T.C.
NECMETTİN ERBAKAN
ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

r –CİRCULANT MATRİSLER İLE AFFİNE HİLL ŞİFRELEME VARYASYONU

Şeyma YILDIRIM

YÜKSEK LİSANS TEZİ

Matematik Anabilim Dalı

Haziran - 2024
KONYA
Her Hakkı Saklıdır

TEZ KABUL VE ONAYI

Şeyma YILDIRIM tarafından hazırlanan "**r-Circulant Matrisler ile Affine Hill Şifreleme Varyasyonu**" adlı tez çalışması 27 / 06 / 2024 tarihinde aşağıdaki jüri tarafından **oy birliği** ile Necmettin Erbakan Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda YÜKSEK LİSANS olarak kabul edilmiştir.

Jüri Üyeleri	**İmza**
Başkan Prof. Dr. Ahmet İPEK	……..
Danışman Doç. Dr. Fikri KÖKEN	……..
Üye Prof. Dr. Emine Gökçen KOÇER	……..

Fen Bilimleri Enstitüsü Yönetim Kurulu'nun …./…/20.. gün ve …….. sayılı kararıyla onaylanmıştır.

Prof. Dr. Havvanur UÇBEYİAY
FBE Müdürü

TEZ BİLDİRİMİ

Bu tezdeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edildiğini ve tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

DECLARATION PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

İmza

Şeyma YILDIRIM

Tarih:

ÖZET

YÜKSEK LİSANS TEZİ

r −CİRCULANT MATRİSLER İLE AFFİNE HİLL ŞİFRELEME VARYASYONU

Şeyma YILDIRIM

Necmettin Erbakan Üniversitesi Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Danışman: Doç. Dr. Fikri KÖKEN

2024, 75 Sayfa

Jüri

Prof. Dr. Emine Gökçen KOÇER
Prof. Dr. Ahmet İPEK
Doç. Dr. Fikri KÖKEN

İlk olarak kriptografi bilimi için gerekli temel ve teoremler verilirken, her sistem için belirlediğimiz temel bir cümle örnek olarak değerlendirildi. Genel olarak ele alınan gizli anahtarlı Hill şifreleme ile açık anahtarlı RSA ve El-Gamal şifreleme sistemlerinin birleştirilmesi ile melez bir şifreleme yöntem önerisi verildi.

Simetrik şifrelemenin öncülerinden Hill şifrelemenin gizli anahtarı, asimetrik şifrelemenin öncülerinden RSA ve El-Gamal şifreleme yöntemleri şifrelenerek ortaya melez bir yöntem ortaya konulur. Ayrıca, Hill şifrelemeyi genelleştirmek için Affine vektörü eklemesi kullanıldı.

Affine Hill şifreleme yönteminde gizli anahtar olarak $n \times n$ mertebeden r-Circulant matrisleri ele alınarak, metin şifreleme ve deşifreleme süreçlerini incelendi. Fakat, anahtar matrisin basit ifade edilebilmesi için belirli parametreler alfabe değişkeni, matris boyutu ve matris r değişkeni $(t, n, r,)$ ile, sırasıyla, matris elemanları için Fibonacci veya Lucas dizisi, diziler için indis başlangıç değeri ve artım miktarı değişkenleri $(dizi, s, l)$ kullanıldı. Gizli anahtarının güvenli aktarılması için bu değişkenleri RSA veya El-Gamal şifreleme yöntemleri kullanılarak gönderilmesi düşünüldü.

Bu melez bir şifreleme yöntemindeki değişkenler ile örneklemler ortaya konulur. Bir programlama dili içinde sisteme ait program yazılarak $(t, n, r,)$ ve $(Fibonacci, s, l)$ veya $(Lucas, s, l)$ değişkenlerinin farklı değeri için "Matematikte zekadan önce sabır gelir" ifadesi ait şifreli metinlerin, belirlenen parametrelere bağlı olarak nasıl değiştiği tablolar ile gösterildi. Bu tablolar ile, şifreleme sürecinin ve değişkenlerin şifreli metni nasıl etkilediği görsel olarak sunuldu.

Anahtar Kelimeler: Affine Hill Şifreleme, Circulant Matrisler, El-Gamal Şifreleme, Melez Şifreleme Metodu, RSA Şifreleme

ABSTRACT

MS THESIS

AFFINE HILL ENCRYPTION VARIATION WITH r-CIRCULANT MATRICES

Şeyma YILDIRIM

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

Advisor: Assoc. Prof. Dr. Fikri KÖKEN

2024, 75 Pages

Jury

Prof. Dr. Emine Gökçen KOÇER
Prof.Dr. Ahmet İPEK
Assoc. Prof. Dr. Fikri KÖKEN

First, the theorems and definations of cryptography are presented, and a basic sentence is used as an example for each system. A hybrid encryption method is generally proposed by combining the Hill cipher with the public-key RSA and El-Gamal ciphers.

A hybrid method is proposed by encrypting the secret key of Hill encryption, a pioneer of symmetric encryption, and RSA and El-Gamal encryption, pioneers of asymmetric encryption. Furthermore, Affine vector addition is used to generalize Hill encryption.

In the Affine Hill encryption method, n-square r-Circulant matrices are considered as the secret key and the text encryption and decryption processes are analyzed. However, for a simple expression of the key matrix, certain parameters are used such as the alphabet variable, the matrix size and the matrix r variable (t, n, r) and, respectively, the Fibonacci or Lucas sequence for the matrix elements, the index initial value and the increment amount variables $(array, s, l)$ for the arrays. For secure transmission of the secret key, these variables are considered to be sent using RSA or El-Gamal encryption methods.

This is a hybrid encryption method in which variables and samples are introduced. By writing a program of the system in a program language, tables show how the ciphertexts of the phrase “Patience comes before intelligence in mathematics” for different values of the variables (t, n, r) and $(Fibonacci, s, l)$ or $(Lucas, s, l)$ change depending on the determined parameters. With these tables, it is visually presented how the encryption process and the variables affect the ciphertext.

Keywords: Affine Hill Cipher, Circulant Matrices, El-Gamal Cipher, Hybrid Encryption Method, RSA Cipher

ÖNSÖZ

Tez yazarken kızımızla ilgilenip bana zaman tanıyan ve beni daima mutlu edip çalışmama teşvik eden çok kıymetli hayat arkadaşım Mehmet YILDIRIM'a ne kadar teşekkür etsem azdır.

Tez yazmaya başladığımda aklımda dahi olmayıp şu an bir yaşında olacak olan kızım Ahsen'e, şirinlikleriyle beni her zaman motive ettiği için teşekkür ederim.

Anne olunca anneliğin kıymetini tekrar fark ettim. Bu sebeple çalışmama manevi büyük destek olan anneme ayrı bir kısım ayırmak isterim. Senin kızın olmaktan hep gurur duydum. Teşekkür ederim anne.

Çalışmamda destekleriyle her zaman yanımda hissettiğim babama, kardeşime ve çalışmama şiiriyle katkı sağlayan amcam Ahmet ÖZMEN'e teşekkürlerimi sunarım.

Aynı anda teze başlayıp sürekli birbirimizi motive ettiğimiz yol arkadaşım Naciye KERVAN'a teşekkür ederim.

Yaptığım bu çalışmada olumlu tavrıyla beni cesaretlendiren, bilgi birikimi ile çalışmama farklı açılardan bakmamı sağlayan, tezimde çok büyük emekleri olan, iyi ki öğrencisiyim dediğim ve bununla onur duyduğum çok kıymetli danışman hocam Doç. Dr. Fikri KÖKEN'e sonsuz teşekkürlerimi sunarım.

Ayrıca tezimdeki algoritma kısımlarına yardımcı olan Dr. Öğr. Üyesi Halime ERGÜN'e teşekkürü bir borç bilir ve çok teşekkür ederim.

Şeyma YILDIRIM
KONYA-2024

İÇİNDEKİLER

ÖZET ..... **iv**

ABSTRACT ..... **v**

ÖNSÖZ ..... **vi**

İÇİNDEKİLER ..... **vii**

SİMGELER VE KISALTMALAR ..... **iv**

TABLOLAR VE ŞEKİLLER TABLOSU ..... **v**

1. GİRİŞ **6**

1.1 Sayılar Teorisindeki Temel Tanımlar ve Teoremler 6
1.1.1 Modüler Aritmetik İle İlgili Bilgiler 6
1.1.2 Fibonacci ve Lucas Dizileri İle İlgili Bilgiler 8
1.2 Matrisler ve Bazı Özellikleri 9
1.2.1 Fibonacci ve Lucas Matrisleri ve Özellikleri 11
1.2.2 Circulant Matrisler ve Özellikleri 15
1.3 Şifreleme Biliminde Kullanılan Temel Tanımlar ve Bazı Özellikler 18
1.3.1 Şifreleme Çeşitleri ve Karşılaştırmaları 20
1.3.2 Hill Şifreleme 32
1.3.3 Affine-Hill Şifreleme 37

2. KAYNAK ARAŞTIRMASI **42**

2.1 Hill Şifreleme İle İlgili yapılan Çalışmalar 42
2.2 Circulant Matris İle İlgili Yapılan Çalışmalar 45

3. r-CİRCULANT MATRİSLER İLE AFFİNE HİLL ŞİFRELEME **47**

3.1 Melez Affine-Hill Şifreleme 47
3.2 Uygulama Örnekleri 62

4. SONUÇLAR VE ÖNERİLER **67**

4.1 Sonuçlar 67
4.2 Öneriler 67

5. KAYNAKLAR **69**

EKLER **72**

SİMGELER VE KISALTMALAR

$\mathbb{Z}$	Tam sayılar kümesi
$\mathbb{Z}_m$	m modülüne göre kalan sınıfları kümesi
Z_n^*	Z_n'in çarpımsal grubu
$\equiv$	Denklik simgesi
$\bar{a}$	a elemanına ait denklik sınıfı
$\|a\|$	a tamsayısının mutlak değeri
$ebob(a,b)$	a, b tam sayılarının en büyük ortak böleni
$\varphi(n)$	n tamsayısı için Euler'in φ fonksiyonu
F_n	n'inci Fibonacci sayısı
L_n	n'inci Lucas sayısı
α, β	Altın oran, $1-\alpha=\beta=(1-\sqrt{5})/2$ oran
$A_{n\times m}=[a_{ij}]$	Dikdörtgen matris gösterimi
$det(A)=\|A\|$	A matrisinin determinantı
A^T	A matrisinin taranspozu
$\overline{A}$	A matrisinin eşlenik
A^*	A matrisinin eşlenik transpozu
$sgn(\sigma)$	σ permütasyonun işaret fonksiyonu
m_{ij}	a_{ij} elemanına ait minör
c_{ij}	a_{ij} nin işaretli minörü (kofaktörü)
A^{-1}	A matrisinin tersi
S_n	n elemanlı permütasyonlar kümesi
$GL(n,F)$	F cismi üzerinde genel lineer grup
$SL(n,F)$	F cismi üzerinde özel lineer grup
$C_n(F)$	F cismi üzerinde $n\times n$ tipinde bir Circulant matris
π_n	$(0,1,0,\ldots,0), n\times n$ tipinde bir permütasyon matris
$C_{n,r}$	$r-$circulant matris
$C_{n,s}$	Semi Circulant matris
SC_n	Skew Circulant (negacyclic) matris
$G_{n^2,c}$	G_n matrisi için katsayı (coefficient) matrisi
RSA	Asimetrik bir şifreleme metodu (Rivest-Shamir-Adleman)
(n,e)	RSA algoritması için açık anahtar
d	RSA algoritması için özel anahtar
El-Ga	Asimetrik bir şifreleme metodu-El Gamal metodu
(p,β,β^a)	El Gamal algoritması için açık anahtar
a	El Gamal algoritması için özel anahtar

TABLOLAR VE ŞEKİLLER TABLOSU

Tablo 1.1 Şifreleme Metotları 21
Tablo 1.2 Türk alfabesinin sayısal değerlerin bir örneği 22
Tablo 1.3 Ceaser şifreleme ile harflerin karşılığı 22
Tablo 1.4 El Gamal ile sayısal değerin şifrelenmiş değerleri 30
Tablo 1.5 El Gamal ile şifrelenmiş değerlerin sayısal değerleri ve karakterleri 31
Tablo 1.6 Düz metindeki karakterlerin sayısal değerleri 33
Tablo 1.7 Şifrelenmiş metindeki sayısal değerler 34
Tablo 1.8 Sayısal değerlerin şifrelenmiş harf karşılıkları 34
Tablo 1.9 Şifrelenmiş harflerin sayısal değer karşılıkları 36
Tablo 1.10 Düz metindeki sayısal değerler 36
Tablo 1.11 Sayısal değerlerin düz metindeki karakter değerleri 37
Tablo 1.12 Düz metindeki karakterlerin sayısal değerleri 38
Tablo 1.13 Şifrelenmiş metindeki sayısal değerler 38
Tablo 1.14 Sayısal değerlerin şifrelenmiş harf karşılıkları 39
Tablo 1.15 Şifrelenmiş harflerin sayısal değer karşılıkları 40
Tablo 1.16 Düz metindeki sayısal değerler 40
Tablo 1.17 Sayısal değerlerin düz metindeki karakter değerleri 41
Tablo 3.1 Harf, karakter ve-sayısal değerlerin t parametresine bağlı sayısal değerleri. 48
Tablo 3.2 Düz metnin $t = 5$ için sayısal değer karşılıkları 53
Tablo 3.3 Sayısal değerlerin şifrelenmiş harf karşılıkları 56
Tablo 3.4 Şifrelenmiş harf karşılıklarının sayısal değerleri 59
Tablo 3.5 Sayısal değerlerin deşifrelenmiş harf karşılıkları 61
Tablo 3.6 t, n, r, s, l değişkenlerine göre Fibonacci sayıları örneklemi 63
Tablo 3.7 t, n, r, s, l değişkenlerine göre Lucas sayıları örneklemi 64
Tablo 5.1 Tablo 3.1'de $t = 8$ değerine göre düz metnin sayısal değerleri 72
Tablo 5.2 Şifrelenmiş metne ait sayısal değerler 72
Tablo 5.3 Şifrelenmiş metnin 36'lı blok hali 73
Tablo 5.4 Düz metnin 36'lı blok hali 73
Tablo 5.5 Şifrelenmiş metne ait sayısal değerler 74
Tablo 5.6 Şifrelenmiş metnin 36'lı blok hali 74
Tablo 5.7 Düz metnin 36'lı blok hali 75

Şekil 3.1 Affine Hill şifreleme, RSA ve El-Gamal yöntemleri ile şifreleme şeması 51
Şekil 3.2 Affine Hill şifreleme, El-Gamal ve RSA yöntemleri ile şifreleme şeması 51
Şekil 3.3 RSA, El-Gamal ve Affine Hill şifreleme yöntemleri ile deşifreleme şeması 52
Şekil 3.4 El-Gamal, RSA ve Affine Hill şifreleme yöntemleri ile deşifreleme şeması 52
Şekil 3.5 Affine Hill şifreleme ve deşifreleme yöntemi akış şeması 62

1. GİRİŞ

Bu bölümde, tez çalışmamız içerisinde kullanılacak olan sayılar teorisi, matris teorisi ve kriptoloji ile ilgili genel bilgilere değinilecektir.

1.1 Sayılar Teorisindeki Temel Tanımlar ve Teoremler

En temel denklik bağıntısı örneklerinden olan kalan sınıfları, kriptoloji bilimi için çok önemli bir kavramdır. Çünkü denklik bağıntısı ile denklik sınıfları oluşturularak küme parçalanışını garanti edilir. Modüler aritmetik ile ilgili temel teoremler ve özelliklerinden bahsedilir. Ayrıca, tamsayı dizilerinin en önemli örneklerinden Fibonacci ve Lucas dizileri hakkında genel bilgiler verilir (Grimaldi, 2011), (Debnath, 2011), (Altındiş, 2011), (Cangül ve Çelik, 2013), (Koshy, 2019).

1.1.1 Modüler Aritmetik İle İlgili Bilgiler

Tanım 1.1 m bir pozitif tam sayı, a ve b tam sayılar olmak üzere, eğer $a-b$, m'nin bir tam sayı katı ise, a, b'ye mod m de denktir denilir ve $a \equiv b \ (mod\, m)$ şeklinde yazılır.

$$8 \equiv 1 \ (mod\, 7) \qquad 19 \equiv 4 \ (mod\, 5)$$
$$-1 \equiv 32 \ (mod\, 33) \qquad 16 \equiv 0 \ (mod\, 4)$$

Tanım 1.2 $\mathbb{Z}$ tam sayılar kümesi üzerindeki, " $\equiv$ " denklik bağıntısının belirtiği denklik sınıflarına, m modülüne göre $(mod\, m)$ kalan sınıfları denir ve tüm kalan sınıfları kümesi $\mathbb{Z}_m$ ile gösterilir. $a \in \mathbb{Z}$'nın denklik sınıfı, $\bar{a} = \{x \in \mathbb{Z} : m|a-x\}$ şeklindedir.

Herhangi bir m modu için her a tam sayısının mod m de tam olarak

$$0,1,2,\ldots,m-1$$

tam sayılarından birisine denk olduğu bilinmektedir. Bu tam sayıya a'nın mod m'de kalanı denir ve mod m deki kalanların kümesini göstermek için

$$Z_m = \{0,1,2,\ldots,m-1\}$$

yazılabilir.

Eğer a negatif olmayan bir tam sayı ise, a'nın $mod\, m$ de kalanı a'nın m ile bölümünde kalandır. Herhangi bir a tam sayısı için, kalan aşağıdaki teorem kullanılarak bulunabilir.

Teorem 1.1 Herhangi bir a tam sayısı ve m modu için,

$$R = \frac{|a|}{m} \tag{1.1}$$

olur ki buna göre, a nın $modm$'deki kalanı r olmak üzere

$$r = \begin{cases} R & eğer \text{ a} \geq 0 \; ise \\ m - R & eğer \text{ a<0 ve } R \neq 0 \; ise \\ 0 & eğer \text{ a<0 ve } R = 0 \; ise \end{cases} \quad (1.2)$$

şeklinde verilir.

Tanım 1.3 a, Z_m de bir sayı olmak üzere, eğer $aa^{-1} = a^{-1}a \equiv 1(mod\, m)$ ise, Z_m deki a^{-1} sayısına mod m de a nın bir tersi veya çarpımsal tersi denir.

Tanım 1.4 $ax \equiv b\ (mod\, m)$ şeklindeki bir denkleme bir bilinmeyenli lineer kongrüans denir. Bu denklemi sağlayan x tamsayılarının kümesine de kongrüansin çözüm kümesi denir.

$ax \equiv b\ (mod\, m)$'nin bir çözümü $x_0 \in \mathbb{Z}$ ise $\overline{x_0} \in \mathbb{Z}_m$ sınıfındaki tüm sayılar da bir çözümdür. $(a, m) = 1$ ise $ax \equiv b\ (mod\, m)$'nin çözümü var ve bu $(mod\, m)$'ye göre tek bir sınıftır.

$(2,5) = 1$ olduğundan $2x \equiv 1\ (mod\, 5)$'nin çözümü vardır ve lineer kongrüans denkleminin çözüm kümesi $Ç = \{\dots, -7, -2, 3, 8, 13, \dots\}$.'dir.

$ax \equiv b\ (mod\, m)$'nin bir çözümünün olması için gerek ve yeter şart $(a, m)|b$ olmasıdır.

Her $b \in \mathbb{Z}_m$ için $ax \equiv b\ (mod\, m)$ denkleminin tek türlü bir $x \in \mathbb{Z}_m$ çözümünün olması için gerek ve yeter şart $(a, m) = 1$ olmasıdır.

Eğer a ve m ortak asal çarpına sahip değillerse, a nın m modunda tek terse sahip olduğu ve tersine a ve m ortak asal çarpanına sahiplerse, a nın m modunda bir terse sahip olmadığı gösterilebilir.

$a \in Z$ olsun. a'nın $mod\, m$'e göre çarpımsal tersi $ax \equiv 1\ (mod\, m)$ olacak şekilde $x \in Z_m$ bir x tamsayısı mevcutsa tektir ve a'ya terslenebilir denir. a'nın tersi a^{-1} ile ifade edilir.

Z_m'in çarpımsal grubu $Z_m^* = \{a \in Z_m : (a, m) = 1\}$ dir. Özel olarak m asal ise $Z_m^* = \{a \in Z_m : 1 \leq a \leq n - 1\}$ dir.

n'yi geçmeyen $(n \geq 1)$ ve n ile aralarında asal olan pozitif tamsayıların sayısı $\varphi(n)$ ile gösterilir ve Eulerin φ fonksiyonu olarak adlandırılır. Kısaca

$$\varphi(n) = \{x \in \mathbb{Z} : 0 \leq x \leq n - 1, (x, n) = 1\}$$

şeklinde tanımlanır.

$n, m \geq 1$ ve $(n, m) = 1$ ise $\varphi(nm) = \varphi(n)\varphi(m)$ olur ki buradaki asallık şartı kaldırılamaz.

$\varphi(1) = 1$ ve p asal olmak üzere $\varphi(p) = p - 1$ ve

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}, (\alpha \geq 1)$$

$$\varphi(n) = n\prod_{p|n}\left(1-\frac{1}{p}\right)$$

ifadeleri doğrudur.

Teorem 1.2 $n \geq 2$ tamsayısı için $(a,n)=1$ ise

$$a^{\varphi(n)} \equiv 1(mod\, n)$$

ifade edilir. Eğer ki p asal sayı ve $(a,p)=1$ ise $a^{p-1} \equiv 1(mod\, p)$ şeklindedir.

Örneğin $(3,8)=1$ için $3^{\varphi(8)} \equiv 1(mod\, 8)$ dir. Gerçekten

$$\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 4$$

$$3^{\varphi(8)} \equiv 3^4 \equiv 81 \equiv 1(mod\, 8)$$

dir.

1.1.2 Fibonacci ve Lucas Dizileri İle İlgili Bilgiler

Tanım 1.5 F_n, n'inci Fibonacci sayısı olmak üzere, başlangıç değerleri $F_0 = 0$ ve $F_1 = 1$ olan ikinci mertebeden bir indirgeme bağıntısı ile,

$$F_{n+2} = F_{n+1} + F_n, \qquad n \geq 0 \tag{1.3}$$

şeklinde tanımlanan sayılara Fibonacci sayıları denir. Bu sayıların oluşturduğu diziye Fibonacci dizisi denir ve $\{F_n\}_{n=0}^{\infty}$ ile gösterilir. Fibonacci dizisinin ilk birkaç terimi şöyledir: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55.

Fibonacci sayıları, yukarıdaki indirgeme bağıntısından başka bir cebirsel yöntem ile de elde edilebilmektedir. Bunun için $x^2 - x - 1 = 0$ denkleminin kökleri kullanılır. Bu ikinci dereceden denklemin kökleri

$$\alpha = \frac{1+\sqrt{5}}{2} \text{ ve } \beta = \frac{1-\sqrt{5}}{2} \tag{1.4}$$

olmak üzere $n \geq 0$ için F_n, n'inci Fibonacci sayısı

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \tag{1.5}$$

kapalı formu ile verilebilir. Bu formül, Binet formülü olarak bilinir. (1.5) ile verilen bu formül, Fibonacci dizisi ile ilgili pek çok özelliğin ispatlanmasında kullanılmaktadır. Örneğin, negatif indisli Fibonacci sayıları için

$$F_{-n} = (-1)^{n+1}F_n\,, \qquad n \geq 1 \tag{1.6}$$

eşitliği (1.5) ile verilen Binet formülü ile kolayca görülebilir.

