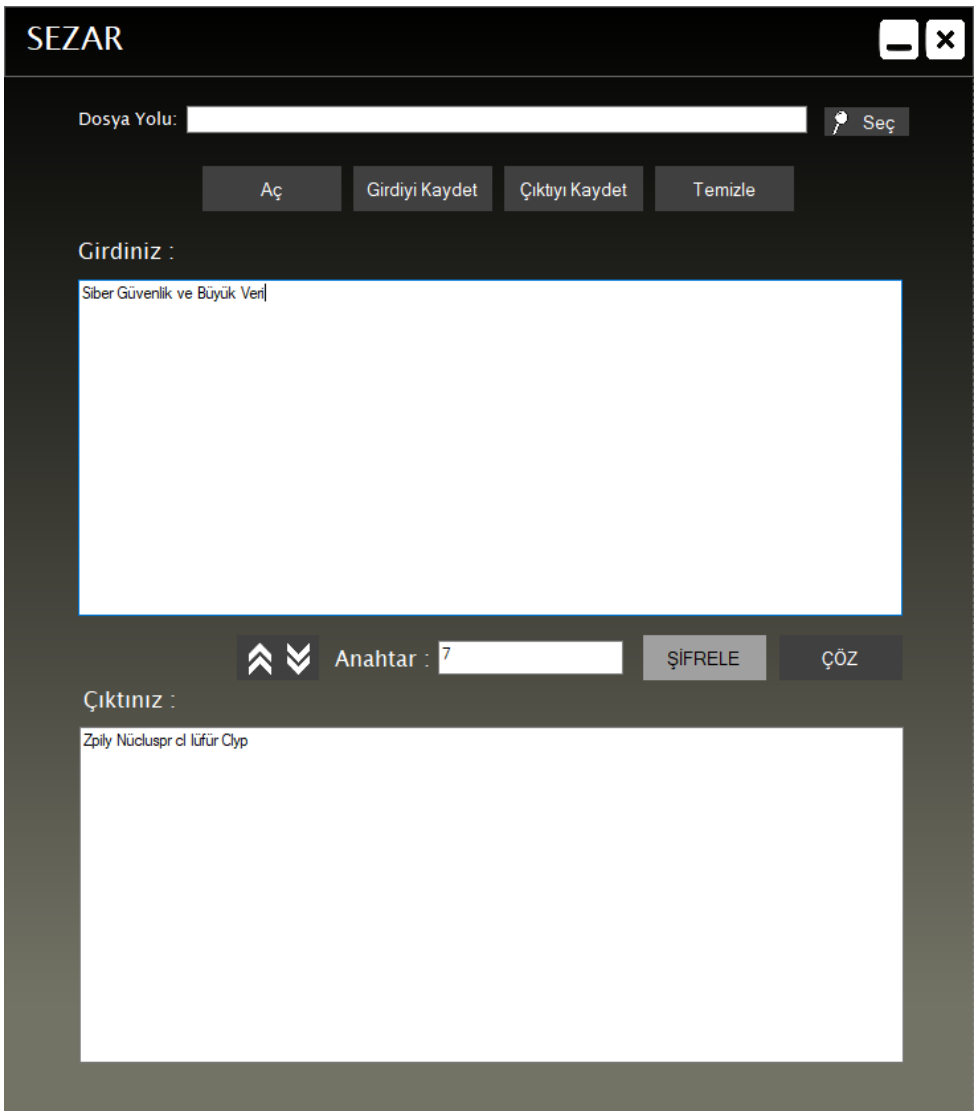
UYGULAMA

Programın arayüzü Şekil 6'da görüldüğü gibi kullanılacak algoritmanın seçim ekranından ibarettir.

