T.C.
PAMUKKALE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

REKÜRANS BAĞINTILARI YARDIMIYLA ŞİFRELEME ALGORİTMASI

YÜKSEK LİSANS TEZİ

SEREL MADAK

DENİZLİ, KASIM - 2022

T.C.
PAMUKKALE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

REKÜRANS BAĞINTILARI YARDIMIYLA ŞİFRELEME ALGORİTMASI

YÜKSEK LİSANS TEZİ

SEREL MADAK

DENİZLİ, KASIM - 2022

Bu tezin tasarımı, hazırlanması, yürütülmesi, araştırmalarının yapılması ve bulgularının analizlerinde bilimsel etiğe ve akademik kurallara özenle riayet edildiğini; bu çalışmanın doğrudan birincil ürünü olmayan bulguların, verilerin ve materyallerin bilimsel etiğe uygun olarak kaynak gösterildiğini ve alıntı yapılan çalışmalara atfedildiğine beyan ederim.

SEREL MADAK

ÖZET

REKÜRANS BAĞINTILARI YARDIMIYLA ŞİFRELEME ALGORİTMASI
YÜKSEK LİSANS TEZİ
SEREL MADAK
PAMUKKALE ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

(TEZ DANIŞMANI: DOÇ. DR. CANAN CELEP YÜCEL)

DENİZLİ, KASIM - 2022

İnsanlığın varlığından bu yana bilgi güvenliği oldukça önem taşır. Şifreleme algoritmaları da bilgi güvenliğinin geliştirilmesine yardımcı olmak açısından önemlidir. Günümüzde gelişen teknolojiyle bu güvenliği sağlamak daha da güçleşmiştir. Bu tezde eski çağlardan bu yana kullanılmış olan bazı önemli şifreleme yöntemlerinden ayrıntılı olarak bahsedilmiştir. Bunun yanı sıra Fibonacci Q-matrisi kullanılarak elde edilmiş olan şifreleme algoritması da detaylı olarak incelenmiştir. İncelenen bu algoritmada, karşı tarafa iletilmek istenen mesaj matrisi 2×2 lik alt matrislere bölünerek şifrelenmiştir. Bu tezde ise karşı tarafa iletilen mesaj matrislerini sadece 2×2 lik alt matrislerle sınırlı bırakmayıp n×n tipindeki alt matrislere ayırarak yeni bir şifreleme algoritması oluşturulmuştur. Aynı zamanda incelenmiş olan şifreleme algoritmasından esinlenilerek özel sayı dizilerinden birçok yeni şifreleme algoritması geliştirilmiştir. Bunlardan biri Pell sayıları ile oluşturulan Q-matrisidir. Bu matris yardımıyla yeni bir şifreleme algoritması bulunmuştur. Son olarak rekürans bağıntısı yardımıyla yeni bir Q-matrisi üretilip daha genel bir algoritma tanımlanmıştır. Bu yöntemler örneklerle desteklenmiştir.

ANAHTAR KELİMELER: Fibonacci Sayıları, Kodlama/Kod Çözme Algoritması, Fibonacci Q-matrisi, Pell sayıları, Rekürans bağıntısı

ABSTRACT

AN ENCRYPTION ALGORITHM WITH THE HELP OF RECURRENCE RELATIONS
MSC THESIS
SEREL MADAK
PAMUKKALE UNIVERSITY INSTITUTE OF SCIENCE MATHEMATICS

(SUPERVISOR: ASSOC. PROF. DR. CANAN CELEP YÜCEL)

DENİZLİ, NOVEMBER 2022

Information security is extremely important since the beginning of human existence. Encryption algorithms are also important to help improving information security. Today, with the developing technology, it has become even more difficult to provide this security. In this thesis, some important encryption methods that have been used since ancient times are mentioned in detail. In addition to this, the encryption algorithm obtained using the Fibonacci Q-matrix has also been examined in detail. In this algorithm, the encryption was accomplished by dividing the message matrix to be delivered to the receiving party into 2×2 submatrices. In the new encryption algorithm created in this thesis, this restriction is removed, and the encryption is accomplished by dividing the message matrices to be delivered to the receiving party into n×n submatrices. At the same time, inspired by the encryption algorithm studied, many new encryption algorithms are developed using special sequences of numbers. One of them is the Q-matrix created with Pell numbers. With the help of this matrix, a new encryption algorithm is found. Finally, with the help of recurrence relation, a new Q-matrix is generated, and a more general algorithm is defined. These methods are supported by examples.

KEYWORDS: Fibonacci Numbers, Coding/Decoding Algorithm, Fibonacci Q-matrix, Pell numbers, Recurrence relation

İÇİNDEKİLER

Sayfa

ŞEKİL LİSTESİ

Sayfa

TABLO LİSTESİ

Sayfa

ÖNSÖZ

Öncelikle çalışma sürecimdeki zorlu yolda sonsuz ışığıyla yolumu aydınlatan, zaman ve mekânın önemi olmadığını her an yanımda olmasıyla hissettiren, bilgileri ve birikimiyle tek idolüm, öğrencisi olmaktan gurur ve onur duyduğum değerli danışman hocam Doç. Dr. Canan CELEP YÜCEL' e sonsuz teşekkürlerimi borç bilirim. Ayrıca bu süreçte her daim yanımda olup bilgisiyle bana destek olan sayın hocam Prof. Dr. Mustafa AŞÇI' ya sonsuz teşekkür ederim.

Tüm hayatım boyunca her türlü desteğiyle arkamda olan canım babam Mahmut MADAK' a ve fedakarlığı ile hiçbir zaman hakkını ödeyemeyeceğim annem Rabia MADAK' a ve biricik teyzem Ayten ASLAN' a sonsuz teşekkür ederim.

1. GİRİŞ

Bilgi, yazının icadından günümüze kadar her zaman çok kıymetli olmuştur. İnsanlar yazının icadından sonra yazıyla haberleşmeye başlamışlardır. Bu süreçte insanların karşı koyamadığı merakı nedeniyle gizli bilgiyi saklamak güçleşmiştir. Böylece gönderilen mesajları gizleme yöntemleri gerekli hale gelmiştir. Bu yöntemler bilgi güvenliğini sağlamış, üretilen verilerin izinsiz veya yetkisiz bir biçimde ele geçirilerek kullanımını engellemiş, değiştirilmesini ve ifşa edilmesini önlemiştir. Teknolojinin gelişmesiyle bilgi güvenliği gün geçtikçe daha çok önemli hale gelmiştir. Kullandığımız bilgisayarların gücünün ve kapasitesinin artmasıyla birlikte bilgiler hızlı bir şekilde şifrelenerek daha güvenilir bir hale gelmiştir. Fakat şifreleme hızı artarken deşifre edilme hızı da yükselmiştir. Bu noktada Kriptoloji biliminin önemi artmıştır. Kriptoloji kısaca şifreleme bilimidir. Günümüze kadar şifreleme yöntemleri üzerine birçok çalışmalar yapılmış ve yapılmaya devam etmektedir (Afacan, 2016). Kriptoloji için bir matematik bilimi denilebilir. Genelde sayılar teorisi üzerine kuruludur. Kriptoloji kendi içerisinde kriptografi ve kriptoanaliz olmak üzere iki farklı bölüme ayrılır. Kriptografi bilginin istenmeyen kişiler tarafından okunamayacak hale getirilmesi için kullanılan matematiksel tekniklerdir. İlk kriptografik belge, yaklaşık olarak M.Ö. 1900 yılında yazıldığı tahmin edilen Rosetta tabletidir. Teknoloji hızla geliştikçe bilginin gizli kalması açısından daha işlevsel şifreleme teknikleri oluşturulmuştur. Son dönemlerde Fibonacci Q-matrisi yardımıyla oluşturulan yeni şifreleme algoritması bunlardan biridir.

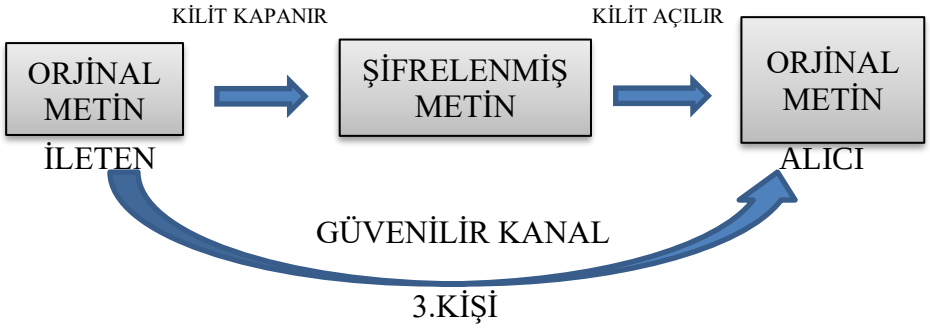
Leonardo Fibonacci tarafından tanımlanan Fibonacci sayıları bilimin birçok alanında yaygın olarak kullanılır. Horadam (1961), King (1960), Koshy (2017) ve Lee (2001) bunlara örnek verilebilir. Bunun yanı sıra Stakhov (1999), Gould (1981) gibi bilim insanlarının da Fibonacci Q-matrisi üzerine çalışmaları bulunmaktadır. Ayrıca Fibonacci Q-matrisi kodlamada da önemli yere sahiptir. Tas ve diğ. (2018) yapılan çalışmada şifrelenmek istenen metin, kare matris haline dönüştürüldükten sonra 2x2 tipindeki alt matrislere bölünerek bir öteleme sayısı yardımıyla şifrelenmektedir. Ana metne dönmek için Fibonacci Q-matrisi kullanılmıştır. Fibonacci dizisinin oluşumunun ardından genelleştirilmiş Fibonacci sayıları baz alınarak birçok sayı

dizileri ortaya çıkmıştır. Pell sayıları bunlardan biridir. Pell sayıları 17. yüzyıl ingiliz entelektüel tarihinde önemli bir yer tutan John Pell tarafından ortaya konulmuştur. Pell sayıları dizisi Fibonacci dizilerinden faydalanılarak oluşturulmuştur. Bu tezde bahsedilen bu özel sayı dizilerinden yararlanılarak oluşturulan yeni şifreleme algoritmaları ile literatüre katkı sağlanmaya çalışılmıştır.

