T.C.
NECMETTİN ERBAKAN
ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

FARK DENKLEMLERİ KULLANILARAK TASARLANAN ŞİFRELEME ALGORİTMASININ GÜVENLİK ANALİZİ

Muhlise ÜSTÜN

YÜKSEK LİSANS TEZİ

Matematik Anabilim Dalı

Mayıs-2022
KONYA

ÖZET

YÜKSEK LİSANS TEZİ

FARK DENKLEMLERİ KULLANILARAK TASARLANAN ŞİFRELEME ALGORİTMASININ GÜVENLİK ANALİZİ

Muhlise ÜSTÜN

Necmettin Erbakan Üniversitesi Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Danışman: Dr. Öğr. Üyesi Ahmet DUMAN

2022, 65 Sayfa

Jüri
Doç. Dr. Tuncer ACAR
Dr. Öğr. Üyesi Ahmet DUMAN
Dr. Öğr. Üyesi Ahmet SINAK

Bu tez çalışmasında 2019 yılında C. Flaut tarafından fark denklemleri kullanılarak tanımlanan şifreleme algoritması ayrıntılı olarak ele alınmıştır ve bu algoritmanın güvenlik analizi yapılmıştır. Şifreleme sistemlerinin güvenirliğini test etmek için yapılan saldırı yöntemlerinden biri olan "Bilinen Açık Metin Saldırısı" belirli uzunluktaki açık metin ve kapalı metin çifti kullanılarak anahtarı bulma işlemine dayanır. Bu tez çalışmasında C. Flaut tarafından önerilen şifreleme algoritmasının güvenirliği bilinen açık metin saldırısı ile test edilmiştir ve algoritmanın bu saldırı yöntemi ile kırılabildiği gösterilmiştir. Bu saldırı yönteminde açık metin-kapalı metin çifti arasındaki bağlantı kullanılarak yeterli sayıda denklemden oluşan lineer denklem sistemi oluşturulmuştur ve bu sistem Gauss eliminasyon yöntemiyle çözülerek şifrelemede kullanılan gizli anahtar ele geçirilmiştir. Böylece bu şifreleme sisteminin bilinen açık metin saldırısına karşı güvensiz olduğu gösterilmiştir.

Anahtar Kelimeler: Bilinen açık metin saldırısı, Fark denklemleri, Kriptanaliz, Kriptoloji, Şifreleme, Şifre çözme

ABSTRACT

MS THESIS

SECURITY ANALYSES OF THE ENCRYPTION ALGORITHM DESİGNED USİNG DIFFERENCE EQUATIONS

Muhlise ÜSTÜN

THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCE OF NECMETTİN ERBAKAN UNIVERSITY
THE DEGREE OF MASTER OF SCIENCE
IN MATHEMATIC

Advisor: Asst. Prof. Dr. Ahmet DUMAN

2022, 65 Pages

Jury
Assoc. Prof. Dr. Tuncer ACAR
Asst. Prof. Dr. Ahmet DUMAN
Asst. Prof. Dr. Ahmet SINAK

In this thesis, an encryption algorithm based on the difference equations proposed by C. Flaut (2019) is discussed in detail and its security analysis is performed. One of the attack methods used to test the reliability of encryption systems, "known-plaintext attack", is based on finding the key using a certain length of known plaintext and ciphertext pairs. In this thesis, the reliability of the encryption algorithm proposed by Flaut (2019) is tested by applying the known-plaintext attack, and it is observed that the algorithm can be broken with this attack. In this attack, a linear equation system that has sufficiently linear equations is formed from the connection between the plaintext-ciphertext pairs. Thus, by solving this linear equation system with the Gaussian elimination method, the secret key of the encryption algorithm is obtained, which approves that this encryption system is insecure against the known-plaintext attacks.

Keywords: Known-plaintext attack, Difference equations, Cryptanalysis, Cryptology, Encryption, Decryption

ÖNSÖZ

Tez çalışmamda değerli bilgi ve birikimlerinden yararlandığım danışman hocam Dr. Öğr. Üyesi Ahmet DUMAN' a ve çalışmamın her aşamasında destek olan özellikle bu tezde ele alınan şifreleme sisteminin güvenlik analizinin yapılmasında değerli bilgi, birikim ve yardımlarını esirgemeyen Dr. Öğr. Üyesi Ahmet SINAK' a teşekkürlerimi sunarım. Ayrıca tez çalışmamın değerlendirilme ve düzeltilmesinde sağladığı katkılarından dolayı Doç. Dr. Tuncer ACAR' a teşekkür ederim.

Çalışmalarım boyunca maddi ve manevi desteklerini esirgemeyen aileme ve sabır göstererek daima yanımda olan eşime sevgi ve minnetlerimi sunarım.

Muhlise ÜSTÜN
KONYA-2022

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

SİMGELER VE KISALTMALAR

Simgeler

$\mathbb{R}$	: Reel Sayılar Kümesi
$\mathbb{Z}$	: Tam Sayılar Kümesi
$\mathbb{N}$	: Doğal Sayılar Kümesi
$\mathbb{Z}_n$	: mod n bağıntısına göre denklik sınıfları kümesi

Kısaltmalar

KPA	: Known Plaintext Attack
CPA	: Chosen Plaintext Attack
CCA	: Chosen Ciphertext Attack
COA	: Ciphertext Only Attack

1. GİRİŞ

Şifreleme bilimi olan kriptografi; mesajların şifrelenmesi, şifrelenmiş mesajların güvenli bir şekilde alıcıya gönderilmesi ve bu mesajların çözümlenmesi için kullanılan teknikleri kapsar. Şifreleme işlemi; şifreleme anahtarı kullanılarak, anlamlı (açık) bir metnin asıl içeriğinin değiştirilerek anlamsız (şifreli) bir metne dönüştürülmesidir. Şifre çözme işlemi ise şifre çözme anahtarı ile şifreli (anlamsız) metnin, anlamlı hâle dönüştürülerek asıl içeriğinin bulunması işlemidir.

Yazının icadından günümüze kadar insanlar haberleşmelerinde gizliliğe önem vermiş ve güvenliği sağlamak için karşı tarafa iletmek istedikleri mesajlarını, şifreleme yöntemini kullanarak göndermişlerdir. Doğru kullanıldığında kırılması neredeyse imkânsız olan şifreleme teknolojisi, elimizdeki bilgileri çeşitli saldırılardan korumamız için günümüzde sahip olduğumuz en önemli araçlardandır. Ayrıca kurumsal web sitelerine ve sayfalarına yetkisi olmayan kişilerin ulaşmasını engellemek de şifreleme teknolojisinin gelişmesine bağlıdır.

Teknolojik gelişmelerle birlikte şifreleme yöntemleri de büyük değişime uğramıştır. Ancak bu durum beraberinde bazı riskleri getirmiştir. Siber Güvenlik, bu riskleri azaltmak ve internet kullanımını güvenli bir hâle getirmek için ortaya çıkan yeni bir endüstri alanıdır.

Bilgi çağının getirdiği şifreleme sistemleri günümüzde önemini daha da arttırmaktadır. Kırılması çok zor olan, ciddi cebirsel temellere dayanan şifreleme sistemleri geliştirilmiştir. Bununla birlikte şifreleme analizi de gelişmiştir. Diğer bir ifadeyle şifreleme sistemlerinin üretilmesiyle şifre analizi yöntemleri birbirini tetiklemektedir.

Açık metin (şifrelenmemiş metin) ve kullanıcı tarafından girilen anahtarla şifreleme yapılabilmekte ve şifrelenen metinin güvenirliğini test etmek için çeşitli saldırı yöntemleri uygulanabilmektedir. Bu tez çalışmasında da (Flaut, 2019) çalışmasında fark denklemleri kullanılarak tasarlanan şifreleme algoritmasının güvenirliği test edilmiştir. Önerilen algoritmanın bilinen açık metin saldırısı karşısında güvensiz olduğu gösterilmiştir.

1.1. Motivasyon ve Tezin Önemi

Literatürde matematiksel modellemeler kullanılarak elde edilen çeşitli şifreleme metotları vardır. Bunlardan bir tanesi Flaut, 2019'da verilen fark denklemleri kullanılarak elde edilen şifreleme metodudur. Bu metot bir açık metni fark denklemleri kullanılarak şifreleyen şifreleme algoritmasıdır. Çalışmamızda bu algoritmanın güvenirliği bilinen açık metin saldırısı ile test edilerek, algoritmanın bu saldırı yöntemi ile kırılıp kırılamadığı incelenecektir. Ayrıca diğer saldırı yöntemlerinde şifrelenen metnin güvenirliğini analiz etmede etkili olup olmadığı araştırılacaktır.

Bu çalışmada Flaut tarafından 2019 yılında yayınlanan "Some Application of Difference Equations in Cryptography and Coding Theory" makalesinde önerilen şifreleme algoritmasının güvenlik analizinin yapılması planlanmaktadır. Ele alınacak analizlerin ilgili çalışmada yapılmamış olması ve çalışmanın güncel bir çalışma olması, bu tezde yapılması planlanan çalışmaları değerli kılmaktadır.

1.2. Organizasyon

Bu tezin sunumu aşağıda verildiği gibi organize edilmiştir.

Bölüm 1' de bu çalışmanın amacı, önemi, literatürdeki yeri ve çalışmada kullanılan tanımlar anlatılmıştır. Bölüm 2'de kaynak araştırması verilmiştir. Bölüm 3'te kriptografik algoritmaların sınıflandırılması ele alınmıştır. Ayrıca şifrelerin güvenilirliğini test etmek için kullanılan saldırı yöntemleri ve bu saldırı yöntemlerinin nerelerde kullanıldığı da anlatılmıştır. Bölüm 4' te fark denklemleri ile ilgili gerekli ön bilgiler verilmiştir. C. Flaut (2019) makalesinde verilen fark denklemleri üzerinde şifreleme yöntemi ile ilgili tanım ve teoremlere yer verilmiştir. Şifreleme algoritması ve şifre çözme algoritması anlatılmıştır. Bölüm 5'de şifrelenmiş metnin güvenirliğini araştırmak için yapılan saldırı yöntemi olan bilinen açık metin saldırısı anlatılmıştır. Sonrasında C. Flaut (2019) makalesinde verilen algoritmaya saldırı yapılarak bir denklem sistemi elde edilmiştir ve bu denklem sistemi çözülerek verilen şifreleme algoritmasının kırılabildiği gösterilmiştir. Ayrıca diğer kriptanaliz yöntemleriyle de algoritmanın güvenliği anlatılmıştır. Son olarak Bölüm 6' da tezde elde edilen sonuçlar tartışılmıştır.

1.3. Kriptoloji Terminolojisi

Bu bölümde kriptoloji biliminde yer alan temel tanımlardan bahsedilmiştir. Tanımlar oluşturulurken (Yeşilbaş, 2016) ve (Kodaz, 2003) çalışmalarından faydalanılmıştır.

Kriptografi (Cryptography): Mesajların saldırı yapan kişiler tarafından anlaşılamayan hale dönüştürülmesinde (şifrelenmesinde) kullanılan yöntemlerdir.

Kriptanaliz (Cryptanalysis): Şifrelenmiş mesajları anahtarı bilmeden deşifre edebilmek için kriptografik sistemlerin güvenliklerini inceleyen bilim dalıdır.

Kriptoloji (Cryptology): Kriptografi ve kriptanaliz bilimlerinden oluşan bilimdir.

Düz Metin (Plaintext): Şifrelenmemiş anlamlı açık metindir.

Şifreli Metin (Ciphertext): Açık metinin kriptografik yöntemlerle şifrelenmiş (anlamsız) halidir. Ayrıca kapalı metin olarak da adlandırılır.

Şifreleme (Encryption): Anlamlı metini anlamsız metine dönüştürme işlemidir.

Şifre Çözme (Decryption): Şifreleme işleminin tersidir, diğer bir ifade ile, anlamsız metini anlamlı metine dönüştürme işlemidir.

Anahtar (Key): Şifreleme ve şifre çözme işlemlerinde kullanılan en önemli bilgidir. Saldırganın bulması istenmez.

Açık Anahtar (Public Key): Herkes tarafından görülebilen anahtardır.

Gizli anahtar (Secret Key): Şifreli mesajı çözmek için kullanılan anahtardır.

Monoalfabetik (Monoalphabetic): Bir harfin her zaman aynı harf olarak şifrelenmesidir.

Polialfabetik (Polyalphabetic): Aynı harfin genellikle farklı harf olarak şifrelenmesidir.

2. KAYNAK ARAŞTIRMASI

Bu bölümde bu tez çalışmasında kullanılan ana kaynaklar verilmektedir.

(Flaut, 2019) makalesinde fark denklemleri kullanarak bir şifreleme algoritma sunmuştur. Bu algoritma için şifreleme ve şifre çözme adımları anlatılmıştır. Ayrıca matris kullanılarak kodlamayla ilgili bir uygulama anlatılmıştır.

(Coşkun & Ülker, 2013) makalesinde bilgi güvenliğine odaklanılarak ülkemizin siber saldırılara karşı milli güvenliğini korumak için bir şifreleme algoritması geliştirilmiştir. Bu algoritmanın harf frekans analizine karşı güvenirliği test edilmiştir.

(Obaid, 2016) çalışmasında kriptoloji incelenmiştir. Kullanılan şifreleme algoritmalarının çalışma zamanları (görüntünün şifrelendiği ve şifreyi çözdüğü zaman) çeşitli kriterlere göre kıyaslanmıştır.

(Yeşilbaş, 2016) çalışmasında şifreleme biliminin tarihi incelenmiştir. Şifreleme işlemlerinde kullanılan tanımlar ile teoremlere yer verilmiş ve şifreleme yöntemleri incelenmiştir.

(Obaid, Arkan, & Akay, 2016) çalışmasında şifreleme algoritmalarıyla ilgili bilgi verilerek, Base 64 tabanlı görüntü üzerindeki kıyaslamaları yapılmıştır.

(Külen, 2013) çalışmasında şifreleme yöntemleri ve bunlarla ilgili örneklere yer verilmiştir. Ayrıca şifreleme sistemlerindeki cebirsel yaklaşımlar ve şifreleri kırmanın yöntemleri incelenmiştir.

(Topaloğlu, Calp, & Türk, 2016) çalışmasında şifreleme bilimi incelenmiş olup, "Tekli Alfabetik Yer Değiştirme" tekniğine göre bir algoritma geliştirilmiştir. Şifreli metnin güvenli bir şekilde saklanması ve herhangi bir saldırıya karşı bilgi güvenliğinin sağlanması üzerinde durulmuştur.

(Tuncay, 2015) çalışmasında kriptografi bilimi incelenmiş, kriptografik ve uygulama özellikleri iyi olan ikili matrislerin üretilmesi için bir yöntem verilmiştir.

(Şahin, 1976) çalışmasında modern şifreleme algoritmaları incelenmiştir. Bu algoritmalardan olan blok şifreleme gücü açıklanmıştır.

(Nasibov, 2015) çalışmasında asimetrik şifreleme olan RSA sisteminin güvenliği incelenmiştir.

(Yerlikaya & Aslanyürek, 2019) "RSA Algoritmasının Şifreleme Hızını Arttıran Algoritmalar ve Performansları" adlı çalışmada asimetrik şifreleme olan RSA algoritması ile oluşturulan şifreleme işlemlerindeki hız problemleri incelenmiştir.

(Kodaz & Botsalı, 2010) çalışmasında simetrik ve asimetrik şifreleme algoritmaları açıklandıktan sonra şifreleme için kullanılan anahtar boyutları incelenmiştir.

(Yerlikaya, Buluş, & Buluş, 2006) çalışmasında simetrik şifreleme algoritması olan DES ve asimetrik şifreleme algoritması olan RSA şifreleme algoritmaları incelenmiştir.

(Vural & Sağıroğlu, 2008) çalışmasında kurumsal bilgi güvenliği sağlanmış ve bu konuda bireylerin bilinçlendirilmesi üzerinde durulmuştur.

(Ülker, 2014) çalışmasında bilgi güvenliği ile ilgili temel bilgiler verilmiş, bilgi güvenliğini sağlama yollarından biri olan kriptoloji bilimi üzerinde durulmuştur. Klasik teknikler kullanılarak bir kriptografi algoritması geliştirilmiş ve güvenirliğini test etmek için bire-bir harf frekans analizi uygulaması yapılmıştır.

(Çetin, 2021) çalışmasında kriptografinin tarihsel süreciyle ilgili genel bilgiler verilmiştir. Büyük bileşik sayıların asal olup olmadığını belirlemek için kullanılan deterministik ve olası asallık testlerinin incelemesi yapılmıştır. Ayrıca olası asallık testlerinin çalışma zamanları ele alınarak bir karşılaştırma yapılmıştır.

(Schneier, 1996) çalışmasında modern kriptografinin kapsamlı bir incelemesini sunmaktadır. Şifreleme algoritmalarında verilerin gizliliğini korumak için kullanılacak kriterleri vermektedir. Ayrıca olası asallık testleri ile ilgili çalışma prensipleri verilmiştir.

(Koblitz, 1994) "A Course in Number Theory and Cryptography" kitabında modern kriptografide kullanılan modüler aritmetik ve sayılar teoritik algoritmalar ele alındıktan sonra modern kriptografi algoritmaları verilmektedir.

(Hill, 1929), “Cryptography in an Algebraic Alphabet” adlı makalesinde geliştirdiği şifreleme sistemini cebirsel ifadelerle anlatmış ve matematiğin şifrelemede ne kadar etkin kullanılabileceğini göstermiştir. İkinci Dünya savaşı sırasında askeri alanda kullanılan şifreleme sistemleri ve bunların çözülmesinde kullanılan algoritmaların çeşitliliği de artmış, böylece bu alandaki çalışmalar hız kazanmıştır.

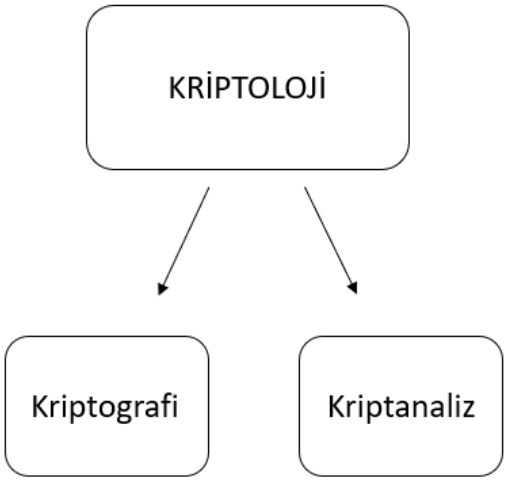
Son olarak, bu tez çalışmasında (Paar & Pelzl, 2009), (Menezes, Van Oorschot, & Vanstone, 2018), (Bulgak & Akın, 1998), (Stinson & Paterson, 2019) kaynaklarından da genel olarak faydalanılmıştır.

3. KRİPTOLOJİ BİLİMİ

Bu bölümde kriptoloji bilimini oluşturan, kriptografi bilimi ve kriptanaliz bilimi ele alınmıştır. Bu bölümde (Arslan, 2009), (Çimen, Akleylek, Akyıldız, 2008), (Çeşmeci, 2009), (Sakallı, 2016), (Şahin, 1976), (URL-1, 2022) ve (URL-2, 2022) kaynaklarından faydalanılmıştır.

Kriptoloji, kelime kökü itibari ile Yunanca 'Kryptos Logos' (gizli kelime) ifadelerinden oluşmuştur. Kriptoloji Bilimi; Kriptografi ve Kriptanaliz olmak üzere iki alandan oluşur. Kriptografi, bir mesajın sadece gönderen kişinin istediği kişilerin anlayabileceği şekle getirilmesinde, şifrelenmesinde ve şifrelenen mesajların, metinlerin çözümlenerek, ilk hâline dönüştürülmesinde kullanılan matematiksel algoritmalardır**.** Kriptanaliz ise anahtar olmadan şifreli mesajı çözme ya da kırmaya çalışma işlemidir. Diğer bir ifadeyle, kriptografi, çeşitli verilerin, mesajların belirli bir sisteme göre şifrelenmesi, bu mesajların güvenli bir şekilde alıcıya aktarılması ve aktarılan bu mesajın çözümlenerek ilk hâline dönüştürülmesi, kriptanaliz ise bu şifreli mesajın anahtar olmadan çözülmesi ya da kırılması için kullanılan yöntemler ve tekniklerin bütünüdür.

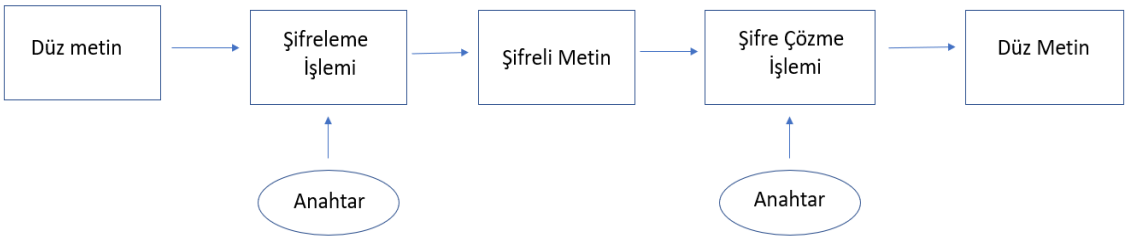
Kriptoloji bilimi, Matematik, Bilgisayar bilimleri ve Elektrik-Elektronik Mühendisliği bilimlerinin ortak disiplinler arası bir bilim dalı olarak kabul edilmektedir.



Şekil 3.1. Kriptoloji bilimi alt bilim dalları

Düz metnin bir anahtar ile şifrelenip, şifreli (kapalı) metne dönüştürülmesine şifreleme denir. Şifreli bir mesajın, düz bir metin şekline dönüştürülmesine şifre çözme ya da deşifre denir.

Şekil 3.2 de şifreleme ve şifre çözme işlemleri sembolik olarak anlatılmaktadır. Kriptosistemde, gönderici bilgilerin gizliliğini sağlamak için düz metni şifreleme algoritması kullanarak şifreli metne dönüştürür ve bu mesajı alıcıya gönderir. Ardından şifreli metin tekrar düz metne dönüştürülür. Algoritma şifre çözme kullanarak alıcının okuyabileceği şekle getirilir. Bunun için uygun olan yöntem seçilerek düz metne ulaşılabilir.

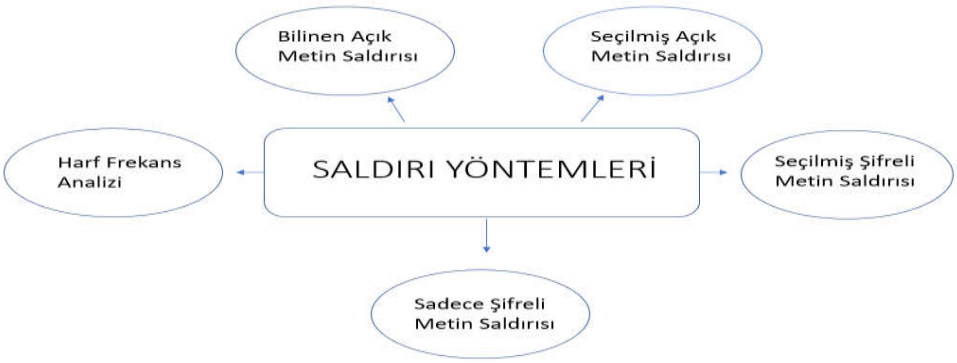


Şekil 3.2. Şifreleme işlemi

3.1. Kriptanaliz

Bu bölümde şifreli metinlerin kriptanaliz için çeşitli saldırı yöntemleri anlatılmıştır. Bu bölümde (Obaid, 2016), (Karaahmetoğlu, 2010), (Beşkirli, Özdemir, & Beşkirli, 2019), (Nasibov, 2015) tez çalışmalarından ve (Kapoor, Nanda, Gundla, 2019) ve (Sadkhan, 2011) kaynaklarından faydalanılmıştır.