Tanım 1.6 L_n, n'inci Lucas sayısı olmak üzere başlangıç değerleri $L_0 = 2$, $L_1 = 1$ için ikinci mertebeden indirgeme bağıntısı ile

$$L_{n+2} = L_{n+1} + L_n, \qquad n \geq 0 \tag{1.7}$$

şeklinde tanımlanan sayılara Lucas sayıları denir. Bu sayılarının oluşturduğu kümeye Lucas dizisi denir ve $\{L_n\}_{n=0}^{\infty}$ şeklinde gösterilir. Bu dizinin bazı terimleri 2, 1, 3, 4, 7, 11, 18, 29, 47,…. dir. Lucas sayılarının bazı özellikleri aşağıda verilmiştir.

(1.4) eşitliğinde verilen $\alpha, \beta = \left(1 \pm \sqrt{5}\right)/2$ olmak üzere $n \geq 0$ için

$$L_n = \alpha^n + \beta^n \tag{1.8}$$

kapalı formu ile verilebilir ve bu formül Binet formülü olarak bilinir. Bu formül ile kolayca görülebilir ki, negatif indisli Lucas sayıları

$$L_{-n} = (-1)^n L_n, \qquad n \geq 1 \tag{1.9}$$

eşitliği ile bulunur.

1.2 Matrisler ve Bazı Özellikleri

Sayıların, satırlar ve sütunlar halinde inşa edilmiş bir dikdörtgen tablo üzerine yerleştirilmesiyle oluşan yapıya matris denir. Bu yapıyı oluşturan sayılara matrislerin girdileri (veya elemanları) denir. Bir matris, $A_{n\times m} = \left[a_{ij}\right];\ 1 \leq i \leq n\,; 1 \leq j \leq m$ şeklinde gösterilir. a_{ij} elemanları herhangi bir F bir cisminden alınabilir. $n \neq m$ ise dikdörtgensel matris, $n = m$ ise $n \times n$ mertebeden (yada $n-$kare) matris olarak adlandırılır. Çalışmamız için lazım olan matris bilgileri aşağıdaki özetlenmiştir. (Tascı, 2018), (Strang,2022).

Tanım 1.7 $A = \left[a_{ij}\right]$, $n \times n$ matris olmak üzere matrisin determinantı $\det(A)$ veya

$$|A| = \begin{vmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & \dots & a_{nn} \end{vmatrix}_{n\times n} \tag{1.10}$$

ile gösterilir. S_n, n elemanlı permütasyonlar kümesi ve $sgn(\sigma)$'de σ permütasyonun işareti olmak üzere

$$|A| = \sum_{\sigma \in S_n} sgn(\sigma) a_{\sigma(1)1} a_{\sigma(2)2} \dots a_{\sigma(n)n} \tag{1.11}$$

kullanılarak hesap edilebilir Örneğin; 2×2 mertebeden bir $A = \left[a_{ij}\right]$ matrisinin determinantı

$$|A| = a_{11}a_{22} - a_{12}a_{21}, \tag{1.12}$$

3×3 mertebeden bir $A = [a_{ij}]$ matrisinin determinantı

$$|A| = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{12}a_{32}a_{13} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{23}a_{32}a_{11}$$

şeklindedir.

Tanım 1.8 $A = [a_{ij}]$ matrisi $m \times n$ tipinde reel sayı elemanlı bir matris olsun. A matrisinin transpozesi (devriği) A^T ile gösterilir ve $A^T = [a_{ji}]$ matrisi $n \times m$ tipinde bir matristir.

Tanım 1.9 $A = [a_{ij}]$ matrisi için, i −inci satır ve j −inci sütunun silinmesiyle elde edilen $(n-1) \times (n-1)$ mertebeden alt matrisi M_{ij} matrisi olsun. M_{ij} matrisinin determinantına a_{ij} elemanına ait minör $m_{ij} = |M_{ij}|$ denir. $c_{ij} = (-1)^{i+j} m_{ij}$ değerine a_{ij} nin işaretli minörü (kofaktörü) denilir.

Örneğin, $A = \begin{bmatrix} 1 & 2 & -1 \\ 4 & 0 & 3 \\ 2 & -3 & 1 \end{bmatrix}$ matrisinin m_{31} minörü ve c_{31} işaretli minörü;

$$m_{31} = \begin{vmatrix} 2 & -1 \\ 0 & 3 \end{vmatrix} = 6 - 0 = 6, \qquad c_{31=}(-1)^{3+1} m_{31} = 6$$

şeklindedir.

$A = [a_{ij}]$, $n \times n$ mertebeden bir matris olmak üzere A matrisinin determinantının j. sutününa göre açılımı ve i. satırına göre açılımı sırasıyla

$$|A| = \sum_{i=1}^{n} a_{ij}c_{ij} = a_{1j}c_{1j} + a_{2j}c_{2j} + \cdots + a_{nj}c_{nj} \qquad (1.13)$$

$$|A| = \sum_{j=1}^{n} a_{ij}c_{ij} = a_{i1}c_{i1} + a_{i2}c_{i2} + \cdots + a_{in}c_{in} \qquad (1.14)$$

şeklinde verilir.

Tanım 1.10 $A = [a_{ij}]$, $n \times n$ mertebeden bir matris ve c_{ij}, a_{ij} nin işaretli minörü olsun. A matrisinde elemanların yerine işaretli minörlerinin yazılması ile elde edilen matrisin transpozesine A'nın ek (adjoint) matrisi denilir ve $ek(A) = adj(A) = [c_{ij}]^T$ şeklinde gösterilir.

Teorem 1.3 $A = [a_{ij}]$ matrisi $n \times n$ tipinde reel sayı elemanlı bir matris ve $adj(A)$, A matrisinin adjoint matrisi olsun. $det(A) \neq 0$ olmak üzere A matrisinin A^{-1} tersi

$$A^{-1} = \frac{1}{det(A)} adj(A) \tag{1.15}$$

şeklindedir.

Örneğin, $A = [a_{ij}]$ matrisi 2×2 tipinde $det(A) \neq 0$ olacak şekilde bir matris olsun. Bu takdirde A matrisinin tersi

$$A^{-1} = \frac{1}{det(A)} \begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix} \tag{1.16}$$

olacaktır.

Teorem 1.4 Girdileri Z_m de olan bir $n \times n$ mertebeden A matrisinin $mod\ m$ de tersi, ancak ve ancak $det(A)$'nın $mod\ m$'deki kalanı $mod\ m$'de bir terse sahipse

$$det(A)\big(det(A)\big)^{-1} \equiv 1(mod\ m)$$

şeklinde alınabilir.

Tanım 1.11 m bir pozitif tam sayı olmak üzere, girdileri Z_m de olan bir A, $n \times n$ mertebeden matrisine, eğer

$$AB \equiv BA \equiv I\ (mod\ m)$$

olacak şekilde girdikleri Z_m'de olan bir B matrisi varsa, m modunda tersi alınabilir denir.

Tanım 1.12 F bir cisim olmak üzere $GL(n,F) = \{A \in M(n \times n, F): det(A) \neq 0\}$ cümlesi matrislerde çarpma işlemine göre bir gruptur. Bu gruba genel lineer grup denir. Özel olarak ise $SL(n,F) = \{A \in M(n \times n, F): det(A) = 1\}$ grubuna özel lineer grup denir.

1.2.1 Fibonacci ve Lucas Matrisleri ve Özellikleri

(Debnath, 2011), (Koshy, 2019)'nin çalışmalarında tam sayı elemanlı 2×2 boyutlu Q ve M matrisleri;

$$Q = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \qquad M = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \tag{1.17}$$

şeklinde tanımlanmış ve $n \geq 1$ için

$$Q^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} \qquad M^n = \begin{pmatrix} F_{2n-1} & F_{2n} \\ F_{2n} & F_{2n+1} \end{pmatrix} \tag{1.18}$$

olduğu verilmiştir. Ayrıca, $L_{n+1} = F_{n+1} + 2F_n$ ve $L_n = 2F_{n+1} - F_n$ eşitliklerine göre

$$RQ^n = \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} = \begin{pmatrix} L_{n+1} & L_n \\ L_n & L_{n-1} \end{pmatrix} \tag{1.19}$$

tanımlanan R matrisi kullanılarak Fibonacci sayılarından Lucas sayılarına geçiş yapılmıştır.

Fibonacci ve Lucas sayısının birçok özelliği, matris teorideki bazı kavramlar ve nitelikler kullanarak yeniden ve basit bir yaklaşımla üretilmiştir. Matrislerle ilgili tanımları ve fikirleri temel alan özelliklerden bazılarını verelim.

Determinant özellikleri ile

$$det(Q^n) = (-1)^n \quad \Rightarrow \quad F_{n+1}F_{n-1} - F_n^2 = (-1)^n \tag{1.20}$$

$$det(RQ^n) = det(R)\, det(Q^n) \quad \Rightarrow \quad L_{n+1}L_{n-1} - L_n^2 = 5(-1)^{n+1} \tag{1.21}$$

şeklinde Cassini's formülleri elde edilebilmektedir.

Fibonacci Q^n matrisinin karakteristik denklemi $|Q^n - I\lambda| = \lambda^2 - L_n\lambda + (-1)^n$ ile $L_n = F_{n+1} + F_{n-1}$ ve $L_n^2 - 4(-1)^n = 5F_n^2$ olmak üzere

$$\alpha^n = \frac{L_n + F_n\sqrt{5}}{2} \qquad \beta^n = \frac{L_n - F_n\sqrt{5}}{2} \tag{1.22}$$

eşitlikleri verilir ki; (1.22) eşitliklerinin taraf tarafa toplanması veya çıkarılması ile Fibonacci ve Lucas sayıları için Binet formülleri elde edilebilir.

$(I + Q + Q^2 + \ldots + Q^n)(Q - I) = Q^{n+1} - I$ matris eşitliği kullanılarak

$$\sum_{i=1}^{n} F_i = F_{n+2} - 1 \tag{1.23}$$

eşitliğinin farklı bir ispatı gösterilmiştir.

Kuvvet özelliklerinin $Q^m Q^n = Q^{m+n}$ ve $Q^m Q^n Q^l = Q^{m+n+l}$eşitliği ile

$$F_{m+n} = F_m F_{n+1} + F_{m-1} F_n$$
$$F_{m+n+l} = F_{m+1} F_{n+1} F_{l+1} + F_m F_n F_l - F_{m-1} F_{n-1} F_{l-1} \tag{1.24}$$

indis toplam eşitlikleri verilir. (1.20) denklemi tersinin varlığını doğrular ki ters matris yöntemi ile

$$(Q^n)^{-1} = Q^{-n} = \begin{bmatrix} F_{-n+1} & F_{-n} \\ F_{-n} & F_{-n-1} \end{bmatrix}$$

şekilde verilir.

(Hoggatt ve Bicknell, 1964)'ın çalışmalarında ikincil köşegen altındaki elemanları Pascal üçgenin satırları olarak verilen 3×3 boyutlu P matrisi;

$$P = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix} \tag{1.25}$$

olmak üzere $f(x) = x^n$ kuvvet fonksiyonu altındaki görüntüsü $f(P) = P^n$ matrisi;

$$P^n = \begin{pmatrix} F_{n-1}^2 & F_{n-1}F_n & F_n^2 \\ 2F_{n-1}F_n & F_{n+1}^2 - F_{n-1}F_n & F_n F_{n+1} \\ F_n^2 & F_n F_{n+1} & F_{n+1}^2 \end{pmatrix} \tag{1.26}$$

olduğu verilmiştir.

(Koken ve Bozkurt, 2010; Demirtürk, 2010) çalışmalarında tanımlanan 2×2 boyutlu matrisler

$$Q_L = \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix} \qquad S = \frac{1}{2}\begin{pmatrix} 1 & 5 \\ 1 & 1 \end{pmatrix} \tag{1.27}$$

şeklinde olmak üzere matrislerin kuvvet özellikleri düşünülerek,

$$Q_L^{2n} = 5^n \begin{pmatrix} F_{2n+1} & F_{2n} \\ F_{2n} & F_{2n-1} \end{pmatrix} \qquad Q_L^{2n+1} = 5^n \begin{pmatrix} L_{2n+2} & L_{2n+1} \\ L_{2n+1} & L_{2n} \end{pmatrix}$$
$$S^n = \frac{1}{2}\begin{pmatrix} L_n & 5F_n \\ F_n & L_n \end{pmatrix} \tag{1.28}$$

matrisleri elde edilir. Ayrıca bu matrisler ile Fibonacci ve Lucas sayıları arasındaki

$$\begin{pmatrix} L_{n+1} \\ L_n \end{pmatrix} = Q_L \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} \qquad \begin{pmatrix} 5F_{n+1} \\ 5F_n \end{pmatrix} = Q_L \begin{pmatrix} L_n \\ L_{n-1} \end{pmatrix} \tag{1.29}$$

ilişkiler kurulmuştur.

Ayrıca Lucas matrislerinin üzerinde matris teorideki Fibonacci dizilerindeki benzer çalışmaların yapılmasıyla Fibonacci ve Lucas sayıları ile ilgili birçok özellik farklı ve basit şekilde elde edilmiştir.

(Koken, 2019)'ın çalışmasında Pascal matrisleri ile ilgili 3×3 boyutlu R_L matrisi tanımlanmıştır. İki farklı yöntem ile R_L^n matris kuvvetinin hesaplanması yapılmıştır. Elde edilen kuvvetlerin eşitlenmesi ile birçok Fibonacci-Lucas eşitliği bulunur. Ayrıca, $R_L - 5I$ matrisi düşünülmüş ve $(R_L - 5I)^n$ kuvvet matrisi elde edilmiştir. $(R_L - 5I)^n$ ve R_L^n matrislerinin ilişkileri ve Fibonacci ve Lucas eşitlik uygulamaları verilmiştir.

Başlangıç değerleri $f_0 = f_1 = f_2 = \cdots = f_{\lambda-2} = 0, f_{\lambda-1} = 1$ olmak üzere genelleştirilmiş Fibonacci dizisi λ'inci dereceden indirgeme ilişkisi ile

$$f_{k+\lambda} = f_{k+\lambda-1} + f_{k+\lambda-2} + \cdots + f_{k+1} + f_k, \qquad k \geq 0 \tag{1.30}$$

şeklinde verilir.

λ mertebesine sahip uygun multinacci Q_λ matrisi Brenner (Grimaldi, 2011; Koshy, 2019) tarafından tanıtılmış ve Fibonacci Q_λ matrisi

$$Q_\lambda = \begin{bmatrix} 1 & 1 & \ldots & 1 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \ddots & 0 & \vdots \\ \vdots & \vdots & \ddots & \vdots & 0 \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}_{\lambda \times \lambda}$$

değerleri Fibonacci sayılarına göre

$$Q_\lambda = \begin{bmatrix} f_\lambda & f_{\lambda-1} + \cdots + f_1 & f_{\lambda-1} + \cdots + f_2 & \cdots & f_{\lambda-1} \\ f_{\lambda-1} & f_{\lambda-2} + \cdots + f_0 & f_{\lambda-2} + \cdots + f_1 & \cdots & f_{\lambda-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ f_2 & f_1 + \cdots + f_{1-(\lambda-2)} & f_1 + \cdots + f_{1-(\lambda-3)} & \cdots & f_1 \\ f_1 & f_0 + \cdots + f_{0-(\lambda-2)} & f_0 + \cdots + f_{0-(\lambda-3)} & \cdots & f_0 \end{bmatrix}$$

şu şekilde verilir ki tümevarım yoluyla

$$Q_\lambda^k = \begin{bmatrix} f_{k+\lambda-1} & f_{k+\lambda-2}+\cdots+f_k & f_{k+\lambda-2}+\cdots+f_{k+1} & \cdots & f_{k+\lambda-2} \\ f_{k+\lambda-2} & f_{k+\lambda-3}+\cdots+f_{k-1} & f_{k+\lambda-3}+\cdots+f_k & \cdots & f_{k+\lambda-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ f_{k+1} & f_k+\cdots+f_{k-(\lambda-2)} & f_k+\cdots+f_{k-(\lambda-3)} & \cdots & f_k \\ f_k & f_{k-1}+\cdots+f_{k-\lambda+1} & f_{k-1}+\cdots+f_{k-\lambda+2} & \cdots & f_{k-1} \end{bmatrix} \quad (1.31)$$

olduğu kolayca doğrulanabilir. Ayrıca, genelleştirilmiş negatif multinacci dizisi için (1.30)'deki yineleme ilişkisi şu şekilde yeniden yazılabilir ki $k \leq -1$ için

$$f_k = f_{k+\lambda} - (f_{k+\lambda-1} + f_{k+\lambda-2} + \cdots + f_{k+1}) \quad (1.32)$$

veya eşdeğer olarak (1.30)'daki gibi verilen aynı başlangıç değerleri ile $k \leq -1$ için

$$f_{-k} = f_{-k+\lambda} - (f_{-k+\lambda-1} + f_{-k+\lambda-2} + \cdots + f_{-k+1}) \quad (1.33)$$

şeklinde verilebilir.

Multinacci matrisinin tersinin varlığı konusunda, $\lambda \in Z^+$ olmak üzere her $k \in Z$ tamsayısı için, Q_λ^k Multinacci matrislerinin tersi (1.31)'deki denklemde tanımlandığı gibi

$$Q_\lambda^{-k} = \begin{bmatrix} f_{-k+\lambda-1} & f_{-k+\lambda-2}+\cdots+f_{-k} & f_{-k+\lambda-2}+\cdots+f_{-k+1} & \cdots & f_{-k+\lambda-2} \\ f_{-k+\lambda-2} & f_{-k+\lambda-3}+\cdots+f_{-k-1} & f_{-k+\lambda-3}+\cdots+f_{-k} & \cdots & f_{-k+\lambda-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ f_{-k+1} & f_{-k}+\cdots+f_{-k-(\lambda-2)} & f_{-k}+\cdots+f_{-k-(\lambda-3)} & \cdots & f_{-k} \\ f_{-k} & f_{-k-1}+\cdots+f_{-k-\lambda+1} & f_{-k-1}+\cdots+f_{-k-\lambda+2} & \cdots & f_{-k-1} \end{bmatrix} \quad (1.34)$$

şeklinde verilir.

1.2.2 Circulant Matrisler ve Özellikleri

Circulant matrisler, Toeplitz matrislerin bir özel tipidir. Bu matrisler, ilk satırları ile temsil edilebilirler, çünkü satır elemanları bir önceki satır elemanlarının sağa kayıp, elemanların başa sarması ile meydana gelen matrislerdir. Bu kolaylık onlara diğer matrisler arasında özel bir yer almasını sağlar. Circulant matrislerin uygulamaları ile ilgili birçok çalışma bulunur. Bu çalışmada şifreleme bilimdeki uygulamaları araştırılır. Şimdi, Circulant matrislerle ilgili bazı özelliklerden bahsedilir (Davis, 1979; Good, 1986; Kalman ve White, 2001; Gray, 2006; Kra, and Simanca, 2012).

Tanım 1.13 $n \times n$ tipinde bir Circulant matris $C_n(F) = (c_1, c_2, c_3, \ldots, c_n)$;

$$C_n = [c_{ij}]_{n\times n} = \begin{pmatrix} c_1 & c_2 & \dots & c_n \\ c_n & c_1 & \dots & c_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_2 & c_3 & \dots & c_1 \end{pmatrix} \tag{1.35}$$

şekilde tanımlanır.

Tanım 1.14 $n \times n$ tipinde bir $\pi_n = (0,1,0,\dots,0)$ Circulant matrisine permütasyon matris denir.

Bu π_n matrisi kullanılarak $n \times n$ mertebeden C_n matrisi

$$C_n = c_1 + c_2\pi + \dots + c_n\pi^{n-1} = \sum_{k=1}^{n} c_k\pi^{k-1} \tag{1.36}$$

şeklinde yazılabilir. π'nin kuvvetleri göz önüne alınırsa işlemler yapıldığında temel satırı $C_n = (c_1, c_2, \dots, c_n)$ olan Circulant matris elde edildiği açıkça görülür.

(1.36)'deki eşitliğini sağlayan bir C_n, $n \times n$ mertebeden Circulant matris şeklindedir. Ayrıca π ve A matrisine göre A matrisinin Circulant matris olması için gerek ve yeter şart

$$A\pi = \pi A \tag{1.37}$$

olmasıdır.

Tanım 1.15 $C_n = (c_1, c_2, \dots, c_n)$ matrisinin esas köşegenin altındaki elemanların işaretinin değiştirilmesiyle oluşan

$$SC_n = \begin{pmatrix} c_1 & c_2 & \dots & c_n \\ -c_n & c_1 & \dots & c_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ -c_2 & -c_3 & \dots & c_1 \end{pmatrix} \tag{1.38}$$

matrise Skew Circulant (negacyclic) matris denir.

$\pi_n = (0,1,0,\dots,0)$ matrisinin Skew Circulant matris hali

$$\eta_n = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \ddots & 1 \\ -1 & 0 & \dots & 0 & 0 \end{bmatrix} = \begin{pmatrix} 0 & I_{n-1} \\ -1 & 0 \end{pmatrix} = \pi \begin{pmatrix} -1 & 0 \\ 0 & I_{n-1} \end{pmatrix} \tag{1.39}$$

şeklindedir.

Ayrıca, $C_n = (c_1, c_2, \dots, c_n)$ Circulant matris ifadesine göre

$$C_{n,s} = \begin{pmatrix} c_1 & c_2 & c_3 & \cdots & c_n \\ 0 & c_1 & c_2 & \cdots & c_{n-1} \\ 0 & 0 & c_1 & \cdots & c_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & c_1 \end{pmatrix} \tag{1.40}$$

şeklinde oluşturulan matrislere semicirculant matris denir.

Tanım 1.16 $n \times n$ tipindeki $C_{n,r} = \left(c_{ij}\right)_n$, $i,j = 1,2,\ldots,n$ ve $r \in \mathbb{C}$ için $r-$circulant matrislerin ij'inci elemanı,

$$c_{ij} = \begin{cases} c_{j-i} & i \leq j \\ rc_{n+j-i} & aksi\ takdirde \end{cases} \tag{1.41}$$

dir. Ayrıca, (1.41)'deki elemanlara sahip $C_{n,r}$ matrisi birinci satıra göre ifade edilmek istenirse $C_{n,r} = \{r(c_0, c_1, \ldots, c_{n-1})\}$ ile gösterilir. Yani $n \times n$ mertebeden $r-$circulant $C_{n,r}$ matris

$$C_{n,r} = \begin{pmatrix} c_0 & c_1 & c_2 & \cdots & c_{n-2} & c_{n-1} \\ rc_{n-1} & c_0 & c_1 & \ddots & c_{n-3} & c_{n-2} \\ rc_{n-2} & rc_{n-1} & c_0 & \ddots & c_{n-4} & c_{n-3} \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ rc_2 & rc_3 & \cdots & \ddots & c_0 & c_1 \\ rc_1 & rc_2 & rc_3 & \cdots & rc_{n-1} & c_0 \end{pmatrix} \tag{1.42}$$

şeklinde yazılabilir.

$r-$circulant $C_{n,r}$ matrisleri r değerlerine göre, C_n Circulant, SC_n Negacyclic ve $C_{n,s}$ Semicirculant matrislerin genel bir halidir.

(1.42) denkleminde $r = 1$ alırsak, (1.35)'deki gibi bir circulant $C_n = (c_0, c_1, \ldots, c_{n-1})$ matris elde edilir.

(1.42) da $r = -1$ alınırsa (1.38) denkleminde verilen gibi bir SC_n Negacyclic Circulant matris elde edilir.

Eğer (1.42) denkleminde $r = 0$ alırsa (1.40) denkleminde verilen gibi bir $C_{n,s}$ Semicirculant matris elde edilir.

Tanım 1.17 $C_n = (c_1, c_2, \ldots, c_n)$ Circulant matris ifadesine göre satır vektörlerinin $ebob$ değeri "1" ($ebob(c_1, c_2, \ldots, c_n) = 1$) ise asal (prime) Circulant matris denir.