Bu tezin ikinci bölümünde kriptoloji bilimine değinilmiştir. Aynı zamanda kriptolojinin alt dalları detaylı olarak açıklanmış ve gizliliğin temel unsurlarından bahsedilmiştir. Üçüncü bölümde kriptoloji algoritmalarının kendi içerisinde sınıflandırmalarından, açıklamalarından ve şifreleme kanalının işlevinden söz edilmiştir. Bununla birlikte kriptoloji sisteminin çok eski bir tarihe dayandığından, belli başlı şifreleme sistemlerine de yer verişmiştir. Dördüncü bölümde ise kısaca Fibonacci sayılarının tarihinden bahsedilip özellikleri incelenmiştir. Ayrıca Tas ve diğ. (2018) makalesinde var olan Fibonacci Q-matrisi kullanılarak elde edilmiş kodlama algoritmaları detaylı olarak araştırılmıştır. Beşinci bölümde de bir önceki bölümde bahsedilen kriptografi modeli, genelleştirilmiş Fibonacci dizisi yardımıyla oluşturulan rekürans Q-matrisi kullanılarak geliştirilmiştir. Böylece literatüre katkıda bulunmak hedeflenmiştir. Amaç şifreleme sistemini daha güvenilir hale getirmektir. Altıncı bölümde literatürde bahsedilen Fibonacci Q-matrisi kullanılarak elde edilmiş kodlama algoritmasında yer verilen Q-matrisi yerine, elemanları pell sayılarından oluşan Q-matrisi oluşturularak buna bağlı olan yeni kriptografi algoritması geliştirilip literatüre katkıda bulunmak amaçlanmıştır. Son bölümde ise Tas ve diğ. (2018) makalesi temel alınarak yeni bir şifreleme algoritması elde edilmiştir. Burada kullanılan şifreleme yöntemi şifrelenecek olan metin kare matrise dönüştürüldükten sonra sadece 2x2 lik alt matrislere bölünerek uygulanmaktadır. Burada bu durum daha genel forma dönüştürülmeye çalışılmıştır. Literatürde bahsedilen k-mertebeli Fibonacci sayıları kullanılarak 2x2 lik alt matrisler yerine, şifrelenecek olan metin 3x3 ,4x4, …, n x n tipindeki alt matrislere bölünmüştür. Elde edilen yeni yöntemlerin hepsi örneklerle desteklenerek literatüre katkı sağlanmak amaçlanmıştır.

2. KRİPTOLOJİ BİLİMİ

Bulunduğumuz çağda birçok teknolojik aletlerle iletişim sağlanmaktadır. Bu iletişim ağlarını kullanırken güvenlik birçok kişinin problemi olmaktadır. Günümüzdeki gizli olan bütün bilgiler telefon veya bilgisayar gibi teknolojik aletlerin içerisine sığdırılmaktadır. Bu nedenle teknolojinin gelişmesiyle birlikte önemli bilgilerin saklandığı dosyaların güvenirliği tehlikeli hale gelmiştir. Bu durumda şifreyi üçüncü kişilerden gizlemek çok önemlidir. Bu aşamada kriptolojiye ihtiyaç duyulur. Kriptoloji bir şifre bilimidir. Kriptoloji iki kişi arasındaki haberleşmeyi üçüncü bir kişi tarafından ele geçirilmeden ve aynı zamanda iletilecek olan metni üçüncü kişi tarafından değişime uğratmadan alıcıya ulaştırmak için çalışılan bir bilim dalıdır (bkz. Şekil 2.1).



Şekil 2.1: Kriptoloji kanalı

Kriptoloji, kriptografi ve kriptoanaliz olmak üzere iki alt dala ayrılır. Kriptografi yunanca kökenlidir ve yunanca gizli anlamına gelen “kriptos” ve yazı anlamına gelen “graphi” den türetilmiştir. Kriptografinin asıl amacı şifrelenmiş olan metni alıcıya ulaştırırken kanal yolunda gizlilik için matematiksel yapı taşlarını kullanarak, bilgiyi şifrelemektir. Kriptoanaliz ise bilgi karşı tarafa iletilirken, güvenliği sağlamak için oluşturulan algoritmanın sağlamasını ve test süreçlerini kapsar. Yani kriptoanaliz ve kriptografi çift yönlü çalışmış olur. Bu kanalda asıl amaç bilgi güvenliğini sağlamaktır. Bilgi güvenliği üç temel unsurdan oluşur.

Gizlilik: Gönderilen bilginin yetkisi olmayan kişilerin eline geçmemesidir.

Bütünlük: Bilgiyi olması gerektiği şekilde tutmak ve korumaktır.

Erişilebilirlik: Bilginin gönderilen tarafından ihtiyaç duyulduğunda ulaşılabilir ve kullanılabilir durumda olmasıdır.

Bu verilen unsurlardan herhangi biri zarar arz ederse güvenlik zafiyeti oluşur.

Kriptografinin temel amacı gönderilmek istenen mesajın kanal üzerinden üçüncü bir kişi tarafından deşifre edilmeden haberleşmeyi sağlamaktır. Aşağıda belirtilen matematiksel notasyonlar kullanılarak Kriptografi tanımlanır. (P, K, C, D, E) şeklindeki sıralı beşli ile ifade edilir.

- P, muhtemel olan sonlu tüm açık metinler kümesidir.
- C, muhtemel olan sonlu tüm şifreli metinler kümesidir.
- K, muhtemel olan sonlu tüm anahtarlar kümesidir.
- ∀ k ∈ K için e_k ∈ E olan şifreleme kuralı ve d_k ∈ D olan bir de şifreleme kuralı mevcuttur. Açık metindeki ∀ x ∈ P düz metni için $d_k(e_k(x)) = x$ eşitliğini sağlar.

Burada e_k : P ⟶ C, düz metni şifreli metne götüren şifreleme fonksiyonudur. Benzer bir şekilde, d_k : C ⟶ P, şifreli metni düz metne geri götüren şifre çözme fonksiyonudur. Bir y düz metni e_k ile şifrelenir ve elde edilen şifreli metin d_k şifresi ile çözülürse sonuç olarak aynı y düz metni elde edilir.

Kendi aralarında gizli olarak haberleşmek isteyen iki kişi k ∈ K anahtarı seçerek, biri diğerine güvensiz bir kanal üzerinden $n \geq 1, 1 \leq i \leq n$ için $x_i \in$ P olmak üzere $x = x_1 x_2\, x_3 \ldots x_n$ şeklinde bir metin göndermek ister. Burada tanımlanan her x_i önceden belirlenmiş olan K anahtarı ile e_k şifreleme kuralı kullanılarak şifrelenir. Burada belirtilen e_k bire-bir fonksiyondur. Böylece $1 \leq i \leq n$ için $y_i = e_K(x_i)$ olacak şekilde $y = y_1\, y_2\, y_3 \ldots y_n$ şifrelenmiş metin elde edilir (Afacan 2016).

3. ŞİFRELEME YÖNTEMLERİ

Bu bölümde şifreleme teknikleri ve yöntemleri detaylı olarak anlatılacaktır. Ayrıca eski zamandan bu yana kullanılan bazı şifreleme teknikleri ayrıntılı olarak verilecektir. Bu kısım Özyılmaz (2014), Afacan (2016) ve Yeşilbaş (2016) kaynaklarından yararlanılarak oluşturulmuştur.

Şifreleme teknikleri, klasik şifreleme sistemleri ve modern şifreleme (Simetrik ve Asimetrik) sistemleri olmak üzere ikiye ayrılır.

3.1 Modern Şifreleme Sistemleri

Kriptografide şifrelemek için kullanılan anahtarların özelliklerine göre iki algoritma sistemi kullanılmaktadır. Bu algoritma sistemleri Simetrik Anahtarlı Şifreleme (gizli anahtarlı şifreleme) ve Asimetrik Anahtarlı Şifreleme (açık anahtarlı şifreleme) olmak üzere ikiye ayrılır.

3.1.1 Simetrik Anahtarlı Şifreleme

Simetrik anahtarlı şifrelemede, karşı tarafa gönderilen mesajların hem şifrelenmesi hem de şifre çözümü için aynı anahtar kullanılır. Bu tip şifreleme algoritması, devletler ve ordular arasında iletişimi gizli tutmak için sıklıkla kullanılır. Simetrik şifreleme sisteminin en önemli avantajlarından birisi oldukça hızlı olmasıdır. Asimetrik algoritmayla karşılaştırıldığında hız açısından simetrik şifreleme algoritması oldukça başarılıdır. Algoritmalar oluşturulan mesajların en hızlı şekilde şifrelenmesi ve şifre çözülmesi açısından tahmin edildiğinden yüksek güvenlik duvarı oluşturur. Simetrik anahtarlı (gizli anahtarlı) şifreleme algoritmaları aşağıda verilmektedir.

- Blok Şifreleme Algoritmaları
- Dizi Akış Şifreleme Algoritmaları
- AES (Advanced Encryption Standard – Gelişmiş şifreleme Standartı)
- DES (Data Encryption Standard – Veri şifreleme standartı)

- Triple Des (3DES)
- IDEA (International Data Encryption Algorithm)
- Blowfish
- Twofish
- IRON, RC4, MD5, SHA.

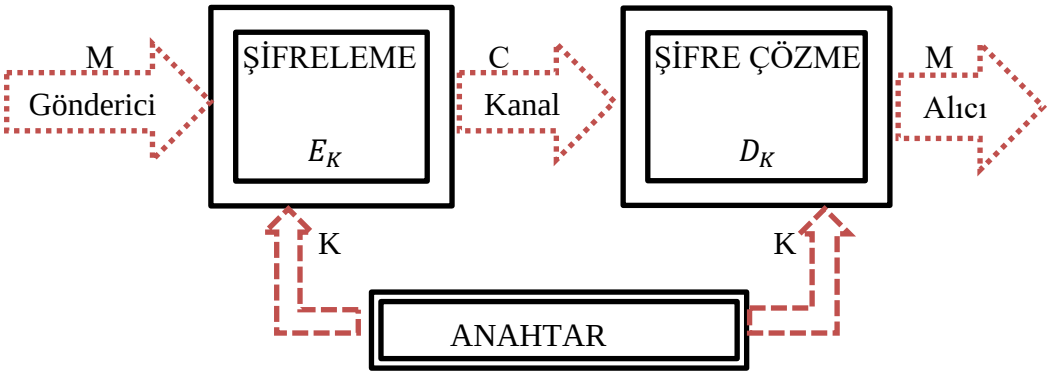
3.1.2 Asimetrik Anahtarlı Şifreleme

Şifreleme ve şifre çözme işlemleri için farklı anahtarların kullanıldığı bir şifreleme algoritmasıdır. Gönderici ve alıcıda bir çift anahtar bulunur. Bu anahtarlar gizli ve açık olmak üzere iki çeşittir. Bu anahtarların biriyle şifreleme yapılırken diğeriyle şifre çözümlenir. Bu üretilen şifreler matematiksel olarak birbirleriyle bağlantılıdır. Açık anahtar altyapısı, internet üzerinden güvenli haberleşmeyi sağlayan TLS protokolü, güvenli e-posta haberleşmesinde kullanılan PGP protokolü, dosya şifreleme ve çözmeye yarayan GPG gibi protokollerde kullanılmaktadır. Asimetrik şifreleme algoritmaları aşağıda verilmektedir.