Kriptanalizde anahtar bilinmeden şifrelenmiş metin çözülmeye çalışılır. Basit şifreleri çözmek için tüm olasılıkları denemek yerine matematik, istatistik ve dilbilim alanlarındaki bilgi kullanılarak şifrenin kırılması amaçlanır. Bu da şifre çözmek (kırmak) için çeşitli saldırı yöntemlerinin ortaya çıkmasını sağlamıştır.
Bu tezde incelenen saldırı yöntemleri şekil 3.3' te verilmiştir.



Şekil 3.3. Saldırı yöntemleri

3.1.1. Bilinen açık metin saldırısı (Known plaintext attack)

Bilinen açık metin saldırısı (KPA), saldırganın hem düz metin hem de şifreli metin örneklerine sahip olduğu, gizli anahtarlar ve kod kitapları gibi daha fazla gizli bilgiyi ortaya çıkarmak için bunları kullanmakta özgür olduğu bir kriptanaliz yöntemidir. Daha açık olarak şifreleme sistemlerinin güvenirliğini test etmek için yapılan saldırı yöntemlerinden biri olan "Bilinen Açık Metin Saldırısı" belirli uzunluktaki açık metin ve kapalı metin çifti kullanılarak anahtarı bulma işlemine dayanır. Saldırganın düz metin ve şifreli metne erişimi olduğu için güvenlik zaafiyeti olan algoritmaların gizli anahtarlarını ele geçirmek kolaydır**.**

Kriptograflar ve kriptoanalistler için bilinen açık metin saldırısı büyük ilgi konusu olmuştur. Saldırganın şifreleme anahtarıyla ilgili verileri elde etmesi çok kolaydır. Bu saldırıda, saldırgan karşılaştırılabilir düz metnin şifreli metnini bildiği için bilgiyi kullanarak anahtara erişebilir. Bilinen açık metin saldırısı 2. Dünya Savaşı'nda kullanıldı.

3.1.2. Seçilmiş açık metin saldırısı (Chosen plaintext attack)

Seçilmiş açık metin saldırısı (CPA)' da rastgele bir düz metin alınır. Saldırganın şifreleme makinesine sahip olduğu (yani seçtiği düz metni şifreleyebildiği) varsayılır. Bu düz metin saldırgan tarafından şifrelenerek şifreli metin elde edilir. Daha sonra saldırgan gizli anahtar hakkında bilgi edinmeye çalışarak şifreli metnin şifresini çözmek için alternatif olarak herhangi bir algoritma bulabilir. Bu saldırı, davetsiz misafir için daha uygundur. Çünkü davetsiz misafir herhangi bir metni seçme şansına sahiptir, dolayısıyla sistem hakkında daha fazla veri elde edebilir ve şifreli metin ile açık metin çiftleri elinde olduğu için anahtarı bulup, şifreyi kırabilir. İlgili anahtarı uygulayan kapsamlı aramanın karmaşıklığı, seçilen düz metin saldırı tekniğinin uygulanmasıyla azaltılır.

Seçilmiş açık metin saldırısı, toplu seçilmiş açık metin saldırısı ve uyarlanabilir açık metin saldırısı olmak üzere ikiye ayrılır. Toplu seçilmiş açık metin saldırısı, kriptanalistin herhangi biri şifrelenmeden önce tüm açık metinleri seçtiği saldırıdır. Bu genellikle "seçilmiş açık metin saldırısı" nın niteliksiz kullanımının anlamıdır. Uyarlanabilir seçilmiş açık metin saldırısı ise önceki şifrelemelerden gelen bilgiler hakkında sonraki açık metinleri temel alan kriptanalistin, bir dizi etkileşimli sorgu yaptığı saldırıdır.

Bilinen açık metin saldırısında saldırgan açık ve şifreli metne sahiptir. Seçilmiş açık metin saldırısında da seçilen açık metne karşılık gelen şifreli metin bulunabileceğinden, bilinen açık metin saldırısıyla benzer şekilde çalışmaktadır.

3.1.3. Seçilmiş şifreli metin saldırısı (Chosen ciphertext attack)

Seçilmiş şifreli metin saldırısı (CCA), kriptanaliz için bir saldırı modelidir. Kriptanalistin en azından kısmen bilgi topladığı bir şifreli metin seçme ve bilinmeyen bir anahtar altında şifresinin çözülmesini sağlama yöntemidir. Saldırıda, bir düşman, bir veya daha fazla bilinen şifreli metni sisteme girme ve ortaya çıkan düz metinleri elde etme şansına sahiptir. Saldırgan, bu bilgilerden faydalanarak, şifre çözme için kullanılan gizli anahtarı elde etmeye çalışabilir yani saldırgan istediği şifreli metinin deşifre edilmiş şekline ulaşabilir.

Bir şifreleme sistemi, seçilen şifreli metin saldırısına karşı savunmasız olduğunda, uygulayıcılar, bir düşmanın seçilen şifreli metinlerin şifresini çözebileceği durumlardan kaçınmak için dikkatli olmalıdır.

Seçilmiş şifreli metin saldırıları, diğer saldırılar gibi, uyarlanabilir veya uyarlanabilir olmayan saldırılar olmak üzere ikiye ayrılır. Uyarlanabilir olmayan bir saldırıda, saldırgan şifresini çözmek için şifreli metni veya şifreli metinleri önceden seçer ve daha fazla şifreli metin için ortaya çıkan düz metinleri kullanmaz. Uyarlanabilir bir seçilmiş şifreli metin saldırısında ise saldırgan şifreli metin seçimlerini uyarlanabilir bir şekilde, yani önceki şifre çözmelerinin sonucuna bağlı olarak yapar.

Seçilmiş şifreli metin saldırısının özel olarak not edilen bir çeşidi, "öğle vakti", "gece yarısı" veya "kayıtsız" saldırıdır. Burada bir saldırgan uyarlanabilir seçilmiş şifreli metin sorguları yapabilir ancak yalnızca belirli bir noktaya kadar saldırganın sisteme saldırmak için gelişmiş bir yetenek göstermesi gerekir. "Öğle vakti saldırısı" terimi, bir kullanıcının bilgisayarının, şifre çözme yeteneğine sahip bir saldırgan tarafından, kullanıcı öğle yemeğine çıkarken kullanılabilir olduğu fikrini ifade eder. Saldırının bu biçimi yaygın olarak tartışılan ilk biçimidir. Saldırganın uyarlanabilir seçilmiş şifreli metin sorguları yapma yeteneği varsa, en azından bu yetenek elinden alınana kadar hiçbir şifreli mesaj güvenli olmayacaktır.

3.1.4. Sadece şifreli metin saldırısı (Chiphertext only attack)

Sadece şifreli metin saldırısı (COA)'da, saldırgan sadece şifreli metne erişebilirken hiçbir açık metne erişemez. Saldırganın görevi, verilen şifreli metin aracılığıyla gizli anahtarı bulmak ve düz metni kurtarmak için bir yöntem geliştirmektir. Karşılık gelen düz metin bulanabiliyorsa ve anahtara ulaşılabiliyorsa, saldırı tamamen başarılıdır. En zor saldırı türüdür, detaylar için (Kapoor, Nanda, Gundla, 2019) bakınız.

Kriptografi tarihinde, kalem ve kâğıt kullanılarak uygulanan ilk şifreler, rutin olarak yalnızca şifreli metinler kullanılarak kırıldı. Kriptoanalistler, şifreli metine saldırmak için frekans analizi gibi istatistiksel saldırı yöntemleri geliştirdiler. Enigma gibi mekanik şifreleme cihazları, bu saldırıları çok daha zor hâle getirdi.

3.1.5. Harf frekans analizi

Frekans analizi, bir dile ait yapısal bazı özellikleri kullanarak şifreli metinden düz metni elde etmeyi amaçlar. Şifreli metinde en sık kullanılan harf, metnin yazıldığı dilde en çok kullanılan harf ile eşleştirilir ve bu işlem tüm harfler için uygulanır. Her harfin kullanım sıklığı hesaplanır ve sırası ile harflerin yerleştirilmesi işlemi devam eder.

Frekans analizinin yapılabilmesi için uzun metinlere ihtiyaç duyulmaktadır. Uzun metinler, elde edilen metinlerin geçerli ve güvenilir olmasını sağlamaktadır. Frekans analizinde birebir eşleme dışında harf ikililerine, üçlülerine de bakılabilir. Bir dilde daha çok yan yana gelen sıralılar, şifreli metinde en çok yan yana gelen sıralıların yerine yerleştirilerek de çözümleme yapılabilir.

Günümüze ulaşan ve kriptanalizin ilk örneklerini içeren eser, 9. yüzyılda yaşayan Arap filozofu Al-Kindi' nin yazdığı 'Kriptografik Mesajların Deşifresi' isimli eserdir. Bu eser İstanbul' da Süleymaniye Osmanlı Arşivinde bulunmaktadır. Bu eser ile birlikte frekans analizi kavramı ortaya çıkmıştır. Detaylı bilgi için (Coşkun & Ülker, 2013) dergisinden faydalanabilirsiniz.

3.2. Kriptografi

Bu bölümde klasik şifreleme sistemlerinin bazıları tanıtılacaktır ve güvenlik analizleri sunulacaktır. Ayrıca modern kriptografi hakkında kısa bilgi verilecektir. Bu bölümde, (Külen , 2013), (Yerlikaya, Buluş, & Buluş, 2006), (Topaloğlu, Calp, & Türk, 2016) ve (Obaid, Arkan, & Akay, 2016) tez çalışmalarından faydalanılmıştır. Kriptografi temel olarak klasik şifreleme ve modern şifreleme olmak üzere iki ana bölüme ayrılır.

3.2.1. Klasik Şifreleme Yöntemleri

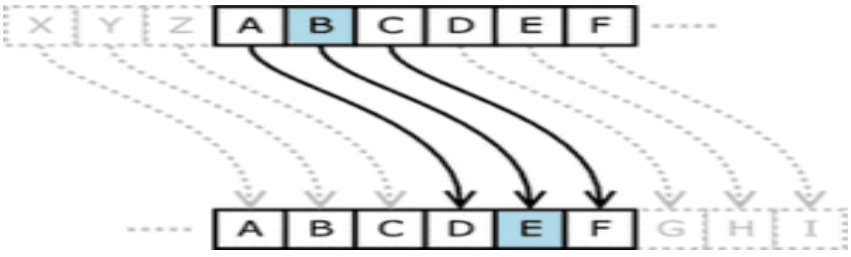
Klasik şifreleme sistemlerinin sunumunda (Çetin, 2021), (Obaid, 2016), (Paar & Pelzl, 2009) ve (Stinson, 2002), (Ülker, 2014) kaynaklarından faydalanılmıştır.

Klasik şifreleme yöntemleri en az 4000 yıllık bir geçmişe sahiptir. İlk olarak M.Ö. 2000 yıllarında Eski Mısırlılar kullanmıştır. Bu da eski zamanlardan beri insanlar iletişim kurarken mesajlarını gizleme ihtiyacı duyduklarını gösterir. Klasik şifreleme yöntemleri geçmişte sadece askeri ve bazı ileri akademik alanlarda kullanılmıştır İlkel şifreleme yöntemlerinin kullanıldığı bu dönemler, mekaniğin ve elektronik cihazların hayatımıza girmesiyle değişime uğramıştır. Klasik şifreleme yöntemleri, şifrelemenin yöntem ve mantığını anlamamızı kolaylaştırır.

Sezar Şifreleme, Kaydırma Şifreleme, Yer Değiştirme, Permütasyon Şifreleme, Afin Şifreleme, Hill Şifreleme, Vigenere Şifreleme ve Vernam Şifreleme sistemleri klasik şifreleme yöntemlerinden bazılarıdır.

Sezar Şifreleme Yöntemi

Sezar tarafından M.Ö 58 yılında kullanılmıştır. İmparator Sezar generallerine ileteceği mesajları gizlemek için kendi ismiyle anılan Sezar algoritmasını geliştirmiştir. Bu teknik karakterleri başka karakterlerle değiştirerek bilgiyi gizleme yöntemidir. Sezar, savaş döneminde askeri mesajlarını her harfin yerini değiştirerek karşı tarafa gönderdiği için düşman bu mesajlara ulaşsa bile mesajı anlayamamıştır. Bu şifreleme yöntemi kısaca şöyle yürütülmektedir; şifrelenmek istenen metin ya da kelimedeki her harf alfabede kendisinden 3 harf sonraki harfle değiştirilir ve şifreli metin elde edilir.



Şekil 3.4. Sezar şifreleme yöntemi (URL-3, 2022)

$m, c \in \mathbb{Z}_n$ olmak üzere Sezar şifreleme yöntemi matematiksel olarak aşağıdaki gibi çalışmaktadır. Burada m şifrelenecek olan açık mesajı, c şifrelenmiş olan kapalı mesajı ve n kullanılan alfabedeki karakter sayısını göstermektedir.

Şifreleme: $E_3\ (m) = m + 3\ mod\ n$

Şifre Çözme: $D_3(c) = c - 3\ mod\ n$.

Sezar şifrelemesi Türk alfabesine göre uygulanırsa karakter sayısı $n = 29$ olur. Türk alfabesindeki karakterlerin sayısal değerleri Tablo 3.1 de verilmiştir.

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

Tablo 3.1. Türk alfabesindeki karakterlerin sayısal karşılığı

Örnek 3.1. Türk alfabesini kullanarak 'NECMETTİN ERBAKAN' ismini Sezar şifreleme ile şifreleyelim. NECMETTİNERBAKAN düz metninin Tablo 3.1' e göre karakter karşılıkları olan 16, 5, 2, 4, 15, 5, 23, 23, 11, 16, 5, 20, 1, 0, 13, 0, 16 sayıları, anahtar $k = 3$ olduğundan 3 basamak kaydırılarak şifreleme yapılır. İlk harf için aşağıdaki şifreleme işlemi uygulanır:

$$E_3(16) = (16 + 3) \bmod 29 = 19$$

Benzer şekilde diğer harflerin şifreleme işlemi yapılır ve 19, 8, 5, 7, 18, 8, 26, 26, 14, 19, 8, 23 şifreli değerleri elde edilir. Tablo 3.1' e göre şifreli metin PĞEGÖĞVVLPĞT olarak elde edilir.

Kaydırma (Shift) Şifreleme Yöntemi

Sezar şifresinin genel halidir. Sezar şifresinde anahtar olarak 3 seçilirken, kaydırma şifresinde anahtar kullanıcı tarafından isteğe göre girilir. Her düz metin harfi kullanıcı tarafından girilen anahtar değerine göre kaydırılır ve şifreli metin elde edilir. $m, c, k \in \mathbb{Z}_n$ olmak üzere Kaydırma şifreleme yöntemi matematiksel olarak aşağıdaki gibi çalışmaktadır. Burada m şifrelenecek olan açık mesajı, c şifrelenmiş olan kapalı mesajı, k anahtarı kaydırma miktarını ve n kullanılan alfabedeki karakter sayısını göstermektedir.

Şifreleme: $c = E_k(m) = m + k\ mod\ n$

Şifre Çözme: $m = D_k(c) = c - k\ mod\ n$

Örnek 3.2. "FEN BİLİMLERİ ENSTİTÜSÜ" kelimelerini şifreleyelim ve anahtar olarak $k = 4$' ü seçelim.

Şifreleme: $m =$ FENBİLİMLERİENSTİTÜSÜ düz metninin Türk alfabesine göre sayısal değer karşılıkları 6, 5, 16, 1, 11, 14, 11, 15, 14, 5, 20, 11, 5, 16, 21, 23, 11, 23, 25, 21, 25 olur. Türk alfabesi kullanıldığı için mod 29' a göre işlem yapılır. Dolayısıyla, her değer $mod\ 29$ a göre 4 kaydırılırsa şifreli değerler 10, 9, 20, 5, 15, 18, 15, 19, 18, 9, 24, 15, 9, 20, 25, 27, 15, 27, 0, 25, 0 olarak elde edilir. Türk alfabesinin sayısal değerlerine (Bkz Tablo 3.1) göre $c =$IHREMÖMPÖHUMHRÜYMYAÜA şifreli metini elde edilir.
Şifre Çözme: $c =$IHREMÖMPÖHUMHRÜYMYAÜA şifreli metininin Türk alfabesine göre sayısal değer karşılıkları 10, 9, 20, 5, 15, 18, 15, 19, 18, 9, 24, 15, 9, 20, 25, 27, 15, 27, 29, 25, 29 olur. Türk alfabesi kullanıldığı için mod 29' a göre işlem yapılır. Dolayısıyla, her değer $mod\ 29$ a göre 4 geri kaydırılarak 6, 5, 16, 1, 11, 14, 11, 15, 14, 5, 20, 11, 5, 16, 21, 23, 11, 23, 25, 21, 25 sayısal değerlerine ulaşılır ve şifre çözülür. Türk alfabesinin sayısal değerlerine (Bkz Tablo 3.1) göre $m =$ FENBİLİMLERİENSTİTÜSÜ anlamlı metnine ulaşılır.

Kaydırma şifreleme yönteminin güvenliğini kısaca inceleyelim. Kaydırma (Shift) şifresine saldırı yapılırsa, 29 harfli Türk alfabesi üzerindeki Kaydırma şifresinde olası anahtar sayısı toplam 28 tanedir. Dolayısıyla, 28 anahtar denenerek tam arama yöntemi ile gerçek anahtar bulunabilir. Diğer taraftan, kaydırma şifresi monoalfabetik olduğu için bir harf her zaman aynı harf olarak şifrelenir. Dolayısıyla, açık metindeki frekans dağılımı korunduğu için frekans analizi saldırısı uygulanabilir. Ayrıca, açık metin – kapalı metin çifti kullanılarak kaydırma miktarı kolaylıkla elde edilebileceği için bilinen açık metin saldırısı da kolaylıkla uygulanabilir. Sonuç olarak kaydırma şifresi, tam arama yöntemi, frekans saldırısı ve bilinen açık metin saldırısına karşı güvensizdir.

Yer Değiştirme Yöntemi

Yer değiştirme yönteminde açık metindeki karakterlerin yerleri sabittir ve kullanılan alfabeye göre yazılır. Açık metindeki harflerin yerleri rastgele değiştirilerek açık metin ile eşleşecek şekilde tekrar yazılır ve şifreli metin elde edilir. Yer değiştirme yöntemi matematiksel olarak aşağıdaki gibi çalışmaktadır. m şifrelenecek olan açık mesajı ve c şifrelenmiş olan kapalı mesajı göstermektedir. n kullanılan alfabedeki karakter sayısı olmak üzere $m, c \in \mathbb{Z}_n$ dir ve anahtar uzayı $K =$ $\{\mathbb{Z}_n$ kümesi üzerindeki permütasyonlar$\}$ kümesidir. Anahtar olarak kullanılan permütasyonun uzunluğu alfabedeki karakter sayısı kadardır. $\mathbb{Z}_n$ kümesi üzerindeki anahtar π permütasyonu olmak üzere

Şifreleme: $E(m) = \pi(m) = c$

Şifre çözme: $D(c) = \pi^{-1}(c) = m$.

Örnek 3.3. NECMETTİN ERBAKAN açık metnini yerine koyma yöntemini kullanarak Türk alfabesine göre şifreleyelim. Anahtar olarak Tablo 3.2 de verilen 29 uzunluğundaki permütasyonu kullanalım.

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
M	U	H	L	İ	S	E	K	O	Ç	A	Ş	Ü	T	N	B	Z	V	J	C	Y	F	G	Ö	Ğ	D	P	I	R

Tablo 3.2. Yerine koyma yöntemi için uygulama örneği

N E C M E T T İ N E R B A K A N açık metni Tablo 3.2 deki anahtarla şifrelenirse Z S H B S Ö Ö Ş Z S Y U M T M Z şifreli metni elde edilir.

Yer değiştirme yönteminin güvenliğini kısaca inceleyelim. Yer değiştirme şifresine saldırı uygulanırsa, 29 harfli Türk alfabesi üzerindeki yer değiştirme şifresinde olası anahtar sayısı toplam 29! tanedir. Dolayısıyla, tam arama yöntemi ile anahtarı bulmak çok zordur. Diğer taraftan, yer değiştirme şifresi monoalfabetik (tek alfabeli) olduğu için bir harf her zaman aynı harf olarak şifrelenir. Dolayısıyla, açık metindeki frekans dağılımı korunur ve bu yüzden frekans analizi saldırısı uygulanabilir.

Permütasyon Şifreleme Yöntemi

Permütasyon şifreleme yöntemi, yer değiştirme yöntemine benzemektedir. Yer değiştirme yönteminde alfabedeki tüm harfler kullanılırken, Permütasyon şifrelemede kullanılacak olan anahtar uzunluğu isteğe göre girilebilir. Permütasyon şifreleme yöntemi matematiksel olarak aşağıdaki gibi çalışmaktadır. M şifrelenecek olan açık mesaj bloğunu, C şifrelenmiş olan kapalı mesaj bloğunu ve n kullanılan alfabedeki karakter sayısını göstermektedir. d pozitif bir tam sayı öyle ki $1 \leq d \leq n$ olmak üzere $K = \{1, \dots, d\}$ kümesi üzerindeki π permütasyonlarının kümesi anahtar uzayını oluşturur. Bu durumda şifreleme ve şifre çözme anahtarları d uzunluğundaki permütasyonlardır ve bu permütasyonlar birbirinin tersidir. Aynı zamanda, d sayısı blok uzunluğu olur ve $M, C \in \mathbb{Z}_n^d$ dir. $M = (m_1, \dots, m_d)$ ve $C = (c_1, \dots, c_d)$ olmak üzere π permütasyon anahtarı ile şifreleme ve şifre çözme işlemleri aşağıdaki gibi çalışmaktadır.

Şifreleme: $E_\pi(M) = E_\pi(m_1, \dots, m_d) = (m_{\pi(1)} \dots, m_{\pi(d)}) = (c_1, \dots, c_d) = C$

Şifre çözme: $D_{\pi^{-1}}(C) = D_{\pi^{-1}}(c_1, \dots, c_d) = \left(c_{\pi^{-1}(1)} \dots, c_{\pi^{-1}(d)}\right) = (m_1, \dots, m_d) = M$

Örnek 3.4. MATEMATİK ÖĞRETMENLİĞİ açık metnini Türk alfabesini kullanarak permütasyon şifreleme yöntemiyle şifreleyelim. Anahtar uzunluğu $d = 7$ olmak üzere anahtarımız $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 6 & 2 & 3 & 1 & 5 \end{pmatrix}$ permütasyonu olsun. $d = 7$ olduğu için açık metini 7 uzunluğunda bloklara bölerek her bloğu ayrı ayrı şifreleyelim.

Şifreleme: $E_\pi(M) = E_\pi(m_1, \dots, m_d) = (M, A, T, E, M, A, T) = (T, E, A, A, T, M, M) = C$

Diğer iki blokta benzer şekilde şifrelenir ve $M =$ MATEMAT İKÖĞRET MENLİĞİ açık metninin şifrelenmiş metni $C =$ TEAATMM TĞEKÖİR İLĞENMİ olarak bulunur.

$C =$ TEAATMM TĞEKÖİR İLĞENMİ şifreli metni çözmek için π permütasyonunun tersi olan $\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 4 & 5 & 2 & 7 & 3 & 1 \end{pmatrix}$ permütasyonu kullanılır.

Şifre çözme:

$$D_{\pi^{-1}}(C) = D_{\pi^{-1}}(c_1, \dots, c_d) = (T, E, A, A, T, M, M) = (M, A, T, E, M, A, T) = M$$

Diğer iki blokta da benzer şekilde şifre çözme işlemi yapılır. Dolayısıyla, C= TEAATMMTĞEKÖİRİLĞENMİ şifreli metinine karşılık gelen açık metin olarak $M =$ MATEMATİKÖĞRETMENLİĞİ elde edilir.