Tanım 1.18 $n \times n$ mertebeden bir G_n matrisi ve G'nin $i.$ satır için C_n Circulant matrisi değerlerine göre $G_{n^2,c}$ ile gösterilen

$$G_{n^2,c} = C_n\left(C_n(G'nin\ 1.satır), C_n(G'nin\ 2.satır), \ldots, C_n(G'nin\ n.satır)\right)$$

matrisine katsayı (coefficient) matris denir.

Örneğin, 2×2 mertebeden $G_2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ matrisi için 4×4 mertebeden katsayı matrisi

$$G_{4,c} = \begin{pmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{pmatrix}$$

şeklindedir.

1.3 Şifreleme Biliminde Kullanılan Temel Tanımlar ve Bazı Özellikler

Metin bilgilerinin güvenli iletişimi dünya genelinde birincil öneme sahiptir. Her ne kadar gizli kodlar yazılı iletişimin ilk günlerine kadar gitse de, iletişimin genel hatları üzerinden iletilen bilginin gizliliğini koruma ihtiyacı sebebiyle bu konuda yeni bir ilgi dalgası vardır. Kriptografi (şifreleme), güvenliği sağlama yöntemlerinden biridir.

Bu bölümde şifreleme ile ilgili temel tanımlardan bahsedilecektir (Stinson, 2005), (Cimen, ve Ark. 2009), (Lüy, 2012), (Bayar, 2012).

Tanım 1.19 Şifreleme bilimine **kriptoloji** *(İng, Cryptology)*, kriptoloji ile ilgilenen insanlara **kriptograf** (*İng. Cryptographer*) denilir.

Tanım 1.20 Bilgileri çeşitli metotlarla gizlenip şifrelemesini ve mesajın tekrar eski orijinal haline geri döndürülmesini sağlayan matematiksel yöntemler bilimine **kriptografi** (*İng. Cryptography*) adı verilir. Kriptografi dilinde kodlara **şifreler** *(İng. codes)* denilir.

Tanım 1.21 Bir haberleşmede şifrelenmiş bilgiyi meşru olarak gönderen kişiye **gönderici** (*İng., Sender*) denilir.

Tanım 1.22 Bir haberleşmede şifrelemede bilgiyi alan kişiye **alıcı** (*İng., Receiver*) denilir.

Tanım 1.23 Alıcı ve gönderici tarafından bilinen, metnin şifrelemesinde ve deşifrelemesinde kullanılan kritik bilgilere **anahtar** (*İng., Key*) denilir.

Tanım 1.24 Göndericiden alıcıya giden bilgilerin iletilmesini sağlayan iletişim aracına **kanal** (*İng. Channel*) denilir.

Tanım 1.25 Şifrelenecek olan metine **açık (düz) metin** (*İng., Plaintext*) veya orijinal metin denilir.

Tanım 1.26 Açık metinden şifreleme ile dönüştürülen metine **şifreli metin** (*İng., Ciphertext*) denilir.

Tanım 1.27 Açık metnin çeşitli dönüşümler uygulanarak şifreli metin haline getirilme sürecine **şifreleme** (*İng., Encryption*) denilir.

Tanım 1.28 Şifreli metnin orijinal hale getirilmesi işlemine **deşifreleme (şifre çözme)** (*İng., Decryption*) denilir.

Tanım 1.29 Bilginin tanımlandığı karakter dizisine **kod** *(İng. code)* denir. Ayrıca kod, bilgisayarın algılayacağı özel komutlar kullanılarak bilginin gösterilmesidir.

Tanım 1.30 Şifreleme ve deşifreleme işlemlerinde kullanılan matematiksel işlemler bütününe **kriptografik algoritma** (*İng Cryptographic Algorithm*) denilir.

Tanım 1.31 Bir kanal içerisinde şifrelenmiş metnin bir kısmını veya tamamına ulaşmak için yapılan her tülü girişimine **saldırı** *(İng. attack)* denilir.

Tanım 1.32 Bir haberleşmede, alıcı veya gönderici kişi olmayıp bilginin güvenliğini kırmaya çalışan başka kişiye **saldırgan** (*İng., Adversary*) denilir.

Tanım 1.33 Bir sistemin düz metin veya şifrelenmiş metin parçalarını inceleyerek, herhangi bilgi veya bir anahtar olmaksızın düz metin verilerine ulaşmayı amaçlayan yasa dışı analize **kriptanaliz** (*İng. Cryptanalysis*) denilir. Aynı zamanda **kod kırma** (*İng., Codbreaking*) olarak da adlandırılır.

Tanım 1.34 Kriptanalizin uygulayıcılarına **kriptanalist** (*İng., Cryptanalyst*) denilir.

Tanım 1.35 Sistemlerdeki kullanılan anahtarları veya sistemi öğrenmek amacıyla yapılan işleme **Şifre Kırma** (*İng. Crack*) adı verilir.

Tanım 1.36 Hem şifreleme hem deşifreleme de kullanılan anahtara **özel (gizli, kişisel) anahtar** (*İng. Private Key*) denilir.

Tanım 1.37 Sadece metnin şifrelenmesinde kullanılan ve deşifre edilmesinde kullanılmayan anahtara **açık anahtar** (*İng., Public Key*) denilir.

Tanım 1.38 Gizli anahtarın kullanıldığı kriptografik algoritmalara **simetrik algoritma** (*İng.* S*ymmetric Algorithm*) denilir.

Tanım 1.39 Açık anahtarın kullanıldığı kriptografik algoritmalara **asimetrik algoritma (** *İng. asymmetric Algorithms)* ya da **açık anahtarlı Algoritmalar** (*İng. Public Key Algorithms*) denilir.

Tanım 1.40 Herhangi bir kişinin gerçek alıcı veya gönderici olduğunu belirlenmesi için yapılan işleme **kimlik belirleme** (*İng. Authentication*) denilir.

Tanım 1.41 Bilginin göndericiden alıcıya iletilmesi sırasında kazara veya kasıtlı olarak değiştirilmesinin önlenmesi **veri bütünlüğü** (*İng. Data Integrity*) olarak adlandırılır.

Tanım 1.42 Elektronik yazışmalara dahil edilen, gönderenin kimliğini doğrulamaya ve iletim sırasında mesajın bütünlüğünü tasdik etmeye yarayan bileşen, **imza doğrulama** (*İng. Signature Schema*) olarak adlandırılır.

Düz veya şifreli metnin içeriğine ve imzalayanın gizli anahtarına bağlı olan kriptografik bir yöntemle dijital imzalar elde edilir. Sonuç olarak, dijital imzayı doğrulamak için imzalayanın açık anahtarı kullanılır.

Bilgi güvenliğinin de bir yönü olan bu kriptografi biliminin dört temel amacı vardır

Gizlilik, kodlanmış bilgiyi açma/soyma yetkisine veya gizli anahtara sahip olanlar dışında bilginin içeriğini herkesten uzak tutmak için kullanılan bir hizmettir.

Kimlik doğrulama, hem sistemin bütünlüğü hem de bilginin kendisi açısından tanımlama/tanıma ile ilgilidir. Birbirleriyle iletişim kuran iki tarafın birbirlerine kendilerini tanıtmaları gerekir. Kanal aracılığıyla iletilen bilginin gerçekliği, verinin içeriği, teslim süresi ve diğerlerinin doğrulanması gerekir.

İnkar etmeme, bilgiyi gönderen/yapan kişi tarafından bilginin iletilmesinin inkar edilmesini önlemeye yönelik bir girişimdir.

Veri bütünlüğü, gerçek verilere başka verilerin eklenmesi, silinmesi ve ikame edilmesi de dahil olmak üzere yetkisiz taraflarca yapılan veri bütünlüğünü bozan uygulamalardır.

1.3.1 Şifreleme Çeşitleri ve Karşılaştırmaları

Gelişen teknoloji ile şifreleme için uygulanan yöntemler de değişkenlik sergilemiştir. Şifreleme teknikleri bakımından klasik ve modern teknikler olarak ikiye ayrılabilir (Stinson, 2005), (Obaid, 2016), (Öztürkmenoğlu, 2016).

Klasik teknikler olarak yerine koyma ve yer değiştirme olarak yerine koymada tek alfabeli ve çok alfabeli şeklinde bölümlendirilir.

Modern teknikler, gizli (simetrik) ve açık (asimetrik) anahtarlı olmak üzere ikiye ayrılabilir. Simetrik şifrelemede kendi içinde Blok ve akış şifreleme altında incelenir. Asimetrik şifreleme RSA, DSA ve Diffie-Hellman şifreleme altında incelenir.

Modern teknikler zaman içinde simetrik, asimetrik şifrelemeler birleştirilerek karışık (melez) şifrelemeler olmak üzere aşağıdaki şekilde de görüldüğü gibi üç ana başlık altında değerlendirilir.

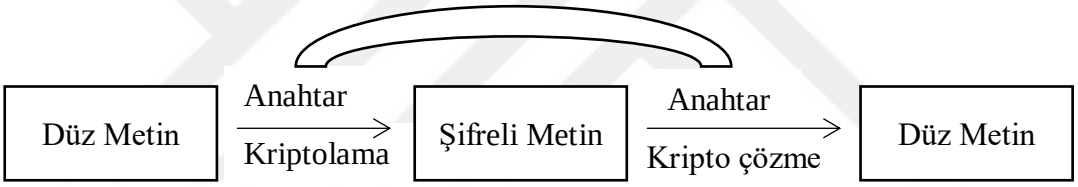
Tablo 1.1 Şifreleme Metotları

KLASİK TEKNİKLER		**MODERN TEKNİKLER**		
Yerine Koymalı	**Yer Değiştirme**	**Simetrik (Gizli Anahtarlı)**		**Asimetrik (Açık Anahtarlı)**
Monoalfabetik	Ceasar	**Blok**	**Akış**	RSA
Polialfabetik		AES	RCA	DSA
Tek Kullanımlık		DES	SEAL	Diffie Hellman
		3DES		El Gamal
				Eliptik Eğri Şifrelemesi
Melez (Karışık) Şifreleme			FGP	True Cryft

Şimdi, Tablo 1.1'deki ana metotlara ait bazı genel bilgiler verilecektir.

Simetrik (Gizli Anahtarlı) Kriptosistemler

Bu sistemlerde aynı anahtar hem şifreleme hem de şifre çözme için kullanılır. Tek anahtarlı kriptografi veya gizli anahtar algoritmaları olarak da bilinirler.



Şekil 1.1. Simetrik algoritma şifrelemesi

Simetrik şifrelemede, gönderici ve alıcı iletişime başlamadan önce ortak bir anahtar üzerinde anlaşmalıdır. Bunun nedeni şifreleme ve şifre çözme anahtarlarının aynı olmasıdır, bu da anahtarın gizli tutulmasının iletişimin güvenliği için gerekli olduğu anlamına gelir. Anahtar ortaya çıkarsa, herkes mesajları şifreleyebilir ve şifrelerini çözebilir, bu da iletişimin gizliliğini tehlikeye atabilir.

Bu algoritmaların avantajı basit ve kolay uygulanabilir, hızlı ve verimli olmalarıdır. Ancak bu algoritmaların zayıf yönü, aynı anahtarın hem şifreleme hem de şifre çözme için kullanılmasıdır.

Simetrik şifre örneklerinden birisi olarak, alfabedeki her harfin yerine başka bir harfle değiştirmesiyle oluşan şifreleme yöntemine **y**erine koyma *(Substitution)* şifrelemeleri denilir.

Düz metindeki harfler sabittir. Şifreli metni elde etmek için bu harflerin yerine başka bir alfabeden sayılar, semboller veya harfler yerleştirilir.

Yer değiştirme yöntemleri (Transposition Methods) Düz metindeki harfler yer değiştirir. Düz metindeki harflerin kimlikleri sabittir, ancak konumları değiştirilir.

Tablo 1.2 Türk alfabesinin sayısal değerlerin bir örneği

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

Gizli anahtar şifrelemesinden yerine koyma yöntemine örnek olarak geçmişten gelen en güzel örneklerden biri olan Ceasar şifreleme yöntemi aşağıda verilmiştir.

Ceasar, alfabenin her harfini üç harf ilerisindeki harfle değiştirerek şifreli metni elde etmiştir. Yani Ceasar şifreleme metodu için

$$E = (M + r)(mod29), \qquad 0 \leq E \leq 28 \tag{1.43}$$

bağıntısı kurulabilir. Buradaki M açık metindeki her bir harfin sayısal karşılığı, r harflerin ne kadar kaydırılacağı, E ise şifre metinde bu harflere karşılık gelen sayısal değerlerdir. $r = 3$ için Tablo 1.2'deki düz metin değerlerine göre şifrelenmiş metin değerlerine karşılık gelen değerleri Tablo 1.3 ile verilmiştir. **Tablo 1.3**

Tablo 1.3 Ceaser şifreleme ile harflerin karşılığı

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

Yerine koyma şifresinde düz metin harfi *A, Ç* ile değiştirilmiştir, düz metin harfi *B, D* ile ve *C, E* ile vs. şeklinde değiştirilmiştir. Bu şifre ile (1.44)'deki gibi verilen bir cümle;

"MATEMATİKTE ZEKADAN ÖNCE SABIR GELİR" (1.44)

olan düz metin mesajı

"ÖÇVĞÖÇVLNVĞ CĞNÇGÇP SPEĞ ÜÇDKT IĞOLT"

Tablo 1.3'deki yerine koyma yöntemi ile şifrelenmiş olur. Alıcı bu mesajı deşifre edebilmek için harfleri önce sayısal eşitliklerine çevirir ki, sonra da

$$M \equiv (E-3)(mod\ 29), \qquad 0 \leq M \leq 28$$

denkliğini kullanarak açık metini bulabilir.

Yerine koyma şifrelerinin bir dezavantajı aynı harflerin frekanslarını koruduklarından dolayı istatistiksel metotlarla kodu kırmayı oldukça kolay olmasıdır. Bu problemin üstesinden gelmenin bir yolu, düz metni harf gruplarına ayırmak ve düz metni grup halinde şifrelemektir. Bu yüzden, Monoalfabetik, Polialfabetik, vs. gibi yeni şifreleme yöntemleri geliştirilmeye çalışılmıştır.

Düz metnin, her biri bir n şifre harfi ile değiştirilen n harfli kümelere ayrıldığı bir kriptografi sistemine bir ***poligrafik sistem*** denir. Poligrafik sisteme örnek olarak, Hill şifreleme vb. algoritmalardan bahsedeceğiz.

Asimetrik (Açık Anahtarlı) Kriptosistemler

Simetrik kriptografinin tarihi binlerce yıl öncesine dayanmasına rağmen asimetrik kriptografinin uzun bir geçmişi yoktur. Simetrik kriptografideki anahtar dağıtım problemi asimetrik şifreleme ile çözülür. Simetrik kriptografide gizli anahtarın karşı tarafa bir şekilde gönderilmesi gerekirken, asimetrik kriptografide gizli anahtarın karşı tarafa herhangi bir şekilde gönderilmesine gerek yoktur.

Açık anahtar kriptografisi, yalnızca sahibinin bilmesi gereken diğer iki anahtardan gizli tutulan anahtardır. Şifrelenmiş verilerin şifresini çözmek veya verileri imzalamak için ilgili açık anahtar kullanılır. Güvenlik açısından sistemin temel dayanağı, özel anahtarın sahibinden başka kimse tarafından kullanılamamasıdır. Bu nedenle özel anahtarın korunması gereklidir.

Açık anahtar kriptografisinde, açık anahtar herkes tarafından kullanılabilir. Yalnızca özel anahtarın sahibi tarafından çözülebilen verileri bir eş ile şifrelemek veya özel anahtarın sahibi tarafından şifrelenen verilerin şifresini çözmek için kullanılır.

Şifreleme ve şifre çözmenin farklı anahtarlar kullanılarak gerçekleştirildiği kriptografik algoritmalardır. Bunlar, şifre çözme anahtarının şifreleme anahtarından türetilemediği algoritmalardır. Açık anahtar ve bu anahtarın karşılığı olan özel anahtar bir anahtar ikilisi oluşturur. İki anahtarlı kriptografi veya asimetrik şifreleme olarak da bilinirler. Diffie-Hellman, El-Gamal ve RSA anahtar değişim algoritması gibi şifreleme algoritmaları en iyi bilinenleridir.

Asimetrik şifreleme iki farklı anahtar kullanır: bir açık anahtar ve bir özel anahtar. Açık anahtar şifreleme için kullanılırken, özel anahtar şifre çözme için

kullanılır. Açık anahtarın gizli tutulması gerekmezken, özel anahtar kesinlikle gizli tutulmalıdır ve özel anahtarı saklamak anahtar sahibinin sorumluluğundadır. Açık anahtara sahip olan kişi bilgiyi şifreleyebilir ancak şifreli metnin şifresini çözemez.

Asimetrik şifrelemede, gönderici alıcının açık anahtarını alır ve mesajı şifrelemek için kullanır. Bu şifrelenmiş mesajın şifresi açık anahtar ile çözülemez. Alıcıya şifreli metin ulaştığında, kendi özel anahtarı ile alıcı şifreli metnin şifresini çözebilir.

Şekil 1.2. Asimetrik şifreleme ve Deşifreleme şeması

Açık anahtar kriptografisinin temel amacı, önceden bir güvenlik anlaşması olmayan taraflar arasında güvenli mesaj alışverişini sağlamaktır. Bu tür şifrelemede gizli anahtarın karşı tarafa herhangi bir şekilde gönderilmesi gerekmez, bu da çok yüksek bir güvenlik seviyesi sağlar. Asimetrik şifrelemenin bir diğer avantajı da inkar edilemeyen dijital imzalar sağlayabilmesidir.

Açık anahtar kriptografisi, 1976 yılında Whitfield Diffie ve Martin Hellman tarafından icat edilen anahtar paylaşım protokolü ile doğmuştur. İki yıl sonra Rivest, Shamir ve Adleman tarafından tarihteki ilk açık anahtar şifreleme algoritması olan RSA geliştirildi. DSA (Dijital İmza Algoritması), MOR kriptosistemi, Merkle-Hellman, Diffie-Hellman Anahtar Anlaşması, El-Gamal, Eliptik Eğri Algoritması (ECC) asimetrik şifreleme örnekleridir.

1976 yılında Diffie ve Hellman tarafından bulunan ilk asimetrik şifreleme DH (Diffie-Hellman) algoritmasıdır. DH, iki kişinin önceden herhangi bir bilgi alışverişinde bulunmadan güvensiz bir kanal üzerinden ortak bir şifre üzerinde (güvenli bir şekilde) anlaşmasını sağlayan bir protokoldür.

Algoritmada anahtar değişiminin temel amacı, iki kullanıcının birbirlerine güvenli bir şekilde bir anahtar iletmesine ve daha sonra bu anahtarı birbirlerine şifreli mesajlar göndermek için kullanmasına izin vermektir. Diffie-Hellman algoritmasının tasarımı, simetrik şifreleme algoritmalarında önemli bir sorun olan gizli anahtarın korunması ve dağıtılması sorununun büyük ölçüde üstesinden gelir. Bununla birlikte, simetrik şifrelemede Diffie-Hellman algoritması yalnızca paylaşılan gizli anahtarı belirlemek için kullanılır.

RSA (Rivest-Shamir-Adleman) 1977 yılında Ron Rivest, Adi Shamir ve Leonard Adleman adlı üç bilim insanı tarafından geliştirilen bir asimetrik şifreleme algoritmasıdır. Algoritma adını soyadlarının ilk harflerinden almıştır.

Anahtar dağıtımına ek olarak, şifreleme ve şifre çözme işlemleri aynı anda gerçekleştirilir. RSA, güvenilirliği çok büyük tamsayıları işlemenin zorluğuna dayanan bir şifreleme tekniğidir. Açık anahtarlı bir şifreleme tekniği olan RSA, çok büyük tamsayıları üretmenin ve manipüle etmenin zorluğuna dayanır. Anahtar üretimi için asal sayılar kullanılarak daha güvenli bir yapı oluşturulur. Genel olarak RSA, hem mesaj şifreleme hem de elektronik imzalar için kullanılan ticari uygulamalarda çoğunlukla tercih edilen, tam sayıların arıtılmasıyla üretilen değerlerden anahtarların üretildiği bir şifreleme tekniğidir.

RSA algoritmasında kullanılacak anahtarın sayısal büyüklüğü sistemin hem güvenilirliği hem de hızı açısından önemlidir. Yeterli güvenilirlik seviyesine ulaşmak için gereken asal sayı büyüklüğü Eliptik Eğri Şifre (ECC) algoritması kullanılarak belirlenir. RSA ile 1024 bitlik (yaklaşık 300 basamaklı) bir anahtar basit uygulamalar için yeterli bir şifreleme tekniği olarak kullanılabilir.

RSA algoritması nispeten basit bir şifreleme algoritmasıdır. Ancak, sürekli olarak çok büyük bir asal sayı üretmek çok zordur. RSA şifreleme sisteminin oluşturulmasıyla birlikte asimetrik şifreleme algoritmaları günümüzde daha yaygın olarak kullanılmaktadır.

Burada RSA ve El-Gamal şifreleme yöntemleri incelenmektedir.

RSA Algoritması

RSA, 1978 yılında 'Dijital imzalar ve açık anahtarlı kriptosistemler elde etmek için bir yöntem' başlıklı bir makalede yayınlanmıştır. RSA, göndericinin bir yöntem ve herkes tarafından bilinen bir açık anahtar kullanarak mesajları şifrelediği bir kriptosistem olarak tanımlanır. Önceki simetrik anahtar sistemlerinin aksine, anahtarın bilinmesi şifre çözme anahtarını ortaya çıkarmaz. Bu sistemin güvenliği, tam sayılar için çarpanlara ayırma probleminin zorluğuna dayanmaktadır.

RSA'da kişilere şifreli mesaj gönderebilmek için bu kişilerin açık anahtarlarına ihtiyaç duyulur. Mesajı alan kişinin de mesajı okuyabilmesi için özel bir anahtara sahip olması gerekmektedir (Okumuş, 2012), (Santoso, 2021). RSA kullanılarak anahtar çifti oluşturma, şifreleme ve şifre çözme aşamaları aşağıda verilmiştir.

Anahtar üretme algoritması: Her A kişisi anahtarını aşağıdaki gibi üretir. Yaklaşık olarak eşit uzunlukta iki farklı rastgele p ve q asal sayıları seçer.

$$n = p.q \text{ ve } \varphi(n) = (p-1).(q-1)$$

değerini hesaplar. $2 < e < \varphi(n)$ ve $(\varphi(n), e) = 1$ olacak şekilde bir e tamsayısı seçer. Ayrıca,

$$e.d \equiv 1 \ (mod\ \varphi(n))$$

sağlayacak şekilde $1 < d < \varphi(n)$ aralığında d değeri hesaplar. A'nın açık anahtarı (n, e) ve özel anahtarı d'dir.

Şifreleme İşlemleri: B şahsı, A'ya bir m mesajını göndermek istediğini düşünelim. B, m mesajını şifrelemek için sırasıyla şu adımları yapar. Öncelikle A'nın açık anahtarı (n, e)'yi elinde olmalıdır. m mesajını $[0, n-1]$ aralığında değerler olarak yazar. Daha sonra $E \equiv m^e \ (mod\ n)$ değerini hesaplamalıdır. Şimdi, E şifresini A'ya gönderebilir.

Deşifreleme İşlemleri: A şahsı d gizli anahtarı ile $m \equiv E^d \ (mod\ n)$ işlemini uygularsa m açık metnine ulaşılabilir.

RSA anahtar üretiminde e ve d tamsayıları sırasıyla şifreleme ve şifre çözme üslerini, n ise mod sayısını gösterir. Günümüz teknolojisinde RSA'nın güvenli bir şekilde kullanılabilmesi için p ve q asal sayılarının en az 512 bit büyüklüğünde olması gerekir. Yani iki n asalının çarpımı 1024 bittir. Günümüz bilgisayarları ile 1024 bitlik bir sayıyı çarpanlarına ayırmak ve asal çarpanlarını bulmak yıllar alacaktır.