- RSA
- Eliptik eğri sistemleri
- El Gamal
- Diffie-hellman anahtar belirlemesi
- Kod tabanlı kriptosistemler

3.2 Klasik Şifreleme Sistemleri

Bu bölümde bazı klasik şifreleme sistemleri ayrıntılı olarak verilmiştir. Burada Afacan (2016) kaynağından yararlanılmıştır. Şekil 3.1 de klasik bir şifreleme sisteminin şeması verilmektedir.



Şekil 3.1: Şifreleme Kanalı

Şekil 3.1 de kullanılan simgelerin anlamları aşağıda verilmektedir.

M: Orijinal Düz Metin

C: Şifreli Metin

E_K: Mesajın k anahtarı ile şifrelenmesini sağlayan kuraldır.

D_K: Mesajın şifresinin k anahtarı ile çözülmesini sağlayan kuraldır.

Orijinal M mesajı e_K şifreleme fonksiyonu ve K anahtarı ile şifrelenir. Elde edilen C şifreli metin güvenilir olmayan bir kanal üzerinden alıcıya gönderilir. Alıcı, C şifreli metnin şifresini d_k şifre çözme kuralı ve K anahtarını kullanılarak çözer ve M mesajını oluşturur. Sonuç olarak, M ve C arasında C = $E_K(M)$, M = $D_K(C)$ ilişki elde edilir.

Şifreleme sisteminde kullanılacak olan İngilizce alfabe ve harflerin sayı karşılıkları Tablo 3.1 de verilmektedir.

Tablo 3.1: İngilizce harfler ve sayı karşılıkları

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

Şifreleme sisteminde kullanılacak olan Türkçe alfabe ve harflerin sayı karşılıkları Tablo 3.2 de verilmektedir.

Tablo 3.2: Türkçe harfler ve sayı karşılıkları

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

Kriptolojinin uzun ve çok eskilere dayanan bir tarihi vardır. Yazı bulunduktan sonra haberleşmede olan gizlilik daha çok önem arz etmiştir. Gizli haberleşme bundan yaklaşık olarak 4000 yıl önce kullanılmaya başlamıştır. Devletler arası sırlar savaşlar ve askeri alanlarda büyük önem taşır. Osmanlı Devleti'nin son padişahlarından II. Abdülhamid İngiltere Kraliyet Ailesi ile haberleşmede benzer teknikleri kullanmıştır. Dünya'da devletler arası sırların gizlenmesi gibi pek çok alanda kullanılan kriptolojinin büyük bir önemi vardır. Kriptolojinin en eski tarihçesi arkeologların yaptığı araştırmalar sonucunda ilk kullanılmaya başlandığı yer Antik Mısırdır. M.Ö. 1900 döneminde mısırlıların yazdığı kitabelerde hiyeroglifler kullanılmıştır. Bu kitabeler ise bilinen ilk yazılı kriptografik belgelerdir. Aynı zamanda çömlek yapımı Anadolu, Kuzey Suriye ve Kuzey Mezopotamya'da yaklaşık olarak 8200 yıl önce ortaya çıkmış ve 2000 yıl gibi kısa bir sürede dünyaya yayılmıştır. Dıştan bakıldığında, çanak çömlek parçaları önemsiz olan şeyler gibi görünür fakat arkeologlar için önemi çok büyüktür. Geçmiş tarihimize bakıldığında kriptografik olarak bir önemi olduğu görülür. Çömlek yapımının eşsiz tarifini eski yıllarda insanlar gizlemek için kriptolojiye başvurmuşlardır. Şimdi ise bazı kriptografik belgeler verilecektir.

- İlk kriptografik belge, yaklaşık olarak M.Ö. 1900 yılında yazıldığı tahmin edilen Rosetta tabletidir.
- Bir diğeri M.Ö. 480 tarihinde eski yunanca tarihçisi Herodot tarafından yazılan Histories kitabında bulunan ilk Stenografi örneğidir. Yıllar önce Yunan ve Pers İmparatorluğu arasında geçen savaş esnasında Pers yöneticisi olan Histiaeus'un isyan başlatmasını istemek için kölesinin saçlarını kazıtıp gizli

mesajı yazmasını ve saçları uzadığında bu köleyi Aristagoras'a yollaması ve mesajını iletmesi ile olmuştur.

- M.Ö. 500-600 yılları arasında eski ahitte yeremya Peygamberin (İbrani Peygamber) kehanet ve uyarılarında bazı şifreli kelimelere rastlanmıştır. Babil saldırısını önceden haber veren Peygamber ATBASH isimli bir şifre kullanmıştır. Kısaca ATBASH şifreleme sisteminden aşağıda bahsedilmiştir.

3.2.1 Atbash Şifreleme Yöntemi

İnsanlığın bildiği en eski Ortadoğu'da kullanılan eski şifreleme yönteminden biridir. ATBASH şifreleme algoritması Arami alfabesinin tersten yazılması ile oluşturulan bir kodlama sistemine sahiptir. Babilliler, Yahudiler ve Araplar tarafından sıkça kullanılmıştır. Tablo 3.3'de Atbash şifreleme tablosu görülmektedir. Bu tabloya göre "MATEMATIK" kelimesi "LZFULZFQN" olarak şifrelenir.

Tablo 3.3: Atbash şifreleme tablosu

PLAİN	a	b	c	d	e	f	g	h	ı	j	k	l	m	n	o	q	r	s	t	u	w	x	y	z
CİPHER	Z	Y	X	W	U	T	S	R	Q	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

3.2.2 Scytale Şifreleme Yöntemi

2500 yıldan uzun bir süre öncesinde Yunanlılar tarafından veri güvenliğini sağlamak amacıyla kullanılan askeri şifreleme yöntemidir. Şifrelenen metnin uygulama sistemi yer değiştirme şeklindedir. Göndermek istenilen mesaj şeridin üzerine sopa boyunca yazılır. Şerit sopadan çıkardıktan sonra açık bir şekilde gönderilir. Şifrelenen metin karşı tarafa ulaştıktan sonra aynı yarıçapa sahip bir sopa

alınır ve aynı şekilde metin sopaya sarıp mesaj okunur. Kullanılan şifreleme sistemine SCYTALE şifreleme yöntemi denir. Bu cihaz ilk kriptografik cihaz kabul edilmiştir.

3.2.3 Sezar Şifreleme Yöntemi

Sezar şifreleme yöntemi, Roma imparatoru Jül Sezar tarafından kullanılmıştır. Savaş döneminde önemli bilgiler bu şifreleme yöntemi ile taşınmıştır. Bu teknik günümüzde oldukça yetersizdir. Bu şifreleme yönteminde her harf, alfabede kendisinden sonra gelen üçüncü harf ile değiştirilir.

Örneğin "MATEMATİK" kelimesi Sezar şifreleme algoritması kullanılarak aşağıdaki şekilde şifrelenmiştir.

1. "MATEMATİK" kelimesi anahtar $k = 3$ alınarak şifrelenir.
2. Tablo 3.2'den yararlanılarak şifrelenecek olan mesajın her bir harfine karşılık gelen sayılar bulunur. $k = 3$ olduğundan her bir sayısal değere karşılık $A + 3\ (mod\ 29)$ fonksiyonu oluşturulur. $(mod\ 29)$ a göre işlem yapıldıktan sonra yeni oluşan sayısal değere karşılık gelen harf ile şifrelenir.

Böylece " MATEMATİK " kelimesini $k = 3$ anahtarı ile "ÖÇVĞÖÇVLN" şeklinde şifrelenir.

3.2.4 Yerine Koyma Algoritması

Bu algoritmada P (muhtemel olan sonlu tüm açık metinler kümesi), C (muhtemel olan sonlu tüm şifreli metinler kümesi) olmak üzere P = C = Z_{29} şeklinde olup ve K, 29 tane harfin (0,1,2,…,28) tüm olası permütasyonlarını içermektedir. Gönderilmek istenen metin $\forall\ \pi \in K$ için $e_\pi(x) = \pi\ (\ x\ )$ fonksiyonu kullanılarak şifrelenir. Karşı tarafa iletilen şifrelenmiş metin $d_\pi(y) = \pi^{-1}(y)$ fonksiyonu ile çözülür.

Örneğin "HER PENCERE BÜYÜKLÜĞÜNE GÖRE IŞIK ALIR" cümlesini yer değiştirme şifreleme yöntemi ile şifrelemek için aşağıda keyfi bir permütasyon oluşturulmuştur.

Tablo 3.4: Yerine koyma şifreleme tablosu

a	b	c	ç	d	e	f	g	ğ	h
P	H	Z	Ö	Ğ	Y	O	G	V	N
ı	i	j	k	l	m	n	o	ö	p
F	Ü	M	E	U	L	D	T	K	Ç
r	s	ş	t	u	ü	v	y	z	
Ş	J	C	S	İ	B	R	I	A	

Bu tabloda verilen permütasyon fonksiyonu yardımı ile bu cümle aşağıdaki şekilde şifrelenir.

"NYŞ ÇYDZYŞY HBIBEUBVBDY GKŞY FCFE PUFŞ"

Şifrelenmiş metin ters permütasyon fonksiyonu yardımıyla çözümlenir. Aşağıda keyfi olarak oluşturulan permütasyonun ters görüntüsü verilmektedir.

Tablo 3.5: Yerine koyma şifreleme tablosu tersi

A	B	C	Ç	D	E	F	G	Ğ	H
z	ü	ş	p	n	k	ı	g	d	b
I	İ	J	K	L	M	N	O	Ö	P
y	u	s	ö	m	j	h	f	ç	a
R	S	Ş	T	U	Ü	V	Y	Z	
v	t	r	o	l	i	ğ	e	c	

3.2.5 Afin Şifreleme Algoritması

Afin şifreleme algoritmasında $\mathrm{P} = \mathrm{C} = \mathrm{Z}_{29}$, $a, b \in \mathrm{Z}_{29}$ için $\mathcal{K} = \{ (a,b) \in \mathrm{Z}_{29}\, x\, \mathrm{Z}_{29} : (a, 29) = 1 \}$, $\mathrm{K} = (\mathrm{a}, \mathrm{b}) \in \mathcal{K}$ şeklinde tanımlanır. Şifrelenmek istenen metin $x, y \in \mathrm{Z}_{29}$ olmak üzere $e_k(x) \equiv ax + b \ (mod\ 29)$ dönüşümü ile karşı tarafa iletilir. Şifre çözümü için ise $d_k(y) \equiv a^{-1}(y - b) \ (mod\ 29)$ fonksiyonu kullanılır.