Permütasyon şifreleme yönteminin güvenliğini kısaca inceleyelim. Permütasyon şifrelemeye saldırı uygulanırsa, olası anahtar sayısı toplam $d!$ tanedir. Dolayısıyla, blok uzunluğu d' ye bağlı olarak tam arama yöntemi uygulanabilir. Diğer taraftan, permütasyon şifrelemesi frekans analizi saldırısı uygulanamaz. Ayrıca açık metin ve kapalı metin elimizde olduğunda anahtara kolayca ulaşabileceğimiz için bilinen açık metin saldırısına karşı güvensizdir.

Afin Şifreleme Yöntemi

Afin (doğrusal) şifreleme, geometrik bir şifreleme yöntemidir. Afin şifreleme yöntemi matematiksel olarak aşağıdaki gibi çalışmaktadır. m şifrelenecek mesajı, c şifrelenmiş mesajı, $k = (a, b)$ anahtarını ifade etmektedir. Kullanılan alfabedeki karakter sayısı n olmak üzere $m, c \in \mathbb{Z}_n$ olur ve anahtar uzayı $K = \{(a, b) \in \mathbb{Z}_n \times \mathbb{Z}_n : obeb\,(a, n) = 1\}$ kümesidir. Burada, $obeb\,(a, n) = 1$ olduğu için $\mathbb{Z}_n$ kümesinde a sayısının (anahtarının) tersi vardır. $a^{-1} \in \mathbb{Z}_n$ sayısı şifre çözme işleminde anahtar olarak kullanlacaktır. Eğer $obeb\,(a, n) \neq 1$ olursa şifre çözme işlemi doğru çalışmaz.

Şifreleme: $c = E(m) = (a \cdot m + b)\ mod\ n$

Şifre çözme: $m = D(c) = a^{-1}(c - b)\ mod\ n.$

Türk alfabesi kullanılarak yapılacak şifreleme işlemi için, Türk alfabesindeki karakterlerin sayısal değerleri Tablo 3.1' de verilmiştir. Örneğin 29 karakterli Türk alfabesinde $n = 29$ için olası anahtar sayısı $\#\,\mathbb{Z}_{29}^{*} \cdot \#\,\mathbb{Z}_{29} = 28 \cdot 29 = 812$ olarak bulunur. Şimdi 'MATEMATİK' kelimesini şifreleyelim.

Örnek 3.5. Türk alfabesi kullanarak 'MATEMATİK' kelimesini Afin şifreleme ile şifrelemek için anahtar olarak $k = (a, b) = (3,5)$ seçelim. $(3,5) \in \mathbb{Z}_{29} \times \mathbb{Z}_{29}$ öyle ki $obeb(3,29) = 1$. Şifreleme, MATEMATİK düz metninin Tablo 3.1' e göre karakter karşılıkları 15, 0, 23, 5, 15, 0, 23, 11, 13 olur ve ilk harf 15 için aşağıdaki gibi şifreleme işlemi uygulanır:

$E_k(M) = (3 \cdot 15 + 5) \bmod 29 = 21.$

Benzer şekilde diğer harflerin şifreleme işlemi yapılır ve 21, 5, 16, 20, 21, 5, 16, 9, 15 şifreli değerleri elde edilir. Tablo 3.1' e göre şifreli metin SENRSENHM olarak elde edilir.

Şifre Çözme, 'SENRSENHM' şifreli metninin, Tablo 3.1' e göre sayısal değerler 21, 5, 16, 20, 21, 5, 16, 9, 15 olur. Şifre çözme işlemi için $m = D(c) = a^{-1}(c - b) \bmod n$ şifre çözme fonksiyonu uygulanır. Burada $a^{-1} = 3^{-1} = 10 \bmod 29$. İlk harf $S = 21$ için $D(S) = 10(21-5) \bmod 29 = 15$ şifre çözme işlemi uygulanır. Benzer şekilde diğer harflerin şifre çözme işlemi yapılır ve $15, 0, 23, 5, 15, 0, 23, 11, 13$ değerleri elde edilir. Tablo 3.1' e göre;

$$15 = M,\ 0 = A, 23 = T,\ 5 = \mathrm{E}, 15 = \mathrm{M}, 0 = \mathrm{A}, 23 = \mathrm{T}, 11 = \mathrm{İ}, 13 = \mathrm{K}$$

olarak bulunur. Dolayısıyla, 'MATEMATİK' açık metni elde edilir.

Afin şifreleme yönteminin güvenliğini kısaca inceleyelim**.** Afin şifreleme sistemine Tam Arama Saldırısı uygulanırsa, 29 harfli Türk alfabesi üzerindeki afin şifresinde olası anahtar sayısı toplam 812 tane olduğu için tam arama yöntemi ile gerçek anahtar kolaylıkla bulunabilir. Diğer taraftan, afin şifresi monoalfabetik olduğu için bir harf her zaman aynı harf olarak şifrelenir. Dolayısıyla, açık metindeki frekans dağılımı korunur ve bu yüzden frekans analizi saldırısı uygulanabilir.

Bilinen açık metin saldırısının uygulanabilirliğini inceleyelim. 'MATEMATİK' kelimesinin şifreli hali 'SENRSENHM' metnidir. Açık metin 'MATEMATİK' ve kapalı metin 'SENRSENHM' çifti için Bilinen Açık Metin Saldırısını uygulayalım. 'MATEMATİK' açık metnindeki ilk iki harfinin Tablo 3.1' e göre sayısal değeri (15, 0) dır. 'SENRSENHM' kapalı metnindeki ilk iki harfin Tablo 3.1' e göre sayısal değeri (21,

5) dir. Şifreleme anahtarları $a, b \in \mathbb{Z}_{29}$ olan Afin şifreleme algoritmasını kullanarak aşağıdaki gibi iki bilinmeyenli iki denklem

$$15a + b = 21$$
$$0a + b = 5$$

oluşturulur. Bu denklem sistemini yok etme metodu ile çözerek $a \equiv 3 \bmod 29$ ve $b \equiv 5 \bmod 29$ anahtarlarını kolayca elde edebiliriz. Böylece, Bilinen Açık Metin Saldırısıyla $k = (a, b) = (3,5)$ anahtarına ulaşmış oluruz, diğer bir ifadeyle, şifre kırılmış olur.

Hill Şifreleme Yöntemi

Hill şifreleme yöntemi 1929 yılında Lester Hill tarafından önerilmiştir. Amerikan matematikçi Lester Hill, Lineer Cebir kullanan ilk şifreleme sistemini tasarlamıştır. Bu şifreleme sistemi matris ve vektör (anahtar ile mesaj) çarpımına dayanır. Hill şifreleme sistemi matematiksel olarak aşağıdaki gibi çalışmaktadır. d pozitif bir tam sayı ve n şifreleme yapılacak dilin karakter sayısı olmak üzere açık mesaj ve kapalı mesaj uzayları $\mathbb{Z}_n^d$ olsun. $M = [m_1 m_2 \dots m_d] \in \mathbb{Z}_n^d$ açık mesaj, $C = [c_1\ c_2 \dots\ c_d] \in \mathbb{Z}_n^d$ şifreli mesaj ve

$$K = \begin{pmatrix} k_{11} & \cdots & k_{1d} \\ \vdots & \ddots & \vdots \\ k_{d1} & \cdots & k_{dd} \end{pmatrix} \in M_{d\times d}(\mathbb{Z}_n)$$

şifreleme anahtarı olmak üzere

Şifreleme: $C = E_K(M) = M \cdot K \bmod n$

Şifre Çözme: $M = D_K(C) = C \cdot K^{-1} \bmod n$

Şifre çözme işleminin yapılabilmesi için K anahtar matrisinin tersinir matris olması gerekmektedir. $\mathbb{Z}_n$ halkası üzerinde matrisin tersinin olması için $det(K) \neq 0$ ve $obeb\,(det\,(K), n) = 1$ olmalıdır.

Örnek 3.6. '$\ddot{O}\breve{G}RENMEK$' açık metnini $K = \begin{bmatrix} 5 & 4 \\ 30 & 25 \end{bmatrix}$ anahtar matrisini Türk alfabesi kullanarak, $\mathbb{Z}_{29}$ üzerinde Hill şifreleme sistemi ile şifreleyelim. İlk olarak matrisin determinantını bulalım. $det\,(K) = 5$ olarak bulunur ve $det\,(K) \neq 0$ ve $obeb\,(5, 29) = 1$ olduğu için K tersinir bir matristir. Şifreleme yaparken daha önce Tablo 3.1 de verilen Türk alfabesindeki harf karşılıkları kullanılmıştır.

Anahtar 2×2 matris olduğundan, $d = 2$ ve düz metin Türk alfabesine göre şifrelendiğinden, $n = 29$ olur. Şifrelenecek metin $d = 2$ olduğundan 2 uzunluklu

bloklara ayrılır ve harflere karşılık gelen sayı değerleri bulunur. Açık metinin sayısal değerleri

$$(\text{Ö}, \text{Ğ}) = (18,8), (R,E) = (20,5), (N,M) = (16,15), (E,K) = (5,13)$$

şeklindedir. Birinci blok aşağıdaki gibi şifrelenir.

Şifreleme: $C = (c_1, c_2) = E_K(M) = (18,8) \cdot \begin{bmatrix} 5 & 4 \\ 30 & 25 \end{bmatrix} \bmod 29 \equiv (11,11)$.

Benzer şekilde diğer bloklar için de yukarıdaki gibi şifreleme işlemi yapılarak, (11, 11), (18, 2), (8, 4), $(9,26)$ değerleri elde edilir. Bu değerlere karşılık gelen harfler Tablo 3.1 den bulunur ve "*İİÖCĞDHV*" şifreli metni elde edilir.

Şifre çözme: Şimdi şifreli "*İİÖCĞDHV*" metnini çözmeye çalışalım. Şifrelemede kullanılan K anahtarı 2×2 matris olduğundan $d = 2$ dir. "*İİÖCĞDHV*" metni ikişer parçaya ayrılıp, harflere karşılık gelen sayı değerleri bulunur,

$$(\text{İ}, \text{İ}) = (11,11), (\text{Ö}, C) = (18,2), (\text{Ğ}, D) = (8,4), (H,V) = (9,26)$$

Şifre çözme işlemi için şifreleme anahtarı olan $K = \begin{bmatrix} 5 & 4 \\ 30 & 25 \end{bmatrix}$ matrisinin tersi $K^{-1} = \begin{bmatrix} 5 & 5 \\ 23 & 1 \end{bmatrix}$ elde edilir. Şifreli halde verilen "*İİÖCĞDHV*" kelimesini $d = 2$ parçaya ayırarak alfabedeki karşılıklarını yazalım. $(\text{İ}, \text{İ}) = (11,11), (\text{Ö}, C) = (18,2), (\text{Ğ}, D) = (8,4), (H,V) = (9,26)$ olarak bulunur. Şifreli metin $M = D_K(C) = C \cdot K^{-1} \bmod n$ şifre çözme fonksiyonu kullanılarak çözülür. Örneğin, $(\text{İ}, \text{İ}) = (11,11)$ bloğunun şifre çözümü

$$\left([11 \quad 11] \cdot \begin{bmatrix} 5 & 5 \\ 23 & 1 \end{bmatrix}\right) \bmod 29 = [18 \quad 8]$$

şeklinde yapılır ve $(18,8) = (\text{Ö}, \text{Ğ})$ olarak bulunur. Benzer şekilde diğer ikili harf blokları çözülür ve $(18,8), (20,5), (16,15), (5,13)$ sayısal değerleri elde edilir. Karşılık gelen harfler $(\text{Ö}, \text{Ğ}), (R,E), (N,M), (E,K)$ olduğu için "ÖĞ*RENMEK*" açık metnine ulaşılır.

Hill şifreleme yönteminin güvenliğini kısaca inceleyelim. K şifreleme anahtarında d^2 tane bilinmeyen olduğu için d nin büyüklüğüne bağlı olarak Tam Arama yöntemi uygulanabilir. Hill şifreleme sistemi polialfabetik olduğu (aynı harf çoğunlukla farklı harf olarak şifrelenir) için açık metindeki frekans dağlımı korunmaz. Dolayısıyla, frekans saldırısı uygulanamaz. Fakat, $d = 2$ durumunda frekans analizi uygulanabilir. Bilinen açık metin saldırısı ile d^2 tane açık metin – kapalı metin çifti kullanılarak anahtar kolayca elde edilebilir. Örneğin, açık metin "ÖĞ*RENMEK*" ve kapalı metin "*İİÖCĞDHV*" çiftini

alalım. $E_K(M) = M \cdot K \bmod n$ şifreleme dönüşümünü kullanarak K anahtar matrisini bulalım.

$$(18,8) \cdot \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix} \bmod 29 \equiv (11,11)$$

$$(20,5) \cdot \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix} \bmod 29 \equiv (18,2)$$

Bu dönüşümlerden

$$18k_{11} + 8k_{21} = 11 \qquad 18k_{12} + 8k_{22} = 11$$

$$20k_{11} + 5k_{21} = 18 \qquad 20k_{12} + 5k_{22} = 2$$

dört bilinmeyenli dört denklem sistemi elde edilir. Bu denklem sistemini Yok Etme Metodu ile çözerek $K = \begin{bmatrix} 5 & 4 \\ 30 & 25 \end{bmatrix}$ anahtarı elde edilir. Böylece, Bilinen Açık Metin Saldırısıyla şifre kırılmış olur.

Vigenère Şifreleme Yöntemi

Uzun yıllardır kırılması mümkün olmayan Vigenère Şifresi, Çifre Giovan Batista isimli bir İtalyan tarafından 1553' te tanıtılmıştır. Bu şifre 1586 yılında Fransız diplomat Blaise De Vigenere tarafından düzenlenerek kullanılmış ve 'Vigenere Şifresi' ismini almıştır. Şifrelenecek metinde bulunan her bir harf farklı bir alfabeyle şifrelenir. Hangi alfabenin seçileceğine anahtar kelimeye bakılarak karar verilir. Şifrelenecek metnin uzunluğuna göre anahtar tekrarlı olarak yazılır ve şifreleme yapılır. Uzun yıllar güvenilirliğini koruyabilen bu şifre İngiliz matematikçi Charles Babbage ve Avusturya ordusunda görevli Kriptograf Friedrich Kasiski tarafından kırılmıştır.

Karakterlerin birebir değiştirilmesi yerine anahtar uzunluğunda bir metnin bir algoritma ile aynı anda şifrelenmesi bu yöntemin en önemli özelliğidir. Bu metoda çoklu alfabe (polyalphabetic) metodu denir. Vigenère şifreleme yöntemi matematiksel olarak aşağıdaki gibi çalışmaktadır. d pozitif tam sayısı anahtar uzunluğu ve n şifreleme yapılacak alfabenin karakter sayısı olsun. $M = (m_1, m_2, \dots, m_d) \in \mathbb{Z}_n^d$ açık mesaj, $C = (c_1, c_2, \dots c_d) \in \mathbb{Z}_n^d$ şifreli mesaj ve $K = (k_1, k_2, \dots, k_d) \in \mathbb{Z}_n^d$ şifreleme anahtarı olmak üzere;

Şifreleme: $E_K(M) = (m_1 + k_1, \dots, m_d + k_d) = (c_1, \dots, c_d) = C$

Şifre çözme: $D_K(C) = D_k(c_1, \dots, c_d) = (c_1 - k_1, \dots, c_d - k_d) = (m_1, \dots, m_d) = M$

Anahtar uzunluğu d olduğu için şifrelenecek metin d uzunluğunda bloklara ayrılarak her blok ayrı ayrı şifrelenir.

Türk Alfabesi için Oluşturulmuş Vigenère Tablosu. Vigenere Şifreleme için alfabedeki harflerin yer aldığı bir tablo kullanılır. Vigenère şifreleme algoritması 26×26 bir tablo oluşturularak kullanılmaktadır. Bu tabloda ilk satır ve sütunda alfabe yer almaktadır. Daha sonraki satırlar oluşturulurken alfabe bir adım sola kaydırılarak tabloya yerleştirilir. Biz Türk alfabesi ile şifreleme yapacağımız için 29×29 lık bir tablo kullanacağız. Aşağıdaki sıralı sütunlarda her satırdaki harfler 1adım sola kaydırılarak oluşturulur**.**

	A	B	C	Ç	D	E	F	G	Ğ	H	İ	I	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
A	A	B	C	Ç	D	E	F	G	Ğ	H	İ	I	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
B	B	C	Ç	D	E	F	G	Ğ	H	İ	I	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A
C	C	Ç	D	E	F	G	Ğ	H	İ	I	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B
Ç	Ç	D	E	F	G	Ğ	H	İ	I	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C
D	D	E	F	G	Ğ	H	İ	I	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç
E	E	F	G	Ğ	H	İ	I	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D
F	F	G	Ğ	H	İ	I	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E
G	G	Ğ	H	İ	I	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F
Ğ	Ğ	H	İ	I	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G
H	H	İ	I	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ
İ	İ	I	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H
I	I	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	İ
J	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	İ	I
K	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	İ	I	J
L	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	İ	I	J	K
M	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	İ	I	J	K	L
N	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	İ	I	J	K	L	M
O	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	İ	I	J	K	L	M	N
Ö	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	İ	I	J	K	L	M	N	O
P	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	İ	I	J	K	L	M	N	O	Ö
R	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	İ	I	J	K	L	M	N	O	Ö	P
S	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	İ	I	J	K	L	M	N	O	Ö	P	R
Ş	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	İ	I	J	K	L	M	N	O	Ö	P	R	S
T	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	İ	I	J	K	L	M	N	O	Ö	P	R	S	Ş
U	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	İ	I	J	K	L	M	N	O	Ö	P	R	S	Ş	T
Ü	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	İ	I	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U
V	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	İ	I	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü
Y	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	İ	I	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V
Z	Z	A	B	C	Ç	D	E	F	G	Ğ	H	İ	I	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y

Tablo 3.3. Tük alfabesi için oluşturulmuş Vigenère tablosu

Tablo 3.3'te Türk alfabesi için oluşturulmuş Vigenere tablosu görülmektedir. Şifreleme işlemi yapılırken anahtar olarak seçilen kelime şifrelenecek metnin uzunluğu kadar tekrarlı bir şekilde yazılır. Vigenere tablosunda şifrelenecek metnin harfleri satır, anahtar kelimenin harfleri sütun olmak üzere satır ve sütunun kesişimindeki harfler alınarak şifreleme işlemi yapılır. Bu işlem her harf için yapılır ve şifreli metin elde edilir.

Örnek 3.7. "İLKÖĞRETİM MATEMATİK ÖĞRETMENLİĞİ" metnini Vigenère tablosuna göre şifreleyip çözelim.

Şifrelenecek metin : İ L K Ö Ğ R E T İ M M A T E M A T İ K Ö Ğ R E T M E N L İ Ğİ

Anahtar : BİLGİSAYAR

Şifrelenecek metin 31 karakter uzunluğunda, anahtarımız ise 10 karakter uzunluğundadır. Öncelikle anahtar metni şifrelenecek metin uzunluğu kadar tekrarlı yazılır.

İ	L	K	Ö	Ğ	R	E	T	İ	M	M	A	T	E	M	A	T	İ	K	Ö	Ğ	R	E	T	M	E	N	L	İ	Ğ	İ
B	İ	L	G	İ	S	A	Y	A	R	B	İ	L	G	İ	S	A	Y	A	R	B	İ	L	G	İ	S	A	Y	A	R	B

Tük alfabesi için oluşturulmuş Vigenère tablosundan ilk harf satır ikinci harf sütun eşleştirmesi yapılırsa, İ-satır, B-sütun kesişimindeki harf olan "I" alınır. Aynı şekilde diğer harfler için de bu işlem yapılarak şifreli metin

I U Y Ü Ö J E S İ F N İ Ğ J Ü S T Ğ K H H B P Ü V N J İ Z T

şeklinde elde edilir. Şimdi şifreli metni Vigenère tablosu yardımıyla çözelim. Şifre çözmek için anahtar şifresi çözülecek metin uzunluğu kadar tekrarlı yazılır.

I	U	Y	Ü	Ö	J	E	S	İ	F	N	İ	Ğ	J	Ü	S	T	Ğ	K	H	H	B	P	B	Ü	V	N	J	İ	Z	I
B	İ	L	G	İ	S	A	Y	A	R	B	İ	L	G	İ	S	A	Y	A	R	B	İ	L	G	İ	S	A	Y	A	R	B

Şifreli metni çözmek için verilen metindeki ilk harf olan I harfinin karşılığını bulmak için anahtar olan B sütunundaki I harfi bulunup buna karşılık gelen satıra bakılır. I harfine karşılık gelen harf "İ" harfidir. Aynı şekilde anahtar olan İ sütunundaki U harfi bulunup buna karşılık gelen satıra bakılır. U harfine karşılık gelen harf "L" harfidir. Bu şekilde devam edilerek, Y → K, Ü → Ö, Ö → Ğ, J → R, E → E, S → T, İ → İ, F → M, N → M, İ → A, Ğ → T, J → E, Ü → M, S → A, T → T, Ğ → İ, K → K, H → Ö, H →Ğ, B →R, P →E, B →T, Ü →M, V →E, N →N, J →L, İ →İ, Z →Ğ, I →İ karşılıkları bulunur. Açık metin olan "İLKÖĞRETİM MATEMATİK ÖĞRETMENLİĞİ" metnine ulaşılır.

Vigenère şifreleme yönteminin güvenliğini kısaca inceleyelim**.** Vigenère şifreleme sisteminde d uzunluğundaki anahtar kelimelerin sayısı n^d tanedir. 29 harfli Türk alfabesi üzerindeki vigenère şifrelemesinde olası anahtar sayısı 29^d olduğu için tam arama yöntemi uygulanamaz. Diğer taraftan, vigenère şifresi polyalfabetik olduğu için aynı harf genellikle farklı harf olarak şifrelenir. Dolayısıyla, açık metindeki frekans dağılımı korunmaz. Anahtarın uzunluğu $1 < d < 5$ için frekans analizi yapılabilir. Ancak büyük d' ler için bu çok zordur. d adet açık metin-şifreli metin çifti kolayca kırılabilir. Dolayısıyla vigenère şifreleme yöntemi bilinen açık metin saldırısına karşı güvensizdir.

Vernam Şifreleme Yöntemi

Gilbert Vernam 1917'de bu yöntemi geliştirmiş olup telgraf bağlantılarında kullanılmıştır. Bu yöntem Vigenere yöntemine benzemektedir. Ancak kullanılan şifreleme anahtarı tekrar etmez. Anahtar en az şifrelenecek metin büyüklüğündedir, rastgeledir ve tek kullanımlıktır. Vernam şifreleme yönteminde, rastgele üretilen bir harf veya rakam kullanılarak şifreleme yapılır. Düz metindeki her bir karakter üretilmiş olan karakter dizisinde karşılık gelen karakterlerle işleme alınarak şifreli metin elde edilir.

Vernam Şifrelemede, her şifrelemeden sonra anahtar değiştirilmesi bu yöntemi güvenli hale getirir. Ancak anahtarı karşı tarafa güvenli olarak iletmek güçtür ve masraflıdır. Aynı zamanda bu şifreleme yönteminin güvenliği, rastgele üretilen karakter dizisine bağlıdır. Bu dizi bir kurala bağlı olarak üretilir ve bu kural bulunursa sistem kırılabilir. Ancak bu etkenler dışında Vernam şifreleme mükemmel çalışan bir şifreleme sistemidir.

Enigma

Enigma, Alman elektrik mühendisi Arthur Scherbius tarafından I. Dünya Savaşı'nın sonlarında (1918) icat edilen elektro-mekanik bir şifreli haberleşme makinesidir. İkinci Dünya Savaşı sırasında Nazi Almanya'sı tarafından gizli mesajların şifrelenmesi ve tekrar çözülmesi amacı ile kullanılan şifre makinesi Enigma; savaşın sonucunu belirlemede büyük öneme sahiptir. İlk olarak 1920' li yıllarda ticari amaçla kullanılmaya başlanan Enigma; daha sonra pek çok ülkede ordu ve devlet kurumlarında kullanılmak üzere özel olarak üretilmiştir. Son versiyonu "Enigma-I" adıyla 1932 yılında üretilmiş ve Alman Ordusu, münhasır üretim haklarını edinmiştir. Enigma 1939 yılında tam anlamıyla Alman silahlı kuvvetlerinin iletişim cihazı haline gelmiştir.