Burada verilecek örneklerde kolaylık açısından $p = 43, q = 59$ sayılar seçilmiştir. Örneğin, (1.44)'de verilen

"MATEMATİKTE ZEKADAN ÖNCE SABIR GELİR"

cümlesi RSA algoritması ile şifrelensin.

$$p = 43, q = 59$$

olmak üzere $n = 43.59$ için $\varphi(n) = (p-1).(q-1) = 2436$ olur.

e için $2 < e < \varphi(n)$ olup $e = 13$ olsun.

$$(n, e) = (2537, 13)$$

olur. Mesaj ikili bloklara ayrılıp sayısal değerleri bulunsun. Burada M şifreli değerler ve s de şifrelenecek her bir bloğu temsil etmek üzere;

MA TE MA Tİ KT EZ EK AD AN ÖN CE SA BI RG EL İR

şeklinde ayrılı ve Tablo 1.2'deki harflerin alfabedeki sayısal karşılıkları yazılır.

1500 2305 1500 2311 1323 0528 0513 0004

0016 1816 0205 2100 0110 2007 0514 1120

Her bir s bloğunu şifrelemek için $s^{13} \equiv M\ (mod\ 2537)$ bağıntısı kullanılarak şifreli M blokları elde edilir. İlk blok için

$$1505^{13} \equiv 784\ (mod\ 2537)$$

olur. Diğer bloklar için de aynı işlem tekrar edilirse

1320 784 1931 607 1981 2439 140 1841 2446 1209 466 1614 2125 752 1828

şifre bloklar elde edilir. Bütün olarak şifrelenmiş blok değerleri

0784 1320 784 1931 607 1981 2439 140 1841 2446 1209 466 1614 2125 752 1828

gönderilir.

Deşifrelemede kullanılacak olan d yi bulmada kullanılacak mod değeri ise $mod(\ \varphi(43.59)\ ) = mod(42.58\ ) = mod(\ 2436\ )$ olarak bulunur.

$e = 13$'ün tersi Öklid algoritması kullanılarak $e^{-1} = d = 937$ olarak bulunur.

$$M^{937} \equiv s\ (\ mod\ 2537\ )$$

kullanılarak her bir blok deşifre edilir.

$$784^{\ 937} \equiv 1500\ (\ mod\ 2537\ )$$

olup diğer bloklar için de aynı işlemler uygulanırsa açık metin:

2305 1500 2311 1323 0528 0513 0004 0016 1816 0205 2100 0110 2007 0514 1120

olarak bulunur. Tablo 1.2'deki sayısal değerlerin alfabedeki harfleri bulunursa deşifreleme işlemi sonlanır.

RSA algoritmasına yapılan en önemli saldırı, elde edilen açık anahtarı kullanarak gizli anahtara erişme girişimidir. Saldırgan n sayısının çarpanları olan p ve q değerlerini hesaplamaya çalışır. Bu değerler hesaplanabilirse gizli anahtara erişilebilir. Bu sürecin en zorlu yanı n'nin çarpanlarına ayrılmasıdır. Ancak n değeri yeterince büyük değilse ya da (p, q) çifti ve e değeri en uygun şekilde seçilmezse RSA'nın güvenli olduğu söylenemez.

El-Gamal Kriptosistemi

Bu sistem ilk olarak 1985 yılında Taher El-Gamal isimli Mısırlı bir matematikçi olan tarafından önerilmiştir. El-Gamal'ın açık anahtarlı şifre sistemi, anahtar transfer modunda bir Diffie-Hellman anahtar anlaşması olarak kabul edilebilir. Bu sistemin güvenilirliği ayrık logaritma problemine ve Diffie-Hellman problemini basit bir şekilde çözmenin zorluğuna bağlıdır (Elgamal, 1985).

Bu sistem de bir açık anahtar kriptosistemidir, ancak ayrık logaritma probleminin (DLP) zorluğuna dayandığı için RSA'dan farklıdır.

Anahtar üretim işlemleri: Her birey kendi açık anahtarını ve buna bağlı gizli anahtarını üretir. Daha sonra alıcının (B) anahtarı oluşturmak için aşağıdaki adımları gerçekleştirmesi gerekir.

Rastgele bir p asal sayısı ve $mod\ p$ ye göre tamsayıların oluşturduğu Z_p^* çarpım grubu ve bu grubun bir üreteci β değeri seçilir.

$1 \leq a \leq p-2$ şeklinde olan bir a tamsayısı seçilir ve $\beta^a mod\ p$ değerini hesaplanır.

B'nin açık anahtarı (p, β, β^a) ve B'nin gizli anahtarı ise a olur.

Şifreleme İşlemleri: Gönderici şahıs A, alıcı şahıs B için M uzunluğundaki bir mesajı şifrelemek isterse eğer, sırasıyla aşağıdaki adımları yapmalıdır.

- Alıcının açık anahtarı olan (p, β, β^a) alınır.
- Düz metindeki M uzunluğundaki her karakter $\{0,1,\dots,p-1\}$ aralığındaki bir m tamsayısı olarak ifade edilir.
- $1 \leq k \leq p-2$ eşitsizliğini sağlayan rastgele bir k tamsayısı seçilir.
- Bu k değeri kullanılarak $\gamma = \beta^k$ ve $\delta = m.(\beta^a)^k$ değerleri $modp$ ye göre hesaplanılır.
- Son olarak $E = (\gamma, \delta)$ kapalı metni alıcıya B gönderilir.

Böylelikle şifreli metin alıcıya ulaştığında deşifreleme işlemine başlayabilir.

Deşifreleme İşlemleri: Şifrelenmiş metin olan E sayısal değerli ifadesinden M açık metine ulaşmak için alıcı şahıs sırasıyla aşağıdaki adımları izlemelidir.

- Alıcı gizli anahtarı ile $\gamma^{p-1-a} = \beta^{p-1-ak}$ eşitliğini kullanarak γ^{-a} değerini $mod\ p$'ye göre hesaplanılır.
- Biliniyor ki $\gamma^{p-1-a} = \gamma^{-a} = \beta^{-ak}$ eşitliği sağlanır ki $\gamma^{-a}.\delta$ değeri hesaplanılır.
- Hesaplanılan değer karakter karşılığında değeri için

$$\gamma^{-a}.\delta \equiv m\ (mod\ p)$$

hesaplayarak m düz metin karakter değerleri bulunur.

Önceki örneklerde kullanılan metin ve $p = 2357$ asal sayısı seçilerek El-Gamal algoritması ile (1.44)'de verilen

"MATEMATİKTE ZEKADAN ÖNCE SABIR GELİR"

cümlesi için şifreleme ve deşifreleme işlemlerini verelim.

Bir anahtar oluşturmak için alıcı şahıs yeterince büyük bir $p = 2357$ asal sayısı seçer ve Z_{2357}^* çarpımsal grubu için $\beta = 2 \in Z_{2357}^*$ bir üretecini ele alalım.

Ayrıca gizli anahtar olarak $a = 1751 \leq 2355$ değerini seçelim. Daha sonra

$$\beta^a = 2^{1751} \equiv 1185 \ (mod\ 2357)$$

değeri hesaplanır. Alıcını açık anahtarı $(p, \beta, \beta^a) = (2357, 2, 1185)$ olur.

Herhangi bir gönderici alıcıya ait olan $(p, \beta, \beta^a) = (2357, 2, 1185)$ açık anahtarını alıp mesajı şifrelemek istediğinde

MA TE MA Tİ KT EZ EK AD AN ÖN CE SA BI RG EL İR

şeklinde parçalayıp ve Tablo 1.2'deki harflerin alfabedeki sayısal karşılıkları

1500 2305 1500 2311 1323 0528 0513 0004

0016 1816 0205 2100 0110 2007 0514 1120

yazılır. Her karakter iki basamaklı sayı olmak üzere düzenlenmiş 4 basamaklı sayılar ile 2 karakterin şifreli sayısal karşılıkları elde edilir.

Bunun için gönderinin kendisine ait gizli anahtarı olan bir $k = 1520$ tamsayısı seçelim. $m_1 = 1500$ mesajını şifrelemek için

$$\gamma = 2^{1520} \equiv 1430 \ (mod\ 2357)$$

$$\delta = 1500.1185^{1520} \equiv 618 \ (mod\ 2357)$$

değerleri hesaplanır. Gönderici şahıs ile iki karakteri $E_1 = (\gamma, \delta) = (1430, 618)$ şeklinde şifrelemiş olur.

Tüm m değerlerini $k = 1520$ için şifreleme yapılırsa gerekirse $\gamma = 1430$ değeri aynı olacağından tekrar hesaplanması verilmemiştir.

$m_2 = 2305$ için $\delta = 2305.1185^{1520} \equiv 54 \ (mod\ 2357)$

$m_3 = 1500$ için $\delta = 1500.1185^{1520} \equiv 618 \ (mod\ 2357)$

$m_4 = 2311$ için $\delta = 2311.1185^{1520} \equiv 773 (mod\ 2357)$

$m_5 = 1323$ için $\delta = 1323.1185^{1520} \equiv 1799 \ (mod\ 2357)$

$m_6 = 0528$ için $\delta = 528.1185^{1520} \equiv 1990 \ (mod\ 2357)$

$m_7 = 0513$ için $\delta = 513.1185^{1520} \equiv 1371 \ (mod\ 2357)$

$m_8 = 0004$ için $\delta = 4.1185^{1520} \equiv 1265 \ (mod\ 2357)$

$m_9 = 0016$ için $\delta = 16.1185^{1520} \equiv 346 \ (mod\ 2357)$

$m_{10} = 1816$ için $\delta = 1816.1185^{1520} \equiv 1559 \ (mod\ 2357)$

$m_{11} = 0205$ için $\delta = 205.1185^{1520} \equiv 603 \ (mod\ 2357)$

$m_{12} = 2100$ için $\delta = 2100.1185^{1520} \equiv 1880 \ (mod\ 2357)$

$m_{13} = 0110$ için $\delta = 0110.1185^{1520} \equiv 611 \ (mod\ 2357)$

$m_{14} = 2007$ için $\delta = 2007.1185^{1520} \equiv 1270\ (mod\ 2357)$

$m_{15} = 0514$ için $\delta = 514.1185^{1520} \equiv 1098\ (mod\ 2357)$

$m_{16} = 1120$ için $\delta = 1120.1185^{1520} \equiv 650\ (mod\ 2357)$

değerleri hesaplanır.

Tablo 1.4 El Gamal ile sayısal değerin şifrelenmiş değerleri

Düz metin	M A	T E	M A	T İ	K T	E Z	E K	A D
m_i	1500	2305	1500	2311	1323	0528	0513	0004
δ_i	0618	0054	0618	0773	1799	1990	1371	1265
Düz metin	A N	Ö N	C E	S A	B I	R G	E L	İ R
m_i	0016	1816	0205	2100	0110	2007	0514	1120
δ_i	0346	1559	0603	1808	0611	1270	1098	0650

E_i değerlerin de $\gamma = 1430$ değeri sabit olduğu için tabloda sadece δ_i değerlerine yer verilmiştir. Gönderici şifrelenmiş metin olarak alıcıya $E_i = (\gamma\ ,\ \delta_i),\ 1 \leq i \leq 16$ şekli ile gönderebilir.

Alıcı, göndericiden gelen şifrelenmiş metni çözmek için $\gamma^{p-1-a} = 1430^{-1751}$ eşitliğini kullanarak

$$1430^{605} \equiv 872\ (mod\ 2357)$$

ifadesini hesaplar ki γ^{-a} değerlerini elde edilir. M mesajına ulaşmak için karakter değerlerine teker teker

$$m_i = 872.\delta_i (mod\ 2357)$$

denkliğindeki değerler bulunur. Sırasıyla tüm m_i değerlerini hesaplamak gerekirse,

$$m_1 = 872.618 \equiv 1500 (mod\ 2357)$$
$$m_2 = 872.54 \equiv 2305 (mod\ 2357)$$
$$m_3 = 872.618 \equiv 1500 (mod\ 2357)$$
$$m_4 = 872.773 \equiv 2311 (mod\ 2357)$$
$$m_5 = 872.1799 \equiv 1323 (mod\ 2357)$$
$$m_6 = 872.1990 \equiv 528 (mod\ 2357)$$
$$m_7 = 872.1371 \equiv 513 (mod\ 2357)$$
$$m_8 = 872.1265 \equiv 4 (mod\ 2357)$$
$$m_9 = 872.346 \equiv 16 (mod\ 2357)$$
$$m_{10} = 872.1559 \equiv 1816 (mod\ 2357)$$
$$m_{11} = 872.603 \equiv 205 (mod\ 2357)$$
$$m_{12} = 872.1808 \equiv 2100 (mod\ 2357)$$
$$m_{13} = 872.611 \equiv 110 (mod\ 2357)$$

$$m_{14} = 872.1270 \equiv 2007(mod\ 2357)$$
$$m_{15} = 872.1098 \equiv 514(mod\ 2357)$$
$$m_{16} = 872.650 \equiv 1120(mod\ 2357)$$

değerleri hesaplanır ki Tablo 1.2'deki sayısal değerlerin harf karşılıkları göz önüne alınırsa Tablo 1.5'deki görüldüğü gibi düz metnin parçalı hali elde edilir.

Tablo 1.5 El Gamal ile şifrelenmiş değerlerin sayısal değerleri ve karakterleri

δ_i	618	54	618	773	1799	1990	1371	1265
m_i	1500	2305	1500	2311	1323	0528	0513	0004
Düz metin	M A	T E	M A	T İ	K T	E Z	E K	A D
δ_i	346	1559	603	1808	611	1270	1098	650
m_i	0016	1816	0205	2100	0110	2007	0514	1120
Düz metin	A N	Ö N	C E	S A	B I	R G	E L	İ R

El-Gamal şifreleme ile şifreleme gücünün her seferinde değiştirilmesi şifrelemenin güvenliğini artırır.

Açık ve gizli anahtarlı şifreleme sistemlerin karşılaştırılması

Açık ve gizli anahtar şifreleme sistemleri birbirlerine entegre etme avantajlarına sahiptirler. Günümüzün şifreleme sistemleri genellikle her ikisinin gücünü kullanmak için geliştirilmiştir. Bu sistemlerin bazı avantaj ve dezavantajlarını aşağıda listeleyebiliriz:

1. Anahtar uzunluğu açık anahtar şifrelemeyle karşılaştırıldığında daha kısadır.

2. Gizli anahtar şifrelemesinde, iki ayrı taraf arasındaki iletişim, her iki tarafın anahtara sahip olmasını ve onu gizli tutmasını gerektirir, ancak açık anahtardaki şifrelemede, tarafların yalnızca kendi özel anahtardan gizli kalmaları yeterlidir.

3. Gizli anahtar şifrelemelerinde, şifreleme açık anahtara kıyasla oldukça hızlıdır.

Gizli anahtar şifrelemesinde, anahtara güvenlik açısından sık sık güncelleme yapılması gerekirken, açık anahtardaki şifrelemede, genel-özel anahtardan oluşan çiftin uzun süreli olarak değiştirilmesi gerekmeyebilir.

Melez Kriptosistemler

Günümüzde bilgi güvenli kullanımı, iletimi, depolaması ve iletişimlerin geniş ve hızlı teslimatı giderek daha önemli hale geldi. Bunun sonucunda simetrik ve asimetrik algoritma sistemleri aynı anda kullanıldı. Böyle karmaşık sistemlerin avantajlarını ve dezavantajlarını değerlendirirken, anahtar şifreleme, sayısal imzalar gibi işlemler

asimetrik sistemlerle gerçekleştirilirken, grup veri işleme ve veri bütünlüğü koruma işlemleri simetrik algoritma sistemleri kullanılarak gerçekleştirilir.

Bu tezde incelenecek olan sistem bir melez kriptosistem çeşidi değerlendirmesidir. Bu yüzden poligrafik şifreleme çeşitlerinden Hill şifrelemeye ve bir varyasyonu olan Affine-Hill şifrelemeye açıklık getirmeye çalışalım.

1.3.2 Hill Şifreleme

Hill şifreleme algoritması (Hill,1929; Hill,1931), doğrusal dönüşüme dayalı bir poligrafik şifreleme algoritmasıdır ve 1929'da Lester S. Hill tarafından icat edilmiştir. Hill şifreleme, düz metnin eşit boyutlu bloklara bölündüğü bir blok şifreleme algoritmasıdır. Klasik kriptografide, Hill şifresi (Stinson, 2005), (Obaid, 2016), (Öztürkmenoğlu, 2016) çalışmalarında verildiği üzere 1929 yılında matematikçi Lester Hill tarafından geliştirilen kalan (mod) sistemi ve matris dönüşümlerine dayanan ilk poligrafik yer değiştirme şifrelemelerinden birisidir (Thilaka, 2005), (Ismail ve ark. 2006), (Gupta, 2007), (Toorani, 2009), (Mahmoud ve Chefranov, 2010), (Viswanath ve Kumar, 2015).

Araştırmalar, Hill şifrelemenin klasik kriptografik algoritmalar arasında güvenlik açısından çok güçlü olduğunu, çünkü Hill Şifresinin düz metindeki her aynı alfabeyi şifreli metindeki aynı diğer alfabe ile değiştirmediğini göstermektedir.

Bir Hill şifrelemede, gizli anahtar $n \times n$ boyutunda K tekil olmayan bir matristir. Hill şifreleme algoritmasında, anahtar matris K, $n \times n$ boyutlu olduğu için n ardışık düz metin harfi, sayısal bir değer karşılığına atanıp anahtar matris kullanılarak bulunan değerlerin yine aynı sayısal değerlerin bu tablodaki n şifreli metin harfiyle değiştirir. Yani, düz metin için $P = [p_{i1}]$, $n \times 1$ sütun matrisi

$$P = [p_1 \quad p_2 \quad \dots \quad p_n]^T \tag{1.45}$$

anahtar matrisi için $K = [k_{ij}]$, $n \times n$ boyutunda matrisi

$$K = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1n} \\ k_{21} & k_{22} & \dots & k_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ k_{n1} & k_{n2} & \dots & k_{nn} \end{bmatrix} \tag{1.46}$$

şifreli metin (şifreli matris) için $C = [c_{i1}]$, $n \times 1$ sütun matrisi

$$C = [c_1 \quad c_2 \quad \dots \quad c_n]^T \tag{1.47}$$

gösterimini kullanılırsa; C şifreli metin bloğu

$$C = KP \, mod(m) \tag{1.48}$$

olarak şifrelenir.

Şifreli metnin çözülmesi için,

$$ebob\ ((det\ (K) mod\ m), m)\ = 1 \tag{1.49}$$

şartı sağlanıyor ise

$$P\ =\ K^{-1}\ C\ mod\ m \tag{1.50}$$

olarak düz metin üretilebilir. Eğer çok sayıda blok ile çalışılacaksa P_i'ler ve C_i'ler $1 \times n$ boyutunda blok matrisler ve p asal sayısı için $ebob(det(K), p) = 1$ olmak üzere, Hill şifreleme-şifre çözme tekniği

$$Şifreleme(P)\colon C_i \equiv KP_i(modp) \tag{1.51}$$

$$Deşifreleme(C)\colon P_i \equiv K^{-1}C_i(modp) \tag{1.52}$$

şeklinde $i = 1, ,2, \ldots,$ sayıda tekrarlanır.

Sistemi (1.44)'de verilen bir örnek cümle üzerinde anlatacak olursak;

"MATEMATİKTE ZEKADAN ÖNCE SABIR GELİR"

cümlesini Hill şifreleme yöntemi ile 2×2 lik bir anahtar matris kullanarak şifreleyelim.

Adım 1. m kullanılan alfabedeki karakter sayısına göre $ebob(det(K), m) = 1$ şartını sağlayan $n \times n$ boyutunda tekil olmayan bir anahtar matris seçilmelidir.

(1.27)'deki Q_L Lucas matrisi 2×2 lik bir anahtar matrisi olarak

$$Q_L = \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix}$$

seçelim ki $|Q_L| = 5$ olduğundan $ebob(|Q_L|, 29) = 1$ olduğu için uygun bir matristir.

Adım 2. Düz metindeki harfler 2×2 lik bir anahtar matrisi olduğu için ikililer halinde gruplanır. Gruplanan ikililer Tablo 1.2'deki harflerin alfabedeki sayı değerine göre Tablo 1.6'deki gibi yazılır.

Tablo 1.6 Düz metindeki karakterlerin sayısal değerleri

Metin	M A	T E	M A	T İ	K T	E Z	E K	A D
P_i	$\begin{bmatrix}15\\0\end{bmatrix}$	$\begin{bmatrix}23\\5\end{bmatrix}$	$\begin{bmatrix}15\\0\end{bmatrix}$	$\begin{bmatrix}23\\11\end{bmatrix}$	$\begin{bmatrix}13\\23\end{bmatrix}$	$\begin{bmatrix}5\\28\end{bmatrix}$	$\begin{bmatrix}5\\13\end{bmatrix}$	$\begin{bmatrix}0\\4\end{bmatrix}$
Metin	A N	Ö N	C E	S A	B I	R G	E L	İ R
P_i	$\begin{bmatrix}0\\16\end{bmatrix}$	$\begin{bmatrix}18\\16\end{bmatrix}$	$\begin{bmatrix}2\\5\end{bmatrix}$	$\begin{bmatrix}21\\0\end{bmatrix}$	$\begin{bmatrix}1\\10\end{bmatrix}$	$\begin{bmatrix}20\\7\end{bmatrix}$	$\begin{bmatrix}5\\14\end{bmatrix}$	$\begin{bmatrix}11\\20\end{bmatrix}$

Adım 3. (1.51)'deki değerler yerlerine yazılarak, düz metin ikililerinin seçilen (1.27)'deki Q_L matrisi çarpılır. Şifreli metin için sayısal değerli sütün vektörü oluşturulur. Örneğin $i = 1$ için $C_1 \equiv KP_1(mod29)$ hesaplayalım:

$$\begin{bmatrix}3 & 1\\1 & 2\end{bmatrix}\begin{bmatrix}15\\0\end{bmatrix} \equiv \begin{bmatrix}45\\15\end{bmatrix}(mod29)$$

29 dan büyük sayılar çıkarsa, bu tam sayıların 29 ile bölümünden kalan değer alınacaktır.

$$\begin{bmatrix}3 & 1\\1 & 2\end{bmatrix}\begin{bmatrix}15\\0\end{bmatrix} = \begin{bmatrix}45\\15\end{bmatrix}(mod29) \equiv \begin{bmatrix}16\\15\end{bmatrix} = C_1$$

$i = 2,3, \dots 16$ değerleri için (1.51)'de değerler hesaplanırsa;

Tablo 1.7 Şifrelenmiş metindeki sayısal değerler

i	$KP_i(modp) \equiv C_i$	i	$KP_i(modp) \equiv C_i$
2	$\begin{bmatrix}3 & 1\\1 & 2\end{bmatrix}\begin{bmatrix}23\\5\end{bmatrix} \equiv \begin{bmatrix}16\\4\end{bmatrix}(mod29)$	10	$\begin{bmatrix}3 & 1\\1 & 2\end{bmatrix}\begin{bmatrix}18\\16\end{bmatrix} \equiv \begin{bmatrix}12\\21\end{bmatrix}(mod29)$
3	$\begin{bmatrix}3 & 1\\1 & 2\end{bmatrix}\begin{bmatrix}15\\0\end{bmatrix} \equiv \begin{bmatrix}16\\15\end{bmatrix}(mod29)$	11	$\begin{bmatrix}3 & 1\\1 & 2\end{bmatrix}\begin{bmatrix}2\\5\end{bmatrix} \equiv \begin{bmatrix}11\\12\end{bmatrix}(mod29)$
4	$\begin{bmatrix}3 & 1\\1 & 2\end{bmatrix}\begin{bmatrix}23\\11\end{bmatrix} \equiv \begin{bmatrix}22\\16\end{bmatrix}(mod29)$	12	$\begin{bmatrix}3 & 1\\1 & 2\end{bmatrix}\begin{bmatrix}21\\0\end{bmatrix} \equiv \begin{bmatrix}5\\21\end{bmatrix}(mod29)$
5	$\begin{bmatrix}3 & 1\\1 & 2\end{bmatrix}\begin{bmatrix}13\\23\end{bmatrix} \equiv \begin{bmatrix}4\\1\end{bmatrix}(mod29)$	13	$\begin{bmatrix}3 & 1\\1 & 2\end{bmatrix}\begin{bmatrix}1\\10\end{bmatrix} \equiv \begin{bmatrix}13\\21\end{bmatrix}(mod29)$
6	$\begin{bmatrix}3 & 1\\1 & 2\end{bmatrix}\begin{bmatrix}5\\28\end{bmatrix} \equiv \begin{bmatrix}14\\3\end{bmatrix}(mod29)$	14	$\begin{bmatrix}3 & 1\\1 & 2\end{bmatrix}\begin{bmatrix}20\\7\end{bmatrix} \equiv \begin{bmatrix}9\\5\end{bmatrix}(mod29)$
7	$\begin{bmatrix}3 & 1\\1 & 2\end{bmatrix}\begin{bmatrix}5\\13\end{bmatrix} \equiv \begin{bmatrix}28\\2\end{bmatrix}(mod29)$	15	$\begin{bmatrix}3 & 1\\1 & 2\end{bmatrix}\begin{bmatrix}5\\14\end{bmatrix} \equiv \begin{bmatrix}0\\4\end{bmatrix}(mod29)$
8	$\begin{bmatrix}3 & 1\\1 & 2\end{bmatrix}\begin{bmatrix}0\\4\end{bmatrix} \equiv \begin{bmatrix}4\\8\end{bmatrix}(mod29)$	16	$\begin{bmatrix}3 & 1\\1 & 2\end{bmatrix}\begin{bmatrix}11\\20\end{bmatrix} \equiv \begin{bmatrix}24\\22\end{bmatrix}(mod29)$
9	$\begin{bmatrix}3 & 1\\1 & 2\end{bmatrix}\begin{bmatrix}0\\16\end{bmatrix} \equiv \begin{bmatrix}16\\3\end{bmatrix}(mod29)$		

Adım 4. Elde edilen $C_i, i = 1,2, \dots 16$ değerlerine karşılık gelen şifreli metin vektöründeki sayı değerlerinin Tablo 1.2'deki alfabedeki harf değerine dönüştürülüp şifrelenmiş metin karakterleri elde edilir.