Örnek 3.2.5.1: "ON" kelimesine afin şifreleme algoritması uygulanacak olursa O→17 ve N→16 karşılık gelir.

$K = (7,3)$ şeklinde keyfi bir anahtar seçilecek olursa yukarıda verilen tanımdan yararlanarak $a = 7, b = 3$ olur. (7,29) = 1 olduğundan şifreleme fonksiyonu $e_k(x) \equiv 7x + 3 \ (mod\ 29)$ olur. Buna göre;

$7.17 + 3 \equiv 6\ (mod\ 29)$ ve $7.16 + 3 \equiv 28\ (mod\ 29)$ olur.

Tablo 3.2'den yararlanılarak sayıların rakam karşılığı oluşturulacak olursa 6→ F, 28→Z harflerine karşılık gelir. Böylece "ON" kelimesinin şifrelenmiş hali "FZ" olarak elde edilir.

Şifrelenen metin K anahtarı yardımıyla açık metne dönüştürülür. Şimdi şifrelenmiş "FZ" metnine bu uygulanacak olursa;

$a\,.a^{-1} \equiv 1(mod\ 29)$ olduğundan $a\,.a^{-1} - 29y \equiv 1\ (mod\ 29)$ elde edilip $K = (7,3)$ anahtarı yardımıyla $7a^{-1} - 29y \equiv 1\ (mod\ 29)$ fonksiyonu bulunur. Öklid algoritması yardımıyla a^{-1} aşağıdaki şekilde elde edilir.

29 = 4.7 + 1

7 = 7.1 + 0.

O halde,

1 = 29 – 4.7

1 = 7. (-4) – 29.(-1) olup $a^{-1} \equiv -4 \equiv -4 + 29 \equiv 25\ (mod 29)$

olur. Dolayısıyla

$y \equiv 7x + 3\ (mod\ 29)$

olup

$y\text{-}3 \equiv 7x\ (mod 29)$

elde edilir. Böylece

$25(y - 3) \equiv (25.7)x \equiv x\ (mod 29)$

Denkliği yardımıyla

$d_K(y) \equiv 25(y-3) \equiv 25y - 75 \equiv 25y - 17\ (mod 29)$

fonksiyonu bulunur.

y → 6 alınırsa, $d_K(y) \equiv 25(6-3) \equiv 17(mod 29)$ fonksiyonu yardımıyla x → 17 elde edilir. Bu ise Tablo 3.2' de "O" harfine karşılık gelir. Benzer şekilde

y → 28 alınırsa, $d_K(y) \equiv 25(28-3) \equiv 16(mod 29)$ fonksiyonu ile x → 16 elde edilir. Bunun ise Tablo 3.2'deki karşılığı "N" harfidir. Böylece "ON" açık metnine ulaşılır.

3.2.6 Vigenere Şifreleme Algoritması

Vigenere şifreleme algoritması, keyfi seçilen bir kelime yardımıyla öteleme yapılarak şifreleme işlemi gerçekleştirilir. Bu algoritmada keyfi seçilen kelime anahtarı oluşturur. Bu K ile gösterilecek olursa, uzunluğu m olan bir harf dizisine karşılık gelir, buna anahtar sözcük denir. Vigenere şifreleme algoritması matematiksel olarak ifade edilecek olursa, $m \in \mathbb{Z}^+$ olmak üzere $P = K = C = (\mathbb{Z}_{29})^m$ olsun. $K = (k_1, k_2, \ldots, k_m)$ anahtarı için $e_K(x_1, x_2, \ldots, x_m) = (x_1 + k_1, x_2 + k_2, \ldots, x_m + k_m)$ şeklinde metin şifrelenir. Ayrıca $d_K(y_1, y_2, \ldots, y_m) = (x_1 - k_1, x_2 - k_2, \ldots, y_m - k_m)$ ile ana metne ulaşılır.

Örnek 3.2.6.1: " VİGENERE "kelimesi vigenere şifreleme algoritması ile şifrelenecek olursa, $m = 5$ olmak üzere anahtar sözcük "PAMUK" olarak kabul edilsin. Bu durumda $K = (19,0,15,24,13)$ olur.

V	İ	G	E	N	E	R	E
26	11	7	5	16	5	20	5
19	0	15	24	13	19	0	15

Sütunlardaki rakamlar alt alta topladığında şifrelenmiş metin elde edilir. Bu durumda "VİGENERE" kelimesi aşağıdaki şekilde şifrelenmiş olur.

45	11	22	29	29	24	20	20
N	İ	Ş	A	A	U	R	R

Son olarak şifrelenen metni çözümlemek için d_K fonksiyonu kullanılır. Böylece orijinal metin aşağıda görüldüğü şekilde elde edilir.

26	11	7	5	16	5	20	5
V	İ	G	E	N	E	R	E

4. FİBONACCİ SAYILARI İLE YENİ BİR KRİPTOGRAFİ ALGORİTMASI

Bu bölümde son zamanlarda kullanılan Fibonacci sayıları yardımıyla oluşturulan şifreleme algoritmasından bahsedilecektir. Bu algoritma günümüzde birçok algoritmaya nazaran daha güvenilirdir.

Şifreleme algoritmasına geçmeden önce genel olarak Fibonacci sayılarını incelemek yerinde olacaktır. Fibonacci sayılarını ortaya koyan İtalyan matematikçi Leonardo Fibonacci'dir. Leonarda Fibonacci İtalya'da dünyaya gelip, doğanın kanunlarını matematik düşünceleriyle açıklamaya çalışmıştır. Doğunun ilmini batıya yaymak için pek çok alanla ilgilenmiştir. Çocuk yaşlarında Güney Afrika'ya gidip burada matematik bilimiyle ilk kez tanışmış ve İslam bilginlerinden doğu matematiğindeki tüm gelişmeleri öğrenmiştir. Güney Afrika'da Hint Arap sayılarıyla işlemler yapmanın roma rakamlarıyla işlem yapmaktan daha kolay olduğunu görmüştür. İtalyan matematikçi yazdığı kitapların birinde tavşanlarla ilgili bir teori ortaya koymuştur. Bu teoriyi tavşanların ilk iki ay doğum yapmadıklarını, üçüncü aydan itibaren her çift her ay bir çift yavru dünyaya getirmesinden yola çıkarak oluşturmuştur. Buna göre Fibonacci bir çift tavşanla başlayıp, kaç ay sonra kaç tavşan olduğunun sorusunun cevabını öne süren genel bir çalışma ortaya koymuştur. Buna göre Fibonacci dizisi matematiksel olarak aşağıdaki şekilde ifade edilir (Tas ve diğ. 2018).

$F_0 = 0$ ve $F_1 = 1$ olmak üzere $n \geq 2$ için

$$F_n = F_{n-1} + F_{n-2} \tag{4.1}$$

Çalışmamıza konu olan Fibonacci şifreleme sisteminde kullanılan Fibonacci dizisine kısaca değindikten sonra Tas ve diğ. (2018) makalesinde incelenen şifreleme algoritmasından bahsederek devam etmek doğru olacaktır. Bu algoritma detaylı olarak aşağıda ifade edilmiştir. İlk olarak şifrelenecek olan metin $2mx2m$ tipinde bir kare matrise dönüştürülür. Bu matris içine eksik kalan matris elemanları yerine sıfır alınarak yerleştirilir. Bundan sonra bu matris soldan başlayarak $2x2$ tipinde alt matrislere ayrılır. Bu alt matrisler aşağıda gösterildiği gibi $A_{\text{İ}}$ $(1 \leq \text{İ} \leq m^2)$ şeklinde ifade edilir.

$$A_1 = \begin{bmatrix} a_1^1 & a_2^1 \\ a_3^1 & a_4^1 \end{bmatrix} \qquad A_2 = \begin{bmatrix} a_1^2 & a_2^2 \\ a_3^2 & a_4^2 \end{bmatrix}$$

$$A_3 = \begin{bmatrix} a_1^3 & a_2^3 \\ a_3^3 & a_4^3 \end{bmatrix} \qquad A_4 = \begin{bmatrix} a_1^4 & a_2^4 \\ a_3^4 & a_4^4 \end{bmatrix}$$

$$\ldots \quad A_n = \begin{bmatrix} a_1^n & a_2^n \\ a_3^n & a_2^n \end{bmatrix}$$

Bu matrislerin elemanlarının Tablo 3.1'deki karşılıkları yazılır. Daha sonra elde edilen alt matris sayısı n olarak simgelenerek,

$$k = \begin{cases} n & n \leq 3 \\ \left[\left|\frac{n}{2}\right|\right] & n > 3 \end{cases} \tag{4.2}$$

ifadesi yardımıyla öteleme sayısı bulunur.

Her bir alt matrisin elemanları ötelendikten sonra A_n matrislerinin determinantları alınır. Alt matrislerin determinantları ve bileşenleri aşağıdaki şekilde verildiği gibi oluşturulan şifreli matrise satır olarak yerleştirilir. Alt matrislerin determinantları keyfi sütuna yerleştirilebilir. Bu matris oluşturulurken alt matrislerin istenilen herhangi bir bileşeni gizlenir. Örneğin aşağıdaki oluşturulan şifreli matriste bu alt matrislerin üçüncü elemanları gizlenmiştir.

$$\mathrm{K} = \begin{bmatrix} detA_1 & a_1^1 + k & a_2^1 + k & a_4^1 + k \\ detA_2 & a_1^2 + k & a_2^2 + k & a_4^2 + k \\ detA_3 & a_1^3 + k & a_2^3 + k & a_4^3 + k \\ . & . & . & . \\ . & . & . & . \\ detA_n & a_1^n + k & a_2^n + k & a_4^n + k \end{bmatrix}$$

Oluşturulan bu matris, şifrelenen metnin yeni bir hali olarak karşı tarafa iletilir.

Şimdi ise alıcı tarafından alınan şifrelenmiş matrisi çözmek için aşağıdaki adımları takip etmek gerekir. İlk olarak bunun için gerekli olan Fibonacci Q-matrisini vermek yerinde olacaktır.