Polonyalı kriptograflar, mesaj ayarlarını belirtmek için güvenli olmayan bir protokolden yararlanarak Enigma' nın yalnızca şifreli metinden oluşan başarılı bir kriptanalizini gerçekleştirebildiler. Sadece şifreli metin saldırıları Enigma' da yapılan mekanik şifreleme ile Bletchley Park' ta 2. Dünya Savaşı sırasında kesişen şifreli metinlere karşılık gelen açık metinlerin akıllıca tahmin edilmesiyle kırılmıştır.

Şekil 3.5. Enigma (URL-7, 2022)

Enigma makinesi bir klavye, alfabenin her harfi için bir ışık kümesi, üç rotor (bazı makinelerde 4 veya 5) ve altta bir fiş kartından oluşuyordu. Mekanik ve elektrik arasındaki sınırda yer alan Enigma, dışarıdan büyük bir daktilo gibi görünüyordu ve bu mantıkla çalışıyordu. Klavyedeki bir tuşa basıldığında, rotorlar bir harfi başka bir harf olarak kodlayacak şekilde hareket eder ve akım makineden geçtiğinde lamba panosunda çıkış harfini gösteren lamba yanar. Örneğin; klavyeden "P" harfine basılırsa ve Enigma makinesi bu harfi "B" olarak kodlarsa, lamba panosunda "B" harfinin bağlı olduğu lamba yanar. Yani bir harfe basıldığında o harfi rastgele bir harfle eşleştirir ve şifreli metin ortaya çıkar. Bu şifreleme işlemi kolayca yapılabilmektedir. Ancak farklı olan yönü aynı harfe tekrar basıldığında Enigma makinesi yeniden rastgele bir harf ile eşleştirme yapar. Örneğin "U" tuşuna basıldığında "H" harfi ile eşleştiriliyorsa, "U" tuşuna yeniden basıldığında başka bir harf ile eşleştirilir. Bir düz metin şifreleneceği zaman, makinenin üst kısmında bulunan ve rotor olarak adlandırılan şifreli çantalara benzeyen 3 farklı çift haneli sayının seçilebileceği bir alan bulunuyor. Buradaki sayılar ve şifreli mesaj bir kâğıda yazılır ve bir telsiz vasıtası ile Mors alfabesi kullanılarak radyo operatörü tarafından alıcıya gönderilirdi. Bu şekilde mesaj, mesajı ileten personelden bile gizlenmiş ve kilometrelerce uzakta, karada, havada ya da denizde bulunan Nazi subaylarına iletilmiş olurdu. Mesajı alan karşı taraf da bir Enigma makinesi kullanıyordu. Mesaj alındığında makine 3 adet doğru sayı düzenine ayarlanıyor ve mesaj deşifre ediliyordu. Enigma makinesi ile şifreleme yapılırken aynı harf girilse bile farklı harfle eşleştirme yaptığından, Almanlar bu sistemin kırılamaz olduğunu düşündüler. İkinci Dünya Savaşında Bletchley Park-Birleşik Krallık'ta üslenen Amerikalı ve İngiliz şifre çözücüler, o zamanın en

yetenekli ve değerli bilim insanı, matematikçi ve mühendislerinden oluşmaktaydı. Bunlardan bazıları, daha sonra Bilgisayar biliminin kurucularından sayılacak Alan Matthison Turing, Enigma makinesi ile üretilen Enigma şifreli mesajını icat ettiği bir makine ile kırdı. Enigma makinesin deşifre edilmesi; İkinci Dünya Savaşı'nın müttefiklerin lehine gelişmesini sağladı, Nazi Almanya'sının gerçekleştireceği planlar ortaya çıkarıldı ve savaş çok daha kısa bir süre içerisinde bitti. İkinci Dünya Savaşı ve stratejik planların aktarılmasında kullanılan şifre sistemleri ve bunların çözülmesinde kullanılan algoritmalar, buluşlar, şifre çözücü makineler bilgisayar bilimin ortaya çıkmasını sağlamıştır.

Bu bölümde verilen bilgiler için (Hill, 1929), (URL-6, 2022), (URL-7, 2022) kaynaklarından faydalanılmıştır.

3.2.2. Modern Şifreleme Yöntemleri

Bilgisayar ve haberleşme güvenliğinin temeli olan modern şifreleme yöntemleri kısa fakat karmaşıktır. Modern şifreleme yöntemlerindeki bütün algoritmalar şifreleme ve şifre çözme işlemlerini kontrol etmek için bir anahtar kullanırlar ve bir mesaj sadece kullanılan anahtar ile uyuştuğunda çözülebilir**.** Verilerin elektronik ortamda bitlerle ifade edilebilmesinden sonra şifrelemede bitler kullanılarak yapılmaya başlanmıştır. Böylece modern kriptografi çağı başlamıştır. Modern kriptografide iki ana şifreleme yöntemi vardır. Bunlar simetrik şifreleme (gizli anahtarlı şifreleme) ve asimetrik şifreleme (açık anahtarlı şifreleme) yöntemleridir.

Simetrik şifreleme şifreleme ve şifre çözme işlemleri için tek bir gizli anahtar kullanmaktadır. Bu durum veri şifreleme için matematiksel açıdan daha az problem çıkaran bir yaklaşımdır ve çok kullanılan bir yöntemdir. Bu tip algoritmalarda şifreleme işlemi gerçekleştirildikten sonra şifreli metni alıcıya gönderirken güvenli bir kanal üzerinden gizli anahtarı da alıcıya göndermek gerekmektedir. Simetrik şifrelemede kullanılan gizli anahtar sadece şifrelemeyi yapan ve şifreli mesajı okuma yetkisi olan kişilerde olmalıdır. Anahtarın başka kişilerce bilinmesi, iletilecek olan mesajın güvenliğini tehlikeye atar.

Asimetrik şifreleme Açık Anahtarlı Şifreleme olarak da bilinir. Asimetrik şifrelemede birbiri ile bağlantılı bir adet genel ve bir adet özel anahtar olmak üzere iki

farklı anahtar vardır. Açık mesaj genel anahtar ile şifrelenir ve karşılık gelen özel anahtar ile çözülür.

Modern kriptografik algoritmalar için (Koblitz, 1994), (Schneier, 1996), (Stinson & Paterson, 2019), (Menezes, Van Oorschot, & Vanstone, 2018), (Paar & Pelzl, 2009), (Tuncay, 2015) ve (Yerlikaya & Aslanyürek, 2019) kaynaklarından faydalanılabilir.

4. FARK DENKLEMLERİ ÜZERİNDE ŞİFRELEME SİSTEMİ

Fark denklemlerin kullanılarak şifreleme algoritmasını tanıtmadan önce fark denklemleri hakkında gerekli bilgileri verelim.

Bir fark denklemi genel olarak

$$F\big(n, d(n), d(n+1), \dots, d(n+k)\big) = 0$$

şeklinde gösterilir ve fark denklemlerinin çözümleri

$$d: \mathbb{Z} \to \mathbb{R}; d: n \to d(n), n = 0, \pm 1, \pm 2, \dots$$

şeklinde tanımlanan fonksiyonlardır.

Bir fark denkleminde, $d(n+j)$ terimlerinden en büyük indisli ile en küçük indisli olanın farkına *denklemin mertebesi* ve denklemde bulunan en yüksek dereceli terimin derecesine de *denklemin derecesi* denir.

Örneğin, $d(n+3) - 5d^4(n+1) + 7d(n-2) = 0$ fark denkleminin mertebesi $(n+3) - (n-2) = 5$ ve derecesi 4 dür.

Eğer fark denkleminde bütün terimlerin dereceleri 1 ve denklemin içinde $d(n+i) \cdot d(n+j)$ şeklinde terimlerin herhangi bir çarpımları bulunmuyor ise bu fark denklemine *lineer fark denklemi* denir.

$a_i(n)$ $(i = 1, 2, \dots, k)$ ve $g(n)$, $n \geq n_0$ için tanımlı reel değerli fonksiyon ve $n \geq n_0$ için $a_k(n) \neq 0$ olmak üzere k. mertebeden lineer fark denklemi

$$d(n) + a_1(n)d(n-1) + \dots + a_k(n)d(n-k) = g(n) \qquad (4.1)$$

şeklinde gösterilir (Elaydi, 2005).

Eğer

- $a_i \in \mathbb{R}$ $(i = 0,1, \dots, k)$ ise (4.1) denklemi sabit katsayılı fark denklemi
- $a_i(n)$ $(i = 0,1, \dots, k)$, n bağımsız değişkeninin bir fonksiyonu ise (4.1) denklemi değişken katsayılı fark denklemi
- $g(n) = 0$ ise (4.1) denklemi homogen fark denklemi
- $g(n) \neq 0$ ise (4.1) denklem homogen olmayan fark denklemi

olarak adlandırılır.

Çalışmamızda güvenlik analizi yaptığımız Cristina Flaut 2019' da verilen algoritmada kullanılan fark denklemi sabit katsayılı lineer homogen bir başlangıç değer problemi dir. Başlangıç şartları ile verilen bir fark denkleminin çözümü iterasyon ile bulunabilir. Örneğin birinci mertebeden sabit katsayılı homogen lineer

$$d(n) = ad(n-1), d(0) = d_0, n \geq 1$$

başlangıç değer problemini ele alalım. Bu başlangıç değer probleminin çözümünü iterasyon uygulayarak elde edelim.

$n = 1$ için $d(1) = ad(0) = ad_0$
$n = 2$ için $d(2) = ad(1) = a^2 d_0$
$n = 3$ için $d(3) = ad(2) = a^3 d_0$

$\vdots$

buradan kolayca başlangıç değer probleminin çözümü $d(n) = a^n d_0$ olduğu görülür.

Sabit katsayılı homogen lineer bir başlangıç değer probleminin mertebesi büyüdükçe genel çözümü iterasyon ile hesaplamak her zaman kolay olmayabilir. Bu neden ile verilen yüksek mertebeden sabit katsayılı homogen lineer bir başlangıç değer problemini kompanyan matris yardımıyla birinci mertebeden sabit katsayılı lineer bir denklem sistemine dönüştürüp çözümü iterasyon ile hesaplanabilir. Mesela üçüncü mertebeden sabit katsayılı homogen lineer

$$d(n) = a_1 d(n-1) + a_2 d(n-2) + a_3 d(n-3) \tag{4.2}$$

fark denklemini $d(0) = d_0, d(-1) = d_{-1}, d(-2) = d_{-2}, n \geq 1$ başlangıç şartları altında ele alalım. (4.2) denklemini kompanyan matris yardımıyla birinci mertebeden bir sisteme dönüştürelim.

$x(n) = \begin{pmatrix} d(n-3) \\ d(n-2) \\ d(n-1) \end{pmatrix}$ ve $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ a_3 & a_2 & a_1 \end{pmatrix}$ olmak üzere (4.2) denklemi

$$x(n+1) = Ax(n) \tag{4.3}$$

birinci mertebeden sabit katsayılı lineer fark denklem sistemine dönüşür. (4.3) denklem sistemini $x(0) = \begin{pmatrix} d(-3) \\ d(-2) \\ d(-1) \end{pmatrix}$ başlangıç şartı altında ele alırsak verilen problem

$$x(n+1) = Ax(n), x(0) = x_0 \; ; n \geq 0$$

başlangıç değer problemine dönüşür. Bu başlangıç değer probleminin çözümü iterasyon ile kolayca

$$x(n) = A^n x_0$$

olduğu kolayca görülür (Akın ve Bulgak, 1998).

Böylece sabit katsayılı homogen lineer bir fark denkleminin verilen başlangıç şartları altında genel çözümünün iterasyon ile nasıl hesaplanacağını göstermiş olduk. Şimdi tezimizde güvenlik analizini yaptığımız şifreleme algoritmasını tanıtan makalede (Flaut 2019) kullanılan *k*. mertebeden sabit katsayılı lineer fark denklemini tanıtalım.

$n, k \in \mathbb{N}$, $k \geq 2, n \geq k$ olmak üzere.

$$d(n) = a_1 d(n-1) + a_2 d(n-2) + \cdots + a_k d(n-k), a_k \neq 0 \qquad (4.4)$$

fark denklemini $d_0 = d_1 = \cdots = d_{k-2} = 0, d_{k-1} = 1$ başlangıç şartları altında ele alalım.

Tanım 4.1. (d_n) pozitif tamsayıların bir dizisi her bir $n \geq 0$ için

$$n = c_1 d_1 + \cdots + c_m d_m; \; c_1, \ldots c_m \in \{0,1\}$$

olarak ifade edilebiliyorsa (d_n) dizisine tam dizi denir (Flaut, 2019).

Tanım 4.2. (d_n) pozitif tamsayıların bir dizisi her bir $n \geq 0$ için

$$n = c_1 d_1 + \cdots + c_q d_q; \; c_0, \ldots, c_q \in \mathbb{N}, c_q \neq 0$$

denklemini sağlayan $q \geq 0$ doğal sayısı bulanabiliyorsa (d_n) dizisi genel tam (g-tam) olarak adlandırılır (Flaut 2019).

Teorem 4.1. Terimleri (4.4) başlangıç değer problemi tarafından üretilen (d_n) pozitif tamsayı dizisi g-tamdır (Flaut 2019).

İspat. Teoremde verilen fark denkleminin ürettiği pozitif tamsayı dizisi (d_n) olsun. n , q doğal sayılar, $q \geq k \geq 2$ olmak üzere $d_q \leq n < d_{q+1}$ eşitsizliğini sağlayan dizinin d_q elemanını belirleyelim. Burada Bölüm Kalan Teoremi (Quotient Remainder Theorem)' ni kullanacağız. Bölüm Kalan Teoremi n ve d_q doğal sayıları için c_q ve r_q doğal sayılarının bulunduğunu belirtir.

$c_q, c_{q-1}, \dots, c_{k-1}$ ve $r_q, r_{q-1}, \dots, r_k$ doğal sayıları için

$n = d_q c_q + r_q, 0 \leq r_q < d_q,$

$r_q = d_{q-1} c_{q-1} + r_{q-1}, 0 \leq r_{q-1} < d_{q-1},$

$r_{q-1} = d_{q-2} c_{q-2} + r_{q-2}, 0 \leq r_{q-2} < d_{q-2},$

$\vdots$

$r_{k+1} = d_k c_k + r_k, 0 \leq r_k < d_k,$

$r_k = d_{k-1} c_{k-1}.$

Fark denkleminin tanımındaki başlangıç değeri $d_{k-1} = 1$ olduğundan $c_{k-1} = r_k$ olur. Dolayısıyla; $n = d_q c_q + r_q$ da r_q yerine $r_q = d_{q-1} c_{q-1} + r_{q-1}$, r_{q-1} yerine de $r_{q-1} = d_{q-2} c_{q-2} + r_{q-2}$ yazılarak ve bu şekilde devam ederek,

$n = d_q c_q + d_{q-1} c_{q-1} + d_{q-2} c_{q-2} + \cdots + d_k c_k + d_{k-1} c_{k-1}$ elde edilir.

Şimdi Flaut 2019 çalışmasında önerilen ve (4.4) de verilen fark denklemi kullanılarak tasarlanan şifreleme algoritmasını tanıtalım.

4.1. Şifreleme Algoritması

$\mathcal{A}$; 0 ile $N-1$ arasında etiketlenmiş, N sayıda harfle oluşan bir alfabe,
m; harflerden oluşan bir metin,
n; *m* metninden gelen harfleri kullanarak elde edilen sayı
dır. Aşağıda verilen algoritmada, *m* metni aynı uzunluktaki $m_1, m_2, \dots, m_r$ bloklarına bölünerek, bu bloklara İngiliz alfabesinde ki harflere karşılık gelen sayılar ile $n_1, n_2, \dots, n_r$ sayıları elde edilmiştir.

Algoritmanın Adımları:

1. $k \geq 2$ olmak üzere $a_1, a_2, \dots, a_k$ doğal sayıları kullanıcı tarafından girilsin.

2. $a_1, a_2, \dots, a_k$ katsayıları (4.4) fark denkleminde kullanarak (d_n) dizisinin terimleri belirlenir ($a_1, a_2, \dots, a_k$ doğal sayıları kullanıcı tarafından girildiği için fark denkleminde yerine yazılarak (d_n) dizisinin terimleri bulunur).

3. $d_q \leq n_i < d_{q+1}, i \in \{1,2, \dots, \mathrm{r}\}$ olmak üzere n_i sayısına karşılık d_q elemanı belirlenir (Bölüm Kalan Teoremine bu bulduğumuz d_q elemanından başlanır).

4. (4.4) fark denklemi kullanarak

$$n_i = d_q c_{iq} + d_{q-1} c_{i(q-1)} + d_{q-2} c_{i(q-2)} + \cdots + d_k c_{ik} + d_{k-1} c_{i(k-1)}$$

(d_n) dizisinin terimleri ve $c_{iq}, c_{i(q-1)}, \dots, c_{i(k-1)}$ katsayıları belirlenir (Bölüm Kalan Teoremine göre bulunur).

5. $(c_{iq}, c_{i(q-1)}, \dots., c_{i(k-1)})$ katsayılarının İngiliz alfabesine göre harf karşılıkları bulunarak şifreli metin oluşturulur. Burada

$c_{ij} \leq N - 1$ ise c_{ij} sayısına $\mathcal{A}$ İngiliz alfabesinden karşılık gelen L_j harfi yazılır.

$c_{ij} > N - 1$ olan c_{ij} sayısı tek ise bu sayı metne direkt yazılır.

$c_{ij} > N - 1$ olan c_{ij} sayısı birden fazla ise bu sayılardan basamak sayısı en uzun olan c_{ij} sayısının basamak sayısına diğer sayıların sol taraflarına 0 konularak basamak sayıları eşit uzunluğa getirilip T_i şifreli metni oluşturulur (Ancak c_{ij} sayısal değeri çift basamaklıysa aynen yazılır, bundan sonra kendinden sonra gelen c_{ij} değeri tek basamaklı olsa bile sol tarafına 0 konularak iki basamağa tamamlanır).

6. c_{ij} sayısal değerlerinin İngiliz alfabesine göre harf karşılıkları bulunarak, m_1, m_2,…, m_r bloklarına karşılık gelen $T_1 T_2 \dots . T_r$ şifreli metni oluşturulur.

7. $s = q - k + 2$ eşitliği kullanılarak s değeri hesaplanıp $(a_1, a_2, \dots, a_k, s)$ şifre anahtarı ve $T_1 T_2 \dots . T_r$ şifreli metni diğer kullanıcıya gönderilir.

4.2. Şifre Çözme Algoritması

1. $(a_1, a_2, \dots, a_k, s)$ anahtarı ve $T_1 T_2 \dots . T_r$ şifreli metni alınır.

2. Şifreleme metnini s uzunluğundaki bloklara bölünür ve (4.4) fark denklemi kullanılarak $d_k, d_{k+1}, \dots., d_q$ elemanları hesaplanır ve her bir bloğun

$(c_{iq}, c_{i(q-1)}, \ldots., c_{i(k-1)})$ katsayıları $n_i = d_q c_{iq} + d_{q-1} c_{i(q-1)} + d_{q-2} c_{i(q-2)} + \cdots + d_k c_{ik} + d_{k-1} c_{i(k-1)}$ denkleminde yerine konulur ($(c_{iq}, c_{i(q-1)}, \ldots., c_{i(k-1)})$ katsayılarını $T_1 T_2 \ldots. T_r$ şifreli metnini kullanarak elde ederiz).

3. $i \in \{1,2, \ldots, r\}$ olmak üzere n_i sayıları hesaplanıp, düz metin elde edilir (n_i sayılarına karşılık gelen $m_1, m_2, \ldots, m_r$ blokları bulunarak açık metne ulaşılır).

Aşağıdaki örnekte bu algoritmayı kullanarak şifreleme ve şifre çözme işlemleri yapalım.

Örnek 4.1. 26 harfli İngiliz alfabesi büyük karakterler ile ve *x* metinde boşluğu ifade etmek üzere

$$\mathcal{A} = \begin{Bmatrix} A & B & C & D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z & x \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 \end{Bmatrix}$$

alfabeyi etiketleyelim. Şifreleyeceğimiz metin olarak Flaut 2019'da örnek olarak verilen JOHN HAS A DOG metnini ele alalım.

JOHNxHASxAxDOG mesajını şifreleyelim.

k = 4 olarak kullanıcı tarafından belirlenir ise bloklar;

JOHN xHAS xAxD OGxx

olur. 1. bloğun sayısal değeri $n_1 = 9140713$, 2. bloğun sayısal değeri $n_2 = 26070018$, 3. bloğun sayısal değeri $n_3 = 26002603$, 4. bloğun sayısal değeri $n_4 = 140602626$ dir. Şifreleme işlemi aşağıdaki gibi yapılır.

I. Blok JOHN

1. $k = 4, a_1 = 18, a_2 = 10, a_3 = 13, a_4 = 3$ kullanıcı tarafından verilsin. Anahtar değerleri rastgele girilmiş olup aralarında bir örüntü bulunmamaktadır. Bu değerler bilindiği için aşağıdaki fark denkleminde değerleri yerine yazılarak $d_4, d_5, d_6, d_7, d_8, d_9$ değerleri bulunur.

2. $a_1, a_2, a_3 \; ve \; a_4$ değerleri (4.4) fark denkleminde yerine yazılarak

$$d_4 = a_1 = 18$$
$$d_5 = {a_1}^2 + a_2 = 18^2 + 10 = 334$$
$$d_6 = a_1 d_5 + a_2 d_4 + a_3 d_3 + a_4 d_2 = 6205$$
$$d_7 = a_1 d_6 + a_2 d_5 + a_3 d_4 + a_4 d_3 = 115267$$
$$d_8 = a_1 d_7 + a_2 d_6 + a_3 d_5 + a_4 d_4 = 2141252$$
$$d_9 = a_1 d_8 + a_2 d_7 + a_3 d_6 + a_4 d_5 = 39776873$$

$d_8 \leq n_1 = 9140713 < d_9$ olduğundan fark denkleminde iterasyon durdurulur.

3. $d_8 \leq n_1 = 9140713 < d_9$ olduğundan fark denkleminden d_8, d_7, d_6, d_5, d_4 sayıları belirlenir.

4. (4.4) fark denklemi kullanarak

$$n_1 = d_8c_{11} + d_7c_{12} + d_6c_{13} + d_5c_{14} + d_4c_{15} + d_3c_{16}$$

$c_{11}, c_{12}, c_{13}, c_{14}, c_{15}$ ve c_{16} katsayıları belirleyelim.

$n_1 = 9140713$ olduğundan

$n_1 = \mathbf{4} \,.\, d_8 + 575705$ (4'ün İngiliz alfabesindeki harf karşılığı E).

$575705 = \mathbf{4} \,.\, d_7 + 114637$ (4'ün alfabedeki harf karşılığı E).

$114637 = \mathbf{18} \,.\, d_6 + 2947$ (18'in İngiliz alfabesindeki harf karşılığı S harfi).

$2947 = \mathbf{8} \,.\, d_5 + 275$ (8'in İngiliz alfabesindeki harf karşılığı I harfidir).

$275 = \mathbf{15} \,.\, d_4 + 5$ (15'in İngiliz alfabesindeki harf karşılığı P harfidir).

$5 = \mathbf{5} \,.\, d_3$ (5'in İngiliz alfabesindeki harf karşılığı F dir).

5. $(c_{11}, c_{12}, c_{13}, c_{14}, c_{15}, c_{16})$ katsayılarının İngiliz alfabesine göre harf karşılıkları EESIPF dir.

Böylece verilen metnin 1. bloğu JOHN metni algoritmanın ilk 5 maddesinden EESIPF şifreli metni oluşturulur.

Şimdi verilen metnin kalan bloklarını algoritmanın ilk 5 maddesini uygulayarak benzer şekilde şifreleyelim.