Tablo 1.8 Sayısal değerlerin şifrelenmiş harf karşılıkları

i	1	2	3	4	5	6	7	8
C_i	$\begin{bmatrix}16\\15\end{bmatrix}$	$\begin{bmatrix}16\\4\end{bmatrix}$	$\begin{bmatrix}16\\15\end{bmatrix}$	$\begin{bmatrix}22\\16\end{bmatrix}$	$\begin{bmatrix}4\\1\end{bmatrix}$	$\begin{bmatrix}14\\3\end{bmatrix}$	$\begin{bmatrix}28\\2\end{bmatrix}$	$\begin{bmatrix}4\\8\end{bmatrix}$
Şif. Met.	N M	N D	N M	Ş N	D B	L Ç	Z C	D Ğ
i	9	10	11	12	13	14	15	16
C_i	$\begin{bmatrix}16\\3\end{bmatrix}$	$\begin{bmatrix}12\\21\end{bmatrix}$	$\begin{bmatrix}11\\12\end{bmatrix}$	$\begin{bmatrix}5\\21\end{bmatrix}$	$\begin{bmatrix}13\\21\end{bmatrix}$	$\begin{bmatrix}9\\5\end{bmatrix}$	$\begin{bmatrix}0\\4\end{bmatrix}$	$\begin{bmatrix}24\\22\end{bmatrix}$
Şif. Met.	N Ç	J S	İ J	E S	K S	H E	A D	U Ş

Bu karakterler istenilirse düz metinin sahip olduğu kelimeler şeklinde parçalanarak yada tamamen birleştirilmiş şekilde ard arda birleştirilir. Örneğimizi düz metindeki gibi

"NMNDNMŞNDBL ÇZCDĞNÇ JSİJ ESKSH EADUŞ"

şeklinde elde şifreleyip alıcıya iletiriz.

Her kullanılabilir şifreme metoduna göre, şifrelenmiş metni çözmek için bir yönteme sahip olmak zorundadır.

Bir Hill şifresinde şifre çözme için anahtar matrisinin $(modm)$'de tersinin alınabilir olduğunu ve bunların terslerinin nasıl elde edildiğini bilmek önemlidir. Yani Tanım 1.11'deki gibi terslenebilir bir anahtar matris seçilmesi gerekir.

$n \times n$ mertebeden bir A matrisi için Teorem 1.3 ve Teorem 1.4' e göre bahsedildiği için burada sadece kısaca tekrar edilecektir.

Girdileri Z_m'de olan $n \times n$ mertebeden bir K matrisinin $(modm)$ de tersi, ancak ve ancak $det(K)$'nın $(modm)$'deki kalanı $(modm)$ de bir terse sahipse alınabilir.

$det(K)$'nın $(mod\ m)$'deki kalanının $(mod\ m)$'de tersi ancak ve ancak bu kalan m sayısının ortak asal çarpanına sahip olmadığında tersi alınabilir.

O halde Tablo 1.2'deki alfabedeki harf değerine göre $m = 29$ asal olduğu için $det(K) \neq 0$ ve $det(K) \neq 29k, k \in Z$ şeklindeki herhangi bir anahtar matrisine göre tersi allanabilir bir matris olur.

(1.27)'deki Q_L Lucas matrisi için $|Q_L| = 5$ ve $ebob(|Q_L|, 29) = 1$'e göre Q_L^{-1} matrisini hesaplayalım. $|Q_L| = 5$'nın $mod\ 29$'da bir tersi alınabilir ki

$$5\big(det(A)\big)^{-1} \equiv 1(mod\ 29)$$

$$\big(det(A)\big)^{-1} \equiv 6(mod\ 29)$$

elde edilir. O halde anahtar matrisini tersi $(mod\ 29)$'a göre farklı şekillerde

$$Q_L^{-1} \equiv \begin{pmatrix} 12 & -6 \\ -6 & 18 \end{pmatrix} (mod\ 29)$$

$$Q_L^{-1} \equiv \begin{pmatrix} 12 & 23 \\ 23 & 18 \end{pmatrix} (mod\ 29)$$

yazılabilir. Genel olarak matris işlemleri için elemanları farklı işaretli olanını tercih edeceğiz. Bu yüzden (1.50)'daki $P = K^{-1}\, C\ mod\ m$ işlemleri 2×2 lik bir anahtar matrisi olduğu için şifreli metindeki harfler ikililer halinde gruplanır. Gruplanan ikililer Tablo 1.2'deki harflerin alfabedeki sayı değerine göre Tablo 1.9'daki gibi yazılır.

Tablo 1.9 Şifrelenmiş harflerin sayısal değer karşılıkları

i	1	2	3	4	5	6	7	8
Şif. Met.	N M	N D	N M	Ş N	D B	L Ç	Z C	D Ğ
C_i	$\begin{bmatrix}16\\15\end{bmatrix}$	$\begin{bmatrix}16\\4\end{bmatrix}$	$\begin{bmatrix}16\\15\end{bmatrix}$	$\begin{bmatrix}22\\16\end{bmatrix}$	$\begin{bmatrix}4\\1\end{bmatrix}$	$\begin{bmatrix}14\\3\end{bmatrix}$	$\begin{bmatrix}28\\2\end{bmatrix}$	$\begin{bmatrix}4\\8\end{bmatrix}$
i	9	10	11	12	13	14	15	16
Şif. Met.	N Ç	J S	İ J	E S	K S	H E	A D	U Ş
C_i	$\begin{bmatrix}16\\3\end{bmatrix}$	$\begin{bmatrix}12\\21\end{bmatrix}$	$\begin{bmatrix}11\\12\end{bmatrix}$	$\begin{bmatrix}5\\21\end{bmatrix}$	$\begin{bmatrix}13\\21\end{bmatrix}$	$\begin{bmatrix}9\\5\end{bmatrix}$	$\begin{bmatrix}0\\4\end{bmatrix}$	$\begin{bmatrix}24\\22\end{bmatrix}$

(1.52)'deki değerler yerlerine yazılarak, şifreli metin ikililerinin anahtar matris Q_L ile çarpılır. Düz metin için sayısal değerli sütün vektörü oluşturulur. Örneğin $i = 1$ için $P_1 \equiv K^{-1}C_1(mod29)$ hesaplayalım:

$$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\begin{bmatrix}16\\15\end{bmatrix} \equiv \begin{bmatrix}15\\0\end{bmatrix}(mod29)$$

29 dan büyük sayılar çıkarsa, bu tam sayıların 29 ile bölümünden kalan değer alınacaktır.

Tablo 1.10 Düz metindeki sayısal değerler

i	$K^{-1}C_i(modp) \equiv P_i$	i	$K^{-1}C_i(modp) \equiv P_i$
2	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\begin{bmatrix}16\\4\end{bmatrix} \equiv \begin{bmatrix}23\\5\end{bmatrix}(mod29)$	10	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\begin{bmatrix}12\\21\end{bmatrix} \equiv \begin{bmatrix}18\\16\end{bmatrix}(mod29)$
3	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\begin{bmatrix}16\\15\end{bmatrix} \equiv \begin{bmatrix}15\\0\end{bmatrix}(mod29)$	11	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\begin{bmatrix}11\\12\end{bmatrix} \equiv \begin{bmatrix}2\\5\end{bmatrix}(mod29)$
4	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\begin{bmatrix}22\\16\end{bmatrix} \equiv \begin{bmatrix}23\\11\end{bmatrix}(mod29)$	12	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\begin{bmatrix}5\\21\end{bmatrix} \equiv \begin{bmatrix}21\\0\end{bmatrix}(mod29)$
5	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\begin{bmatrix}4\\1\end{bmatrix} \equiv \begin{bmatrix}13\\23\end{bmatrix}(mod29)$	13	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\begin{bmatrix}1\\10\end{bmatrix} \equiv \begin{bmatrix}1\\10\end{bmatrix}(mod29)$
6	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\begin{bmatrix}14\\3\end{bmatrix} \equiv \begin{bmatrix}5\\28\end{bmatrix}(mod29)$	14	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\begin{bmatrix}9\\5\end{bmatrix} \equiv \begin{bmatrix}20\\7\end{bmatrix}(mod29)$
7	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\begin{bmatrix}28\\2\end{bmatrix} \equiv \begin{bmatrix}5\\13\end{bmatrix}(mod29)$	15	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\begin{bmatrix}0\\4\end{bmatrix} \equiv \begin{bmatrix}5\\14\end{bmatrix}(mod29)$
8	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\begin{bmatrix}4\\8\end{bmatrix} \equiv \begin{bmatrix}0\\4\end{bmatrix}(mod29)$	16	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\begin{bmatrix}24\\22\end{bmatrix} \equiv \begin{bmatrix}11\\20\end{bmatrix}(mod29)$
9	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\begin{bmatrix}16\\3\end{bmatrix} \equiv \begin{bmatrix}0\\16\end{bmatrix}(mod29)$		

Elde edilen $P_i, i = 1,2, \dots 16$ değerlerine karşılık gelen düz metin vektöründeki sayı değerlerinin Tablo 1.2'deki alfabedeki harf değerine dönüştürülüp şifrelenmiş düz karakterleri Tablo 1.11'da elde edilir.

Tablo 1.11 Sayısal değerlerin düz metindeki karakter değerleri

i	1	2	3	4	5	6	7	8
P_i	$\begin{bmatrix}15\\0\end{bmatrix}$	$\begin{bmatrix}23\\5\end{bmatrix}$	$\begin{bmatrix}15\\0\end{bmatrix}$	$\begin{bmatrix}23\\11\end{bmatrix}$	$\begin{bmatrix}13\\23\end{bmatrix}$	$\begin{bmatrix}5\\28\end{bmatrix}$	$\begin{bmatrix}5\\13\end{bmatrix}$	$\begin{bmatrix}0\\4\end{bmatrix}$
Düz metin	M A	T E	M A	T İ	K T	E Z	E K	A D
i	9	10	11	12	13	14	15	16
P_i	$\begin{bmatrix}0\\16\end{bmatrix}$	$\begin{bmatrix}18\\16\end{bmatrix}$	$\begin{bmatrix}2\\5\end{bmatrix}$	$\begin{bmatrix}21\\0\end{bmatrix}$	$\begin{bmatrix}1\\10\end{bmatrix}$	$\begin{bmatrix}20\\7\end{bmatrix}$	$\begin{bmatrix}5\\14\end{bmatrix}$	$\begin{bmatrix}11\\20\end{bmatrix}$
Düz metin	A N	Ö N	C E	S A	B I	R G	E L	İ R

Görülüyor ki, şifrelenecek metinin uzun (32 karakter) ve anahtar matris boyutu (2×2) işlemlerin sayısını ve zorluğunu etkilemektedir. Düz metin ikili gruplara ayrılır ve 2×2 lik bir anahtar matris kullanılarak şifrelenirse ***Hill 2-şifresi*** olarak anılır. Düz metni üçlüler halinde gruplamak ve tam sayı girdili 3×3'lük bir matrisle şifrelenirse ***Hill 3-şifresi*** denir. Genel olarak, bir ***Hill n-şifresi*** için düz metin n harfli kümelere gruplanır ve tam sayı girdili $n \times n$'lik matrisle şifrelenir.

1.3.3 Affine-Hill Şifreleme

Yer değiştirme şifresinin özel durumlarından biri Affine Şifresidir (Stinson, 2005), (Toorani, ve Ark., 2011), (Sundarayya ve Ark., 2019), (Prasad ve Ark., 2021).

$a, b, x, y \in Z_m$ ve $gcd(a, m) = 1$ olmak üzere Affine Şifresi

Şifreleme (x): $$y \equiv (ax + b)(modm) \quad (1.53)$$

şekilde tanımlanır. $gcd(a, m) = 1$ ifadesi a^{-1}'in varlığını doğruladığı için

Deşifreleme (y): $$x \equiv a^{-1}(y - b)(modm) \quad (1.54)$$

şeklinde tanımlanır.

Affine-Hill Şifresi, yukarıda açıklandığı gibi Hill Şifresi kavramını genişleten poligrafik bir blok şifredir. Şifreleme-şifre çözme tekniğini tanımlamak için P_i, C_i ve B, $n \times 1$ boyutlu matrisleri, K, $n \times n$ boyutlu anahtar matrisi, m düz metinde kullanılan farklı karakter sayısı olmak üzere

Şifreleme (P): $$C_i \equiv (KP_i + B)(modm) \quad (1.55)$$

Deşifreleme (C): $$P_i \equiv K^{-1}(C_i - B)(modm) \quad (1.56)$$

şekilde verilir.

Sistemi (1.44)'deki örnek cümle üzerinde anlatacak olursak;

"MATEMATİKTE ZEKADAN ÖNCE SABIR GELİR"

cümlesini Affline-Hill ile şifrelenme yöntemi ile 2×2 lik bir anahtar matris olarak $K = Q_L = \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix}$ ve 2×1 lik bir vektör matris $B = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$ olsun kullanarak şifreleyelim. Cümledeki karakterleri kili gruplara ayıralım.

MA TE MA Tİ KT EZ EK AD AN ÖN CE SA BI RG EL İR

Gruplanan ikililer Tablo 1.2'deki harflerin alfabedeki sayı değerine göre Tablo 1.12'deki gibi yazılırsa

Tablo 1.12 Düz metindeki karakterlerin sayısal değerleri

Metin	M A	T E	M A	T İ	K T	E Z	E K	A D
P_i	$\begin{bmatrix} 15 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 23 \\ 5 \end{bmatrix}$	$\begin{bmatrix} 15 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 23 \\ 11 \end{bmatrix}$	$\begin{bmatrix} 13 \\ 23 \end{bmatrix}$	$\begin{bmatrix} 5 \\ 28 \end{bmatrix}$	$\begin{bmatrix} 5 \\ 13 \end{bmatrix}$	$\begin{bmatrix} 0 \\ 4 \end{bmatrix}$
Metin	A N	Ö N	C E	S A	B I	R G	E L	İ R
P_i	$\begin{bmatrix} 0 \\ 16 \end{bmatrix}$	$\begin{bmatrix} 18 \\ 16 \end{bmatrix}$	$\begin{bmatrix} 2 \\ 5 \end{bmatrix}$	$\begin{bmatrix} 21 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 1 \\ 10 \end{bmatrix}$	$\begin{bmatrix} 20 \\ 7 \end{bmatrix}$	$\begin{bmatrix} 5 \\ 14 \end{bmatrix}$	$\begin{bmatrix} 11 \\ 20 \end{bmatrix}$

olur. $C_i \equiv (KP_i + B)(modp)$ bağıntısını kullanarak şifreleme yapılırsa

Tablo 1.13 Şifrelenmiş metindeki sayısal değerler

i	$KP_i(modp) \equiv C_i$	i	$KP_i(modp) \equiv C_i$
1	$\begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 15 \\ 0 \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \end{bmatrix} \equiv \begin{bmatrix} 18 \\ 16 \end{bmatrix} (mod 29)$	9	$\begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 0 \\ 16 \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \end{bmatrix} \equiv \begin{bmatrix} 18 \\ 4 \end{bmatrix} (mod 29)$
2	$\begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 23 \\ 5 \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \end{bmatrix} \equiv \begin{bmatrix} 18 \\ 5 \end{bmatrix} (mod 29)$	10	$\begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 18 \\ 16 \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \end{bmatrix} \equiv \begin{bmatrix} 14 \\ 22 \end{bmatrix} (mod 29)$
3	$\begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 15 \\ 0 \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \end{bmatrix} \equiv \begin{bmatrix} 18 \\ 16 \end{bmatrix} (mod 29)$	11	$\begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 2 \\ 5 \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \end{bmatrix} \equiv \begin{bmatrix} 13 \\ 13 \end{bmatrix} (mod 29)$
4	$\begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 23 \\ 11 \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \end{bmatrix} \equiv \begin{bmatrix} 24 \\ 17 \end{bmatrix} (mod 29)$	12	$\begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 21 \\ 0 \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \end{bmatrix} \equiv \begin{bmatrix} 7 \\ 22 \end{bmatrix} (mod 29)$
5	$\begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 13 \\ 23 \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \end{bmatrix} \equiv \begin{bmatrix} 6 \\ 2 \end{bmatrix} (mod 29)$	13	$\begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 1 \\ 10 \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 22 \end{bmatrix} (mod 29)$
6	$\begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 5 \\ 28 \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \end{bmatrix} \equiv \begin{bmatrix} 16 \\ 4 \end{bmatrix} (mod 29)$	14	$\begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 20 \\ 7 \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \end{bmatrix} \equiv \begin{bmatrix} 11 \\ 6 \end{bmatrix} (mod 29)$
7	$\begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 5 \\ 13 \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \end{bmatrix} \equiv \begin{bmatrix} 1 \\ 3 \end{bmatrix} (mod 29)$	15	$\begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 5 \\ 14 \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \end{bmatrix} \equiv \begin{bmatrix} 2 \\ 5 \end{bmatrix} (mod 29)$
8	$\begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 0 \\ 4 \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \end{bmatrix} \equiv \begin{bmatrix} 6 \\ 9 \end{bmatrix} (mod 29)$	16	$\begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 11 \\ 20 \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \end{bmatrix} \equiv \begin{bmatrix} 26 \\ 23 \end{bmatrix} (mod 29)$

şifrelenmiş metindeki sayısal değerler Tablo 1.13'deki gibi elde edilir. Elde edilen $C_i, i = 1,2, \ldots 16$ değerlerine karşılık gelen şifreli metin vektöründeki sayı değerlerinin Tablo 1.2'deki alfabedeki harf değerine dönüştürülüp şifrelenmiş metin karakterleri elde edilir.

Tablo 1.14 Sayısal değerlerin şifrelenmiş harf karşılıkları

i	1	2	3	4	5	6	7	8
C_i	$\begin{bmatrix}18\\16\end{bmatrix}$	$\begin{bmatrix}18\\5\end{bmatrix}$	$\begin{bmatrix}18\\16\end{bmatrix}$	$\begin{bmatrix}24\\17\end{bmatrix}$	$\begin{bmatrix}6\\2\end{bmatrix}$	$\begin{bmatrix}16\\4\end{bmatrix}$	$\begin{bmatrix}1\\3\end{bmatrix}$	$\begin{bmatrix}6\\9\end{bmatrix}$
Şif. Met.	Ö N	Ö E	Ö N	U O	F C	N D	B Ç	F H
i	9	10	11	12	13	14	15	16
C_i	$\begin{bmatrix}18\\4\end{bmatrix}$	$\begin{bmatrix}14\\22\end{bmatrix}$	$\begin{bmatrix}13\\13\end{bmatrix}$	$\begin{bmatrix}7\\22\end{bmatrix}$	$\begin{bmatrix}15\\22\end{bmatrix}$	$\begin{bmatrix}11\\6\end{bmatrix}$	$\begin{bmatrix}2\\5\end{bmatrix}$	$\begin{bmatrix}26\\23\end{bmatrix}$
Şif. Met.	Ö D	L Ş	K K	G Ş	M Ş	İ F	C E	V T

Bu karakterler istenilirse düz metinin sahip olduğu kelimeler şeklinde parçalanarak yada tamamen birleştirilmiş şekilde ard arda birleştirilir. Örneğimizi düz metindeki gibi

"ÖNÖEÖNUOFCN DBÇFHÖD LŞKK GŞMŞİ FCEVT"

şeklinde elde şifreleyip alıcıya iletiriz.

Benzer şekilde Affiline-Hill şifreme metoduna göre, şifrelenmiş metni çözmek için bir yönteme sahip olmak gerekir.

Affline-Hill Deşifreleme: Hill şifrelemedekine benzer şekilde bir yöntem izlenerek deşifreleme yapılacaktır. $P_i \equiv K^{-1}(C_i - B)(modp)$ bağıntısını kullanarak deşifreleme yapılır. Öncelikle Q_L matrisinin tersini bulalım.

$$Q_L^{-1} = \frac{1}{|Q_L|}\begin{bmatrix}2 & -1\\-1 & 3\end{bmatrix}(mod29)$$

$|Q_L| = 5$'nın $mod\ 29$'da bir tersi alınabilir ki

$$5(|Q_L|)^{-1} \equiv 1(mod\ 29)$$

$$(|Q_L|)^{-1} \equiv 6(mod\ 29)$$

elde edilir. O halde anahtar matrisini tersi $(mod\ 29)$'a göre farklı şekillerde

$$Q_L^{-1} \equiv \begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}(mod\ 29) \text{ veya } Q_L^{-1} \equiv \begin{pmatrix}12 & 23\\23 & 18\end{pmatrix}(mod\ 29)$$

yazılabilir. 2×2 lik bir anahtar matrisi olduğu için şifreli metindeki harfler ikililer halinde gruplanır. Gruplanan ikililer Tablo 1.2'deki harflerin alfabedeki sayı değerine göre Tablo 1.15'daki gibi yazılır.