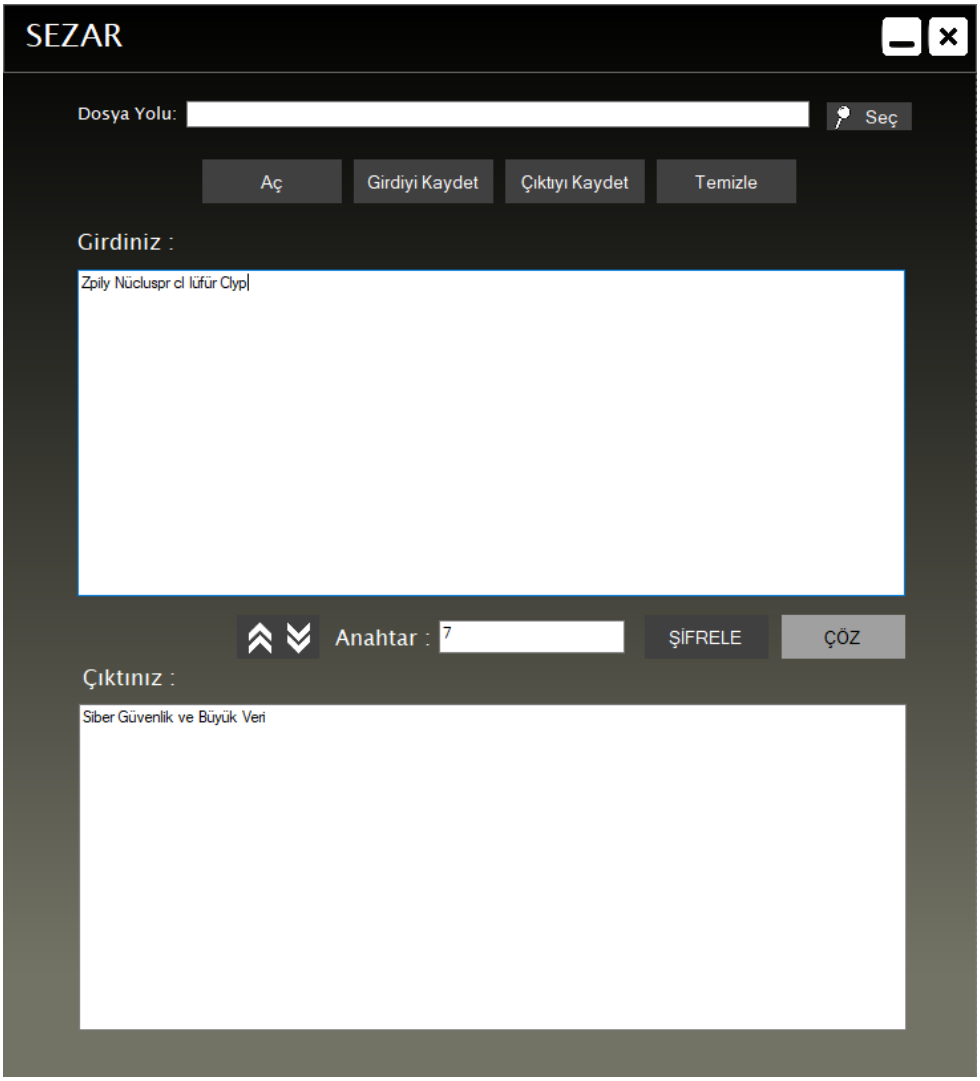


Şekil 6. Encoder programı arayüzü

Sezar butonuna basıldıktan sonra Şekil 7'de girdi yerine "Siber Güvenlik ve Büyük Veri" yazılmış anahtar olarak ise 7 girilmiştir. Şifrele butonuna basıldığında girilen her harfi 7 ileri öteleyerek "Zpily Nücluspr cl lüfür Clyp" çıktısı elde edilmiştir. Şekil 8'de ise elde edilen çıktı girdi bölümüne yazılmış, çöz butonuna basılarak şifrelenmiş verinin orjinali elde edilmiştir.