II. Blok xHAS

1. $k = 4, a_1 = 18, a_2 = 10, a_3 = 13, a_4 = 3$ kullanıcı tarafından verildi.

2. $a_1,\ a_2, a_3\ ve\ a_4$ değerleri (4.4) fark denkleminde yerine yazılarak $d_3 = 1$, $d_4 = 18, d_5 = 334, d_6 = 6205, d_7 = 115267, d_8 = 2141252$ ve $d_9 = 39776873$

3. $d_8 \leq n_2 = 26070018 < d_9$ olduğundan fark denkleminden d_8, d_7, d_6, d_5, d_4 sayıları kullanılır.

4. (4.4) fark denklemi kullanarak

$$n_2 = d_8c_{21} + d_7c_{22} + d_6c_{23} + d_5c_{24} + d_4c_{25} + d_3c_{26}$$

$c_{21}, c_{22}, c_{23}, c_{24}, c_{25}$ ve c_{26} katsayıları belirleyelim.

$n_2 = 26070018$ olduğundan

$n_2 = \mathbf{12} \,.\, d_8 + 374994$

$374994 = \mathbf{3} \,.\, d_7 + 29193$

$29193 = \mathbf{4} \,.\, d_6 + 4373$

$4373 = \mathbf{13} \,.\, d_5 + 31$

$31 = \mathbf{1} \,.\, d_4 + 13$

$13 = \mathbf{13} \,.\, d_3$

5. $(c_{21}, c_{22}, c_{23}, c_{24}, c_{25}, c_{26})$ katsayılarının İngiliz alfabesine göre harf karşılıkları MDENBN şifreli metni elde edilir. Böylece verilen metnin 2. bloğu xHAS metni algoritmanın ilk 5 maddesinden MDENBN şifreli metni oluşturulur.

III. Blok xAxD

1. $k = 4, a_1 = 18, a_2 = 10, a_3 = 13, a_4 = 3$ kullanıcı tarafından verildi.

2. $a_1,\ a_2, a_3\ ve\ a_4$ değerleri (4.4) fark denkleminde yerine yazılarak $d_3 = 1$, $d_4 = 18, d_5 = 334, d_6 = 6205, d_7 = 115267$, $d_8 = 2141252$,$d_9 = 39776873$

3. $d_8 \leq n_3 = 26002603 < d_9$ olduğundan fark denkleminden d_8, d_7, d_6, d_5, d_4 sayıları kullanılır.

4. (4.4) fark denklemi kullanarak

$$n_3 = d_8c_{31} + d_7c_{32} + d_6c_{33} + d_5c_{34} + d_4c_{35} + d_3c_{36}$$

$c_{31}, c_{32}, c_{33}, c_{34}, c_{35}$ ve c_{36} katsayıları belirleyelim.

$n_3 = 26002603$ olduğundan

$n_3 = \mathbf{12} \,.\, d_8 + 307579$

$307579 = \mathbf{2} \,.\, d_7 + 77045$

$77045 = \mathbf{12} \,.\, d_6 + 2585$

$2585 = \mathbf{7} \,.\, d_5 + 247$

$247 = \mathbf{13} \,.\, d_4 + 13$

$13 = \mathbf{13} \,.\ d_3$

5. $(c_{31}, c_{32}, c_{33}, c_{34}, c_{35}, c_{36})$ katsayılarının İngiliz alfabesine göre harf karşılıkları MCMHNN şifreli metni elde edilir.

Böylece verilen metnin 3. bloğu xAxD metni algoritmanın ilk 5 maddesinden MCMHNN şifreli metni oluşturulur.

IV. Blok OGxx

1. $k = 4, a_1 = 18, a_2 = 10, a_3 = 13, a_4 = 3$ kullanıcı tarafından verildi.

2. $a_1,\ a_2, a_3\ ve\ a_4$ değerleri (4.4) fark denkleminde yerine yazılarak $d_3 = 1$, $d_4 = 18, d_5 = 334, d_6 = 6205, d_7 = 115267$, $d_8 = 2141252$,$d_9 = 39776873$

3. $d_8 \leq n_4 = 14062626 < d_9$ olduğundan fark denkleminden d_8, d_7, d_6, d_5, d_4 sayıları kullanılır.

4. (4.4) fark denklemi kullanarak

$$n_4 = d_8c_{41} + d_7c_{42} + d_6c_{43} + d_5c_{44} + d_4c_{45} + d_3c_{46}$$

$c_{41}, c_{42}, c_{43}, c_{44}, c_{45}$ ve c_{46} katsayıları belirleyelim.

$n_4 = 14062626$ olduğundan

$n_4 = \mathbf{6} \,.\, d_8 + 1215114$

$1215114 = \mathbf{10} \,.\, d_7 + 62444$

$62444 = \mathbf{10} \,.\, d_6 + 394$

$394 = \mathbf{1} \,.\, d_5 + 60$

$60 = \mathbf{3} \,.\, d_4 + 6$

$6 = \mathbf{6} \,.\, d_3$

5. $(c_{41}, c_{42}, c_{43}, c_{44}, c_{45}, c_{46})$ katsayılarının İngiliz alfabesine göre harf karşılıkları GKKBDG şifreli metni elde edilir.

Böylece verilen metnin 4. bloğu OGxx metni algoritmanın ilk 5 maddesinden GKKBDG şifreli metni oluşturulur. 4 bloktan elde edilen şifreli metinler kullanılarak algoritmanın 6. ve 7. maddelerinden şifreli metin elde edilir.

6. JOHN, xHAS, xAxD ve OGxx bloklarına karşılık gelen EESIPF, MDENBN, MCMHNN ve GKKBDG şifreli blokları elde edilir.

7. $(a_1, a_2, a_3, a_4, s) = (18, 10, 13, 3, 6)$ anahtarı ve

EESIPFMDENBNMCMHNNGKKBDG şifreli metni diğer kullanıcıya gönderilir.

Şifre Çözme: Şifre çözme için, anahtarı $(a_1, a_2, a_3, a_4, s) =$ (18, 10, 13, 3, 6) kullanıyoruz. $s = 6$ olduğundan şifreli metni 6 karakter uzunluğundaki EESIPF, MDENBN, MCMHNN, GKKBDG bloklarına bölelim.

Sonrasında fark denkleminde a_1, a_2, a_3 ve a_4 değerleri yerine yazılarak $d_4, d_5, d_6, d_7, d_8, d_9$ değerleri bulunur.

$$d_n = a_1d_{n-1} + a_2d_{n-2} + a_3d_{n-3} + a_4d_{n-4}$$

d_4 = 18, d_5 = 334, d_6 = 6205, d_7 = 115267, d_8 = 2141252, $d_9 = 39776873$ olarak hesapladık. Şimdi d_3, d_4, d_5, d_6, d_7, d_8 değerlerini ve EESIPF metnindeki harflerin İngiliz alfabesine göre sayı karşılıklarını kullanarak n_1 hesaplanır.

EESIPF bloğu için

n_1= 2141252× **4**+115267×**4**+6205×**18**+334×**8**+18×**15**+1×**5** = **9140713**

olur ve bu değerin İngiliz alfabesindeki harf karşılıkları bulunursa 9 sayısal değeri J harfine, 14 sayısal değeri O harfine, 07 sayısal değeri H harfine, 13 sayısal değeri N harfine karşılık gelir. Böylece EESIPF şifreli metninin karşılığı olarak JOHN metnini bulmuş oluruz. Benzer olarak 2., 3. ve 4. şifreli metinlerinin şifresi çözülürse bu metinlerin karşılıklarının sırasıyla xHAS, xAxD ve OGxx metinleri olduğu görülür. Sonuç olarak, JOHNxHASxAxDOG düz metnini elde ederiz.

Aşağıdaki örnekte, (Flaut, 2019) çalışmasında önerilen ve yukarıda açıklanan şifreleme algoritmasını kullanarak yeni bir metin şifreleyelim ve elde edilen şifreli metini çözelim.

Örnek 4.2. 'HANGİ EĞİTİM SİSTEMİ İÇİNDE OLURSA OLSUN, TEKNOLOJİ NE KADAR GELİŞİRSE GELİŞSİN, ÖĞRETMENİN ÖĞRENCİYLE GÖZ GÖZE GELDİĞİ BİR AN VARDIR. O AN ÖĞRETMEN, ÖĞRENCİNİN GÖNÜL KAPISINDAN GİREREK ZİHNİNE ULAŞIR' açık metnini blok uzunluğu olarak $k = 6$ seçerek şifreleyelim ve şifreyi çözelim. Türk alfabesi kullandığımız için $A, B, C, Ç \dots, Z$ alfabesinin sayısal değerleri sırasıyla $0, 1, 2, \dots, 28$ ve x boşluk karakterini göstermek üzere x in sayısal değeri 29 olsun.

$$\mathcal{A} = \begin{Bmatrix} A & B & C & Ç & D & E & F & G & Ğ & H & I & İ & J & K & L & M & N & O & Ö & P & R & S & Ş & T & U & Ü & V & Y & Z & x \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 \end{Bmatrix}$$

$k = 6$ olduğu için verilen metin her blokta 6 harf olmak üzere 33 bloğa ayrılır. Şifreleme işlemi aşağıdaki adımlar izlenerek yapılır. Aşağıda şifreleme algoritmasını bloklara uygularken elde edilen en büyük q değeri 14 olduğundan şifrelenmiş bütün blokların uzunlukları eşit olması için q değeri 14 den küçük olan bloklarda $c_{i(q+1)} = c_{i(q+2)} = \dots = c_{i14} = 0$ olarak alınarak algoritma uygulanmıştır.

I. Blok HANGİx

1. $k = 6, a_1 = 16, a_2 = 8, a_3 = 12, a_4 = 6, a_5 = 14, a_6 = 5$ kullanıcı tarafından verildi.

2. $a_1, a_2, a_3, a_4, a_5 \; ve \; a_6$ değerleri (4.4) fark denkleminde yerine konularak $d_6 = 16, d_7 = 264, d_8 = 4364, d_9 = 72134, d_{10} = 1192334, \; d_{11} = 19708597, d_{12} = 325771792, d_{13} = 5384820676, d_{14} = 89007972196, \; d_{15} = 14712506869$ sayıları elde edilir.

3. $d_{13} \leq n_1 = 9016071129 < d_{14}$ olduğundan fark denkleminden $d_{13}, d_{12}, d_{11}, d_{10}, d_9, d_8, d_7, d_6, d_5$ sayıları kullanılır.

4. (4.4) fark denklemini kullanarak

$$n_1 = d_{14}c_{11} + d_{13}c_{12} + d_{12}c_{13} + d_{11}c_{14} + d_{10}c_{15} + d_9c_{16} + d_8c_{17} + d_7c_{18} + d_6c_{19} + d_5c_{1,10}$$

$c_{11}, c_{12}, c_{13}, c_{14}, c_{15}, c_{16}, c_{17}, c_{18}, c_{19}$, ve $c_{1,10}$ katsayılarını belirleyelim.

$n_1 = 9016071129$ olduğundan

$$n_1 = \mathbf{0} \,.\, d_{14} + 9016071129$$
$$9016071129 = \mathbf{1} \,.\, d_{13} + 3631250453$$
$$3631250453 = \mathbf{11} \,.\, d_{12} + 47760741$$
$$47760741 = \mathbf{2} \,.\, d_{11} + 8343547$$
$$8343547 = \mathbf{6} \,.\, d_{10} + 1189543$$
$$1189543 = \mathbf{16} \,.\, d_9 + 35399$$
$$35399 = \mathbf{8} \,.\, d_8 + 487$$
$$487 = \mathbf{1} \,.\, d_7 + 223$$
$$223 = \mathbf{13} \,.\, d_6 + 15$$
$$15 = \mathbf{15} \,.\, d_5$$

5. $(c_{11}, c_{12}, c_{13}, c_{14}, c_{15}, c_{16}, c_{17}, c_{18}, c_{19}, c_{1,10})$ katsayılarının Türk alfabesine göre harf karşılıkları ABİCFNĞBKM şifreli metni elde edilir.

Böylece verilen metnin 1. bloğu HANGİx metni algoritmanın ilk 5 maddesinden ABİCFNĞBKM şifreli metni oluşturulur.

II. BLOK EĞİTİM

1. $k = 6\,, a_1 = 16\,, a_2 = 8\,, a_3 = 12, a_4 = 6\,, a_5 = 14\,, a_6 = 5$ kullanıcı tarafından verildi.

2. $a_1,\ a_2, a_3, a_4, a_5\ ve\ a_6$ değerleri (4.4) fark denkleminde yerine konularak $d_6 = 16, d_7 = 264, d_8 = 4364, d_9 = 72134, d_{10} = 1192334,\ d_{11} = 19708597, d_{12} = 325771792, d_{13} = 5384820676, d_{14} = 89007972196,\ d_{15} = 14712506869$ sayıları elde edilir.

3. $d_{13} \leq n_2 = 5811231115 < d_{14}$ olduğundan fark denkleminden $d_{13}, d_{12}, d_{11}, d_{10}, d_9, d_8, d_7, d_6, d_5$ sayıları kullanılır.

4. (4.4) fark denklemini kullanarak

$$n_2 = d_{14}c_{21} + d_{13}c_{22} + d_{12}c_{23} + d_{11}c_{24} + d_{10}c_{25} + d_9c_{26} + d_8c_{27} + d_7c_{28} + d_6c_{29} + d_5c_{2,10}$$

$c_{21}, c_{22}, c_{23}, c_{24}, c_{25}, c_{26}, c_{27}, c_{28}, c_{29}$, ve $c_{2,10}$ katsayılarını belirleyelim.

$n_2 = 5811231115$ olduğunda

$$n_2 = \mathbf{0} \,.\, d_{14} + 5811231115$$
$$5811231115 = \mathbf{1} \,.\, d_{13} + 3631250453$$

$3631250453 = \mathbf{1} \,.\, d_{12} + 47760741$

$47760741 = \mathbf{5} \,.\, d_{11} + 8343547$

$8343547 = \mathbf{1} \,.\, d_{10} + 1189543$

$1189543 \;\; = \mathbf{12} \,.\, d_{9} + 35399$

$35399 = \mathbf{8} \,.\, d_{8} + 487$

$487 = \mathbf{10} \,.\, d_{7} + 223$

$223 = \mathbf{10} \,.\, d_{6} + 15$

$15 = \mathbf{8} \,.\, d_{5}$

5. $(c_{21}, c_{22}, c_{23}, c_{24}, c_{25}, c_{26}, c_{27}, c_{28}, c_{29}, c_{2,10})$ katsayılarının Türk alfabesine göre harf karşılıkları ABBEBJĞIIĞ şifreli metni elde edilir.

Böylece verilen metnin 2. Bloğu EĞİTİM metni algoritmanın ilk 5 maddesinden ABBEBJĞIIĞ şifreli metni oluşturulur.

III. BLOK xSİSTE

1. $k = 6\,, a_1 = 16\,, a_2 = 8\,, a_3 = 12, a_4 = 6\,, a_5 = 14\,, a_6 = 5$ kullanıcı tarafından verildi.

2. $a_1,\ a_2, a_3, a_4, a_5\ ve\ a_6$ değerleri (4.4) fark denkleminde yerine konularak $d_6 = 16, d_7 = 264, d_8 = 4364, d_9 = 72134, d_{10} = 1192334,\ d_{11} = 19708597, d_{12} = 325771792, d_{13} = 5384820676, d_{14} = 89007972196,\ d_{15} = 14712506869$ sayıları elde edilir.

3. $d_{14} \leq n_3 = 292111212305 < d_{15}$ olduğundan fark denkleminden $d_{13}, d_{12}, d_{11}, d_{10}, d_9, d_8, d_7, d_6, d_5$ sayıları kullanılır.

4. (4.4) fark denklemini kullanarak

$$n_3 = d_{14}c_{31} + d_{13}c_{32} + d_{12}c_{33} + d_{11}c_{34} + d_{10}c_{35} + d_9c_{36} + d_8c_{37} + d_7c_{38} + d_6c_{39} + d_5c_{3,10}$$

$c_{31}, c_{32}, c_{33}, c_{34}, c_{35}, c_{36}, c_{37}, c_{38}, c_{39}$, ve $c_{3,10}$ katsayılarını belirleyelim.

$n_3 = 292111212305$ olduğundan

$n_3 = \mathbf{3} \,.\, d_{14} + 25087295717$

$25087295717 = \mathbf{4} \,.\, d_{13} + 3548013013$

$3548013013 = \mathbf{10} \,.\, d_{12} + 290295093$

$290295093 = \mathbf{14}.\, d_{11} + 14374735$

$14374735 = \mathbf{12} \,.\, d_{10} + 66727$

$66727 = \mathbf{15} \,.\, d_{8} + 1267$

$1267 = \mathbf{4} \,.\, d_{7} + 211$

$211 = \mathbf{13} \,.\, d_{6} + 3$

$3 = \mathbf{3} \,.\, d_5$

5. $(c_{31}, c_{32}, c_{33}, c_{34}, c_{35}, c_{36}, c_{37}, c_{38}, c_{39}, c_{3,10})$ katsayılarının Türk alfabesine göre harf karşılıkları ÇDILJAMDKÇ şifreli metni elde edilir.

Böylece verilen metnin 3. Bloğu xSİSTE metni algoritmanın ilk 5 maddesinden ÇDILJAMDKÇ şifreli metni oluşturulur.

IV. BLOK MİxİÇİ

1. $k = 6\,, a_1 = 16\,, a_2 = 8\,, a_3 = 12, a_4 = 6\,, a_5 = 14\,, a_6 = 5$ kullanıcı tarafından verildi.

2. $a_1,\ a_2, a_3, a_4, a_5\ ve\ a_6$ değerleri (4.4) fark denkleminde yerine konularak $d_6 = 16, d_7 = 264, d_8 = 4364, d_9 = 72134, d_{10} = 1192334,\ d_{11} = 19708597, d_{12} = 325771792, d_{13} = 5384820676, d_{14} = 89007972196,\ d_{15} = 14712506869$ sayıları elde edilir.

3. $d_{14} \leq n_4 = 151129110311 < d_{15}$ olduğundan fark denkleminden $d_{13}, d_{12}, d_{11}, d_{10}, d_9, d_8, d_7, d_6, d_5$ sayıları kullanılır.

4. (4.4) fark denklemini kullanarak

$$n_4 = d_{14}c_{41} + d_{13}c_{42} + d_{12}c_{43} + d_{11}c_{44} + d_{10}c_{45} + d_9c_{46} + d_8c_{47} + d_7c_{48} + d_6c_{49} + d_5c_{4,10}$$

$c_{41}, c_{42}, c_{43}, c_{44}, c_{45}, c_{46}, c_{47}, c_{48}, c_{49}$, ve $c_{4,10}$ katsayılarını belirleyelim.

$n_4 = 151129110311$ olduğundan

$n_4 = \mathbf{1} \,.\, d_{14} + 62121138115$

$62121138115 = \mathbf{11} \,.\, d_{13} + 2888110679$

$2888110679 = \mathbf{8} \,.\, d_{12} + 281936343$

$281936343 = \mathbf{14}.\, d_{11} + 6015985$

$6015985 = \mathbf{5} \,.\, d_{10} + 54315$

$54315 = \mathbf{12} \,.\, d_8 + 1947$

$1947 = \mathbf{7} \,.\, d_7 + 99$

$99 = \mathbf{6} \,.\, d_6 + 3$

$3 = \mathbf{3} \,.\, d_5$

5. $(c_{41}, c_{42}, c_{43}, c_{44}, c_{45}, c_{46}, c_{47}, c_{48}, c_{49}, c_{4,10})$ katsayılarının Türk alfabesine göre harf karşılıkları BİĞLEAJGFÇ şifreli metni elde edilir.

Böylece verilen metnin 4. Bloğu MİxİÇİ metni algoritmanın ilk 5 maddesinden BİĞLEAJGFÇ şifreli metni oluşturulur.

V. BLOK NDExOL

1. $k = 6\,, a_1 = 16\,, a_2 = 8\,, a_3 = 12, a_4 = 6\,, a_5 = 14\,, a_6 = 5$ kullanıcı tarafından verildi.

2. $a_1,\ a_2, a_3, a_4, a_5\ ve\ a_6$ değerleri (4.4) fark denkleminde yerine konularak $d_6 = 16, d_7 = 264, d_8 = 4364, d_9 = 72134, d_{10} = 1192334,\ d_{11} = 19708597, d_{12} = 325771792, d_{13} = 5384820676, d_{14} = 89007972196,\ d_{15} = 14712506869$ sayıları elde edilir.

3. $d_{14} \leq n_5 = 160405291714\ < d_{15}$ olduğundan fark denkleminden $d_{13}, d_{12}, d_{11}, d_{10}, d_9, d_8, d_7, d_6, d_5$ sayıları kullanılır.

4. (4.4) fark denklemini kullanarak

$$n_5 = d_{14}c_{51} + d_{13}c_{52} + d_{12}c_{53} + d_{11}c_{54} + d_{10}c_{55} + d_9c_{56} + d_8c_{57} + d_7c_{58} + d_6c_{59} + d_5c_{5,10}$$

$c_{51}, c_{52}, c_{53}, c_{54}, c_{55}, c_{56}, c_{57}, c_{58}, c_{59}$, ve $c_{5,10}$ katsayılarını belirleyelim.

$n_5 = 160405291714$ olduğundan

$$n_5 = \mathbf{1}\,.\,d_{14} + 71397319518$$
$$71397319518 = \mathbf{13}\,.\,d_{13} + 1394650730$$
$$1394650730 = \mathbf{4}\,.\,d_{12} + 91563562$$
$$91563562 = \mathbf{4}\,.\,d_{11} + 12729174$$
$$12729174 = \mathbf{10}\,.\,d_{10} + 805834$$
$$805834 = \mathbf{11}\,.\,d_9 + 12360$$
$$12360 = \mathbf{2}\,.\,d_8 + 3632$$
$$3632 = \mathbf{13}\,.\,d_7 + 200$$
$$200 = \mathbf{12}\,.\,d_6 + 8$$
$$8 = \mathbf{8}\,.\,d_5$$

5. ($c_{51}, c_{52}, c_{53}, c_{54}, c_{55}, c_{56}, c_{57}, c_{58}, c_{59}, c_{5,10}$) katsayılarının Türk alfabesine göre harf karşılıkları BKDDIİCKJĞ şifreli metni elde edilir.

Böylece verilen metnin 5. Bloğu NDExOL metni algoritmanın ilk 5 maddesinden BKDDIİCKJĞ şifreli metni oluşturulur.

VI. BLOK URSAxO

1. $k = 6\,, a_1 = 16\,, a_2 = 8\,, a_3 = 12, a_4 = 6\,, a_5 = 14\,, a_6 = 5$ kullanıcı tarafından verildi.

2. $a_1,\ a_2, a_3, a_4, a_5\ ve\ a_6$ değerleri (4.4) fark denkleminde yerine konularak $d_6 = 16, d_7 = 264, d_8 = 4364, d_9 = 72134, d_{10} = 1192334,\ d_{11} = 19708597, d_{12} =$

$325771792, d_{13} = 5384820676, d_{14} = 89007972196,\ d_{15} = 14712506869$ sayıları elde edilir.

3. $d_{14} \leq n_6 = 242021002917 < d_{15}$ olduğundan fark denkleminden $d_{13}, d_{12}, d_{11}, d_{10}, d_9, d_8, d_7, d_6, d_5$ sayıları kullanılır.

4. (4.4) fark denklemini kullanarak

$$n_6 = d_{14}c_{61} + d_{13}c_{62} + d_{12}c_{63} + d_{11}c_{64} + d_{10}c_{65} + d_9c_{66} + d_8c_{67} + d_7c_{68} + d_6c_{69} + d_5c_{6,10}$$

$c_{61}, c_{62}, c_{63}, c_{64}, c_{65}, c_{66}, c_{67}, c_{68}, c_{69}$, ve $c_{6,10}$ katsayılarını belirleyelim.