Tablo 1.15 Şifrelenmiş harflerin sayısal değer karşılıkları

i	1	2	3	4	5	6	7	8
Şif. Met.	Ö N	Ö E	Ö N	U O	F C	N D	B Ç	F H
C_i	$\begin{bmatrix}18\\16\end{bmatrix}$	$\begin{bmatrix}18\\5\end{bmatrix}$	$\begin{bmatrix}18\\16\end{bmatrix}$	$\begin{bmatrix}24\\17\end{bmatrix}$	$\begin{bmatrix}6\\2\end{bmatrix}$	$\begin{bmatrix}16\\4\end{bmatrix}$	$\begin{bmatrix}1\\3\end{bmatrix}$	$\begin{bmatrix}6\\9\end{bmatrix}$
i	9	10	11	12	13	14	15	16
Şif. Met.	Ö D	L Ş	K K	G Ş	M Ş	İ F	C E	V T
C_i	$\begin{bmatrix}18\\4\end{bmatrix}$	$\begin{bmatrix}14\\22\end{bmatrix}$	$\begin{bmatrix}13\\13\end{bmatrix}$	$\begin{bmatrix}7\\22\end{bmatrix}$	$\begin{bmatrix}15\\22\end{bmatrix}$	$\begin{bmatrix}11\\6\end{bmatrix}$	$\begin{bmatrix}2\\5\end{bmatrix}$	$\begin{bmatrix}26\\23\end{bmatrix}$

Bu yüzden, şifreli metin ikililerinin $P_i \equiv K^{-1}(C_i - B)(modp)$ işlemleri yapılırsa düz metin için sayısal değerli sütün vektörü oluşturulur.

Tablo 1.16 Düz metindeki sayısal değerler

i	$K^{-1}(C_i - B)(modp) \equiv P_i$	i	$K^{-1}(C_i - B)(modp) \equiv P_i$
1	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\left(\begin{bmatrix}18\\16\end{bmatrix}-\begin{bmatrix}2\\1\end{bmatrix}\right)\equiv\begin{bmatrix}15\\0\end{bmatrix}(mod29)$	9	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\left(\begin{bmatrix}18\\4\end{bmatrix}-\begin{bmatrix}2\\1\end{bmatrix}\right)\equiv\begin{bmatrix}0\\16\end{bmatrix}(mod29)$
2	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\left(\begin{bmatrix}18\\5\end{bmatrix}-\begin{bmatrix}2\\1\end{bmatrix}\right)\equiv\begin{bmatrix}23\\5\end{bmatrix}(mod29)$	10	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\left(\begin{bmatrix}14\\22\end{bmatrix}-\begin{bmatrix}2\\1\end{bmatrix}\right)\equiv\begin{bmatrix}18\\16\end{bmatrix}(mod29)$
3	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\left(\begin{bmatrix}18\\16\end{bmatrix}-\begin{bmatrix}2\\1\end{bmatrix}\right)\equiv\begin{bmatrix}15\\0\end{bmatrix}(mod29)$	11	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\left(\begin{bmatrix}13\\13\end{bmatrix}-\begin{bmatrix}2\\1\end{bmatrix}\right)\equiv\begin{bmatrix}2\\5\end{bmatrix}(mod29)$
4	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\left(\begin{bmatrix}24\\17\end{bmatrix}-\begin{bmatrix}2\\1\end{bmatrix}\right)\equiv\begin{bmatrix}23\\11\end{bmatrix}(mod29)$	12	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\left(\begin{bmatrix}7\\22\end{bmatrix}-\begin{bmatrix}2\\1\end{bmatrix}\right)\equiv\begin{bmatrix}21\\0\end{bmatrix}(mod29)$
5	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\left(\begin{bmatrix}6\\2\end{bmatrix}-\begin{bmatrix}2\\1\end{bmatrix}\right)\equiv\begin{bmatrix}13\\23\end{bmatrix}(mod29)$	13	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\left(\begin{bmatrix}15\\22\end{bmatrix}-\begin{bmatrix}2\\1\end{bmatrix}\right)\equiv\begin{bmatrix}1\\10\end{bmatrix}(mod29)$
6	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\left(\begin{bmatrix}16\\4\end{bmatrix}-\begin{bmatrix}2\\1\end{bmatrix}\right)\equiv\begin{bmatrix}5\\28\end{bmatrix}(mod29)$	14	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\left(\begin{bmatrix}11\\6\end{bmatrix}-\begin{bmatrix}2\\1\end{bmatrix}\right)\equiv\begin{bmatrix}20\\7\end{bmatrix}(mod29)$
7	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\left(\begin{bmatrix}1\\3\end{bmatrix}-\begin{bmatrix}2\\1\end{bmatrix}\right)\equiv\begin{bmatrix}5\\13\end{bmatrix}(mod29)$	15	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\left(\begin{bmatrix}2\\5\end{bmatrix}-\begin{bmatrix}2\\1\end{bmatrix}\right)\equiv\begin{bmatrix}5\\14\end{bmatrix}(mod29)$
8	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\left(\begin{bmatrix}6\\9\end{bmatrix}-\begin{bmatrix}2\\1\end{bmatrix}\right)\equiv\begin{bmatrix}0\\4\end{bmatrix}(mod29)$	16	$\begin{pmatrix}12 & -6\\-6 & 18\end{pmatrix}\left(\begin{bmatrix}26\\23\end{bmatrix}-\begin{bmatrix}2\\1\end{bmatrix}\right)\equiv\begin{bmatrix}11\\20\end{bmatrix}(mod29)$

Elde edilen $P_i, i = 1,2, \dots 16$ değerlerine karşılık gelen düz metin vektöründeki sayı değerlerinin Tablo 1.2'deki alfabedeki harf değerine dönüştürülüp şifrelenmiş düz karakterleri Tablo 1.17'deki gibi elde edilir. Göndericiden gelen mesaj alıcı tarafından deşifrelenmiş olup düz metin elde edilir.

Tablo 1.17 Sayısal değerlerin düz metindeki karakter değerleri

i	1	2	3	4	5	6	7	8
P_i	$\begin{bmatrix}15\\0\end{bmatrix}$	$\begin{bmatrix}23\\5\end{bmatrix}$	$\begin{bmatrix}15\\0\end{bmatrix}$	$\begin{bmatrix}23\\11\end{bmatrix}$	$\begin{bmatrix}13\\23\end{bmatrix}$	$\begin{bmatrix}5\\28\end{bmatrix}$	$\begin{bmatrix}5\\13\end{bmatrix}$	$\begin{bmatrix}0\\4\end{bmatrix}$
Düz metin	M A	T E	M A	T İ	K T	E Z	E K	A D
i	9	10	11	12	13	14	15	16
P_i	$\begin{bmatrix}0\\16\end{bmatrix}$	$\begin{bmatrix}18\\16\end{bmatrix}$	$\begin{bmatrix}2\\5\end{bmatrix}$	$\begin{bmatrix}21\\0\end{bmatrix}$	$\begin{bmatrix}1\\10\end{bmatrix}$	$\begin{bmatrix}20\\7\end{bmatrix}$	$\begin{bmatrix}5\\14\end{bmatrix}$	$\begin{bmatrix}11\\20\end{bmatrix}$
Düz metin	A N	Ö N	C E	S A	B I	R G	E L	İ R

2. KAYNAK ARAŞTIRMASI

Bu bölümün ilk kısmında literatürdeki Hill şifreleme genelinde yapılan çalışmalar ile özel matrislere göre yapılan Hill şifreleme ve özel matris şifreleme örnekleri yapılan çalışmalardan bahsedilir. İkinci kısımda Circulant matrisler üzerinde yapılan literatürdeki bazı örnek çalışmalar verilir.

2.1 Hill Şifreleme İle İlgili yapılan Çalışmalar

Hill şifreleme algoritması (Hill,1929; Hill,1931), doğrusal dönüşüme dayalı bir poligrafik şifreleme algoritmasıdır ve 1929'da Lester S.Hill tarafından ortaya konulmuştur. Hill şifreleme, düz metnin eşit boyutlu bloklara bölündüğü bir blok şifreleme algoritmasıdır. 1.3.2 ve 1.3.3 kısımlarında da ayrıntılı anlatıldığından tekrardan kaçınmak için ayrıntı verilmemiştir (Thilaka, 2005), (Ismail ve ark. 2006), (Gupta, 2007), (Toorani, 2009), (Mahmoud ve Chefranov, 2010), (Viswanath ve Kumar, 2015).

Hill şifreleme, bilinen düz metin saldırısına karşı savunmasız olan simetrik bir şifreleme algoritmasıdır ve güvenlik açığı nedeniyle artık kullanılmamaktadır. Fakat, kriptoloji ve lineer cebirde hala önemli bir pedagojik role hizmet etmektedir. Ayrıca, (Saeednia, 2000), (Adinarayana ve ark., 2012) çalışmalarında iddia edildiği üzere Hill şifreleme; frekans analizine karşı dirençli, yüksek hıza ve yüksek verime sahiptir.

Hill şifresinin güvenliğini artırmak için literatürde birçok araştırmalar yapılmıştır. Bunlardan bazılarını aşağıdaki gibi özetlemeye çalışalım.

Sadeenia, (Saeednia, 2000) çalışmasında ana anahtar matrisinin sütun ve satırlarının rastgele permütasyonları ile elde edilen dinamik anahtar matrisini kullanarak Hill şifresini güvenli hale getirmeye çalışmıştır. Bu sistemde gönderici, alıcı tarafa şifreli bir düz metin ve şifreli permütasyon vektörü aktarmıştır. Dinamik anahtarların sayısı $n!$ olarak üretilir burada n, anahtar matrisin boyutunu ifade edilmiştir. Düz metin, düz metne yapılan bilinen düz metin saldırısını önleyen yeni bir anahtar matrisi tarafından şifrelenmiştir, ancak orijinal Hill şifresinin de aynı güvenlik açığı olan permütasyon vektörü üzerindeki bilinen düz metin saldırısına karşı savunmasız kalmıştır.

Hill Şifresinin güvenliğini arttırmak için Thilaka ve Rajalakshmi (Thilaka ve Ark., 2005) Hill şifresi kavramında kullanılan m uzunluğundaki dizeyi affine dönüşümü

ve polinom dönüşümü kullanarak n uzunluğundaki dizeye $(n \geq m)$ şifreleyerek genişletmiştir. Burada boyut değiştirerek güvenliği arttırdıkları sunulmuştur.

Ismail ve Diab (Ismail ve Ark. 2006) çalışmalarında, her bloğun karşılık gelen anahtarını üretmek için mevcut anahtar matrisinin her satırını çarpan bir başlangıç vektörü sunarak Hill şifresinin güvenliğini artırmaya çalışmıştır, fakat hala birkaç doğal güvenlik sorunu var olduğunu kabul edilmiştir.

Gupta (Gupta ve Ark, 2007)'de Hill Şifresinin bu uzantılarının kriptanalitik saldırılara açık olduğunu göstermiştir. Hill şifresindeki değişikliklerin onu önemli ölçüde daha güçlü hale getirmediğini öne sürmüştür.

(Lin CH v ark., 2004), (Li C ve ark, 2008) çalışmalarında yazarlar rasgele sayılar almanın ve tek yönlü hash işlevini kullanmanın, Hill şifresi üzerinde bilinen düz metin saldırısını engellediğini, ancak sistemin seçilen şifreli metin saldırısına karşı savunmasız olduğunu iddia etmişlerdir.

Mohsen ve Falahati (Toorani ve Ark., 2009, 2011), Affine dönüşüme dayalı simetrik bir şifreleme sistemi önermiştir. Bu sistemde bir rasgele sayı kullanılmış ve ard arda işlemlerde *HMAC* kullanarak yinelemeli olarak başka rasgele sayılar üretilmiştir.

Mahmoud ve Chefranov (Mahmoud ve Ark. 2010) anahtar matrisin özdeğerleri için *HCM-EE*'ye dayanan Hill şifresinde bir değişiklik önererek bir modelleme yapılmıştır. *HCM-EE* kullanılarak, özdeğerlerin yardımıyla üs alınarak dinamik şifreleme anahtar matrisleri oluşturulmuştur, ancak bu zaman alıcı ve karmaşık bir süreç getirmiştir.

(Mahmoud, 2012) tez çalışması Hill şifresine (HC) dayalı Diffie-Hellman ve Elgamal anahtar değişim protokolleri ile ilgilenilmiştir. Ayrıca, Hill şifresinde HCM-EE ve HCM-PRE olmak üzere iki değişiklik ve matris tabanlı Diffie-Hellman benzeri bir anahtar değişim protokolü önerilmiştir. Ek olarak, ElGamal Açık Anahtar Şifreleme ve İmza Sistemini genişletilmiştir.

Yazarlar (Yamuna ve Ark., 2013) çalışmalarında, kriptografi için A ve B gibi matrislerle temsil edilen metin konumlarını çarpma ve ters alma gibi basit matris işlemlerine dayanan bir metin şifreleme yöntemi sunmaktadır. Şifreleme sisteminde, gönderici tarafından girilen metinin konumlarını saklamak için bir matris kullanılmıştır. Bu değerleri şifrelemek için matris işlemleri ile bir algoritma kullanılmıştır. Deney sonuçlarına göre, önerilen şifreleme sisteminin makul ölçüde uygulanabilir ve etkili olduğunu iddia etmiştir. Ayrıca güvenli veri depolama ve iletimi amacıyla yaygın olarak kullanılabileceği gösterilmiştir.

Viswanath ve Kumar (Viswanath ve Ark., 2015) çalışmalarında Hill Şifrelemesini kullanarak bir açık anahtarlı kriptografi kavramı üzerinde çalışmışlardır. Mertebesi $n \times m$ olan anahtar matrisler kullanmışlar ve bu anahtar matrisinin tersi için Moore-Penrose Inverse (Pseudo Inverse) yöntemini kullanarak Hill şifreleme sistemi ile açık anahtar kriptografisini geliştirmişlerdir.

(Sundarayya ve Ark., 2019)'de verilen çalışmalarında (Viswanath ve Ark., 2015)'deki kriptografik sistemin üzerinde bazı değişikler yapılmıştır. Ayrıca, iki veya daha fazla dijital imza kullanarak bu sistemin güvenliğini artıran bir yöntem ortaya koymuşlardır.

(Prasad ve Ark., 2021) çalışmasında, anahtar matris olarak büyük k kuvvetine sahip genelleştirilmiş Fibonacci Q_λ^k (multinacci) matrisi ile Affine-Hill Şifresini kullanan bir açık anahtar şifreleme sistemi (anti-simetrik sifreleme) verilmiştir. Bu sistemde, şifreleme-deşifreleme için $\lambda \times \lambda$ mertebeden $K = Q_\lambda^k$ anahtar matrisinin asal modulo altında genelleştirilmiş (multinacci) Fibonacci dizileri yardımıyla bir anahtar oluşturma şeması kullanılmıştır. Bu şemada, anahtar matrisini değiştirmek yerine, sadece (λ, k) sayı çiftinin değiştirilmesi gerekmektedir. Bu gereksinimi de ElGamal tekniğini kullanarak yapmışlardır. Bu da zaman karmaşıklığının yanı sıra uzay karmaşıklığını da azaltılacağı için daha büyük bir anahtar uzayı elde edileceği iddia edilmiştir.

(Prasad ve Ark., 2021)'deki şifreleme yöntemine benzer şekilde genelleştirilmiş Fibonacci dizileri ile ilişkisi olan yüksek mertebeden bir matrisi anahtar matrisi olarak ele alınmıştır. Bu matrisleri Affine-Hill Şifresinde anahtar olarak kullanan değiştirilmiş bir açık anahtar şifrelemesi ve genelleştirilmiş Fibonacci dizilerinin terimlerinin asal modulo altında kombinasyonu ile şifreleme-deşifreleme sistemi ortaya konulmuştur (Billore ve Patel, 2023)

Yogi'nin (Yogi, 2021) çalışmasında kullanılan yöntemler hibrit hill şifresi ve RSA kriptografisidir. Bu çalışmada, 3×3 boyutlu anahtar matrisi ile hibrit hill şifreleme kriptografisinin ve 512 bit anahtarlı RSA'nın veri alışverişi sırasında güvenlik sorunlarının üstesinden gelebileceği gösterilmiştir. Ayrıca böylece gönderilen mesajların yetkisiz kişiler tarafından okunamayacağı iddia edilmiştir.

Santoso, mesajın güvenliğini sağlamak için hill şifreleme algoritması ve RSA'yı birleştirirerek bir Hibrit algoritma üzerinde çalışmaktadır. Bu hibrit algoritmada gönderilecek mesaj Hill cipher yöntemi ile şifrelenmekte, şifreli metin elde edildikten

sonra Hill cipher'dan gelen anahtar RSA yöntemi ile şifrelenmekte, daha sonra şifreli metin şifrelenmiş olan Hill cipher anahtarı ve RSA algoritmasının açık anahtarı ile birlikte gönderilmektedir (Santoso, 2021).

Kodlama/kod çözme algoritmaları, bilgi güvenliğinin geliştirilmesine yardımcı olmak için büyük önem taşımaktadır, çünkü bilgi güvenliği son yıllarda daha önemli bir sorun haline gelmiştir. Matrisler benzersiz güçlü bir konsepte sahip olduğundan ve kolayca anlaşılabildiğinden, metin şifreleme ve saklamanın etkili bir yolu olarak uygulanabilir.

(Tas ve Ark., 2018) çalışmasında, 2×2 boyutlu Fibonacci Q^n matrislerini mesaj metnine ait mesaj matrisini blok matrislere bölmeye dayandıran yeni bir kodlama/kod çözme algoritması yöntemi sunulmuştur. Modelin temel avantajı her bir mesaj matrisinin farklı anahtarlarla şifrelenmesidir. Fibonacci sayılarını kullanan bir algoritma verilerek, kullanılan alfabedeki her harfe karşılık gelen sayılar her yeni mesaj matrisi için değiştirilebilmektedir. Bahsedilen sistemin sadece bilgi güvenliğini artırmakla kalmadığı, aynı zamanda yüksek doğruluk kabiliyetine de sahip olduğu iddia edilmiştir.

(Ucar ve Ark., 2019) çalışmasında 2×2 boyutlu Fibonacci Q^n matrisleri ve R^n matrislerini kullanan iki yeni kodlama/çözme algoritması tanıtılmıştır. (Tas ve Ark. ,2018)'te verilen yöntem ile burada verilen yöntemler benzerseler de arasındaki bazı farklara göre bu yöntemler geliştirilmiş sistemlerdir. Q^n ve R^n matrislerini hesaplamak ve karakter tablosunu oluşturmak n'nin seçim yöntemi küçük sayılar üzerinde örneklendirilmiştir. (Tas ve Ark., 2018)'te verilen yönteme göre hesaplamaları daha kolay yöntemler elde edilmiştir.

2.2 Circulant Matris İle İlgili Yapılan Çalışmalar

Literatürde Circulant matrisler çeşitli kriptografik algoritmalarda kullanılmıştır.

(Saeednia, 2000) çalışmasında gelişmiş şifreleme standardının karıştırma sütunları (Mix Columns) adımında

$$C_4 = (02,03,01,01)_4 = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$$

gibi bir circulant matris kullanılır. Bu karışım sütunu, bit düzeyinde difüzyon sağlar. AES ve WHIRLPOOL'da difüzyon elde etmek için Circulant matrisler kullanılmıştır.

Kafes tabanlı kriptografik fonksiyonların verimliliğini artırmak için dairesel matrisler kullanılabilir.

(Adinarayana ve Ark., 2012) çalışmasında, Circulant matrislere dayalı bir Hill şifreleme yönteminde bazı değişiklikler yaparak güvenilirliğinin artırılmasını sağlamaktadır. Bu modifikasyon kriptosistemde, bir A asal (Prime) Circulant matris gizli anahtar olarak paylaşılır. Tekil olmayan bir G matrisi için determinantı sıfır olacak G_c katsayı (Coefficient) matrisi açık anahtar olarak kullanılır. Bu sistemde sonsuz çözümler üretir ki, bu nedenle gizli anahtar matrisini bulmayı zorlaştırır. Bu kripto sistemde Hill şifresi içinde Circulant matris kombinasyonuna çalışılmıştır.

(Ramakrishna ve Ark., 2013) çalışmasında matrislerle kriptografinin önemli bir yönü olan, bir F cismi üzerinde alınan $n \times n$ boyutlu bir P matris verildiğinde, A, B Circulant matrislerine göre $AGB = P$ denkleminin sonsuz sayıda çözümü olması için tekil bir G_c katsayı Circulant matris olacak şekilde F cisminde bir G matris sınıfının bulunması araştırılmıştır. Özel $n.$ mertebeden bir simetrik Circulant matris üzerinde tersinin bulunması için doğrudan bir yöntem verilmiştir.

(Maxrizal,2019) çalışmasında, polinom simetrik ayrıştırma üzerine bir açık anahtar kriptosistemi circulant matrisler kullanarak modifiye edilmiştir. Anahtar anlaşma protokolü ve anahtar dağıtımı için Circulant matrislerden faydalanılmıştır. Circulant matris üzerinde önerilen bu şekildeki açık anahtar kriptosistemi sistemlerinde, doğrudan saldırılara, doğrusallaştırma denklemleri saldırılarına ve çok değişkenli polinom denklem sistemleri saldırılarına karşı dirençli olduğu iddia edilmiştir.

3. r-CİRCULANT MATRİSLER İLE AFFİNE HİLL ŞİFRELEME

Kriptografi, mesajları güvence altına alma bilimi olarak değerlendirilir. Kriptografik teknikler kullanılarak, gönderilen mesaj bir şifreleme işleminden geçirilerek mesajın yeniden yazılması sağlanır, böylece bu mesaj yalnızca bir anahtara sahip olan kişi tarafından okunabilmesi düşünülür.

Önceki bölümlerde verildiği gibi Affine Hill şifreleme yönteminde gizli anahtar $n \times n$ boyutunda tekil olmayan bir matristir ki; bu çalışmada $n \times n$ boyutlu bir r-Circulant matrisini anahtar matris olarak değerlendireceğimiz bir varyant Hill şifreleme algoritması ele alınır.

3.1 Melez Affine-Hill Şifreleme

(1.42) denkleminde verilen $n \times n$ tipindeki $C_{n,r} = \left(c_{ij}\right)_n$, $i,j = 1,2,\dots,n$, $r \in Z$

$$C_{n,r} = \begin{pmatrix} c_0 & c_1 & c_2 & \cdots & c_{n-2} & c_{n-1} \\ rc_{n-1} & c_0 & c_1 & \ddots & c_{n-3} & c_{n-2} \\ rc_{n-2} & rc_{n-1} & c_0 & \ddots & c_{n-4} & c_{n-3} \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ rc_2 & rc_3 & \cdots & \ddots & c_0 & c_1 \\ rc_1 & rc_2 & rc_3 & \cdots & rc_{n-1} & c_0 \end{pmatrix}_{n\times n} \tag{3.1}$$

için $r-$circulant matrisleri birinci satıra göre ifade edilmek istenirse $C_{n,r} = \{r(c_0, c_1, \dots, c_{n-1})\}$ ile gösterilir ve $ij-$inci elemanı,

$$c_{ij} = \begin{cases} c_{j-i} & i \le j \\ rc_{n+j-i} & aksi\ takdirde \end{cases} \tag{3.2}$$

şeklinde yazılabilir.

Hill şifreleme algoritmasında, anahtar matris $C_{n,r}$, $n \times n$ boyutlu olduğu için n ardışık düz metin harfi, Tablo 3.1 gibi gösterilen sayısal bir değer karşılığına atanıp, $C_{n,r}$ matris kullanılarak bulunan değerlerin yine aynı sayısal değerlerin Tablo 3.1 deki gibi harf karşılıkları n şifreli metin harfiyle değiştirilir. Böylelikle şifrelenmiş metin elde edilir. Bu yüzden, bir değişkene (t) bağlı Tablo 3.1 sayısal değer tablosu hazırlanır ki içinde başlangıç olarak boşluk karakteri, kullanılacak Türkçe karakterler, nokta, virgül, soru işareti ve rakamlar olacak şekilde 43 karakter değerlendirilir. Ayrıca bu karakterlerin sayısal değer karşılıkları değişkene bağlı gösterilir.