Fibonacci Q-matrisi

$$Q = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

olarak ifade edilir. Ayrıca Fibonacci Q-matrisinin k. kuvveti aşağıdaki şekilde oluşturulur.

$$Q^k = \begin{bmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{bmatrix} \tag{4.3}$$

Daha önce belirtilen $A_1, A_2, \ldots, A_n$ alt matrislerinde keyfi olarak gizlenen eleman sabit bırakılarak yeni alt matrisler oluşturulur. Bu matrisler Q^k matrisi ile sırasıyla çarpılır. Elde edilen çarpım sonucunda oluşan eşitlikteki her iki tarafın determinantı alınır. Böylece gizlenen yani şifrelenen eleman bulur. Fibonacci sayılarıyla elde edilen kodlama algoritması aşağıdaki örnekle daha iyi ifade edilecektir.

Örnek 4.1: "GOOD MORNING" cümlesi Fibonacci algoritması kullanılarak aşağıdaki şekilde şifrelenir. İlk olarak şifrelenecek metin boş kalan bileşenler yerine sıfır alınarak kare matris içine yerleştirilir.

$$\begin{bmatrix} G & O & O & D \\ 0 & M & O & R \\ N & I & N & G \\ 0 & 0 & 0 & 0 \end{bmatrix}_{4\times 4}$$

1. Oluşturulan mesaj matrisi soldan sağa $2x2$ tipinde alt matrislere bölünür.

$$\mathrm{A_1} = \begin{bmatrix} \mathrm{G} & \mathrm{O} \\ 0 & \mathrm{M} \end{bmatrix} \qquad \mathrm{A_2} = \begin{bmatrix} \mathrm{O} & \mathrm{D} \\ \mathrm{O} & \mathrm{R} \end{bmatrix}$$

$$\mathrm{A_3} = \begin{bmatrix} \mathrm{N} & \mathrm{I} \\ 0 & 0 \end{bmatrix} \qquad \mathrm{A_4} = \begin{bmatrix} \mathrm{N} & \mathrm{G} \\ 0 & 0 \end{bmatrix}$$

2. Alt matris sayısı $n = 4 > 3$ olduğundan $\left[\left|\frac{4}{2}\right|\right] = 2, k = 2$ olarak hesaplanır. Tablo 3.1'den yararlanılarak her bir harfe karşılık gelen sayılar bulunur ve $k = 2$ ötelenerek aşağıdaki tablo oluşturulur.

G	O	O	D	0	M	O	R	N	I	N	G
8	16	16	5	28	14	16	19	15	10	15	8

3. A_i ($1 \leq i \leq 4$) alt matrislerinin elemanları aşağıdaki şekildedir.

$$a_1^1 = 8 \quad a_2^1 = 16 \quad a_3^1 = 28 \quad a_4^1 = 14$$

$$a_1^2 = 16 \quad a_2^2 = 5 \quad a_3^2 = 16 \quad a_4^2 = 19$$

$$a_1^3 = 15 \quad a_2^3 = 10 \quad a_3^3 = 28 \quad a_4^3 = 28$$

$$a_1^4 = 15 \quad a_2^4 = 8 \quad a_3^4 = 28 \quad a_4^4 = 28$$

4. Bu adımda alt matrislerin determinantları alınır.

$$d_1 = detA_1 = -336$$

$$d_2 = \det A_2 = 224$$

$$d_3 = \det A_3 = 140$$

$$d_4 = \det A_4 = 196$$

5. 3. ve 4. adımlar kullanarak aşağıda verilmiş olan şifrelenmiş K matrisi oluşturulur.

$$K = \begin{bmatrix} -336 & 8 & 16 & 28 \\ 224 & 16 & 5 & 16 \\ 140 & 15 & 10 & 28 \\ 196 & 15 & 8 & 28 \end{bmatrix}$$

Alıcıya gönderilen şifrelenmiş K matrisi, aşağıda belirtildiği şekilde çözülerek açık metin elde edilir.

1. $k = 2$ için Q^2 matrisi hesaplanır.

$$Q^2 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$

2. Her bir alt matris Q^2 matrisi ile çarpılır.

$$A_1.Q^2 = \begin{bmatrix} 8 & 16 \\ 28 & a_1 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 32 & 24 \\ a_1 + 56 & a_1 + 28 \end{bmatrix}$$

$$A_2.Q^2 = \begin{bmatrix} 16 & 5 \\ 16 & a_2 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 37 & 21 \\ a_2 + 32 & a_2 + 16 \end{bmatrix}$$

$$A_3.Q^2 = \begin{bmatrix} 15 & 10 \\ 28 & a_3 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 40 & 25 \\ a_3 + 56 & a_3 + 28 \end{bmatrix}$$

$$A_4.Q^2 = \begin{bmatrix} 15 & 8 \\ 28 & a_4 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 38 & 23 \\ a_4 + 56 & a_4 + 28 \end{bmatrix}$$

3. Yukarıdaki çarpım sonucu elde edilen eşitliğin her iki tarafının determinantı alınarak gizlenen (şifrelenen) elemanlar elde edilir.

$$a_4^1 = 14$$
$$a_4^2 = 19$$
$$a_4^3 = 28$$
$$a_4^4 = 28$$

4. Elde edilen şifrelenmiş bileşenler alt matrislerde yerlerine yazılır.

$$A_1 = \begin{bmatrix} 8 & 16 \\ 28 & 14 \end{bmatrix} A_2 = \begin{bmatrix} 16 & 5 \\ 16 & 19 \end{bmatrix}$$

$$A_3 = \begin{bmatrix} 15 & 10 \\ 28 & 28 \end{bmatrix} A_4 = \begin{bmatrix} 15 & 8 \\ 28 & 28 \end{bmatrix}$$

5. 4. adımda bulunan A_1, A_2, A_3, A_4 alt matrisler soldan sağa doğru aşağıdaki gibi K matrisine yerleştirilir.

$$K = \begin{bmatrix} 8 & 16 & 16 & 5 \\ 28 & 14 & 16 & 19 \\ 15 & 10 & 15 & 8 \\ 28 & 28 & 28 & 28 \end{bmatrix}$$

6. Son olarak K matrisinin her bir bileşeni k sayısı kadar ötelenip Tablo 3.1'deki karşılıkları alınarak şifre çözülür.

$$K = \begin{bmatrix} G & O & O & D \\ 0 & M & O & R \\ N & I & N & G \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Böylece "GOOD MORNING" ana metni elde edilmiş olur.

5. REKÜRANS BAĞINTILARI YARDIMIYLA YENİ BİR ŞİFRELEME YÖNTEMİ

Bu bölümde yeni bir Q-matrisi kullanılarak dördüncü bölümde verilen şifreleme algoritması genelleştirilmiştir. Bu yeni matris gizli bilginin güvenirliğini arttırmaktadır. Önceki bölümde verilen şifreleme ve şifre çözme yöntemleri genel olarak bu yeni oluşturulan algoritma ile benzerdir. Aşağıda ifade edilen U_n dizisi genelleştirilmiş Fibonacci dizisi olarak tanımlanmıştır (Topal, 2018).

Genelleştirilmiş Fibonacci dizisi, $U_0 = 0\,, U_1 = 1$ olmak üzere

$$U_n = a\,.\,U_{n-1} + \ b\,.\,U_{n-2} \tag{5.1}$$

şeklinde tanımlanır. Bu eşitlik yardımıyla yeni Q-matrisi, $a, b \in \mathbb{Z}^+$ olmak üzere $Q = \begin{bmatrix} a & b \\ 1 & 0 \end{bmatrix}$ şeklinde oluşturulmuştur. Yeni elde edilen Q-matrisi, karşı tarafa gönderilen şifrelenmiş mesaj matrisinin çözümlenmesi amacıyla kullanılır. Çözümlenmesi için gerekli olan tüm adımlar Tas ve diğ. (2018) ile benzer niteliktedir. Bu yöntemin daha iyi ifade edilebilmesi için aşağıdaki örnek verilmiştir.

Örnek 5.1: "HOW OLD ARE YOU" cümlesi aşağıda yeni elde edilen bu yöntem kullanılarak şifrelenmiştir. Önce bu metin boş kalan bileşenler yerine sıfır alınarak kare matris içine yerleştirilir.

$$\mathrm{F} = \begin{bmatrix} H & O & W & 0 \\ O & L & D & 0 \\ A & R & E & 0 \\ Y & O & U & 0 \end{bmatrix}_{4x4}$$

1. Oluşturulan mesaj matrisi aşağıda olduğu gibi sağdan sola olacak şekilde $2x2$ tipinde alt matrislere bölünür.

$$\mathrm{A}_1 = \begin{bmatrix} \mathrm{W} & 0 \\ \mathrm{D} & 0 \end{bmatrix} \quad \mathrm{A}_2 = \begin{bmatrix} \mathrm{H} & \mathrm{O} \\ \mathrm{O} & \mathrm{L} \end{bmatrix}$$

$$\mathrm{A}_3 = \begin{bmatrix} \mathrm{E} & 0 \\ \mathrm{U} & 0 \end{bmatrix} \quad \mathrm{A}_4 = \begin{bmatrix} \mathrm{A} & \mathrm{R} \\ \mathrm{Y} & \mathrm{O} \end{bmatrix}$$

2. Alt matris sayısı $n = 4 > 3$ olduğundan $\left[\left|\frac{4}{2}\right|\right] = 2,\ k = 2$ olarak hesaplanır. Tablo 3.1'den yararlanılarak her bir harfe karşılık gelen sayılar bulunur ve $k = 2$ ötelenerek aşağıdaki tablo oluşturulur.

H	O	W	0	O	L	D	0	A	R	E	0	Y	O	U	0
9	16	24	28	16	13	5	28	2	19	6	28	26	16	22	28

3. A_i ($1 \leq i \leq 4$) alt matrislerinin elemanları aşağıdaki şekilde oluşturulur.

$$a_1^1 = 24 \quad a_2^1 = 28 \quad a_3^1 = 5 \quad a_4^1 = 28$$

$$a_1^2 = 9 \quad a_2^2 = 16 \quad a_3^2 = 16 \quad a_4^2 = 13$$

$$a_1^3 = 6 \quad a_2^3 = 28 \quad a_3^3 = 22 \quad a_4^3 = 28$$

$$a_1^4 = 2 \quad a_2^4 = 19 \quad a_3^4 = 26 \quad a_4^4 = 16$$

4. Bu adımda her bir alt matrislerin determinantı alınır.

$$d_1 = detA_1 = 532$$

$$d_2 = \det A_2 = -139$$

$$d_3 = \det A_3 = -448$$

$$d_4 = \det A_4 = -462$$

5. Bundan önceki son iki adım kullanılarak K matrisi oluşturulur. Bu matriste alt matrislerin dördüncü elemanları gizlenmiştir.

$$K = \begin{bmatrix} 532 & 24 & 28 & 5 \\ -139 & 9 & 16 & 16 \\ -448 & 6 & 28 & 22 \\ -462 & 2 & 19 & 26 \end{bmatrix}$$

Böylece şifrelenmiş metin karşı tarafa iletilir.