$n_6 = 242021002917$ olduğundan

$$n_6 = \mathbf{2} \,.\, d_{14} + 64005058525$$
$$64005058525 = \mathbf{11} \,.\, d_{13} + 4772031089$$
$$4772031089 = \mathbf{14} \,.\, d_{12} + 211226001$$
$$211226001 = \mathbf{10} \,.\, d_{11} + 14140031$$
$$14140031 = \mathbf{11} \,.\, d_{10} + 1024357$$
$$1024357 = \mathbf{14} \,.\, d_9 + 14481$$
$$14481 = \mathbf{3} \,.\, d_8 + 1389$$
$$1389 = \mathbf{5} \,.\, d_7 + 69$$
$$69 = \mathbf{4} \,.\, d_6 + 5$$
$$5 = \mathbf{5} \,.\, d_5$$

5. $(c_{61}, c_{62}, c_{63}, c_{64}, c_{65}, c_{66}, c_{67}, c_{68}, c_{69}, c_{6,10})$ katsayılarının Türk alfabesine göre harf karşılıkları CİLIİLÇEDE şifreli metni elde edilir.

Böylece verilen metnin 6. Bloğu URSAxO metni algoritmanın ilk 5 maddesinden CİLIİLÇEDE şifreli metni oluşturulur.

VII. BLOK LSUNxT

1. $k = 6\,, a_1 = 16\,, a_2 = 8\,, a_3 = 12, a_4 = 6\,, a_5 = 14\,, a_6 = 5$ kullanıcı tarafından verildi.

2. $a_1,\ a_2, a_3, a_4, a_5\ ve\ a_6$ değerleri (4.4) fark denkleminde yerine konularak $d_6 = 16, d_7 = 264, d_8 = 4364, d_9 = 72134, d_{10} = 1192334,\ d_{11} = 19708597, d_{12} = 325771792, d_{13} = 5384820676, d_{14} = 89007972196,\ d_{15} = 14712506869$ sayıları elde edilir.

3. $d_{14} \leq n_7 = 142124162923 < d_{15}$ olduğundan fark denkleminden $d_{13}, d_{12}, d_{11}, d_{10}, d_9, d_8, d_7, d_6, d_5$ sayıları kullanılır.

4. (4.4) fark denklemini kullanarak

$$n_7 = d_{14}c_{71} + d_{13}c_{72} + d_{12}c_{73} + d_{11}c_{74} + d_{10}c_{75} + d_9c_{76} + d_8c_{77} + d_7c_{78} + d_6c_{79} + d_5c_{7,10}$$

$c_{71}, c_{72}, c_{73}, c_{74}, c_{75}, c_{76}, c_{77}, c_{78}, c_{79}$, ve $c_{7,10}$ katsayılarını belirleyelim.

$n_7 = 142124162923$ olduğundan

$$n_7 = \mathbf{1} \,.\, d_{14} + 53116190727$$
$$53116190727 = \mathbf{9} \,.\, d_{13} + 4652804643$$
$$4652804643 = \mathbf{14} \,.\, d_{12} + 91999555$$
$$91999555 = \mathbf{4} \,.\, d_{11} + 13165167$$
$$13165167 = \mathbf{11} \,.\, d_{10} + 49493$$
$$49493 = \mathbf{11} \,.\, d_8 + 1489$$
$$1489 = \mathbf{5} \,.\, d_7 + 169$$
$$169 = \mathbf{10} \,.\, d_6 + 9$$
$$9 = \mathbf{9} \,.\, d_5$$

5. $(c_{71}, c_{72}, c_{73}, c_{74}, c_{75}, c_{76}, c_{77}, c_{78}, c_{79}, c_{7,10})$ katsayılarının Türk alfabesine göre harf karşılıkları BHLDİAİEIH şifreli metni elde edilir.

Böylece verilen metnin 7. Bloğu LSUNxT metni algoritmanın ilk 5 maddesinden BHLDİAİEIH şifreli metni oluşturulur.

VIII. BLOK EKNOLO

1. $k = 6\,, a_1 = 16\,, a_2 = 8\,, a_3 = 12, a_4 = 6\,, a_5 = 14\,, a_6 = 5$ kullanıcı tarafından verildi.

2. $a_1,\ a_2, a_3, a_4, a_5\ ve\ a_6$ değerleri (4.4) fark denkleminde yerine konularak $d_6 = 16, d_7 = 264, d_8 = 4364, d_9 = 72134, d_{10} = 1192334,\ d_{11} = 19708597, d_{12} = 325771792, d_{13} = 5384820676, d_{14} = 89007972196,\ d_{15} = 14712506869$ sayıları elde edilir.

3. $d_{13} \leq n_8 = 51316171417 < d_{14}$ olduğundan fark denkleminden $d_{13}, d_{12}, d_{11}, d_{10}, d_9, d_8, d_7, d_6, d_5$ sayıları kullanılır.

4. (4.4) fark denklemini kullanarak

$$n_8 = d_{14}c_{81} + d_{13}c_{82} + d_{12}c_{83} + d_{11}c_{84} + d_{10}c_{85} + d_9c_{86} + d_8c_{87} + d_7c_{88} + d_6c_{89} + d_5c_{8,10}$$

$c_{81}, c_{82}, c_{83}, c_{84}, c_{85}, c_{86}, c_{87}, c_{88}, c_{89}$, ve $c_{8,10}$ katsayılarını belirleyelim.

$n_8 = 51316171417$ olduğundan

$$n_8 = \mathbf{0} \,.\, d_{14} + 51316171417$$
$$51316171417 = \mathbf{9} \,.\, d_{13} + 2852785333$$
$$2852785333 = \mathbf{8} \,.\, d_{12} + 246610997$$
$$246610997 = \mathbf{12} \,.\, d_{11} + 10107833$$

$10107833 = \mathbf{8} \,.\, d_{10} + 569161$

$569161 = \mathbf{7} \,.\, d_9 + 64223$

$64223 = \mathbf{14} \,.\, d_8 + 3127$

$3127 = \mathbf{11} \,.\, d_7 + 223$

$223 = \mathbf{13} \,.\, d_6 + 15$

$15 = \mathbf{15} \,.\, d_5$

5. $(c_{81}, c_{82}, c_{83}, c_{84}, c_{85}, c_{86}, c_{87}, c_{88}, c_{89}, c_{8,10})$ katsayılarının Türk alfabesine göre harf karşılıkları AHĞJĞGLİKM şifreli metni elde edilir. Böylece verilen metnin 8. Bloğu EKNOLO metni algoritmanın ilk 5 maddesinden AHĞJĞGLİKM şifreli metni oluşturulur.

IX. BLOK JİXNEx

1. $k = 6\,, a_1 = 16\,, a_2 = 8\,, a_3 = 12, a_4 = 6\,, a_5 = 14\,, a_6 = 5$ kullanıcı tarafından verildi.

2. $a_1,\ a_2, a_3, a_4, a_5\ ve\ a_6$ değerleri (4.4) fark denkleminde yerine konularak $d_6 = 16, d_7 = 264, d_8 = 4364, d_9 = 72134, d_{10} = 1192334,\ d_{11} = 19708597, d_{12} = 325771792, d_{13} = 5384820676, d_{14} = 89007972196,\ d_{15} = 14712506869$ sayıları elde edilir.

3. $d_{14} \leq n_9 = 121129160529 < d_{15}$ olduğundan fark denkleminden $d_{13}, d_{12}, d_{11}, d_{10}, d_9, d_8, d_7, d_6, d_5$ sayıları kullanılır.

4. (4.4) fark denklemini kullanarak

$$n_9 = d_{14}c_{91} + d_{13}c_{92} + d_{12}c_{93} + d_{11}c_{94} + d_{10}c_{95} + d_9c_{96} + d_8c_{97} + d_7c_{98} + d_6c_{99} + d_5c_{9,10}$$

$c_{91}, c_{92}, c_{93}, c_{94}, c_{95}, c_{96}, c_{97}, c_{98}, c_{99}$, ve $c_{9,10}$ katsayılarını belirleyelim.

$n_9 = 121129160529$ olduğundan

$n_9 = \mathbf{1} \,.\, d_{14} + 32121188333$

$32121188333 = \mathbf{5} \,.\, d_{13} + 5197084953$

$5197084953 = \mathbf{15} \,.\, d_{12} + 310508073$

$310508073 = \mathbf{15} \,.\, d_{11} + 14879118$

$14879118 = \mathbf{12} \,.\, d_{10} + 571110$

$571110 = \mathbf{7} \,.\, d_9 + 66172$

$66172 = \mathbf{15} \,.\, d_8 + 712$

$712 = \mathbf{2}.\, d_7 + 184$

$184 = \mathbf{11} \,.\, d_6 + 8$

$8 = \mathbf{8}\ .\ d_5$

5. ($c_{91}, c_{92}, c_{93}, c_{94}, c_{95}, c_{96}, c_{97}, c_{98}, c_{99}, c_{9,10}$) katsayılarının Türk alfabesine göre harf karşılıkları BEMMJGMCİĞ şifreli metni elde edilir.

Böylece verilen metnin 7. Bloğu JİXNEx metni algoritmanın ilk 5 maddesinden BEMMJGMCİĞ şifreli metni oluşturulur.

X. BLOK KADARx

1. $k = 6\,, a_1 = 16\,, a_2 = 8\,, a_3 = 12, a_4 = 6\,, a_5 = 14\,, a_6 = 5$ kullanıcı tarafından verildi.

2. $a_1,\ a_2, a_3, a_4, a_5\ ve\ a_6$ değerleri (4.4) fark denkleminde yerine konularak $d_6 = 16, d_7 = 264, d_8 = 4364, d_9 = 72134, d_{10} = 1192334,\ d_{11} = 19708597, d_{12} = 325771792, d_{13} = 5384820676, d_{14} = 89007972196,\ d_{15} = 14712506869$ sayıları elde edilir.

3. $d_{14} \leq n_{10} = 130004002029 < d_{15}$ olduğundan fark denkleminden $d_{13}, d_{12}, d_{11}, d_{10},\ d_9, d_8, d_7, d_6, d_5$ sayıları kullanılır.

4. (4.4) fark denklemini kullanarak

$$n_{10} = d_{14}c_{10,1} + d_{13}c_{10,2} + d_{12}c_{10,3} + d_{11}c_{10,4} + d_{10}c_{10,5} + d_9c_{10,6} + d_8c_{10,7} + d_7c_{10,8} + d_6c_{10,9} + d_5c_{10,10}$$

$c_{10,1}, c_{102,}, c_{10,3}, c_{10,4}, c_{10,5}, c_{10,6}, c_{10,7}, c_{10,8}, c_{10,9}$, ve $c_{9,10}$ katsayılarını belirleyelim.

$n_{10} = 130004002029$ olduğundan

$n_{10} = \mathbf{1}\,.\,d_{14} + 40996029833$

$40996029833 = \mathbf{7}\,.\,d_{13} + 3302285101$

$3302285101 = \mathbf{10}\,.\,d_{12} + 44567181$

$44567181 = \mathbf{2}\,.\,d_{11} + 5149987$

$5149987 = \mathbf{4}\,.\,d_{10} + 380651$

$380651 = \mathbf{5}\,.\,d_9 + 19981$

$19981 = \mathbf{4}\,.\,d_8 + 2525$

$2525 = \mathbf{9}\,.\,d_7 + 149$

$149 = \mathbf{9}\,.\,d_6 + 5$

$5 = \mathbf{5}\,.\,d_5$

5. ($c_{10,1}, c_{102,}, c_{10,3}, c_{10,4}, c_{10,5}, c_{10,6}, c_{10,7}, c_{10,8}, c_{10,9}, c_{9,10}$) katsayılarının Türk alfabesine göre harf karşılıkları BGICDEDHHE şifreli metni elde edilir.

Böylece verilen metnin 7. Bloğu JİxNEx metni algoritmanın ilk 5 maddesinden BGICDEDHHE şifreli metni oluşturulur.

Kalan 23 blok da aynı şekilde şifrelenir ve sonuç olarak, verilen metnin bloklarına karşılık gelen ABİCFNĞBKM, ABBEBJĞIIĞ, ÇDILJAMDKÇ, BİĞLEAJGFÇ, BKDDIİCKJĞ, CİLIİLÇEDE, BHLDİAİEIH, AHĞJĞGLİKM, BEMMJGMCİĞ, BGICDEDHHE, ABFĞLDCGKİ, CDGKİDIEĞF, BHİÇFMADNG, ÇDHMLICJLJ, BİFNDEÇCDÇ, CAĞIAİJDAF, BDFIJIİLLK, CALJKDFMIC, AHKIHİDMHL, BDAKIHDIHA, CDIDGAĞĞIA, AAFCĞGCFIB, BMHHĞLBMKB, AMÇJNAEKLE, BKİNGÇİİFK, BKÇİEFÇHMFG, ÇDFICİMINC, ÇDĞFIĞLNDM, BCEIAFCFCÇ, AKÇGBJİFĞD, BĞCHHAIANE, BDÇDBHIHJC, AAFJMNFKMÇ şifreli metin blokları elde edilir. Bu bloklar birleştirilerek

"*ABİCFNĞBKMABBEBJĞIIGÇDILJAMDKÇBİĞLEAJGFÇBKDDIİCKJĞCİLI İLÇEDEBHLDİAİEIHAHĞJĞGLİKMBEMMİGMCİĞBGICDEDHHEABFĞLDCGKİC DGKİDIEĞFBHİÇFMADNGÇDHMLICJLJBİFNDEÇCDÇCAĞIAİJDAFBDFIJIİLLK CALJKDFMICAHKIHİDMHLBDAKIHDIHACDIDGAĞĞIAAAFCĞGCFIBBMHHĞL BMKBAMÇJNAEKLEBKİNGÇİİFKBKÇİEFÇHMGÇDFICİMINCÇDĞFIĞLNDMBCE IAFCFCÇAKÇGBJİFĞDBĞCHHAIANEBDÇDBHIHJCAAFJMNFKMÇ"* şifreli metnine ulaşılır.

Şifre çözme işlemi $(a_1, a_2, a_3, a_4, a_5, a_6, s) = (16, 8, 12, 6, 14, 5, 10)$ anahtarı kullanılarak aşağıdaki adımlar izlenerek yapılır. $s = 10$ olduğundan verilen şifreli metni 10 harf uzunluğundaki bloklara bölünür. Metini 10 uzunluğundaki bloklara bölerek, 33 blok elde edilir. İlk blok ABİCFNĞBKM olur.

ABİCFNĞBKM' deki harflerin Türk alfabesindeki sayı karşılıkları bulunur. A harfi 0' a, B harfi 1' e, İ harfi 11' e, C harfi 2' ye, F harfi 6' ya, N harfi 16' ya, Ğ HARFİ 8' e, B harfi1' e, K harfi 13' e ve M harfi 15' e karşılık gelir. Fark denkleminde $a_1,\ a_2, a_3, a_4, a_5$ ve a_6 değerleri yerine yazalım.

$$a_1 d_{n-1} + a_2 d_{n-2} + a_3 d_{n-3} + a_4 d_{n-4} + a_5 d_{n-5} + a_6 d_{n-6}$$

Denkleminden $d_6 = 16,\ d_7 = 264, d_8 = 4364, d_9 = 72134, d_{10} = 1192334,\ d_{11} = 19708821, d_{12} = 325775376,\ d_{13} = 5384879812, d_{14} = 89008971372$ elde edilir.

ABİCFNĞBKM için

n_1=89007972196 ×**0**+5384820676×**1**+325771792×**11**+19708597×**2**+11923 34×**6**+72134×**16**+4364 ×**8**+264 ×**1**+16 ×**13**+1 × **15** = 9016071129 olur.

$n_1 = 9016071129$ da bulunan değerlerin Türk alfabesindeki karşılıklarına baktığımızda, 9 sayısal değeri H harfine, 0 sayısal değeri A harfine, 16 sayısal değeri N harfine, 07 sayısal değeri G harfine, 11 sayısal değeri İ harfine, 29 sayısal değeri x' e karşılık gelir. Böylece HANGİx metnini elde ederiz.

ABBEBJĞIIĞ için

n_2=89007972196 ×**0**+5384820676×**1**+325771792×**1**+19708597×**5**+119233 4×**1**+72134×**12**+4364 ×8+264 ×**10** +16 ×**10**+1 × **8** = 5811231115 olur.

$n_2 = 5811231115$ de bulunan değerlerin Türk alfabesindeki karşılıklarına baktığımızda, 5 sayısal değeri E harfine, 8 sayısal değeri Ğ harfine, 11 sayısal değeri İ harfine, 23 sayısal değeri T harfine, 11 sayısal değeri İ harfine, 15 sayısal değeri M harfine karşılık gelir. Bu da EĞİTİM kelimesini alacağımız anlamına gelir.

ÇDILJAMDKÇ için

n_3=89007972196 ×**3**+5384820676×**4**+325771792×**10**+19708597×**14**+1192 334×**12** +72134×**0**+4364 ×**15**+264 ×**4**+16 ×**13**+1 × **3** = 292111212305 olur.

$n_3 = 292111212305$ de bulunan değerlerin Türk alfabesindeki karşılıklarına baktığımızda, 29 sayısal değeri x harfine, 21 sayısal değeri S harfine, 11 sayısal değeri İ harfine, 21 sayısal değeri S harfine, 23 sayısal değeri T harfine, 05 sayısal değeri E harfine karşılık gelir. Bu da xSİSTE kelimesini alacağımız anlamına gelir.

BİĞLEAJGFÇ için

n_4=89007972196 ×**1**+5384820676×**11**+325771792×**8**+19708597×**14**+1192 334×**5**+72134×**0**+4364 ×**12**+264 ×**7**+16 ×**6**+1 × **3** = 151129110311 olur.

$n_4 = 151129110311$ de bulunan değerlerin Türk alfabesindeki karşılıklarına baktığımızda, 15 sayısal değeri M harfine, 11 sayısal değeri İ harfine, 29 sayısal değeri x harfine, 11 sayısal değeri İ harfine, 03 sayısal değeri Ç harfine, 11 sayısal değeri İ harfine karşılık gelir. Bu da MİxİÇİ kelimesini alacağımız anlamına gelir.

BKDDIICKJĞ için

n_5=89007972196 ×**1**+5384820676×**13**+325771792×**4**+19708597×**4**+11923 34×**10**+72134× **10**+4364 ×**2**+264 ×**13**+16 ×**12**+1 × **8** = 160405291714 olur.

$n_5 = 160405291714$ de bulunan değerlerin Türk alfabesindeki karşılıklarına baktığımızda, 16 sayısal değeri N harfine, 04 sayısal değeri D harfine, 05 sayısal değeri

E harfine, 29 sayısal değeri x harfine, 17 sayısal değeri O harfine, 14 sayısal değeri L harfine karşılık gelir. Bu da NDExOL kelimesini alacağımız anlamına gelir.

CİLİİLÇEDE için

n_6=89007972196 ×**2**+5384820676×**11**+325771792× **14**+19708597×**10**+1192334×**11**+72134× **14**+4364×**3**+264×**5**+16×**4**+1 × **5** = 242021002917 olur.

$n_6 = 242021002917$ de bulunan değerlerin Türk alfabesindeki karşılıklarına baktığımızda, 24 sayısal değeri U harfine, 20 sayısal değeri R harfine, 21 sayısal değeri S harfine, 00 sayısal değeri A harfine, 29 sayısal değeri x harfine, 17 sayısal değeri O harfine karşılık gelir. Bu da URSAxO kelimesini alacağımız anlamına gelir.

BHLDİAİEIH için

n_7=89007972196 ×**1**+5384820676×**9**+325771792×**14**+19708597×**4**+1192334×**11**+72134×0+4364 ×**11**+264 ×**5**+16 ×**10**+1 × **9** = 142124162923 olur.

$n_7 = 142124162923$ de bulunan değerlerin Türk alfabesindeki karşılıklarına baktığımızda, 14 sayısal değeri L harfine, 21 sayısal değeri S harfine, 24 sayısal değeri U harfine, 16 sayısal değeri N harfine, 29 sayısal değeri x harfine, 23 sayısal değeri T harfine karşılık gelir. Bu da LSUNxT kelimesini alacağımız anlamına gelir.

AHĞJĞGLİKM için

n_8=89007972196 ×**0**+5384820676×**9**+325771792×**8**+19708597×**12**+1192334×**8**+72134× **7** +4364 ×**14**+264 ×**11**+16 ×**13**+1 × **15** = 51316171417 olur.

$n_8 = 51316171417$ de bulunan değerlerin Türk alfabesindeki karşılıklarına baktığımızda, 5 sayısal değeri E harfine, 13 sayısal değeri K harfine, 16 sayısal değeri N harfine, 17 sayısal değeri O harfine, 14 sayısal değeri L harfine, 17 sayısal değeri O harfine karşılık gelir. Bu da EKNOLO kelimesini alacağımız anlamına gelir.

BEMMJGMCİĞ için

n_9=89007972196 ×**1**+5384820676×**5**+325771792×**15**+19708597×**15**+1192334×**12**+72134× **7** +4364 ×**15**+264 ×**2**+16 ×**11**+1 × **8** = 121129161529 olur.

$n_9 = 121129161529$ da bulunan değerlerin Türk alfabesindeki karşılıklarına baktığımızda, 12 sayısal değeri J harfine, 11 sayısal değeri İ harfine, 29 sayısal değeri x harfine, 16 sayısal değeri N harfine, 05 sayısal değeri E harfine, 29 sayısal değeri x harfine karşılık gelir. Bu da JİxNEx kelimesini alacağımız anlamına gelir.

BGICDEDHHE için

n_{10}=89007972196 ×**1**+5384820676×**7**+325771792×**10**+19708597×**2**+1192334×**4**+72134× **5** +4364 ×**4**+264 ×**9**+16 ×9+1 × 5 = 130004002029 olur.

$n_{10} = 130004002029$ da bulunan değerlerin Türk alfabesindeki karşılıklarına baktığımızda, 13 sayısal değeri K harfine, 00 sayısal değeri A harfine, 04 sayısal değeri D harfine, 00 sayısal değeri A harfine, 20 sayısal değeri R harfine, 29 sayısal değeri x harfine karşılık gelir. Bu da KADARx kelimesini alacağımız anlamına gelir.

Diğer bloklarda da şifreli metni alınarak şifre çözme algoritması ile aynı şekilde çözülür ve açık metindeki bloklar elde edilir. Sonuç olarak,

“HANGİ EĞİTİM SİSTEMİ İÇİNDE OLURSA OLSUN, TEKNOLOJİ NE KADAR GELİŞİRSE GELİŞSİN, ÖĞRETMENİN ÖĞRENCİYLE GÖZ GÖZE GELDİĞİ BİR AN VARDIR. O AN ÖĞRETMEN, ÖĞRENCİNİN GÖNÜL KAPISINDAN GİREREK ZİHNİNE ULAŞIR” açık metnine ulaşmış oluruz.

5. ALGORİTMANIN GÜVENİRLİĞİ

Bu bölümde şifrelenmiş metnin güvenirliğini araştırmak için yapılan saldırı yöntemlerinden biri olan bilinen açık metin saldırısı anlatılmıştır. Sonrasında C. Flaut (2019) makalesinde verilen algoritmaya bilinen açık metin saldırısı yapılarak şifreleme algoritmasının kırılabildiği gösterilmiştir. Ayrıca diğer kriptanaliz yöntemleriyle de algoritmanın güvenliği anlatılmıştır.

Bilgilerin yapılan çeşitli saldırılara karşı güvenli bir şekilde korunması, yapılan saldırıların sürekli değiştiği ve geliştirildiği için her geçen gün daha da zorlaşmaktadır. Başkaları tarafından elde edilmesi istenmeyen bilgilerin güvenliğini sağlamak, dışardan gelebilecek saldırıları engellemek için yapılan kriptografi (şifreleme) güvenirliliği, bilgilerin 3. şahısların eline geçmemesi hususunda çok önemlidir.