Tablo 3.1 Harf, karakter ve-sayısal değerlerin *t* parametresine bağlı sayısal değerleri

Harf		A	B	C	Ç	D	E	F	G
Sayı	t	$t+1$	$t+2$	$t+3$	$t+4$	$t+5$	$t+6$	$t+7$	$t+8$
Harf	Ğ	H	I	İ	J	K	L	M	N
Sayı	$t+9$	$t+10$	$t+11$	$t+12$	$t+13$	$t+14$	$t+15$	$t+16$	$t+17$
Harf	O	Ö	P	R	S	Ş	T	U	Ü
Sayı	$t+18$	$t+19$	$t+20$	$t+21$	$t+22$	$t+23$	$t+24$	$t+25$	$t+26$
Harf	V	Y	Z	.	,	?	0	1	2
Sayı	$t+27$	$t+28$	$t+29$	$t+30$	$t+31$	$t+32$	$t+33$	$t+34$	$t+35$
Harf	3	4	5	6	7	8	9		
Sayı	$t+36$	$t+37$	$t+38$	$t+39$	$t+40$	$t+41$	$t+42$		

Tablo 3.1'deki "Sayı" değerleri için $t \in Z$ değerinin seçilmesine bağlı olarak $t+x, 0 \leq x \leq 42$ değerleri $t+x(mod43)$' e göre değerlendirilir.

Anahtar matris olarak kullanılacak (3.1) deki $C_{(n,r)}$ Circulant matrisi ve Tablo 3.1'deki düz metin sayısal değerleri için

$$(alf.değ., mat.boyt, köş.altı çarp.) = (t, n, r) \tag{3.3}$$

gibi üç değişken kullanılır. Bu değişkenleri bilmek gönderici ve alıcı için önemli ölçüde Hill şifreleme için gerekli olan birçok veriyi sağlayacaktır.

Fakat, $C_{(n,r)}$ Circulant anahtar matrisin elemanları ve Affine-Hill için gerekli sütün vektör hakkında bilgi sağlamamaktadır.

Bu yüzden, $C_{(n,r)}$ Circulant matrisin elemanları için 1. Bölümde anlatılan iki tam sayı dizisi kullanılır ki, Fibonacci ve Lucas sayılarına göre ardışık n eleman gerekli olacaktır. (3.1) deki $C_{(n,r)}$ Circulant matrisin ilk satır elemanları

$$C_{(n,r)} = \{r(F_s, F_{s+l}, F_{s+2l}, \dots, F_{s+(n-1)l})\} \tag{3.4}$$

veya

$$C_{(n,r)} = \{r(L_s, L_{s+l}, L_{s+2l}, \dots, L_{s+(n-1)l})\} \tag{3.5}$$

gibi iki vektörden birisi ile anahtar matris tamamen oluşturulabilir.

Affine vektörü için, $C_{(n,r)}$ Circulant matrisinin p. kuvveti $C_{(n,r)}^{p}$ ve düz metindeki karakter sayısı M olmak üzere her bir P_i, $i, p \in \left\{1,2,\dots,\left\lceil\frac{M}{n}\right\rceil\right\}$, düz metin vektörü için $C_{(n,r)}^{p}$ matrisinin j. sütun vektörü C_j^p ise, bu vektörleri Affine vektörü olarak değerlendirelim. Elbette burada $1 \le j \le n$ olduğundan $j > n$ değerleri için $p \equiv j(mod n)$ değerine göre ele alınır. Ancak, sıfırıncı sütün olmadığı için p değerlerinde sıfır "0" denklik sınıfındaki n değeri kullanılır.

O halde, $\{Dizi\ adı\} \in \{F, L\}$ olmak üzere

$$(Fibonacci, Dizi\ baş.ind., \text{İnd.}Art.\text{değ.}) = (F, s, l) \tag{3.6}$$

$$(Lucas, Dizi\ baş.ind., \text{İnd.}Art.\text{değ.}) = (L, s, l) \tag{3.7}$$

gibi üç değişken bir vektör olarak anahtar matrisi ve Affine vektörünü tanımlamaktadır. Elbette Affine vektörünü etkileyen kısımlardan biriside düz metin uzunluğu M değeridir. Fakat bu şifrelemede adım sayısını değiştirir, anahtar oluşturma ile ilgili değildir.

Düz metin sayısal vektörleri P_i, anahtar Circulant matris $C_{(n,r)}$, anahtar matris kuvvetlerinden elde edilen Affine vektörü C_j^i ve şifreli metin vektörleri S_i olmak üzere

$$S_i = C_{(n,r)}\, P_i + C_j^i (mod\, m),\ i \in \left\{1,2,\dots,\left\lceil\frac{M}{n}\right\rceil\right\}, 1 \le j \le n \tag{3.8}$$

olarak şifrelenmiş metne ait sayısal değerler elde edilir. Tablo 3.1'deki karakterleri kullanacağımız için aslında $m = 43$ olarak alınabilir, fakat m alınarak devam edildi.

Şifreli metin S_i, bloğunun şifresinin çözülmesi için,

$$ebob\left(\left(det\left(C_{(n,r)}\right) mod\, m\right), m\right) = 1 \tag{3.9}$$

şeklinde ise $C_{(n,r)}$ Circulant matrisi için tersi vardır ki $C_{(n,r)}^{-1}$ olmak üzere

$$P_i = {C_{(n,r)}}^{-1}\left(S_i - C_j^i\right) mod\, m,\ i, j \in \left\{1,2,\dots,\left\lfloor\frac{M}{n}\right\rfloor\right\} \tag{3.10}$$

olarak düz metin üretilecektir.

Bilindiği gibi RSA anahtar oluşturma algoritmasına göre iki tane farklı p ve q asal sayılarını seçilir ki bu sayıların çarpımını alınarak bir n sayısı belirlenir.

$$n = p.q \tag{3.11}$$

Bu sayı için Euler'in $\varphi(n)$ fonksiyonu değeri hesaplanır ki buda p ve q asal olduğu için

$$\varphi(n) = (p-1).(q-1) \tag{3.12}$$

şeklinde hesaplanabilir. $2 < e < \varphi(n)$ ve $(\varphi(n), e) = 1$ olacak şekilde bir e tamsayısı seçilir. Ayrıca, özel anahtar oluşturulması gereği

$$e.d \equiv 1\ (mod\ \varphi(n)\ ) \tag{3.13}$$

sağlayacak şekilde $1 < d < \varphi(n)$ aralığında d değeri hesaplanılır.

Bu hesaplamalar altında RSA şifrelemedeki açık anahtar (n, e), 2 boyutlu vektörü ve özel anahtarı d değeri olacaktır.

Ayrıca, bilindiği gibi El-Gamal anahtar oluşturma algoritmasına göre rastgele bir p asal sayısı ve $mod\ p$ ye göre Z_p^* nin bir üreteci β değeri seçilir.

Ayrıca, $1 \leq a \leq p-2$ şeklinde olan bir a tamsayısı seçilir ve $\beta^a mod\ p$ değerini hesaplanır. B'nin açık anahtarı $(p, \beta, \beta^a\ )$ ve B'nin gizli anahtarı ise a olur.

RSA şifreleme algoritması ile (3.3) deki (t, n, r) ile (3.6) veya (3.7)'deki $(F\ veya\ L, s, l)$ değerlerine göre Tablo 3.1'deki karakterlere karşılık gelen sayısal değerler kullanılarak Affine Hill şifrelemenin gizli anahtarını göndermek isteniliyor. Bu mesajları şifrelemek için RSA şifrelemenin açık anahtarı olan (n, e)'i değeri kullanılır.

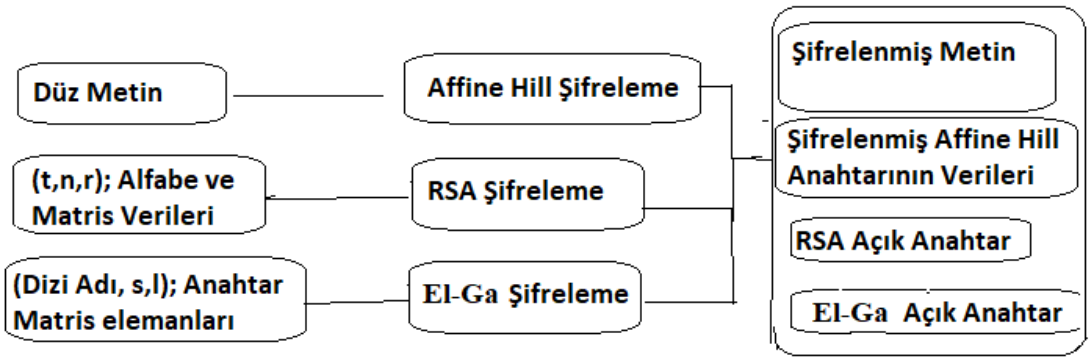
Şekil 3.1 ve Şekil 3.2'deki şifreleme şeması gereği (t, n, r) veya $(F\ veya\ L, s, l)$ mesajları Tablo 3.1'deki sayısal değeler kullanılarak (p_1, p_2, p_3) veya (p_4, p_5, p_6) değerleri yazılır. Sonra

$$E_i \equiv p_i^e\ (\ mod\ n\ ) \tag{3.14}$$

değerleri hesaplanır. Bulunan (E_1, E_2, E_3) veya (E_4, E_5, E_6) şifrelenmiş şekli ile alıcıyaya gönderir.

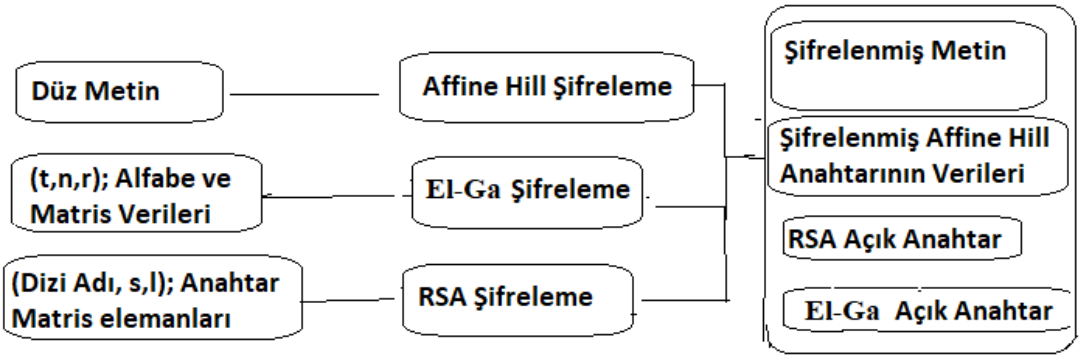
Aynı işlemleri El-Gamal ile alıcının açık anahtarı olan $(\ p, \beta, \beta^a\ )$ alınır ki Tablo 3.1'deki sayısal değeler kullanılarak (p_1, p_2, p_3) veya (p_4, p_5, p_6) değerleri $\{\ 0, , , p-1\ \}$ arasında sağlanacak şekilde yazılır. $1 \leq k \leq p-2$ eşitsizliğini sağlayan rastgele bir k tamsayısı seçilir. Bu k değeri kullanılarak $\gamma = \beta^k$ ve $\delta = m.(\ \beta^a)^k$ değerleri $mod p$ ye göre hesaplanılır. Son olarak $E_i = (\ \gamma, \delta\ ),\ i = 1, \ldots, 6$ şifrelenmiş sayısal değerleri alıcıya gönderilir. Böylelikle şifreli metin alıcıya ulaştığında deşifreleme işlemine başlayabilir.

Şekil 3.1 Affine Hill şifreleme, RSA ve El-Gamal yöntemleri ile şifreleme şeması



veya

Şekil 3.2 Affine Hill şifreleme, El-Gamal ve RSA yöntemleri ile şifreleme şeması



Şekil 3.1 ve Şekil 3.2'deki görselde anlatıldığı üzere önce düz metin Affine Hill şifreleme yöntemi ile şifrelenmekte, şifreli metin elde edildikten sonra Affine Hill şifrelemedeki anahtar matris ve Affine vektör bloğu için gerekli 3 boyutlu iki vektör değeri gizli anahtar olarak RSA ve El-Gamal yöntemleri ile şifrelenmekte, daha sonra şifreli metin, şifrelenmiş olan Affine Hill şifreleme gizli anahtarı, RSA ve El-Gamal algoritmalarının açık anahtarları ile birlikte alıcıya gönderilmektedir.

Bu veriler alıcıya ulaşınca, şifrelenmiş metni deşifre edebilmek için ilk olarak RSA ve El-Gamal açık anahtarlarına göre şifrelenmiş (E_1, E_2, E_3) veya (E_4, E_5, E_6) değerlerini çözmelidir. Bunun için RSA ve El-Gamal deşifreleme adımlarını uygulamalıdır.

RSA deşifreleme algoritması gereğince d gizli anahtarını kullanarak (E_1, E_2, E_3) veya (E_4, E_5, E_6) değerlerine sahip olan şahıs

$$p_i \equiv E_i^d \ (mod\ n\ ) \tag{3.15}$$

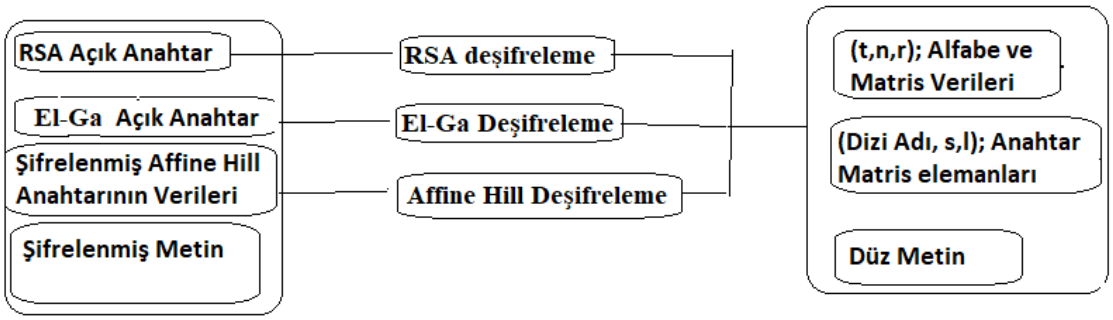
işlemini uygulayarak (p_1, p_2, p_3) veya (p_4, p_5, p_6) Affine Hill şifreleme için gerekli anahtar verilerinin bir kısmına ulaşır.

Ayrıca, diğer kısmına ait parçayı bulabilmek için El-Gamal ile şifrelenmiş metin olan $E_i = (\gamma, \delta_i)$ sayısal değerli ifadesinden (p_1, p_2, p_3) veya (p_4, p_5, p_6) değerlerine ulaşmak için alıcı gizli anahtarı ile $\gamma^{-a} mod\, p$ değeri bulunmalıdır. Daha sonra hesaplanılan değer karakter karşılığında değeri için

$$\gamma^{-a}.\delta_i \equiv p_i \,(mod\, p)$$

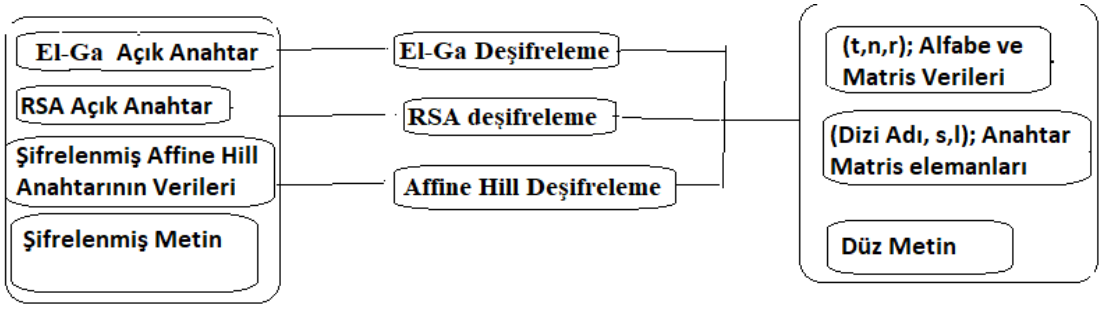
hesaplayarak diğer anahtar gereksinimlerinin değerleri bulunur.

Şekil 3.3 RSA, El-Gamal ve Affine Hill şifreleme yöntemleri ile deşifreleme şeması



veya

Şekil 3.4 El-Gamal, RSA ve Affine Hill şifreleme yöntemleri ile deşifreleme şeması



Şekil 3.3 ve Şekil 3.4'deki görselde anlatıldığı üzere önce açık anahtarları bulunan RSA ve El-Gamal yöntemlerine ait deşifreleme işlemleri ile Affine Hill şifrelemeye ait anahtar matrisin verileri bulunur. Daha sonra Affine Hill deşifreleme işlemleri uygulanarak metin ile düz metin elde edilir.

Görüldüğü gibi Affine Hill şifrelemedeki gizli anahtar RSA ve El-Gamal şifrelemelerinin bir kombinasyonunu kullanarak şifreleme ve şifre çözme sonuçları güvenli hale getirilmeye çalışılmıştır.

Örneğin, gönderilecek mesaj

"MATEMATİKTE ZEKADAN ÖNCE SABIR GELİR"

şeklinde olduğunu düşünelim. Şekil 3.1'deki yöntemi ile uygulayalım.

İlk olarak Tablo 3.1'deki sayı değerleri için $t = 5$, anahtar matrisin boyutu için $n = 4$ ve $C_{n,r}$ Circulant matris için $r = 3$ değerleri seçildiğini düşünelim.

Fibonacci dizisi için başlangıç değerinin indisi $s = 5$ olursa $F_5 = 5$ ile başlayıp indis artış miktarı olarak $l = 2$ alınırsa $C_{4,3} = \{3(F_5, F_7, F_9, F_{11})\}$ satır gösterimi ya da

$$C_{(4,3)} = \begin{pmatrix} F_5 & F_7 & F_9 & F_{11} \\ 3F_{11} & F_5 & F_7 & F_9 \\ 3F_9 & 3F_{11} & F_5 & F_7 \\ 3F_7 & 3F_9 & 3F_{11} & F_5 \end{pmatrix} \tag{3.16}$$

anahtar matrisi oluşturulur.

$t = 5$ için elde edilmiş Tablo 3.1'deki sayısal değerleri boyut $n = 4$ için düz metni uzunluğu $M = 36$ karakter (kelimeler arasındaki boşluklar dahil) olduğundan 4'er li bloklara ayırıp sayısal karşılıklarını Tablo 3.2'deki şekli ile 9 vektör şeklinde gösterilir.

Tablo 3.2 Düz metnin $t = 5$ için sayısal değer karşılıkları

M_i	M	A	T	E	M	A	T	İ	K	T	E		Z	E	K	A
P_i	21	6	29	11	21	6	29	17	19	29	11	5	34	11	19	6
M_i	D	A	N		Ö	N	C	E			S	A	B		I	R		G
P_i	10	6	22	5	24	22	8	11	5	27	6	7	16	26	5	13
M_i	E	L	İ	R												
P_i	11	20	17	26												

Tablo 3.1'deki "Sayı" değerleri için $t = 5$ olduğundan dolayı $(mod 43)$'e göre uygun sayı değerleri elde edilir. $M = 36$ olmak üzere P_i bloklarına göre S_i bloklarının hesaplaması

$$S_i = C_{(4,3)}\, P_i + C_j^i (mod\ 43),\ i \in \{1,2,\dots,9\} \tag{3.17}$$

şeklinde yapılır ki $1 \leq j \leq 4$ olduğundan $4 < j \leq p = 9$ değerleri için $p \equiv j(mod 4)$ ve $p \equiv 0(mod 4)$ için $j = 4$ değerine göre ele alınır.

(3.17) denkleminde (3.16)'daki $C_{(4,3)}$ matrisi ve Tablo 3.2'deki P_i, $i \in \{1,2,\dots,9\}$ değerleri ile C_j^i kuvvet matrisinin sütun vektörleri yerlerine yazılarak, şifreli metinin sayısal değerli sütün vektörü oluşturulur.

Örneğin $i = 1$ için $S_1 = C_{(4,3)}\, P_1 + C_1^1 (mod\, 43)$ hesaplayalım:

$$\begin{pmatrix} 5 & 13 & 34 & 89 \\ 267 & 5 & 13 & 34 \\ 102 & 267 & 5 & 13 \\ 39 & 102 & 267 & 5 \end{pmatrix} \begin{pmatrix} 21 \\ 6 \\ 29 \\ 11 \end{pmatrix} + \begin{pmatrix} 5 \\ 267 \\ 102 \\ 39 \end{pmatrix} = \begin{pmatrix} 2153 \\ 6655 \\ 4134 \\ 9268 \end{pmatrix} mod 43 = \begin{pmatrix} 3 \\ 33 \\ 6 \\ 23 \end{pmatrix}$$

yada $C_{(4,3)}$ matrisinin $(mod\, 43)$'daki değerine göre

$$\begin{pmatrix} 5 & 13 & 34 & 3 \\ 9 & 5 & 13 & 34 \\ 16 & 9 & 5 & 13 \\ 39 & 16 & 9 & 5 \end{pmatrix} \begin{pmatrix} 21 \\ 6 \\ 29 \\ 11 \end{pmatrix} + \begin{pmatrix} 5 \\ 9 \\ 16 \\ 39 \end{pmatrix} = \begin{pmatrix} 1207 \\ 979 \\ 694 \\ 1270 \end{pmatrix} mod 43 = \begin{pmatrix} 3 \\ 33 \\ 6 \\ 23 \end{pmatrix}$$

elde edilir ki bu değerleri Tablo 3.1'deki sayı değeri karşılıklarına uygun mutlaka harf karşılıkları bulunacağından şifrelenmiş blok elde edilebilir.

$i = 2$ için $S_2 = C_{(4,3)}\, P_2 + C_2^2 (mod\, 43)$ hesaplarken $C_{(4,3)}$ matrisinin $(mod\, 43)$'daki değerine göre

$$S_2 = \begin{pmatrix} 5 & 13 & 34 & 3 \\ 9 & 5 & 13 & 34 \\ 16 & 9 & 5 & 13 \\ 39 & 16 & 9 & 5 \end{pmatrix} \begin{pmatrix} 21 \\ 6 \\ 29 \\ 17 \end{pmatrix} + \begin{pmatrix} 11 \\ 29 \\ 33 \\ 17 \end{pmatrix} = \begin{pmatrix} 1231 \\ 1203 \\ 789 \\ 1278 \end{pmatrix} mod 43 = \begin{pmatrix} 27 \\ 42 \\ 15 \\ 31 \end{pmatrix}$$

olur.