Çözme algoritması ise aşağıdaki şekilde adım adım verilmiştir.

1. $k = 2$ için Q^2 matrisi hesaplanır.

$$Q^2 = \begin{bmatrix} a^2+b & ab \\ a & b \end{bmatrix}$$

2. Her bir alt matris Q^2 matrisi ile çarpılır.

$$A_1.Q^2 = \begin{bmatrix} 24 & 28 \\ 5 & x_1 \end{bmatrix}\begin{bmatrix} a^2+b & ab \\ a & b \end{bmatrix} = \begin{bmatrix} 24a^2+28a+24b & 24ab+28b \\ 5a^2+x_1a+5b & x_1b+5ab \end{bmatrix}$$

$$A_2.Q^2 = \begin{bmatrix} 9 & 16 \\ 16 & x_2 \end{bmatrix}\begin{bmatrix} a^2+b & ab \\ a & b \end{bmatrix} = \begin{bmatrix} 9a^2+16a+9b & 9ab+16b \\ 16a^2+x_2a+16b & x_2b+16ab \end{bmatrix}$$

$$A_3.Q^2 = \begin{bmatrix} 6 & 28 \\ 22 & x_3 \end{bmatrix}\begin{bmatrix} a^2+b & ab \\ a & b \end{bmatrix} = \begin{bmatrix} 6a^2+28a+6b & 6ab+28b \\ 22a^2+x_3a+22b & x_3b+22ab \end{bmatrix}$$

$$A_4.Q^2 = \begin{bmatrix} 2 & 19 \\ 26 & x_4 \end{bmatrix}\begin{bmatrix} a^2+b & ab \\ a & b \end{bmatrix} = \begin{bmatrix} 2a^2+19a+2b & 2ab+19b \\ 26a^2+x_4a+26b & x_4b+26ab \end{bmatrix}$$

3. Yukarıdaki çarpım sonucu elde edilen eşitliğin her iki tarafının determinantı alınarak gizlenen (şifrelenen) elemanlar elde edilir.

$$x_1 = a_4^1 = 28$$
$$x_2 = a_4^2 = 13$$
$$x_3 = a_4^3 = 28$$
$$x_4 = a_4^4 = 16$$

4. Elde edilen şifrelenmiş bileşenler alt matrislerde yerlerine yazılır.

$$A_1 = \begin{bmatrix} 24 & 28 \\ 5 & 28 \end{bmatrix} \; A_2 = \begin{bmatrix} 9 & 16 \\ 16 & 13 \end{bmatrix}$$

$$A_3 = \begin{bmatrix} 6 & 28 \\ 22 & 28 \end{bmatrix} \; A_4 = \begin{bmatrix} 2 & 19 \\ 26 & 16 \end{bmatrix}$$

5. 4. adımda bulunan A_1, A_2, A_3, A_4 alt matrisleri sırasıyla soldan sağa doğru aşağıdaki gibi K matrisine yerleştirilir.

$$K = \begin{bmatrix} 9 & 16 & 24 & 28 \\ 16 & 13 & 5 & 28 \\ 2 & 19 & 6 & 28 \\ 26 & 16 & 22 & 28 \end{bmatrix}$$

6. Son olarak K matrisinin her bir bileşeni k sayısı kadar geri ötelenip Tablo 3.1'deki karşılıkları alınarak şifre çözülür.

$$K = \begin{bmatrix} H & O & W & 0 \\ O & L & D & 0 \\ A & R & E & 0 \\ Y & O & U & 0 \end{bmatrix}$$

Böylece ana metin elde edilmiş olur.

6. PELL SAYILARI İLE YENİ BİR KRİPTOGRAFİ ALGORİTMASI

Bu bölümde Pell sayıları yardımıyla elde edilen yeni bir şifreleme algoritmasından bahsedilecektir. Bu algoritma Tas ve diğ. (2019) makalesinden esinlenerek oluşturulmuştur. $U_n = a\,.\,U_{n-1} + b\,.\,U_{n-2}$ şeklindeki genelleştirilmiş Fibonacci dizisinde $a = 1,\ b = 1$ alınacak olursa, Fibonacci dizisi ve $a = 2,\ b = 1$ alınırsa, pell dizisi elde edilmiş olur. Bu eşitlikten yararlanılarak Fibonacci Q-matrisi oluşturulmuştur. Aynı işlemler Pell için uygulanacak olursa, Pell Q-matrisi elde edilmiş olur. Oluşturulan bu matrisin bütün kuvvetleri Pell Q-matrisini verecektir. Aşağıda Pell dizisi genel olarak ifade edilmiştir.

Pell dizisi, $P_0 = 0, P_1 = 1$ olmak üzere

$$P_n = 2P_{n-1} + P_{n-2}\ , n > 1$$

şeklinde tanımlanan bir sayı dizisidir Aktaş (2021). Pell sayıları adını ingiliz matematikçi John Pell'den alır. Pell, Fibonacci sayı dizsine benzer bir sayı dizisidir. Bu Pell sayı dizisinden yararlanarak elde edilen bir Q-matrisi aşağıdaki şekilde ifade edilmiştir.

$$Q^n = \begin{bmatrix} P_n & P_{n-1} \\ P_{n-1} & P_{n-2} \end{bmatrix}$$

Oluşturulan Q-matrisine, Pell Q-matris adı verilir. Bu matris yardımıyla şifrelenmiş olan metin deşifre edilir. Şimdi ise yeni elde edilen şifreleme algoritmasının daha iyi anlaşılır olması için aşağıdaki örnek verilmiştir.

Örnek 6.1: "WHERE ARE YOU" cümlesi bu algoritma ile aşağıdaki şekilde şifrelenmiştir. İlk adım olarak bu metin boş kalan bileşenler yerine sıfır alınarak kare matris içine yerleştirilir.

$$F = \begin{bmatrix} W & H & E & R \\ E & 0 & A & R \\ E & 0 & Y & O \\ U & 0 & 0 & 0 \end{bmatrix}_{4\,X\,4}$$

1. Oluşturulan mesaj matrisi sağdan sola $2x2$ tipinde alt matrislere bölünür.

$$A_1 = \begin{bmatrix} E & R \\ A & R \end{bmatrix} \qquad A_2 = \begin{bmatrix} W & H \\ E & 0 \end{bmatrix}$$

$$A_3 = \begin{bmatrix} Y & O \\ 0 & 0 \end{bmatrix} \qquad A_4 = \begin{bmatrix} E & 0 \\ U & 0 \end{bmatrix}$$

2. Alt matris sayısı $n = 4 > 3$ olduğundan $\left[\left|\frac{4}{2}\right|\right] = 2, k = 2$ olarak hesaplanır. Tablo 3.1'den yararlanılarak her bir harfe karşılık gelen sayılar bulunur ve $k = 2$ ötelenerek aşağıdaki tablo oluşturulur.

W	H	E	R	E	0	A	R	E	0	Y	O	U	0
24	9	6	19	6	28	2	19	6	28	26	16	22	28

3:.A_i ($1 \leq i \leq 4$) alt matrislerinin elemanları aşağıdaki şekilde oluşturulur.

$$a_1^1 = 6 \quad a_2^1 = 19 \quad a_3^1 = 2 \quad a_4^1 = 19$$

$$a_1^2 = 24 \quad a_2^2 = 9 \quad a_3^2 = 6 \quad a_4^2 = 28$$

$$a_1^3 = 26 \quad a_2^3 = 16 \quad a_3^3 = 28 \quad a_4^3 = 28$$

$$a_1^4 = 6 \quad a_2^4 = 28 \quad a_3^4 = 22 \quad a_4^4 = 28$$

4. Bu adımda her bir alt matrislerin determinantı alınır.

$$d_1 = detA_1 = 76$$

$$d_2 = \det A_2 = 618$$

$$d_3 = \det A_3 = 280$$

$$d_4 = \det A_4 = -448$$

5. Bundan önceki son iki adım kullanarak şifrelenmiş K matrisi oluşturulur. Bu matriste alt matrislerin dördüncü elemanları gizlenmiştir.

$$K = \begin{bmatrix} 76 & 6 & 19 & 2 \\ 618 & 24 & 9 & 6 \\ 280 & 26 & 16 & 28 \\ -448 & 6 & 28 & 22 \end{bmatrix}$$

Böylece şifrelenmiş metin karşı tarafa iletilir.

Çözme algoritması ise aşağıda detaylı olarak verilmiştir.

1. $k = 2$ için Q^2 matrisi hesaplanır.

$$Q^2 = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}$$

2. Her bir alt matris Q^2 matrisi ile çarpılır.

$$A_1.Q^2 = \begin{bmatrix} 6 & 19 \\ 2 & x_1 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 32 & 6 \\ x_1 + 4 & 2 \end{bmatrix}$$

$$A_2.Q^2 = \begin{bmatrix} 24 & 9 \\ 6 & x_2 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 57 & 24 \\ x_2 + 12 & 6 \end{bmatrix}$$

$$A_3.Q^2 = \begin{bmatrix} 24 & 16 \\ 28 & x_3 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 64 & 24 \\ x_3 + 56 & 28 \end{bmatrix}$$

$$A_4.Q^2 = \begin{bmatrix} 6 & 28 \\ 24 & x_4 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 40 & 6 \\ x_4 + 44 & 22 \end{bmatrix}$$

3. Yukarıdaki çarpım sonucu elde edilen eşitliğin her iki tarafının determinantı alınarak gizlenen (şifrelenen) elemanlar elde edilir.

$$x_1 = a_4^1 = 19$$
$$x_2 = a_4^2 = 28$$
$$x_3 = a_4^3 = 28$$
$$x_4 = a_4^4 = 28$$

4. Elde edilen şifrelenmiş bileşenler alt matrislerde yerlerine yazılır.

$$A_1 = \begin{bmatrix} 6 & 19 \\ 2 & 19 \end{bmatrix} \quad A_2 = \begin{bmatrix} 24 & 9 \\ 6 & 28 \end{bmatrix}$$

$$A_3 = \begin{bmatrix} 24 & 16 \\ 28 & 28 \end{bmatrix} \; A_4 = \begin{bmatrix} 6 & 28 \\ 24 & 28 \end{bmatrix}$$

5. 4. adımda bulunan A_1, A_2, A_3, A_4 alt matrisleri sırasıyla soldan sağa doğru aşağıdaki gibi K matrisine yerleştirilir.

$$\text{K} = \begin{bmatrix} 24 & 9 & 6 & 19 \\ 6 & 28 & 2 & 19 \\ 6 & 28 & 24 & 16 \\ 24 & 28 & 28 & 28 \end{bmatrix}$$

6. Son olarak K matrisinin her bir bileşeni k sayısı kadar geri ötelenip Tablo 3.1'deki karşılıkları alınarak şifre çözülür.

$$F = \begin{bmatrix} W & H & E & R \\ E & 0 & A & R \\ E & 0 & Y & O \\ U & 0 & 0 & 0 \end{bmatrix}_{4\,X\,4}$$

Böylece şifre çözülerek ana metin elde edilmiş olur.