Şifreleme bilimi; bankacılık işlemleri, cep telefonları, e-posta mesajları, savunma sanayi gibi daha birçok sistemde kullanılmaktadır. Kişilerin ve kurumların işlerini kolaylıkla yapabilmeleri için ihtiyaç duydukları faaliyetler elektronik ortama taşınmıştır. Bu her iki taraf için kolaylık sağlasa da gizli bilgilere kolay ulaşılması açısından bir tehdit oluşturmaktadır. Ayrıca kişi ve kurumların dışında kurumsal web sitelerine ve sayfalarına yetkisi olmayan kişilerin erişimi güvenliğini tehlikeye atmaktadır.

Şifreleme algoritmalarının hangi saldırı yöntemleri ile kırılabildiğinin bilinmesi, bu algoritmaların geliştirilmesi ve daha güvenilir hale getirilebilmesi için önemlidir.

Bu sebeplerden dolayı tez çalışmamızda Flaut, 2019'da verilen şifreleme algoritmasının güvenlik analizi yapılmıştır. Bu algoritma üzerinde bilinen açık metin saldırısı uygulanarak güvenirliği test edilmiştir. Harf frekans analizine karşı uygun bir metin olmadığından bu saldırı yöntemiyle incelenememiştir.

Biz bu çalışmamızda Flaut, 2019'da verilen şifreleme algoritmasının güvenirliğini test edebilmek için bilinen açık metin saldırısını kullandık. Bilinen Açık Metin Saldırısı belirli uzunluktaki açık metin ve kapalı metin çifti kullanılarak anahtarı bulma işlemidir. Bu saldırı yöntemini uygulamak için elimizde yeterli bilgiler mevcuttur. Şifresiz yani açık metin ve şifreli(kapalı) metinlere erişimimiz vardır. Bu metinleri kullanarak anahtarı bulup ve şifreyi elde ederiz.

Güvenlik analizleri için (Gülmüş, 2010), (Ceran, Kiraz, & Uzunkol, 2017) ve (Günden, 2010) kaynaklarından faydalanılmıştır.

5.1. Bilinen Açık Metin Saldırısı

Bilinen Açık Metin Atağı (Known Plaintext): Bir miktar açık-kapalı metin çifti bilinerek yapılan ataktır. Saldırı yapan kişi açık metin ve yapılan şifrelemeyle elde edilen kapalı metin çiftlerine sahiptir. Mesajların bir kısmı tahmin edilerek veya açık gönderilen mesajlar toplanarak atak uygulanabilir. Bu atakta az veri kullanarak anahtar bulunabilir. Bilinen açık metin atağının başarılı olması anahtarın doğru tahmin edilmesine bağlıdır.

Şifreli metnin bazı kısımları tahmin edilerek metin bölümlere ayrılır. Bu şekilde şifreli metin blokları çözümlenir. Şifreli metni oluşturmak için kullanılan anahtar (şifreleme işlemini gerçekleştirmek için kullanılan denklem, tablo, kelime vb.) belirlenerek de çözümleme yapılabilir.

Şimdi Örnek 4.2 de verilen açık metin ve bu metne karşılık gelen şifreli metin elimizde bulunsun. Bilinen Açık Metin saldırısı yaparak Örnek 4.2 de verilen şifreleme algoritmasının (Flaut, 2019) güvenirliğini test edelim. Burada, anahtar uzunluğu olan $k = 6$ ve $q = 14$ değerlerinin şifreleme algoritmasından bilindiği varsayılım Dolayısıyla $(a_1, a_2, a_3, a_4, a_5, a_6)$ anahtarını (katsayılarını) bulmaya çalışalım. Burada, $s = q - k + 2 = 14 - 6 + 2 = 10$ olduğundan bir 10 bilinmeyenli 10 denklem sistemi elde edilip, bu denklem sisteminin çözümü yardımıyla $(a_1, a_2, a_3, a_4, a_5, a_6)$ anahtarını (katsayılarını) bulalım.

Bu örnekteki sistemde 10 bilinmeyen olduğundan elde edilen katsayı matrisi 10 boyutlu karesel A matrisidir. Böylece verilen problem lineer cebirin klasik problemi olan $AX = B$ problemine dönüşür. Lineer cebirin klasik problemi olan $AX = B$ probleminin de $detA \neq 0$ olduğunda tek çözüm elde edileceği bilinmektedir. Dolayısıyla verilen problemimizde 10 bilinmeyen olduğundan tek çözüm elde etmek için 33 bloktan katsayı matrisinin determinantı sıfırdan farklı yapan 10 blok kullanmak Flaut, 2019'da verilen şifreleme algoritmasında kullanılan fark denkleminin katsayılarını bulmamız için yeterlidir. Bu katsayılar yardımıyla şifrelemede kullanılan $(a_1, a_2, a_3, a_4, a_5, a_6)$ anahtarını (katsayılarını) elde edilir. Bu anahtarı elde etmek için, 10 bloktan oluşan açık metin-kapalı metin çiftini kullanıyoruz.

İlk olarak açık metin-kapalı metin çiftini yazalım.

AÇIK METİN (ŞİFRESİZ METİN)	KAPALI METİN (ŞİFRELİ METİN)
HANGİ EĞİTİM SİSTEMİ İÇİNDE OLURSA OLSUN, TEKNOLOJİ NE KADAR GELİŞİRSE GELİŞSİN, ÖĞRETMENİN ÖĞRENCİYLE GÖZ GÖZE GELDİĞİ BİR AN VARDIR. O AN ÖĞRETMEN, ÖĞRENCİNİN GÖNÜL KAPISINDAN GİREREK ZİHNİNE ULAŞIR.	*ABİCFNĞBKMABBEBJĞIIGÇDILJAMDK ÇBİĞLEAJGFÇBKDDIİCKJĞCİLIİLÇED EBHLDİAİEIHAHĞJĞGLİKMBEMMİGM CİĞBGICDEDHHEABFĞLDCGKİCDGKİ DIEĞFBHİÇFMADNGÇDHMLICJLJBİF NDEÇCDÇCAĞIAİJDAFBDFIJIİLLKCAL JKDFMICAHKIHİDMHLBDAKIHDIHAC DIDGAĞĞIAAAFCĞGCFIBBMHHĞLBM KBAMÇJNAEKLEBKİNGÇİİFKBKÇİEFÇ HMGÇDFICİMINCÇDĞFIĞLNDMBCEIA FCFCÇAKÇGBJİFĞDBĞCHHAIANEBD ÇDBHIHJCAAFJMNFKMÇ*

İlk açık metinden HANGİx, EĞİTİM, xSİSTE, MİxİÇİ, NDExOL, URSAxO, LSUNxT, EKNOLO, JİxNEx, KADARx 10 bloğunu ele alalım. Bu bloklara karşılık gelen Türk alfabesindeki sayısal değerler

$$n_1 = 9016071129,$$
$$n_2 = 5811231115,$$
$$n_3 = 292111212305,$$
$$n_4 = 151129110311\,,$$
$$n_5 = 160405291714\,,$$
$$n_6 = 242021002917,$$
$$n_7 = 142124162923,$$
$$n_8 = 51316171417,$$
$$n_9 = 121129161529\,,$$
$$n_{10} = 130004002029$$

dir.

Bu blokların şifrelenmiş hali, ABİCFNĞBKM, ABBEBJĞIIĞ, ÇDILJAMDKÇ, BİĞLEAJGFÇ, BKDDIİCKJĞ, CİLIİLÇEDE, BHLDİAİEIH, AHĞJĞGLİKM, BEMMİGMCİĞ, BGICDEDHHE dir ve bu bloklardaki harflerin Türk alfabesine göre sayısal karşılıkları,

$$\text{ABİCFNĞBKM} \rightarrow \begin{pmatrix} 0, & 1\,, & 11\,, & 2\,, & 6\,, & 16\,, & 8\,, & 1, & 13\,, & 15 \\ A & B & \text{İ} & C & F & N & \text{Ğ} & B & K & M \end{pmatrix}$$

$$\text{ABBEBJĞIIĞ} \rightarrow \begin{pmatrix} 0, & 1\,, & 1\,, & 5\,, & 1\,, & 12\,, & 8\,, & 10, & 10\,, & 8 \\ A & B & B & E & B & J & \text{Ğ} & I & I & \text{Ğ} \end{pmatrix}$$

$$\text{ÇDILJAMDKÇ} \rightarrow \begin{pmatrix} 3, & 4, & 10, & 14, & 12, & 0, & 15, & 4, & 13, & 3 \\ \text{Ç} & D & I & L & J & A & M & D & K & \text{Ç} \end{pmatrix}$$

$$\text{BİĞLEAJGFÇ} \rightarrow \begin{pmatrix} 1, & 11, & 8, & 14, & 5, & 0, & 12, & 7, & 6, & 3 \\ B & \text{İ} & \text{Ğ} & L & E & A & J & G & F & \text{Ç} \end{pmatrix}$$

$$\text{BKDDIİCKJĞ} \rightarrow \begin{pmatrix} 1, & 13, & 4, & 4, & 10, & 11, & 2, & 13, & 12, & 8 \\ B & K & D & D & I & \text{İ} & C & K & J & \text{Ğ} \end{pmatrix}$$

$$\text{CİLIİLÇEDE} \rightarrow \begin{pmatrix} 2, & 11, & 14, & 10, & 11, & 14, & 3, & 5, & 4, & 5 \\ C & \text{İ} & L & I & \text{İ} & L & \text{Ç} & E & D & E \end{pmatrix}$$

$$\text{BHLDİAİEIH} \rightarrow \begin{pmatrix} 1, & 9, & 14, & 4, & 11, & 0, & 11, & 5, & 10, & 9 \\ B & H & L & D & \text{İ} & A & \text{İ} & E & I & H \end{pmatrix}$$

$$\text{AHĞJĞGLİKM} \rightarrow \begin{pmatrix} 0, & 9, & 8, & 12, & 8, & 7, & 14, & 11, & 13, & 15 \\ A & H & \text{Ğ} & J & \text{Ğ} & G & L & \text{İ} & K & M \end{pmatrix}$$

$$\text{BEMMJGMCİĞ} \rightarrow \begin{pmatrix} 1, & 5, & 15, & 15, & 12, & 7, & 15, & 2, & 11, & 8 \\ B & E & M & M & J & G & M & C & \text{İ} & \text{Ğ} \end{pmatrix}$$

$$\text{BGICDEDHHE} \rightarrow \begin{pmatrix} 1, & 7, & 10, & 2, & 4, & 5, & 4, & 9, & 9, & 5 \\ B & G & I & C & D & E & D & H & H & E \end{pmatrix}$$

olarak bulunur. Açık metin-kapalı metin çifti arasındaki bağlantıyı kullanarak şifrelemede kullanılan anahtarı ortaya çıkarmaya çalışalım. Bölüm 4.1 de verilen şifreleme algoritmasına göre ilk 10 bloktaki açık metin-kapalı metin çifti arasındaki bağıntıdan 10 bilinmeyenli 10 denklem sistemi aşağıdaki gibi oluşturulur.

$$\begin{aligned}
&d_{14}c_{11} + d_{13}c_{12} + d_{12}c_{13} + d_{11}c_{14} + d_{10}c_{15} + d_9c_{16} + d_8c_{17} + d_7c_{18} + d_6c_{19} + d_5c_{1,10} = n_1 \\
&d_{14}c_{21} + d_{13}c_{22} + d_{12}c_{23} + d_{11}c_{24} + d_{10}c_{25} + d_9c_{26} + d_8c_{27} + d_7c_{28} + d_6c_{29} + d_5c_{2,10} = n_2 \\
&d_{14}c_{31} + d_{13}c_{32} + d_{12}c_{33} + d_{11}c_{34} + d_{10}c_{35} + d_9c_{36} + d_8c_{37} + d_7c_{38} + d_6c_{39} + d_5c_{3,10} = n_3 \\
&d_{14}c_{41} + d_{13}c_{42} + d_{12}c_{43} + d_{11}c_{44} + d_{10}c_{45} + d_9c_{46} + d_8c_{47} + d_7c_{48} + d_6c_{49} + d_5c_{4,10} = n_4 \\
&d_{14}c_{51} + d_{13}c_{52} + d_{12}c_{53} + d_{11}c_{54} + d_{10}c_{55} + d_9c_{56} + d_8c_{57} + d_7c_{58} + d_6c_{59} + d_5c_{5,10} = n_5 \\
&d_{14}c_{61} + d_{13}c_{62} + d_{12}c_{63} + d_{11}c_{64} + d_{10}c_{65} + d_9c_{66} + d_8c_{67} + d_7c_{68} + d_6c_{69} + d_5c_{6,10} = n_6 \\
&d_{14}c_{71} + d_{13}c_{72} + d_{12}c_{73} + d_{11}c_{74} + d_{10}c_{75} + d_9c_{76} + d_8c_{77} + d_7c_{78} + d_6c_{79} + d_5c_{7,10} = n_7 \\
&d_{14}c_{81} + d_{13}c_{82} + d_{12}c_{83} + d_{11}c_{84} + d_{10}c_{85} + d_9c_{86} + d_8c_{87} + d_7c_{88} + d_6c_{89} + d_5c_{8,10} = n_8 \\
&d_{14}c_{91} + d_{13}c_{92} + d_{12}c_{93} + d_{11}c_{94} + d_{10}c_{95} + d_9c_{96} + d_8c_{97} + d_7c_{98} + d_6c_{99} + d_5c_{9,10} = n_9 \\
&d_{14}c_{10,1} + d_{13}c_{10,2} + d_{12}c_{10,3} + d_{11}c_{10,4} + d_{10}c_{10,5} + d_9c_{10,6} + d_8c_{10,7} + d_7c_{10,8} + d_6c_{10,9} + d_5c_{10,10} = n_{10}
\end{aligned} \tag{5.1}$$

Bu lineer denklem sistemi

$$\begin{pmatrix} c_{11} & c_{12} & c_{13} & c_{14} & c_{15} & c_{16} & c_{17} & c_{18} & c_{19} & c_{1,10} \\ c_{21} & c_{22} & c_{23} & c_{24} & c_{25} & c_{26} & c_{27} & c_{28} & c_{29} & c_{2,10} \\ c_{31} & c_{32} & c_{33} & c_{34} & c_{35} & c_{36} & c_{37} & c_{38} & c_{39} & c_{3,10} \\ c_{41} & c_{42} & c_{43} & c_{44} & c_{45} & c_{46} & c_{47} & c_{48} & c_{49} & c_{4,10} \\ c_{51} & c_{52} & c_{53} & c_{54} & c_{55} & c_{56} & c_{57} & c_{58} & c_{59} & c_{5,10} \\ c_{61} & c_{62} & c_{63} & c_{64} & c_{65} & c_{66} & c_{67} & c_{68} & c_{69} & c_{6,10} \\ c_{71} & c_{72} & c_{73} & c_{74} & c_{75} & c_{76} & c_{77} & c_{78} & c_{79} & c_{7,10} \\ c_{81} & c_{82} & c_{83} & c_{84} & c_{85} & c_{86} & c_{87} & c_{88} & c_{89} & c_{8,10} \\ c_{91} & c_{92} & c_{93} & c_{94} & c_{95} & c_{96} & c_{97} & c_{98} & c_{99} & c_{9,10} \\ c_{10,1} & c_{10,2} & c_{10,3} & c_{10,4} & c_{10,5} & c_{10,6} & c_{10,7} & c_{10,8} & c_{10,9} & c_{10,10} \end{pmatrix} \cdot \begin{pmatrix} d_{14} \\ d_{13} \\ d_{12} \\ d_{11} \\ d_{10} \\ d_9 \\ d_8 \\ d_7 \\ d_6 \\ d_5 \end{pmatrix} = \begin{pmatrix} n_1 \\ n_2 \\ n_3 \\ n_4 \\ n_5 \\ n_6 \\ n_7 \\ n_8 \\ n_9 \\ n_{10} \end{pmatrix}$$

şeklinde yazılabilir. Bu matris gösterimi kısaca $A \cdot X = B$ şeklinde gösterilir öyle ki A $(10 \times 10 \text{ matris})$ matrisine (5.1) lineer denklem sisteminin katsayılar matrisi, B $(10 \times 1 \text{ matris})$ matrisine sütun matrisi denir. A katsayılar matrisine B sütun matrisinin eklenmesiyle elde edilen

$$\left(\begin{array}{cccccccccc|c} c_{11} & c_{12} & c_{13} & c_{14} & c_{15} & c_{16} & c_{17} & c_{18} & c_{19} & c_{1,10} & n_1 \\ c_{21} & c_{22} & c_{23} & c_{24} & c_{25} & c_{26} & c_{27} & c_{28} & c_{29} & c_{2,10} & n_2 \\ c_{31} & c_{32} & c_{33} & c_{34} & c_{35} & c_{36} & c_{37} & c_{38} & c_{39} & c_{3,10} & n_3 \\ c_{41} & c_{42} & c_{43} & c_{44} & c_{45} & c_{46} & c_{47} & c_{48} & c_{49} & c_{4,10} & n_4 \\ c_{51} & c_{52} & c_{53} & c_{54} & c_{55} & c_{56} & c_{57} & c_{58} & c_{59} & c_{5,10} & n_5 \\ c_{61} & c_{62} & c_{63} & c_{64} & c_{65} & c_{66} & c_{67} & c_{68} & c_{69} & c_{6,10} & n_6 \\ c_{71} & c_{72} & c_{73} & c_{74} & c_{75} & c_{76} & c_{77} & c_{78} & c_{79} & c_{7,10} & n_7 \\ c_{81} & c_{82} & c_{83} & c_{84} & c_{85} & c_{86} & c_{87} & c_{88} & c_{89} & c_{8,10} & n_8 \\ c_{91} & c_{92} & c_{93} & c_{94} & c_{95} & c_{96} & c_{97} & c_{98} & c_{99} & c_{9,10} & n_9 \\ c_{10,1} & c_{10,2} & c_{10,3} & c_{10,4} & c_{10,5} & c_{10,6} & c_{10,7} & c_{10,8} & c_{10,9} & c_{10,10} & n_{10} \end{array}\right)$$

matrise (5.1) lineer denklem sisteminin ilaveli matrisi denir ve $[A:B]$ şeklinde gösterilir. Açık metin ve kapalı metin çifti elimizde olduğun için yukarıdaki $AX = B$ lineer sisteminde kapalı metinden A katsayılar matrisini, açık metinden B vektörünü ve çözüm olarak d_5, d_6, …, d_{14} bilinmeyenlerinden oluşan X vektörü aşağıdaki gibi yazılabilir.

$$0d_{14} + d_{13} + 11d_{12} + 2d_{11} + 6d_{10} + 16d_9 + 8d_8 + d_7 + 13d_6 + 15d_5 = 9016071129$$
$$0d_{14} + d_{13} + d_{12} + 5d_{11} + d_{10} + 12d_9 + 8d_8 + 10d_7 + 10d_6 + 8d_5 = 5811231115$$
$$3d_{14} + 4d_{13} + 10d_{12} + 14d_{11} + 12d_{10} + 0d_9 + 15d_8 + 4d_7 + 13d_6 + 3d_5 = 292111212305$$
$$d_{14} + 11d_{13} + 8d_{12} + 14d_{11} + 5d_{10} + 0d_9 + 12d_8 + 7d_7 + 6d_6 + 3d_5 = 151129110311$$
$$d_{14} + 13d_{13} + 4d_{12} + 4d_{11} + 10d_{10} + 11d_9 + 2d_8 + 13d_7 + 12d_6 + 8d_5 = 160405291714$$
$$d_{14} + 11d_{13} + 14d_{12} + 10d_{11} + 11d_{10} + 14d_9 + 3d_8 + 5d_7 + 4d_6 + 5d_5 = 242021002917$$
$$d_{14} + 9d_{13} + 14d_{12} + 4d_{11} + 11d_{10} + 0d_9 + 11d_8 + 5d_7 + 10d_6 + 9d_5 = 142124162923$$
$$d_{14} + 9d_{13} + 8d_{12} + 12d_{11} + 8d_{10} + 7d_9 + 14d_8 + 11d_7 + 13d_6 + 15d_5 = 51316171417$$
$$d_{14} + 5d_{13} + 15d_{12} + 15d_{11} + 12d_{10} + 7d_9 + 15d_8 + 2d_7 + 11d_6 + 8d_5 = 121129160529$$
$$d_{14} + 7d_{13} + 10d_{12} + 2d_{11} + 4d_{10} + 5d_9 + 4d_8 + 9d_7 + 9d_6 + 5d_5 = 130004002029$$

$$\begin{pmatrix} 0 & 1 & 11 & 2 & 6 & 16 & 8 & 1 & 13 & 15 \\ 0 & 1 & 1 & 5 & 1 & 12 & 8 & 10 & 10 & 8 \\ 3 & 4 & 10 & 14 & 12 & 0 & 15 & 4 & 13 & 3 \\ 1 & 11 & 8 & 14 & 5 & 0 & 12 & 7 & 6 & 3 \\ 1 & 13 & 4 & 4 & 10 & 11 & 2 & 13 & 12 & 8 \\ 2 & 11 & 14 & 10 & 11 & 14 & 3 & 5 & 4 & 5 \\ 1 & 9 & 14 & 4 & 11 & 0 & 11 & 5 & 10 & 9 \\ 0 & 9 & 8 & 12 & 8 & 7 & 14 & 11 & 13 & 15 \\ 1 & 5 & 15 & 15 & 12 & 7 & 15 & 2 & 11 & 8 \\ 1 & 7 & 10 & 2 & 4 & 5 & 4 & 9 & 9 & 5 \end{pmatrix} \cdot \begin{pmatrix} d_{14} \\ d_{13} \\ d_{12} \\ d_{11} \\ d_{10} \\ d_9 \\ d_8 \\ d_7 \\ d_6 \\ d_5 \end{pmatrix} = \begin{pmatrix} 9016071129 \\ 5811231115 \\ 292111212305 \\ 151129110311 \\ 160405291714 \\ 242021002917 \\ 142124162923 \\ 51316171417 \\ 121129160529 \\ 130004002029 \end{pmatrix}$$

$AX = B$ lineer sisteminin çözümünü incelemek için gerekli tanım ve teoremleri verelim. Aşağıdaki tanım ve teoremler için (Kolman & Hill, 2011) kitabından faydalanılmıştır.

Tanım 5.1. $m \times n$ tipinde bir matris

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

olsun. $\mathbb{R}^m$' nin vektörleri olarak gözönüne alınan A matrisinin satırlarının germiş olduğu $\mathbb{R}^n$ 'nin alt uzayına A matrisinin satır uzayı denir. Benzer şekilde, $\mathbb{R}^m$' in vektörleri olarak göz önüne alınan A matrisinin sütunlarının germiş olduğu $\mathbb{R}^m$' in alt uzayına A matrisinin sütun uzayı denir.

Tanım 5.2. A matrisinin satır (sütun) uzayının boyutuna A' nın satır (sütun) rankı denir.

Teorem 5.1. $AX = B$ lineer sisteminin bir çözüme sahip olması için gerek ve yeter şart katsayılar ve ilaveli katsayılar matrislerinin ranklarının eşit olmasıdır.

Tanım 5.3. A $m \times n$ tipinde bir matris olsun. Aşağıdaki özellikler sağlanıyor ise A' ya satırca indirgenmiş eşolon şekilde bir matristir denir.

(a) A'nın bütün elemanları 0 olan satırları varsa bunlar matrisin en alt satırlarındandır.

(b) Sıfırdan farklı bir satırın soldan itibaren sıfırdan farklı ilk elemanı 1' dir. Bu elemana bu satırın bir ilk 1' i (pivot) denir.

(c) Sıfırdan farklı her bir satır için, ilk 1, önceki satırların herhangi ilk 1' lerinin sağında ve altında yer alır.

(d) Bir sütun bir ilk 1 içeriyorsa bu sütundaki diğer bütün elemanlar sıfırdır.

Tanım 5.4. Aşağıda verilen işlemlerin herhangi birine bir A matrisi üzerinde elementer satır (sütun) işlemi denir.