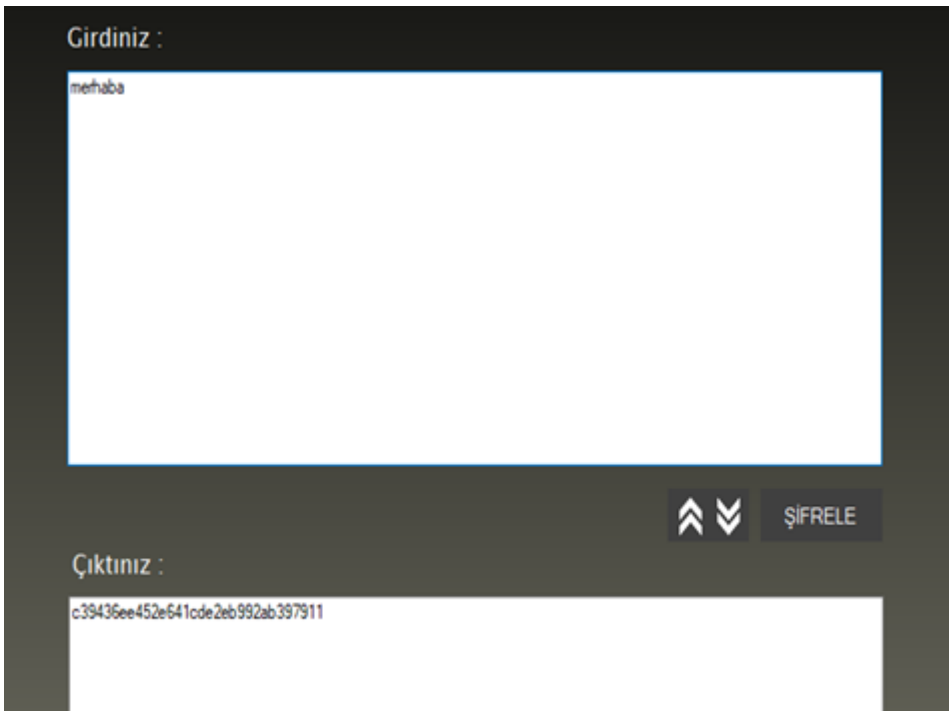


Şekil 7. Sezar Algoritması ile Şifreleme

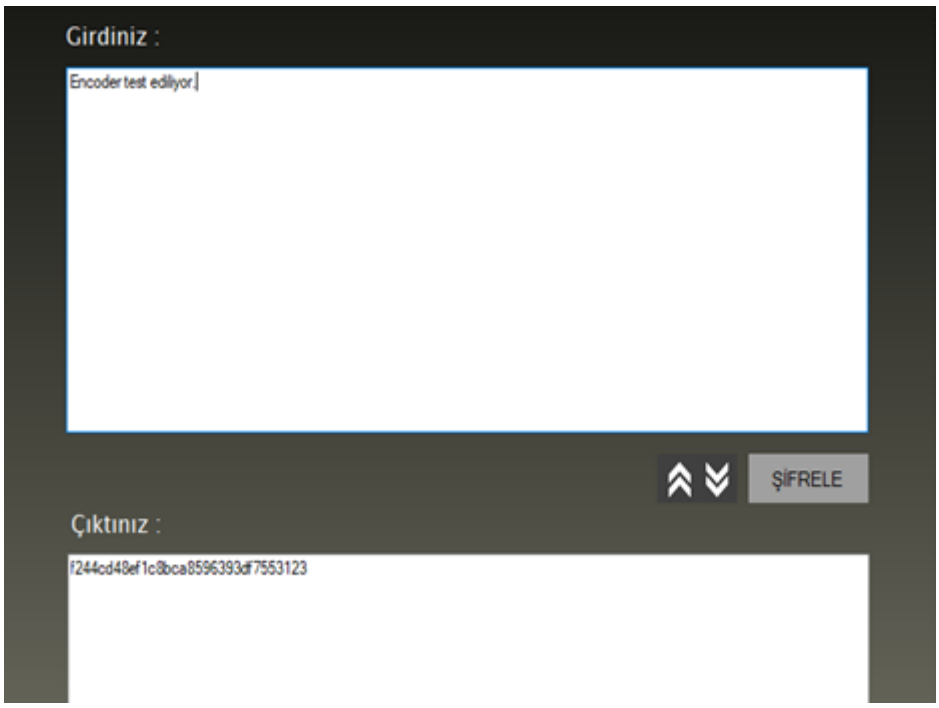


Şekil 8. Sezar Algoritması ile Şifre Çözme

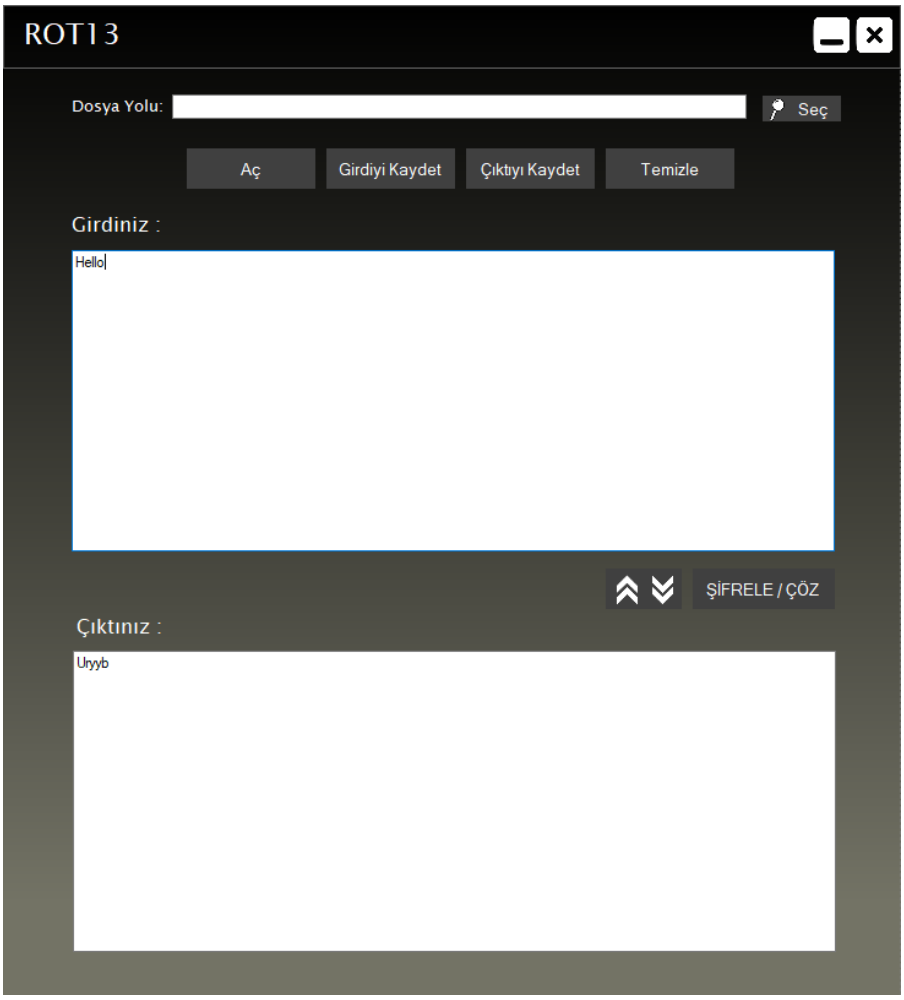
MD5 algoritması seçilerek Şekil 9'a girdi olarak "merhaba", Şekil 10'a ise "Encoder test ediliyor." yazılmış ve şifrele butonuna basılmıştır. Her iki girdinin çıktısı da 32 karakter uzunluğundadır.



Şekil 9. MD5 Algoritması ile şifreleme



Şekil 10. MD5 Algoritması ile şifreleme



Şekil 11. ROT13 Algoritması ile Şifreleme

Şekil 11 incelendiğinde ROT13 algoritması seçilmiştir. “Hello” girdisindeki her harf kendinden sonra gelen 13.harf ile yer değiştirmiş ve “Uryyb” çıktısını üretmiştir.

SONUÇ

Bu çalışmada şifreleme ve özet algoritmaları incelenmiştir. Algoritmaların nasıl bir mantık kullanarak şifreleme yaptıkları ve birbirlerine kıyasla ne derece güvenilir oldukları gözlemlenmiştir. Uygulama test edilmek amacıyla webatic.com ve md5hashgenerator.com’daki gibi birçok encoder aracıyla karşılaştırılmıştır. Diğer encoder araçlarına girdiğimiz girdilerin çıktıları olarak uygulamadaki çıktıların aynısı