7. K-MERTEBELİ FİBONACCİ SAYILARI İLE YENİ BİR KRİPTOGRAFİ ALGORİTMASI

Bu bölümde Tas ve diğ. (2018) makalesinde ifade edilen şifreleme algoritması baz alınarak daha genel yeni bir şifreleme algoritması oluşturulmuştur. Tas ve diğ. (2018) makalesinde temel metot, karşı tarafa iletilmek istenen mesaj matrisi $2x2$ tipindeki alt matrislere bölünerek elde edilirken, bu kısımda ise k-mertebeli Fibonacci matrisi kullanılarak daha genel forma dönüştürülmüştür. Bu yöntemde mesaj matrisi, kxk tipinde alt matrislere bölünür. Bu şifreleme algoritması genel olarak Tas ve diğ. (2018) makalesine benzer şekilde ilerlemektedir. Bu yöntem ile şifrelenen metnin deşifre edilebilmesi için k-mertebeli Fibonacci matrisi kullanılmıştır. Şifrelenen $k\ x\ k$ tipindeki metin matrisinde k asal sayı ise Tas ve diğ. (2018) de ifade edilen şifreleme algoritması ile şifrelenemezken, bu bölümde bahsedilen genelleştirilmiş şifreleme yöntemi ile kolaylıkla şifrelenir. k asal sayı değil ise $2x2$ tipindeki matrisler yerine daha büyük kare matrislere bölerek şifreleme gerçekleştirilir. k asal sayı ise kxk tipinde olan matrislere bölünür. Bu ise şifreleme işlemini hızlandırmaktadır.

Tanım 7.1: k -genelleştirilmiş Fibonacci sayıları $1 - k \leq n \leq 0$ aralığı için başlangıç değerleri

$$g_n^i = \begin{cases} 1, & eğer \quad i = 1 - n \\ 0, & diğer\ durumlarda \end{cases} \tag{7.1}$$

olmak üzere $n > 0$ ve $1 \leq i \leq k$ için $g_n^i = \sum_{j=1}^{k} g_{n-j}^i$ indirgeme bağıntısı ile tanımlanır. Yukarıda tanımlanan başlangıç koşulları ve indirgeme bağıntısında $i = k = 2$ seçilirse Fibonacci sayıları elde edilmiş olur.

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, …

$i = k = 3$ seçilirse Tribonacci sayıları elde edilir.

0, 1, 1, 2, 4, 7, 13, 24,…

Bu adımda ise Q-matris rolü oynayan $k\ x\ k$ boyutlu Q_k ve Q_k^n matrisleri aşağıdaki gibi tanımlanmıştır (Gürel, 2015).

$$Q_k = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}_{k\,x\,k} \qquad ve$$

$$Q_k = \begin{bmatrix} g_{n+1}^{(k)} & \cdots & g_n^{(k)} + g_{n-1}^{(k)} & g_n^{(k)} \\ g_n^{(k)} & \cdots & g_{n+1}^{(k)} + g_n^{(k)} & g_{n-1}^{(k)} \\ \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ g_{n-k+3}^{(k)} & \cdots & g_{n-k+2}^{(k)} + g_{n-k+1}^{(k)} & g_{n-k+2}^{(k)} \\ g_{n-k+2}^{(k)} & \cdots & g_{n-k+3}^{(k)} + g_{n-k+2}^{(k)} & g_{n-k+1}^{(k)} \end{bmatrix}_{k\,x\,k}$$

Yeni elde edilmiş olan bu algoritma aşağıda verilen örneklerle daha iyi ifade edilmiştir.

Örnek 7.1: "THE PEN IS MIGHTIER THAN THE SWORD" cümlesi aşağıda şifrelenmiştir. İlk olarak şifrelenecek metin boş kalan bileşenler yerine sıfır alınarak kare matris içine yerleştirilir.

$$F = \begin{bmatrix} T & H & E & 0 & P & E \\ N & 0 & I & S & 0 & M \\ I & G & H & T & I & E \\ R & 0 & T & H & A & N \\ 0 & T & H & E & 0 & S \\ W & O & R & D & 0 & 0 \end{bmatrix}_{6X6}$$

1. Oluşturulan mesaj matrisi sağdan sola 3 x 3 tipinde alt matrislere bölünür.

$$\mathrm{A}_1 = \begin{bmatrix} 0 & P & \mathrm{E} \\ S & 0 & M \\ \mathrm{T} & I & \mathrm{E} \end{bmatrix} \qquad \mathrm{A}_2 = \begin{bmatrix} \mathrm{T} & H & \mathrm{E} \\ N & 0 & I \\ \mathrm{I} & G & \mathrm{H} \end{bmatrix}$$

$$\mathrm{A}_3 = \begin{bmatrix} \mathrm{H} & A & \mathrm{N} \\ E & 0 & S \\ \mathrm{D} & 0 & 0 \end{bmatrix} \qquad \mathrm{A}_4 = \begin{bmatrix} \mathrm{R} & 0 & \mathrm{T} \\ 0 & T & H \\ \mathrm{W} & O & \mathrm{R} \end{bmatrix}$$

2. Alt matris sayısı $n = 4 > 3$ olduğundan $\left[\left|\frac{4}{2}\right|\right] = 2$, $k = 2$ olarak hesaplanır. Tablo 3.1'den yararlanılarak her bir harfe karşılık gelen sayılar bulunur ve $k = 2$ ötelenerek aşağıdaki tablo oluşturulur.

T	H	E	0	P	E	N	0	I	S	0
21	9	6	28	17	6	15	28	10	20	28

M	I	G	H	T	I	E	R	0	T	H	A	N	0	T	H	E
14	10	8	9	21	10	6	19	28	21	9	2	15	28	21	9	6

0	S	W	O	R	D	0	0
28	20	24	16	19	5	28	28

3. A_i ($1 \leq i \leq 4$) alt matrislerinin elemanları aşağıdaki şekilde oluşturulur.

$a_1^1 = 28 \;\; a_2^1 = 17 \;\; a_3^1 = 6 \;\; a_4^1 = 20 \;\; a_5^1 = 28 \;\; a_6^1 = 14 \;\; a_7^1 = 21$

$a_8^1 = 10 \;\; a_9^1 = 6$

$a_1^2 = 21 \;\; a_2^2 = 9 \;\; a_3^2 = 6 \;\; a_4^2 = 15 \;\; a_5^2 = 28 \;\; a_6^2 = 10 \;\; a_7^2 = 10$

$a_8^2 = 8 \;\; a_9^2 = 9$

$a_1^3 = 9 \;\; a_2^3 = 2 \;\; a_3^3 = 15 \;\; a_4^3 = 6 \;\; a_5^3 = 28 \;\; a_6^3 = 20 \;\; a_7^3 = 5$

$a_8^3 = 28 \;\; a_9^3 = 28$

$a_1^4 = 19 \;\; a_2^4 = 28 \;\; a_3^4 = 21 \;\; a_4^4 = 28 \;\; a_5^4 = 21 \;\; a_6^4 = 9 \;\; a_7^4 = 24$

$a_8^4 = 16 \;\; a_9^4 = 19$

4. Bu adımda ise her bir alt matrislerin determinantı alınır.

$$d_1 = detA_1 = 1414$$

$$d_2 = \det A_2 = 2337$$

$$d_3 = \det A_3 = 2300$$

$$d_4 = \det A_4 = -5179$$

5. Bundan önceki son iki adım kullanarak K matrisini oluşturulur. Bu matriste alt matrislerin dördüncü elemanları gizlenmiştir.

$$K = \begin{bmatrix} 1414 & 28 & 17 & 20 & 28 & 14 & 21 & 10 & 6 \\ 2337 & 21 & 9 & 15 & 28 & 10 & 10 & 8 & 9 \\ 2300 & 9 & 2 & 6 & 28 & 20 & 5 & 28 & 28 \\ -5179 & 19 & 28 & 28 & 21 & 9 & 24 & 16 & 19 \end{bmatrix}$$

Böylece şifrelenmiş metin karşı tarafa iletilir.

Çözme algoritması ise aşağıdaki şekildedir.

1. $k = 2$ için Q^2 matrisi hesaplanır.

$$Q^2 = \begin{bmatrix} 2 & 2 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

2. Her bir alt matris Q^2matrisi ile çarpılır.

$$A_1.Q^2 = \begin{bmatrix} 28 & 17 & x_1 \\ 20 & 28 & 14 \\ 21 & 10 & 6 \end{bmatrix} \begin{bmatrix} 2 & 2 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} x_1 + 73 & 73 & 45 \\ 82 & 68 & 48 \\ 58 & 52 & 31 \end{bmatrix}$$

$$A_2.Q^2 = \begin{bmatrix} 21 & 9 & x_1 \\ 15 & 28 & 10 \\ 10 & 8 & 9 \end{bmatrix} \begin{bmatrix} 2 & 2 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} x_2 + 51 & 51 & 30 \\ 68 & 58 & 43 \\ 37 & 28 & 18 \end{bmatrix}$$

$$A_3.Q^2 = \begin{bmatrix} 9 & 2 & x_3 \\ 6 & 28 & 20 \\ 5 & 28 & 28 \end{bmatrix} \begin{bmatrix} 2 & 2 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} x_3 + 20 & 20 & 11 \\ 60 & 40 & 34 \\ 66 & 38 & 33 \end{bmatrix}$$

$$A_4.Q^3 = \begin{bmatrix} 19 & 28 & x_4 \\ 28 & 21 & 9 \\ 24 & 16 & 19 \end{bmatrix} \begin{bmatrix} 2 & 2 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} x_4 + 66 & 66 & 47 \\ 86 & 77 & 49 \\ 83 & 64 & 40 \end{bmatrix}$$

3. Yukarıdaki çarpım sonucu elde edilen eşitliğin her iki tarafının determinantı alınarak gizlenen (şifrelenen) elemanlar elde edilir.