(a) Herhangi iki satırı (sütunu) yer değiştirmesi

(b) Bir satırı (sütunu) sıfırdan farklı bir sayı ile çarpılması

(c) Bir satırın (sütunun) bir katını diğer bir satıra (sütuna) eklenmesi

Bu tanım ve teoremlerden faydalanarak denklem sisteminin çözümünü elde edelim.

$$\text{rank}\begin{pmatrix} 0 & 1 & 11 & 2 & 6 & 16 & 8 & 1 & 13 & 15 \\ 0 & 1 & 1 & 5 & 1 & 12 & 8 & 10 & 10 & 8 \\ 3 & 4 & 10 & 14 & 12 & 0 & 15 & 4 & 13 & 3 \\ 1 & 11 & 8 & 14 & 5 & 0 & 12 & 7 & 6 & 3 \\ 1 & 13 & 4 & 4 & 10 & 11 & 2 & 13 & 12 & 8 \\ 2 & 11 & 14 & 10 & 11 & 14 & 3 & 5 & 4 & 5 \\ 1 & 9 & 14 & 4 & 11 & 0 & 11 & 5 & 10 & 9 \\ 0 & 9 & 8 & 12 & 8 & 7 & 14 & 11 & 13 & 15 \\ 1 & 5 & 15 & 15 & 12 & 7 & 15 & 2 & 11 & 8 \\ 1 & 7 & 10 & 2 & 4 & 5 & 4 & 9 & 9 & 5 \end{pmatrix}=10$$

A matrisinin satır (sütun) uzayının boyutu, $rankA = 10$' dur. Dolayısıyla $detA \neq 0$ olduğu için sistem tutarlıdır ve tek çözümü vardır. Denklem sisteminin çözümünde; Gauss-Jordan Eliminasyon Yöntemi, Cramer Kuralı, Ters Matris Yöntemi ve Montante Yöntemi kullanılarak bilgisayar ile çözüm yapılmıştır. Aşağıda verilen sistemin Gauss-Jordan eliminasyon yöntemi çözümü verilmiştir.

$$\begin{pmatrix} 0 & 1 & 11 & 2 & 6 & 16 & 8 & 1 & 13 & 15 & 9016071129 \\ 0 & 1 & 1 & 5 & 1 & 12 & 8 & 10 & 10 & 8 & 5811231115 \\ 3 & 4 & 10 & 14 & 12 & 0 & 15 & 4 & 13 & 3 & 292111212305 \\ 1 & 11 & 8 & 14 & 5 & 0 & 12 & 7 & 6 & 3 & 151129110311 \\ 1 & 13 & 4 & 4 & 10 & 11 & 2 & 13 & 12 & 8 & 160405291714 \\ 2 & 11 & 14 & 10 & 11 & 14 & 3 & 5 & 4 & 5 & 242021002917 \\ 1 & 9 & 14 & 4 & 11 & 0 & 11 & 5 & 10 & 9 & 142124162923 \\ 0 & 9 & 8 & 12 & 8 & 7 & 14 & 11 & 13 & 15 & 51316171417 \\ 1 & 5 & 15 & 15 & 12 & 7 & 15 & 2 & 11 & 8 & 121129160529 \\ 1 & 7 & 10 & 2 & 4 & 5 & 4 & 9 & 9 & 5 & 130004002029 \end{pmatrix}$$

Şimdi yukarıda verilen ilaveli matrisi indirgenmiş eşolon formda bir matrise dönüştürmek için, elementer satır işlemlerini kullanalım. Bu denklem sistemimizi Gauss-Jordan yöntemiyle çözerken öncelikle 1. Satırın ilk elemanını pivot yapmak için 1. Satır ile 3. Satır yer değiştirilir. Sonra 1. Satırın ilk elemanı pivot yapılır.

$$\begin{pmatrix} 1 & 4/3 & 10/3 & 14/3 & 4 & 0 & 5 & 4/3 & 13/3 & 1 & 292111212305/3 \\ 0 & 1 & 1 & 5 & 1 & 12 & 8 & 10 & 10 & 8 & 5811231115 \\ 0 & 1 & 11 & 2 & 6 & 16 & 8 & 1 & 13 & 15 & 9016071129 \\ 1 & 11 & 8 & 14 & 5 & 0 & 12 & 7 & 6 & 3 & 151129110311 \\ 1 & 13 & 4 & 4 & 10 & 11 & 2 & 13 & 12 & 8 & 160405291714 \\ 2 & 11 & 14 & 10 & 11 & 14 & 3 & 5 & 4 & 5 & 242021002917 \\ 1 & 9 & 14 & 4 & 11 & 0 & 11 & 5 & 10 & 9 & 142124162923 \\ 0 & 9 & 8 & 12 & 8 & 7 & 14 & 11 & 13 & 15 & 51316171417 \\ 1 & 5 & 15 & 15 & 12 & 7 & 15 & 2 & 11 & 8 & 121129160529 \\ 1 & 7 & 10 & 2 & 4 & 5 & 4 & 9 & 9 & 5 & 130004002029 \end{pmatrix}$$

Bundan sonra 1.satır -1 ile çarpılarak 4, 5, 7, 9 ve 10. Satırlara, 1.satır -2 ile çarpılarak 6.satıra eklenir ve pivotun bulunduğu sütundaki sayılar 0 yapılır. 2. Satırda pivot olduğu için 3. Satıra geçilir ve 11 sayısı 1/11 ile çarpılarak pivot yapılır ve yine aynı şekilde devam edilerek pivotun olduğu sütundaki diğer sayılar 0 yapılmaya çalışılır. Diğer satırlar da aynı şekilde pivot bulup, sütunları 0 yapılarak matrisimiz indirgenmiş eşolon formuna dönüştürülür,

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 89007972196 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5384820676 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 325771792 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 19708597 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1192334 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 72134 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 4364 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 264 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 16 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

ve çözüm aşağıdaki gibi elde edilir.

$$\begin{pmatrix} d_{14}=89007972196 \\ d_{13}=5384820676 \\ d_{12}=325771792 \\ d_{11}=19708597 \\ d_{10}=1192334 \\ d_{9}=72134 \\ d_{8}=4364 \\ d_{7}=264 \\ d_{6}=16 \\ d_{5}=1 \end{pmatrix}$$

Elde edilen çözüm d_n dizisinin terimleridir. Bu da $n, k \in \mathbb{N}, k \geq 2, n \geq k$ için (4.4) de verilen fark denklemini kullanarak; $a_1 , a_2 , \dots , a_6$ doğal sayılarını bulmamızı sağlar. (4.4) fark denkleminde $d_0 = d_1 = \cdots = d_4 = 0, d_5 = 1, a_6 \neq 0$ başlangıç şartları bilindiğinden,

$$d_6 = a_1 d_5 + a_2 d_4 + a_3 d_3 + a_4 d_2 + a_5 d_1 + a_6 d_0$$

olur ve

$$16 = a_1\ 1 + a_2\ 0 + a_3\ 0 + a_4\ 0 + a_5\ 0 + a_6\ 0$$

olduğundan $a_1 = 16$' dır.

$$d_7 = a_1 d_6 + a_2 d_5 + a_3 d_4 + a_4 d_3 + a_5 d_2 + a_6 d_1$$

$$264 = 16\ 16 + a_2\ 1 + a_3\ 0 + a_4\ 0 + a_5\ 0 + a_6\ 0$$

olduğundan $a_2 = 8$

$$d_8 = a_1 d_7 + a_2 d_6 + a_3 d_5 + a_4 d_4 + a_5 d_3 + a_6 d_2$$

$$4364 = 16\ 264 + 8\ 16 + a_3\ 1 + a_4\ 0 + a_5\ 0 + a_6\ 0$$

olduğundan $a_3 = 12$

$$d_9 = a_1 d_8 + a_2 d_7 + a_3 d_6 + a_4 d_5 + a_5 d_4 + a_6 d_3$$

$$72134 = 16\ 4364 + 8\ 264 + a_3\ 16 + a_4\ 1 + a_5\ 0 + a_6\ 0$$

olduğundan $a_4 = 6$

$$d_{10} = a_1 d_9 + a_2 d_8 + a_3 d_7 + a_4 d_6 + a_5 d_5 + a_6 d_4$$

$$1192334 = 16\ 72134 + 8\ 4364 + a_3\ 264 + a_4\ 16 + a_5\ 1 + a_6\ 0$$

olduğundan $a_5 = 14$

$$d_{11} = a_1 d_{10} + a_2 d_9 + a_3 d_8 + a_4 d_7 + a_5 d_6 + a_6 d_5$$

$$19708597 = 16\ 1192334 + 8\ 72134 + a_3\ 4364 + a_4\ 264 + a_5\ 16 + a_6\ 1$$

olduğundan $a_6 = 5$ olur.

10 bloktan oluşan açık metin-kapalı metin çiftini kullanarak bu şifreleme sisteminin $(a_1, a_2, \dots, a_6) = (16, 8, 12, 6, 14, 5)$ anahtarını elde edilir yani şifreleme sistemini kırmış olunur. Dolayısıyla bu şifreleme sistemi bilinen açık metin saldırısına karşı güvensiz olduğu gösterilmiş olur.

Son olarak, diğer kriptanaliz tekniklerinden seçilmiş açık metin, seçilmiş şifreli metin, sadece şifreli metin ve harf frekans analizi yöntemlerinin (Flaut, 2019) tarafından önerilen algoritma üzerinde uygulanabilirliğini inceleyelim.

Seçilmiş Açık Metin Saldırısı. Bu saldırı yönteminde saldırganın rastgele seçilen açık metinlerin şifreli metinlerine ulaşabildiği varsayılmaktadır. Diğer bir ifadeyle, saldırganın kapalı kutu şifreleme cihazına sahip olduğu varsayılmaktadır. Dolayısıyla seçilen açık metinlere karşılık gelen şifreli metinler elde edilebildiği için saldırgan istediği açık metin-kapalı metin çiftine sahiptir. Yukarıda açıklanan bilinen açık metin saldırısında olduğu gibi açık metin – kapalı metin çifti kullanılarak şifrelemede kullanılan anahtar bulunabilir. Diğer bir ifadeyle, (Flaut, 2019) tarafından önerilen şifreleme

algoritması bilinen açık metin saldırısına karşı güvensiz olduğu için seçilmiş açık metin saldırısına karşı da güvensizdir.

Seçilmiş Şifreli Metin Saldırısı. Bu saldırı yönteminde saldırganın istediği şifreli metinlere karşılık gelen açık metinlere erişebildiği varsayılmaktadır. Daha açık bir ifadeyle, saldırgan kapalı kutu şifre çözme cihazı ile istediği şifreli metinleri çözme (anahtarı görmeden/bilmeden) ve açık metinleri elde etme yetkisine sahiptir. Seçilmiş açık metin saldırısında olduğu gibi saldırgan istediği şifreli metnin çözülmüş haline ulaşabileceğinden açık metin – kapalı metin çiftine sahip olabilecektir. Dolayısıyla, saldırgan yukarıda açıklanan bilinen açık metin saldırısında olduğu gibi açık metin – kapalı metin çiftini kullanarak şifrelemede kullanılan anahtarı ele geçirebilir. Diğer bir ifadeyle, (Flaut, 2019) tarafından önerilen şifreleme algoritması bilinen açık metin saldırısına karşı güvensiz olduğu için seçilmiş şifreli metin saldırısına karşı da güvensizdir.

Sadece Şifreli Metin Saldırısı. Bu saldırı yönteminde saldırgan sadece şifreli metine erişebilir. Saldırganın açık metne erişimi yoktur. Sadece şifreli metin saldırısı en zor saldırı yöntemidir çünkü saldırganın elinde sadece şifreli metin olduğu için şifreli metinden anahtar (gerekli güvenlik kriterlerini sağlayan anahtar) hakkında bilgi edinmesi neredeyse imkansızdır. (Flaut, 2019) tarafından önerilen şifreleme algoritmasında kullanılan anahtar gerekli güvenlik kriterlerini sağladığı için sadece şifreli metin kullanılarak bu anahtarın çok zordur. Diğer bir ifadeyle, bu algoritmanın sadece şifreli metin saldırısına karşı güvenli olduğu söylenebilir.

Harf Frekans Analizi. (Flaut, 2019) da önerilen şifreleme algoritması ile şifrelenmiş olan açık metindeki farklı konumlarda bulunan aynı harf şifreli metinde çoğunlukla farklı harf olarak şifrelenmektedir. Diğer bir ifade ile, bu algoritma Poly-Alphabetic (Çok Harfli) bir şifreleme yöntemi sunmaktadır. Örnek 4.2 de verilen örneğimize de bakıldığında harf frekans dağılımının korunmadığı görülmektedir. Dolayısıyla, (Flaut, 2019) tarafından önerilen bu algoritma harf frekans analizine karşı güvenlidir.

6. ARAŞTIRMA SONUÇLARI VE TARTIŞMA

Bu bölümde tez çalışmasında elde edilen sonuçlar tartışılmıştır.

Bu tezde C. Flaut tarafından (Flaut, 2019) makalesinde önerilen şifreleme algoritması ayrıntılı bir şekilde ele alınarak fark denklemi üzerinde bu algoritmanın nasıl tasarlandığı ve çalıştığı incelenmiştir. Bu algoritmanın şifreleme ve şifre çözme adımları anlatılmış ve algoritmaya Türk alfabesinin kullanımı uyarlanmıştır. Türk alfabesi kullanılarak yeni bir örnek (Örnek 4.2) verilmiştir ve bu örnekte yeni bir açık metin bu algoritma ile şifrelenmiştir. Fark denklemi üzerinde tasarlanan bu algoritma ile şifreli metni elde etmek için Bölüm Kalan Teoremi (Quotient Remainder Theorem) kullanılmış ve elde edilen değerlerin Türk alfabesinde hangi harfe karşılık geldiği bulunarak şifreli metin oluşturulmuştur. Daha sonra, bu örnek üzerinde bilinen açık metin saldırısı kullanılarak algoritmanın güvenliği test edilmiş ve sonuç olarak algoritmanın bu saldırıya karşı güvensiz olduğu gözlemlenmiştir. Verilen örnekte kullanılan gizli anahtarın elde edilebilmesi için algoritmanın dayandığı fark denkleminin 10 tane teriminin bilinmesi gerektiği için 10 tane bloğun (açık metin – kapalı metin çiftleri) kullanılması yeterli olmuştur. Diğer bir ifadeyle, 10 bilinmeyenli 10 denklemden oluşan lineer denklem sistemi oluşturulmuştur. Bu denklem sisteminin tek çözümü olduğu gösterilmiştir ve bu sistem Gauss eliminasyon yöntemi ile çözülerek fark denkleminin terimleri olan d_q değerleri elde edilmiştir. d_q değerleri fark denkleminde yerlerine yazılarak şifrelemede kullanılan gizli anahtar olan $a_1, a_2, \ldots, a_k$ değerleri elde edilmiştir. Böylece, (Flaut, 2019) çalışmasında fark denklemi üzerinde tasarlanan şifreleme algoritması bilinen açık metin saldırısı ile kırılmıştır.

7. SONUÇLAR VE ÖNERİLER

7.1. Sonuçlar

Bu çalışmada şifreleme bilimine ve klasik şifreleme yöntemlerine yer verildikten sonra (Flaut, 2019) çalışmasında önerilen şifreleme algoritması ele alınmıştır. Bu şifreleme algoritması ayrıntılı çalışılmış ve "Bilinen Açık Metin Saldırısı" na karşı güvenliği incelenmiştir. Bilinen açık metin saldırısı yöntemiyle yeterli sayıda açık metin - kapalı metin çifti kullanılarak şifrelemede kullanılan gizli anahtar ortaya çıkartılmıştır. Bu saldırı yönteminde, ele aldığımız örnekte (Örmek 4.2) açık metin ve kapalı metin çiftleri kullanılarak lineer denklem sistemi oluşturulmuş ve bu sistem Gauss eliminasyon yöntemiyle çözülerek şifrelemede kullanılan gizli anahtar ortaya çıkarılmıştır. Böylece, (Flaut, 2019) çalışmasında fark denklemleri kullanılarak tasarlanan şifreleme algoritmasının gizli anahtarı bilinen açık metin saldırısıyla ele geçirilmiştir ve algoritmanın bilinen açık metin saldırısına karşı güvensiz olduğu gösterilmiştir.

7.2. Öneriler

Bu tez çalışmasının devamında fark denkleminin parametreleri üzerinde değişiklikler yapılarak daha güvenilir ve verimli çalışan şifreleme algoritması elde edilmeye çalışılabilir. Diğer taraftan, bu şifreleme algoritmasına uygulanan "Bilinen Açık Metin Saldırısı" nın adımları ve çözümleri MAPLE veya başka bir programlama dilinde çalıştırılarak uygulanabilirliği gösterilebilir.

8. KAYNAKLAR

Akın Ö., Bulgak H., (1998), Lineer Fark Denklemleri ve Kararlılık Teorisi, Selçuk Üniversitesi Uygulamalı Matematik Araştırma Merkezi Yayınları No.2, Konya.

Arslan, G., (2009), Kriptoloji Kavramları ve Kripto Analiz Merkezi, Sunum, TÜBİTAK UEKAE.

Beşkirli, A., Özdemir, D. & Beşkirli, M., (2019), Şifreleme Yöntemleri ve RSA Algoritması Üzerine Bir İnceleme, European Journal of Science and Technology, (Special Issue), 284-291.

Ceran, E., Kiraz M.S. & Uzunkol, O., (2017), RSA Sifreleme Sistemlerinin Kleptografik Arka Kapıları için Güvenlik ve Karmaşıklık Analizi, Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 21 (2), 631-643.

Coşkun, A. ve Ülker, Ü., (2013), Ulusal Bilgi Güvenliğine Yönelik Bir Kriptografi Algoritması Geliştirilmesi ve Harf Frekans Analizine Karşı Güvenirlik Tespiti, Bilişim Teknolojileri Dergisi, Cilt:6, Sayı:2.

Çeşmeci, Ü., (2009), Kriptoloji Tarihi, UEKAE Dergisi, 1, 21-29.

Çetin, F., 2021, Kriptografide Kullanılan Asal Sayı Test Yöntemleri Üzerine Bir Çalışma, Yüksek Lisans Tezi, Necmettin Erbakan Üniversitesi Fen Bilimleri Enstitüsü, Konya.

Çimen, C., Akleylek, S., Akyıldız, E., (2007), Şifrelerin Matematiği: Kriptografi, *Orta Doğu Teknik Üniversitesi*, 1. Baskı, ODTÜ Geliştirme Vakfı Yayıncılık, 5-49.

Elaydi, S. N., (2005), An İntroduction to Difference Equations, Springer, New York.

Flaut, C., (2019), Some Application of Difference Equations in Cryptography and Coding Theory, Journal of Difference Equations and Applications, 25(7): 905 – 920.

Gülmüş, M., 2010, Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği, Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Günden, Ü., 2010, Şifreleme Algoritmalarının Performans Analizi, Yüksek Lisans Tezi, Sakarya Üniversitesi Fen Bilimleri Enstitüsü, Sakarya.

Hill, L.S., (1929), Cryptography in an Algebraic Alphabet, The American Mathematical Monthly, Vol.36, No. 6, 306-312.

Kapoor K., Nanda S., Gundla R., (2019), A Comphrehensive Study on Known Plaintext Attack, Chosen Plaintext Attack and Ciphertext Only Attack, Vol.7, No.2, ISSN 2393-9028.

Karaahmetoğlu, O., 2010, Gizli Anahtarlı Kriptosistemlerin Tasarımında Cebirsel Yapıların Önemi ve Kriptanaliz, Doktora Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne.

Koblitz N., (1994), A Course in Number Theory and Cryptography, 2nd Edition, Springer Verlag, New York.

Kodaz, H. ve Botsalı, F. M., (2010), Simetrik ve Asimetrik Şifreleme Algoritmalarının Karşılaştırılması, Selcuk University Journal of Engineering Sciences, 9(1), 10-23.

Kolman B., Hıll D. R., (2011), Uygulamalı Lineer Cebir, (Çev. Ömer Akın), Ankara: Palme Yayıncılık, 86-270.

Külen, F., 2013, Kriptolojide Bazı Şifreleme Yöntemlerinde Cebirsel Yaklaşımlar, Yüksek Lisans Tezi, Gaziosmanpaşa Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı, Tokat.

Menezes, A. & Van Oorschot, P., (1997), Handbook of Applied Cryptography, CRC Press,
169-185.

Nasibov, S., 2015, Kriptoloji Sistemleri ve Uygulamaları Üzerine, Yüksek Lisans Tezi, Ege Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı, İzmir.

Obaid, Z., 2016, Kriptoloji Yöntemlerinin Karşılaştırılması, Yüksek Lisans Tezi, Erciyes Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı, Kayseri.

Obaid, Z., Arkan, S., & Akay, B. (2016). Klasik Kriptoloji Yöntemlerinin Karşılaştırılması, Engineering Sciences, 11(4), 100-108.

Paar, C. & Pelzl, J., (2009), Understanding Cryptography, A Textbook for Students and Practitioners, Springer–Verlag.

Sadkhan D.B, (2011), Methods of Cryptanalysis, Security of Networks, 1-10.

Sakallı, M.T., 2006, Modern Şifreleme Yöntemlerinin Gücünün İncelenmesi, Doktora Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne.

Schneier, B., Applied Cryptography, (1996), Second Edition: Protocols, Algorthms, and Source Code in C (cloth), John Wiley & Sons Inc.

Stinson, D. & Paterson, M. (2019), Cryptography Theory and Practice, Textbooks in Mathematics, Fourth Edition, Crc Press.

Şahin, F., (1976), Modern Blok Şifreleme Algoritmaları, İstanbul Aydın Üniversitesi Dergisi (İAÜD), Sayı 17, 47 - 60.

Topaloğlu, N., Calp, M., & Türk, B., (2016), Bilgi Güvenliği Kapsamında Yeni Bir Veri Şifreleme Algoritması Tasarımı ve Gerçekleştirilmesi, Bilişim Teknolojileri Dergisi, Cilt 9, Sayı 3.

Tuncay, G., 2015, Kriptografik ve Uygulama Özellikleri İyi Olan İkili Matrislerin Üretilmesi İçin Yeni Bir Arama Yöntemi, Yüksek Lisans Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü Hesaplamalı Bilimler Anabilim Dalı, Edirne.

Ülker, Ü., 2014, Klasik Teknikler Kullanılarak Bir Kriptografi Algoritması Geliştirilmesi ve Des Algoritması ile Performans Analizlerinin Karşılaştırılması, Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara.

Vural, Y. ve Sağıroğlu, Ş., (2008), Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme, Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 23(2), 507-522.

Yerlikaya, T., Buluş, E., & Buluş, N., (2006), Kripto Algoritmalarının Gelişimi ve Önemi, Trakya Üniversitesi Bilgisayar Bölümü, Edirne.

Yerlikaya, T., ve Aslanyürek, C., (2019), RSA Algoritmasının Şifreleme Hızını Arttıran Algoritmalar ve Performansları, DÜMF Mühendislik Dergisi 10:3, 853-862.

Yeşilbaş, E., 2016, Cebirsel Kriptoloji Yöntemleri ve Bazı Uygulamaları, Yüksek Lisans Tezi, Recep Tayyip Erdoğan Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı, Rize.

(URL-1), 2022, https://ssd.eff.org/tr/module/%C5%9Fifreleme-nedir (3 Şubat 222)

(URL-2), 2022, https://bilimgenc.tubitak.gov.tr/makale/kriptografi-bilginin-anahtari (5 Şubat 2022)

(URL-3), 2022, tr.wikipedia.org/wiki/Sezar şifrelemesi (8 Şubat 2022)

(URL-4), 2022, science.ankara.edu.tr (15 Şubat 2022)

(URL-5), 2022, https://stringfixer.com/tr/Adaptive_chosen_plaintext_attack (9 Mart 2022)

(URL-6), 2022, https://www.iienstitu.com/blog/enigma-nedir (5 Mayıs, 2022)

(URL-7), 2022, https://www.bilgile.com/nedir/89-enigma-nedir.html (5 Mayıs, 2022)