alınmıştır. Bu da uygulamanın güvenilir olduğunu göstermektedir. Geliştirdiğim encoder uygulamasında 7 şifreleme algoritması bulunmaktadır. Diğer algoritmalar eklenerek içeriği geliştirilebilir.

KAYNAKLAR

1. Tarık Yerlikaya, Ercan Buluş, Nusret Buluş, “Kripto Algoritmalarının gelişimi ve Önemi, Akademik Bilişim, Denizli, 2006.
2. Zainab Hashim Obaid, “Kriptoloji Yöntemlerinin Karşılaştırılması”, Yüksek Lisans Tezi, Kayseri, 2016.
3. Emre Ceran, Mehmet Sabır Kiraz, Osmanbey Uzunkol, “RSA Şifreleme Sistemlerinin Kleptografik Arka Kapıları için Güvenlik ve Karmaşıklık Analizi”, Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi, Cilt 21, 2017.
4. S. Akyelek, H.M. Yıldırım, Z.Y. Tok, “Kriptoloji ve Uygulama Alanları: Açık Anahtar Altyapısı ve Kayıtlı Elektronik Posta”, Akademik Bilişim, Malatya, 2011.
5. Ülkü Ülker, “Ulusal Bilgi Güvenliğine Yönelik Bir Kriptografi Algoritması Geliştirilmesi ve Harf Frekans Analizine Karşı Güvenirlik Tespiti”, Bilişim Teknolojileri Dergisi, Ankara, 2013.
6. Gökhan Dalkılıç, Gülşah Yıldızoğlu, “Tek Anahtarlı Yeni Bir Şifreleme Algoritması Daha”, Akademik Bilişim, Çanakkale, 2008.