$$x_1 = a_4^1 = 6$$
$$x_2 = a_4^2 = 6$$
$$x_3 = a_4^3 = 15$$

$$x_4 = a_4^4 = 21$$

4. Elde edilen şifrelenmiş bileşenler alt matrislerde yerlerine yazılır.

$$A_1 = \begin{bmatrix} 28 & 17 & \mathbf{6} \\ 20 & 28 & 14 \\ 21 & 10 & 6 \end{bmatrix} A_2 = \begin{bmatrix} 21 & 9 & \mathbf{6} \\ 15 & 28 & 10 \\ 10 & 8 & 9 \end{bmatrix}$$

$$A_3 = \begin{bmatrix} 9 & 2 & \mathbf{15} \\ 6 & 28 & 20 \\ 5 & 28 & 28 \end{bmatrix} A_4 = \begin{bmatrix} 19 & 28 & \mathbf{21} \\ 28 & 21 & 9 \\ 24 & 16 & 19 \end{bmatrix}$$

5. 4**.** adımda bulunan A_1, A_2, A_3, A_4 alt matrisleri sırasıyla soldan sağa doğru aşağıdaki gibi K matrisine yerleştirilir.

$$F = \begin{bmatrix} 21 & 9 & 6 & 28 & 17 & 6 \\ 15 & 28 & 10 & 20 & 28 & 14 \\ 10 & 8 & 9 & 21 & 10 & 6 \\ 19 & 28 & 21 & 9 & 2 & 15 \\ 28 & 21 & 9 & 6 & 28 & 20 \\ 24 & 16 & 19 & 5 & 28 & 28 \end{bmatrix}_{6X6}$$

6. Son adımda ise K matrisinin her bir bileşeni k sayısı kadar geri ötelenip Tablo 3.1'deki karşılıkları alınarak şifre çözülür.

$$F = \begin{bmatrix} T & H & E & 0 & P & E \\ N & 0 & I & S & 0 & M \\ I & G & H & T & I & E \\ R & 0 & T & H & A & N \\ 0 & T & H & E & 0 & S \\ W & O & R & D & 0 & 0 \end{bmatrix}_{6X6}$$

Şimdi ise bu algoritma ile ilgili son örnek aşağıda verilmiştir.

Örnek 7.2: "I LIKE TURKISH VAN CATS" cümlesi k-mertebeli Fibonacci sayıları kullanılarak elde edilen şifreleme algoritması ile aşağıdaki şekilde şifrelenmiştir. Şifrelenecek metin boş kalan bileşenler yerine sıfır alınarak kare matris içine yerleştirilir.

$$F = \begin{bmatrix} I & 0 & L & I & K \\ E & 0 & T & U & R \\ K & I & S & H & 0 \\ V & A & N & 0 & C \\ A & T & S & 0 & 0 \end{bmatrix}_{5X5}$$

1. Oluşturulan mesaj matrisi sağdan sola $5x5$ tipinde alt matrislere bölünür.

$$\mathrm{A}_1 = \begin{bmatrix} I & 0 & L & I & K \\ E & 0 & T & U & R \\ K & I & S & H & 0 \\ V & A & N & 0 & C \\ A & T & S & 0 & 0 \end{bmatrix}_{5X5}$$

2. Alt matris sayısı $n = 1 < 3$ olduğundan $n = k = 1$, $k = 1$ olarak hesaplanır. Tablo 3.1'den yararlanılarak her bir harfe karşılık gelen sayılar bulunur ve $k = 1$ ötelenerek aşağıdaki tablo oluşturulur.

I	0	L	I	K	E	0	T	U	R	K	I	S	H
9	27	12	9	11	5	27	20	21	18	11	9	19	8

0	V	A	N	0	C	A	T	S	0	0
27	22	1	14	27	3	1	20	19	27	27

3. A_i ($1 \leq i \leq 4$) alt matrislerinin elemanları aşağıdaki şekilde oluşturulur.

$a_1^1 = 9$ $a_2^1 = 27$ $a_3^1 = 12$ $a_4^1 = 9$ $a_5^1 = 11$ $a_6^1 = 5$ $a_7^1 = 27$

$a_8^1 = 20$ $a_9^1 = 21$ $a_{10}^1 = 18$ $a_{11}^1 = 11$ $a_{12}^1 = 9$ $a_{13}^1 = 19$ $a_{14}^1 = 8$

$a_{15}^1 = 27$ $a_{16}^1 = 22$ $a_{17}^1 = 1$ $a_{18}^1 = 14$ $a_{19}^1 = 27$ $a_{20}^1 = 3$ $a_{21}^1 = 1$

$a_{22}^1 = 20$ $a_{23}^1 = 19$ $a_{24}^1 = 27$ $a_{25}^1 = 27$

4. Bu adımda her bir alt matrislerin determinantını alınır.

$$d_1 = detA_1 = 1759340$$

5. Bundan önceki son iki adım kullanarak K matrisi oluşturulur. Bu matriste alt matrislerin dördüncü elemanları gizlenmiştir.

K =

[1759340 9 27 12 9 5 27 20 21 18 11 9 19 8 27 22 1

14 27 3 1 20 19 27 27]

Böylece şifrelenmiş metin karşı tarafa iletilir.

Bu şifreli metinin deşifre edilmesi için ise çözme algoritması aşağıda detaylı olarak verilmiştir.

1. Öncelikle $k = 1$ için Q^1 matrisi hesaplanır.

$$Q^1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}_{5X5}$$

2. Her bir alt matris Q^1matrisi ile çarpılır.

$$\text{B.}Q^1 = \begin{bmatrix} 9 & 27 & 12 & 9 & x \\ 5 & 27 & 20 & 21 & 18 \\ 11 & 9 & 19 & 8 & 27 \\ 22 & 1 & 14 & 27 & 3 \\ 1 & 20 & 19 & 27 & 27 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 36 & 21 & 18 & x+9 & 9 \\ 32 & 25 & 26 & 23 & 5 \\ 20 & 30 & 19 & 38 & 11 \\ 23 & 36 & 49 & 25 & 22 \\ 21 & 20 & 28 & 28 & 1 \end{bmatrix}$$

3. Yukarıdaki çarpım sonucu elde edilen eşitliğin her iki tarafının determinantı alınarak gizlenen (şifrelenen) elemanlar elde edilir.

$$x_1 = a_4^1 = 11$$

4. Elde edilen şifrelenmiş bileşenler alt matrislerde yerlerine yazılır.

$$A_1 = \begin{bmatrix} 9 & 27 & 12 & 9 & 11 \\ 5 & 27 & 20 & 21 & 18 \\ 11 & 9 & 19 & 8 & 27 \\ 22 & 1 & 14 & 27 & 3 \\ 1 & 20 & 19 & 27 & 27 \end{bmatrix}$$

5. 4. adımda bulunan A_1 alt matrisinin bileşenleri satır olarak sırasıyla soldan sağa doğru aşağıdaki K matrisinde yerleştirilir.

$$F = \begin{bmatrix} 9 & 27 & 12 & 9 & 11 \\ 5 & 27 & 20 & 21 & 18 \\ 11 & 9 & 19 & 8 & 27 \\ 22 & 1 & 14 & 27 & 3 \\ 1 & 20 & 19 & 27 & 27 \end{bmatrix}$$

6. Bu adımda ise K matrisinin her bir bileşeni k sayısı kadar ötelenip Tablo 3.1'deki karşılıkları alınarak şifre çözülür.

$$F = \begin{bmatrix} I & 0 & L & I & K \\ E & 0 & T & U & R \\ K & I & S & H & 0 \\ V & A & N & 0 & C \\ A & T & S & 0 & 0 \end{bmatrix}$$

Böylece "I LIKE TURKISH VAN CATS" ana metni elde edilmiş olur.

8. KAYNAKLAR

Afacan, E., *Kriptografiye giriş,* Ankara: Sözkesen matbaası, (2016).

Aktaş, A., "k-Pell Sayıları ve Polinomları", Yüksek Lisans Tezi, *Erzincan Binali Yıldırım Üniversitesi Fen Bilimler Enstitüsü,* Matematik Ana Bilim Dalı, Erzincan, (2021).

Gould, H. W., A history of the Fibonacci Q-matrix and a higher-dimensional problem, *Fibonacci Quart.* 19, 7-250, (1981).

Gürel, G., "K. Mertebeden Gauss Fibonacci ve K. Mertebeden Gauss Lucas İndirgeme Bağıntıları", Doktora Tezi, *Pamukkale Üniversitesi Fen Bilimler Enstitüsü,* Matematik Ana Bilim Dalı, Denizli, (2015).

Horadam, A. F., "A Generalized Fibonacci Sequence", *American Math. Monthly,* 68(5), 455-459, (1961).

King, C. H., "Some Properties of Fibonacci Numbers", Master's Thesis, *San Jose State College,* San Jose, CA, (1960).

Koshy, T. "Fibonacci and Lucas Numbers with Applications", *A Wiley-Interscience Publication,* (2001).

Lee, G. Y., Lee, S. G., Kim J., S., Shin, H. K., "The Binet Formula and Representations of k-Generalized Fibonacci Numbers", *The Fibonacci quart.,* 39(2), 158-164, (2001).

Özyılmaz, Ç., "Kriptolojiye giriş", Yüksek Lisans Tezi, *Karabük Üniversitesi Fen Bilimler Enstitüsü,* Matematik Ana Bilim Dalı, Karabük, (2014).

Stakhov, A. P., "A Generalized of the Fibonacci Q-matrix", *Rep. Nat. Acad. Sci., Ukraine,* 9, 46-49, (1999).

Topal, N., "Genelleştirilmiş Fibonacci ve Lucas Kuaterniyonları ve Bazı Uygulamaları", Yüksek Lisans Tezi, *Sakarya Üniversitesi Fen Bilimleri Enstitüsü,* Matematik Ana Bilim Dalı, Sakarya, (2018).

Ucar., S., Tas., N., Ozgur., N. Y., "A new cryptography model via and lucas numbers", *Mathematical sciences and Applications E-Notes,* 7 (1) 62-70 (2019).

Ucar., S., Tas., N., Ozgur., N. Y., Kaymak., O. K., "A New Coding/Decoding Algorithm Using Fibonacci Numbers", *Discrete Mathematics, Algorithms and Applications,* 10 (2), 1850028 (2018).

Yeşilbaş, E., "Cebirsel kriptoloji yöntemleri ve bazı uygulamalar", Yüksek Lisans Tezi, *Recep Tayyip Erdoğan Üniversitesi Fen Bilimleri Enstitüsü,* Matematik Ana Bilim Dalı, Rize, (2016).