Bundan sonraki hesaplanan S_i blokları için $mod\ 43$ alınarak,

$$S_3 = C_{(4,3)}\, P_3 + C_3^3 (mod\, 43)$$

$$S_3 = \begin{pmatrix} 5 & 13 & 34 & 3 \\ 9 & 5 & 13 & 34 \\ 16 & 9 & 5 & 13 \\ 39 & 16 & 9 & 5 \end{pmatrix} \begin{pmatrix} 19 \\ 29 \\ 11 \\ 5 \end{pmatrix} + \begin{pmatrix} 38 \\ 14 \\ 4 \\ 6 \end{pmatrix} = \begin{pmatrix} 899 \\ 643 \\ 689 \\ 1335 \end{pmatrix} mod 43 = \begin{pmatrix} 39 \\ 41 \\ 1 \\ 2 \end{pmatrix}$$

$$S_4 = C_{(4,3)}\, P_4 + C_4^4 (mod\, 43)$$

$$S_4 = \begin{pmatrix} 5 & 13 & 34 & 3 \\ 9 & 5 & 13 & 34 \\ 16 & 9 & 5 & 13 \\ 39 & 16 & 9 & 5 \end{pmatrix} \begin{pmatrix} 34 \\ 11 \\ 19 \\ 6 \end{pmatrix} + \begin{pmatrix} 3 \\ 10 \\ 23 \\ 15 \end{pmatrix} = \begin{pmatrix} 980 \\ 822 \\ 839 \\ 1718 \end{pmatrix} mod 43 = \begin{pmatrix} 34 \\ 5 \\ 22 \\ 41 \end{pmatrix}$$

şeklindedir. Fakat, $S_i = C_{(4,3)}\, P_i + C_j^i (mod\, 43)$, $5 \le i \le 9$ olmak üzere eğer $i \equiv 0 (mod 4)$ için $j = 4$, aksi takdirde $i \equiv j (mod 4)$ alınarak kuvvetinin sütun vektörleri kullanılır ki

$$S_5 = C_{(4,3)}\, P_5 + C_1^5 (mod\, 43)$$

$$S_5 = \begin{pmatrix} 5 & 13 & 34 & 3 \\ 9 & 5 & 13 & 34 \\ 16 & 9 & 5 & 13 \\ 39 & 16 & 9 & 5 \end{pmatrix} \begin{pmatrix} 10 \\ 6 \\ 22 \\ 5 \end{pmatrix} + \begin{pmatrix} 0 \\ 35 \\ 35 \\ 11 \end{pmatrix} = \begin{pmatrix} 891 \\ 611 \\ 424 \\ 720 \end{pmatrix} mod 43 = \begin{pmatrix} 31 \\ 9 \\ 37 \\ 32 \end{pmatrix}$$

$$S_6 = C_{(4,3)}\, P_6 + C_2^6 (mod\, 43)$$

$$S_6 = \begin{pmatrix} 5 & 13 & 34 & 3 \\ 9 & 5 & 13 & 34 \\ 16 & 9 & 5 & 13 \\ 39 & 16 & 9 & 5 \end{pmatrix} \begin{pmatrix} 24 \\ 22 \\ 8 \\ 11 \end{pmatrix} + \begin{pmatrix} 9 \\ 1 \\ 15 \\ 31 \end{pmatrix} = \begin{pmatrix} 720 \\ 805 \\ 780 \\ 1446 \end{pmatrix} mod 43 = \begin{pmatrix} 32 \\ 31 \\ 6 \\ 27 \end{pmatrix}$$

$$S_7 = C_{(4,3)}\, P_7 + C_3^7 (mod\, 43)$$

$$S_7 = \begin{pmatrix} 5 & 13 & 34 & 3 \\ 9 & 5 & 13 & 34 \\ 16 & 9 & 5 & 13 \\ 39 & 16 & 9 & 5 \end{pmatrix} \begin{pmatrix} 5 \\ 27 \\ 6 \\ 7 \end{pmatrix} + \begin{pmatrix} 4 \\ 16 \\ 2 \\ 29 \end{pmatrix} = \begin{pmatrix} 605 \\ 512 \\ 446 \\ 745 \end{pmatrix} mod 43 = \begin{pmatrix} 3 \\ 39 \\ 16 \\ 14 \end{pmatrix}$$

$$S_8 = C_{(4,3)}\, P_8 + C_4^8 (mod\, 43)$$

$$S_8 = \begin{pmatrix} 5 & 13 & 34 & 3 \\ 9 & 5 & 13 & 34 \\ 16 & 9 & 5 & 13 \\ 39 & 16 & 9 & 5 \end{pmatrix} \begin{pmatrix} 16 \\ 26 \\ 5 \\ 13 \end{pmatrix} + \begin{pmatrix} 34 \\ 39 \\ 10 \\ 36 \end{pmatrix} = \begin{pmatrix} 661 \\ 820 \\ 694 \\ 1186 \end{pmatrix} mod 43 = \begin{pmatrix} 16 \\ 3 \\ 6 \\ 25 \end{pmatrix}$$

$$S_9 = C_{(4,3)}\, P_9 + C_1^9 (mod\, 43)$$

$$S_9 = \begin{pmatrix} 5 & 13 & 34 & 3 \\ 9 & 5 & 13 & 34 \\ 16 & 9 & 5 & 13 \\ 39 & 16 & 9 & 5 \end{pmatrix} \begin{pmatrix} 11 \\ 20 \\ 17 \\ 26 \end{pmatrix} + \begin{pmatrix} 27 \\ 21 \\ 18 \\ 25 \end{pmatrix} = \begin{pmatrix} 998 \\ 1325 \\ 797 \\ 1057 \end{pmatrix} mod 43 = \begin{pmatrix} 9 \\ 35 \\ 23 \\ 25 \end{pmatrix}$$

bulunur. Elde edilen $S_i, i = 1,2,\dots,9$ değerlerine karşılık gelen şifreli metin vektöründeki sayı değerlerinin Tablo 3.1'deki alfabedeki harf değerine dönüştürülüp şifrelenmiş metin karakterleri elde edilir.

Tablo 3.3 Sayısal değerlerin şifrelenmiş harf karşılıkları

S_i	3 33 6 23	27 42 15 31	39 41 1 2	34 5 22 41
Ş	8 *Y A O*	*S* 4 *H* Ü	1 3 6 7	*Z N* 3
S_i	31 9 37 32	32 31 6 27	3 39 16 14	16 3 6 25
Ş	Ü Ç ? *V*	*V* Ü *A S*	8 1 *I* Ğ	*I* 8 *A P*
S_i	9 35 23 25			
Ş	Ç . *O P*			

Bu karakterler boşluklarda dahil edilerek de yazıldığı için aynı örneğimizi dikkate alarak

"8YAOS4HÜ1367Z N3ÜÇ?VVÜAS81IĞI8APÇ.OP" (3.18)

şeklinde elde edilen şifre Şekil 3.1'de ifade edildiği gibi alıcıya iletilebilir. Şifrelenmiş mesaj, Tablo 3.3'den de anlaşılacağı üzere zaten rastgele harfler şeklinde hatta düz metindeki aynı harflerin bile farklı harflerle şifrelendiğinden anlamlı bir metin oluşturmaz.

Bununla beraber Şekil 3.1'de $(t,n,r) = (5,4,3)$ değerleri için Tablo 3.1'den karakterlere karşılık gelen $(43,42,41) mod 43 \equiv (00,42,41)$ sayısal değerleri RSA şifreleme ile şifrelenmelidir. Bu yüzden, iki asal sayı ve çarpımı olan

$$p = 43, q = 41$$

$$n = p.q = 43.41 = 1763$$

değerler alınır. Daha sonra $\varphi(n) = (p-1).(q-1) = 1680$ hesaplanır. Ayrıca, bir e tamsayısı seçimi $2 < e < \varphi(n)$ ve $(\varphi(n), e) = 1$ şekilde yapılır ki, $(1680, e) = 1$ olacak şekilde $e = 11$ seçildiğini düşünelim. O halde $(n,e) = (1763,11)$ açık anahtar olur. Ayrıca, $11.d \equiv 1 (mod 1680)$ sağlayan şekilde $d = 611$ elde edilir.

Açık anahtarı $(n,e) = (1763,11)$ ve özel anahtarı $d = 611$'dir.

Şimdi $(p_1, p_2, p_3) = (00,42,41)$ sayısal karakterler ve $(n,e) = (1763,11)$ açık anahtar olmak üzere her bir $p_i, i = 1,2,3$ bloğunu şifrelemek için

$$p_i{}^{11} \equiv E_i \ (mod\ 1763), \qquad i = 1,2,3$$

bağıntısı kullanılarak şifreli $E_i,\ i = 1,2,3$ blokları elde edilir. E_1 bloğu için

$$00^{11} \equiv 0 \ (mod\ 1763)$$

olur. E_2 ve E_3 blokları için de aynı işlem tekrar edilirse

$$42^{11} \equiv 42 \ (mod\ 1763)$$

$$41^{11} \equiv 1435 \ (mod\ 1763)$$

elde edilir. RSA açık anahtarı ile şifreli veriler

$$(n, e) = (1763,11) \text{ ve } (E_1, E_2, E_3) = (0000,0042,1435) \tag{3.19}$$

gönderilmeye hazır haldedir.

Şekil 3.1'deki diğer parça $(Dizi, s, l) = (F, 5,2)$ değerlerinin Tablo 3.1'deki sayısal değeri $(F, 5,2) = (12,00,40)$ şeklindedir. Şimdi, El-Gamal şifreleme yöntemine göre şifreleme işlemlerini verelim. Anahtar oluşturma için asal $p = 1279$ ve $\beta = 2$ üretecini ele alalım. Ayrıca $1 \leq \alpha \leq 1277$ için $\alpha = 971$ değerini gizli anahtar olarak seçelim. Daha sonra $\beta^{\alpha} = 2^{971} \equiv 477(mod1279)$ değeri hesaplanır ki alıcının açık anahtarı $(p, \beta, \beta^{a}) = (1279, 2, 477)$ elde edilir. Gizli anahtar olarak $k = 1203$ tam sayısı seçildiğini düşünelim.

Bu k değeri ile $\gamma = \beta^{k} mod p$ ve $\delta = m.(\beta^{a})^{k} mod p$ hesaplanılır ki,

$$E_i = (\gamma, \delta_i),\ i = 4,5,6$$

şifrelenmiş sayısal değerleri alıcıya gönderilir. E_4 değeri için

$$\gamma = 2^{1203} \equiv 651\ (mod\ 1279)$$

$$\delta_4 = 12.477^{1203} \equiv 220\ (mod\ 1279)$$

olur ki $E_4 = (\gamma, \delta_4) = (651, 220)$ olarak şifrelenmiş olur. E_5 ve E_6 değerleri için

$$\delta_5 = 00.477^{1203} \equiv 0\ (mod\ 1279)$$

$$\delta_6 = 40.477^{1203} \equiv 307\ (mod\ 1279)$$

$E_5 = (\gamma, \delta_5) = (651, 0)$ ve $E_6 = (\gamma, \delta_6) = (651, 307)$ şeklinde şifrelenmiş olur. El-Gamal açık anahtarı ile şifreli veriler

$$(p, \beta, \beta^{a}) = (1279, 2, 477)$$
$$(E_4, E_5, E_6) = (\gamma, \delta_4, \delta_5, \delta_6) = (651,220,000,307) \tag{3.20}$$

gönderime hazırdır.

Artık gönderici (3.18), (3.19) ve (3.20)'deki şifrelenmiş metin, RSA açık anahtar, El-Gamal açık anahtar ve Affine Hill şifrelemenin gizli anahtarı şifrelenmiş olarak gönderilir.

Şekil 3.3'daki şemada gösterildiği gibi bir alıcının eline ulaşan (3.18), (3.19) ve (3.20)'deki veriler ile ilk olarak, Affine Hill şifrelemenin gizli anahtarını oluşturmak için (3.19)'daki verileri RSA deşifreleme metodu, (3.20)'deki verileri El-Gamal deşifreleme metodu ve bunlardan oluşturulan anahtar matris kullanılarak (3.18)'deki veriler Affine Hill deşifreleme metodu ile çözümlenir.

(t, n, r) değerlerini deşifrelemede kullanılacak $(n, e) = (1763,11)$ olan d'yi bulmada kullanılacak mod değeri ise $mod(\varphi(1763)) = mod(1680)$ olarak bulunur.

Ayrıca, $11.d \equiv 1\ (mod 1680)$ sağlayan şekilde $d = 611$ elde edilir. O halde bütün $(E_1, E_2, E_3) = (0000,0042,1435)$ bloklarının deşifrelemesi için

$$E_i^{611} \equiv p_i\ (mod\ 1763)$$

kullanılarak her bir blok deşifre edilir.

$$1435^{611} \equiv 41\ (mod\ 1763)$$

$$42^{611} \equiv 42\ (mod\ 1763)$$

$$0^{611} \equiv 0\ (mod\ 1763)$$

şeklindedir. O halde $(p_1, p_2, p_3) = (0,42,41)$ sayısal değerleri Tablo 3.1'deki karakter karşılıkları alınırsa $(t, n, r) = (5,4,3)$ düz metni elde edilir.

$(Dizi, s, l)$ değerlerini deşifrelemede γ ve $(p, \beta, \beta^a) = (1279, 2, 477)$ değerleri kullanılacak olup $\gamma^{p-1-a} = 651^{307} \equiv 1000\ (mod\ 1279)$ ifadesini hesaplar ki γ^{-a} değerlerini elde edilir. $(E_4, E_5, E_6) = (\gamma, \delta_4, \delta_5, \delta_6) = (651,220,000,307)$ verilerini deşifrelemek için

$$p_i = 1000.\delta_i (mod\ 1279), i = 4,5,6$$

işlemi kullanılır ki

$$p_4 = 1000.220 \equiv 12 (mod\ 1279)$$

$$p_5 = 1000.0 \equiv 0 (mod\ 1279)$$

$$p_6 = 1000.307 \equiv 40 (mod\ 1279)$$

şeklindedir. $(p_4, p_5, p_6) = (12,0,40)$ sayısal değerleri hesaplanır. Tablo 3.1'deki karakter karşılıkları alınırsa $(Dizi, s, l) = (F, 5,2)$ düz metni elde edilir.

Gönderilen mesajı alan kişi hala mesajı okuyamaz, ancak mesajı okumak için gönderilen Affine Hill şifresinin gizli anahtarını oluşturup, (3.18)'deki şifreyi Affine - Hill deşifreleme kullanarak düz metine ulaşabilir.

$(t, n, r) = (5,4,3)$ ve $(Dizi, s, l) = (F, 5,2)$ deki veriler kullanılarak (3.16)'daki $C_{(4,3)}$ anahtar matrisi gizli anahtar olarak bulunur.

Şifre çözme işlemi için Tablo 3.1'deki "harf" değerleri için $t = 5$ değeri için $(mod 43)$'e göre düzenleyip Tablo 3.4'de görüldüğü gibi sayısal karşılıkları verilir.

Tablo 3.4 Şifrelenmiş harf karşılıklarının sayısal değerleri

Ş	8 Y A O	S 4 H Ü	1 3 6 7	Z N 3
S_i	3 33 6 23	27 42 15 31	39 41 1 2	34 5 22 41
Ş	Ü Ç ? V	V Ü A S	8 1 I Ğ	I 8 A P
S_i	31 9 37 32	32 31 6 27	3 39 16 14	16 3 6 25
Ş	Ç . O P			
S_i	9 35 23 25			

Tablo 3.4'deki sayısal karşılıklar S_i blokları ile (3.16)'daki $C_{(4,3)}$ anahtar matrisin tersi $C^{-1}_{(4,3)}$ ve bu matrisinin kuvvetlerinin sütün vektörü C_j^i olmak üzere düz metin sayısal değerli P_i bloklarının hesaplaması

$$P_i = C^{-1}_{(4,3)}\left(S_i - C_j^i\right)(mod\ 43),\ i \in \{1,2,\dots,9\} \tag{3.21}$$

şeklinde yapılır ki $1 \le j \le 4$ olduğundan $4 < j \le p = 9$ değerleri için $p \equiv j(mod4)$ ve $p \equiv 0(mod4)$ ise $j = n = 4$ değerlerine göre ele alınır.

İlk olarak $\left|C_{(4,3)}\right| = 1657851791$ yada $\left|C_{(4,3)}(mod43)\right| = 114587$ şeklindedir ki o halde tersi vardır. Ayrıca, $\left|C_{(4,3)}(mod43)\right|(mod43) = 35$ değeri için

$$8\left|C_{(4,3)}\right|^{-1} \equiv 1(mod43)$$

olarak determinantın tersini $\left|C_{(4,3)}\right|^{-1} = 27$ dır. O halde matrisin tersi

$$C^{-1}_{(4,3)} = \left|C_{(4,3)}\right|^{-1}\left(adj\left(C_{(4,3)}mod43\right)\right)$$

$$C^{-1}_{(4,3)} = 27\begin{pmatrix}16 & 37 & 6 & 7\\ 21 & 16 & 37 & 6\\ 18 & 21 & 16 & 37\\ 25 & 18 & 21 & 16\end{pmatrix}$$

$$C^{-1}_{(4,3)}(mod43) = \begin{pmatrix}2 & 10 & 33 & 17\\ 8 & 2 & 10 & 33\\ 13 & 8 & 2 & 10\\ 30 & 13 & 8 & 2\end{pmatrix}$$

olarak elde edilir. (3.21)'de $i = 1$ için bu değerleri yerlerine yazalım

$$P_1 = C^{-1}_{(4,3)}(S_1 - C_1^1)(mod\ 43)$$

$$P_1 = \begin{pmatrix}2 & 10 & 33 & 17\\ 8 & 2 & 10 & 33\\ 13 & 8 & 2 & 10\\ 30 & 13 & 8 & 2\end{pmatrix}\left(\begin{pmatrix}3\\33\\6\\23\end{pmatrix} - \begin{pmatrix}5\\9\\16\\39\end{pmatrix}\right) = \begin{pmatrix}-366\\-596\\-14\\140\end{pmatrix} mod43 = \begin{pmatrix}21\\6\\29\\11\end{pmatrix}$$

$i = 2$ için $P_2 = C^{-1}_{(4,3)}(S_2 - C_2^2)(mod\ 43)$ değeri

$$P_2 = \begin{pmatrix} 2 & 10 & 33 & 17 \\ 8 & 2 & 10 & 33 \\ 13 & 8 & 2 & 10 \\ 30 & 13 & 8 & 2 \end{pmatrix} \left(\begin{pmatrix} 27 \\ 42 \\ 15 \\ 31 \end{pmatrix} - \begin{pmatrix} 11 \\ 29 \\ 33 \\ 17 \end{pmatrix} \right) = \begin{pmatrix} -194 \\ 436 \\ 416 \\ 533 \end{pmatrix} mod 43 = \begin{pmatrix} 21 \\ 6 \\ 29 \\ 17 \end{pmatrix}$$

olur. Bundan sonraki hesaplanan P_i blokları için mod43 alınarak,

$$P_3 = \left(C^{-1}_{(4,3)} (S_3 - C_3^3) \right) (mod\ 43)$$

$$P_3 = \begin{pmatrix} 2 & 10 & 33 & 17 \\ 8 & 2 & 10 & 33 \\ 13 & 8 & 2 & 10 \\ 30 & 13 & 8 & 2 \end{pmatrix} \left(\begin{pmatrix} 39 \\ 41 \\ 1 \\ 2 \end{pmatrix} - \begin{pmatrix} 38 \\ 14 \\ 4 \\ 6 \end{pmatrix} \right) mod 43 = \begin{pmatrix} 19 \\ 29 \\ 11 \\ 5 \end{pmatrix}$$

$$P_4 = \left(C^{-1}_{(4,3)} (S_4 - C_4^4) \right) (mod\ 43)$$

$$P_4 = \begin{pmatrix} 2 & 10 & 33 & 17 \\ 8 & 2 & 10 & 33 \\ 13 & 8 & 2 & 10 \\ 30 & 13 & 8 & 2 \end{pmatrix} \left(\begin{pmatrix} 34 \\ 5 \\ 22 \\ 41 \end{pmatrix} - \begin{pmatrix} 3 \\ 10 \\ 23 \\ 15 \end{pmatrix} \right) mod 43 = \begin{pmatrix} 34 \\ 11 \\ 19 \\ 6 \end{pmatrix}$$

şeklindedir. Fakat, $P_i = C^{-1}_{(4,3)} \left(S_i - C_j^i \right) (mod\ 43)$, $5 \leq i \leq 9$ olmak üzere eğer $i \equiv 0 (mod 4)$ için $j = 4$, aksi takdirde $i \equiv j (mod 4)$ alınarak kuvvetinin sütun vektörleri kullanılır ki

$$P_5 = \left(C^{-1}_{(4,3)} (S_5 - C_1^5) \right) (mod\ 43)$$

$$P_5 = \begin{pmatrix} 2 & 10 & 33 & 17 \\ 8 & 2 & 10 & 33 \\ 13 & 8 & 2 & 10 \\ 30 & 13 & 8 & 2 \end{pmatrix} \left(\begin{pmatrix} 31 \\ 9 \\ 37 \\ 32 \end{pmatrix} - \begin{pmatrix} 0 \\ 35 \\ 35 \\ 11 \end{pmatrix} \right) mod 43 = \begin{pmatrix} 10 \\ 6 \\ 22 \\ 5 \end{pmatrix}$$

$$P_6 = \left(C^{-1}_{(4,3)} (S_6 - C_2^6) \right) (mod\ 43)$$

$$P_6 = \begin{pmatrix} 2 & 10 & 33 & 17 \\ 8 & 2 & 10 & 33 \\ 13 & 8 & 2 & 10 \\ 30 & 13 & 8 & 2 \end{pmatrix} \left(\begin{pmatrix} 32 \\ 31 \\ 6 \\ 27 \end{pmatrix} - \begin{pmatrix} 9 \\ 1 \\ 15 \\ 31 \end{pmatrix} \right) mod 43 = \begin{pmatrix} 24 \\ 22 \\ 8 \\ 11 \end{pmatrix}$$

$$P_7 = \left(C^{-1}_{(4,3)} (S_7 - C_3^7) \right) (mod\ 43)$$

$$P_7 = \begin{pmatrix} 2 & 10 & 33 & 17 \\ 8 & 2 & 10 & 33 \\ 13 & 8 & 2 & 10 \\ 30 & 13 & 8 & 2 \end{pmatrix} \left(\begin{pmatrix} 3 \\ 39 \\ 16 \\ 14 \end{pmatrix} - \begin{pmatrix} 4 \\ 16 \\ 2 \\ 29 \end{pmatrix} \right) mod 43 = \begin{pmatrix} 5 \\ 27 \\ 6 \\ 7 \end{pmatrix}$$

$$P_8 = \left(C^{-1}_{(4,3)} (S_8 - C^8_4) \right) (mod\ 43)$$

$$P_8 = \begin{pmatrix} 2 & 10 & 33 & 17 \\ 8 & 2 & 10 & 33 \\ 13 & 8 & 2 & 10 \\ 30 & 13 & 8 & 2 \end{pmatrix} \left(\begin{pmatrix} 16 \\ 3 \\ 6 \\ 25 \end{pmatrix} - \begin{pmatrix} 34 \\ 39 \\ 10 \\ 36 \end{pmatrix} \right) mod 43 = \begin{pmatrix} 16 \\ 26 \\ 5 \\ 13 \end{pmatrix}$$

$$P_9 = \left(C^{-1}_{(4,3)} (S_9 - C^9_1) \right) (mod\ 43)$$

$$P_9 = \begin{pmatrix} 2 & 10 & 33 & 17 \\ 8 & 2 & 10 & 33 \\ 13 & 8 & 2 & 10 \\ 30 & 13 & 8 & 2 \end{pmatrix} \left(\begin{pmatrix} 9 \\ 35 \\ 23 \\ 25 \end{pmatrix} - \begin{pmatrix} 27 \\ 21 \\ 18 \\ 25 \end{pmatrix} \right) mod 43 = \begin{pmatrix} 11 \\ 20 \\ 17 \\ 26 \end{pmatrix}$$

bulunur. Elde edilen $P_i, i = 1,2,\dots,9$ değerlerine karşılık gelen deşifreli metin vektöründeki sayı değerlerinin Tablo 3.1'deki alfabedeki harf değerine dönüştürülüp düz metin karakterleri elde edilir.

Tablo 3.5 Sayısal değerlerin deşifrelenmiş harf karşılıkları

P_i	21 6 29 11	21 6 29 17	19 29 11 5	34 11 19 6
M	M A T E	M A T İ	K T E	Z E K A
P_i	10 6 22 5	24 22 8 11	5 27 6 7	16 26 5 13
M	D A N	Ö N C E	S A B	I R G
P_i	11 20 17 26			
M	E L İ R			

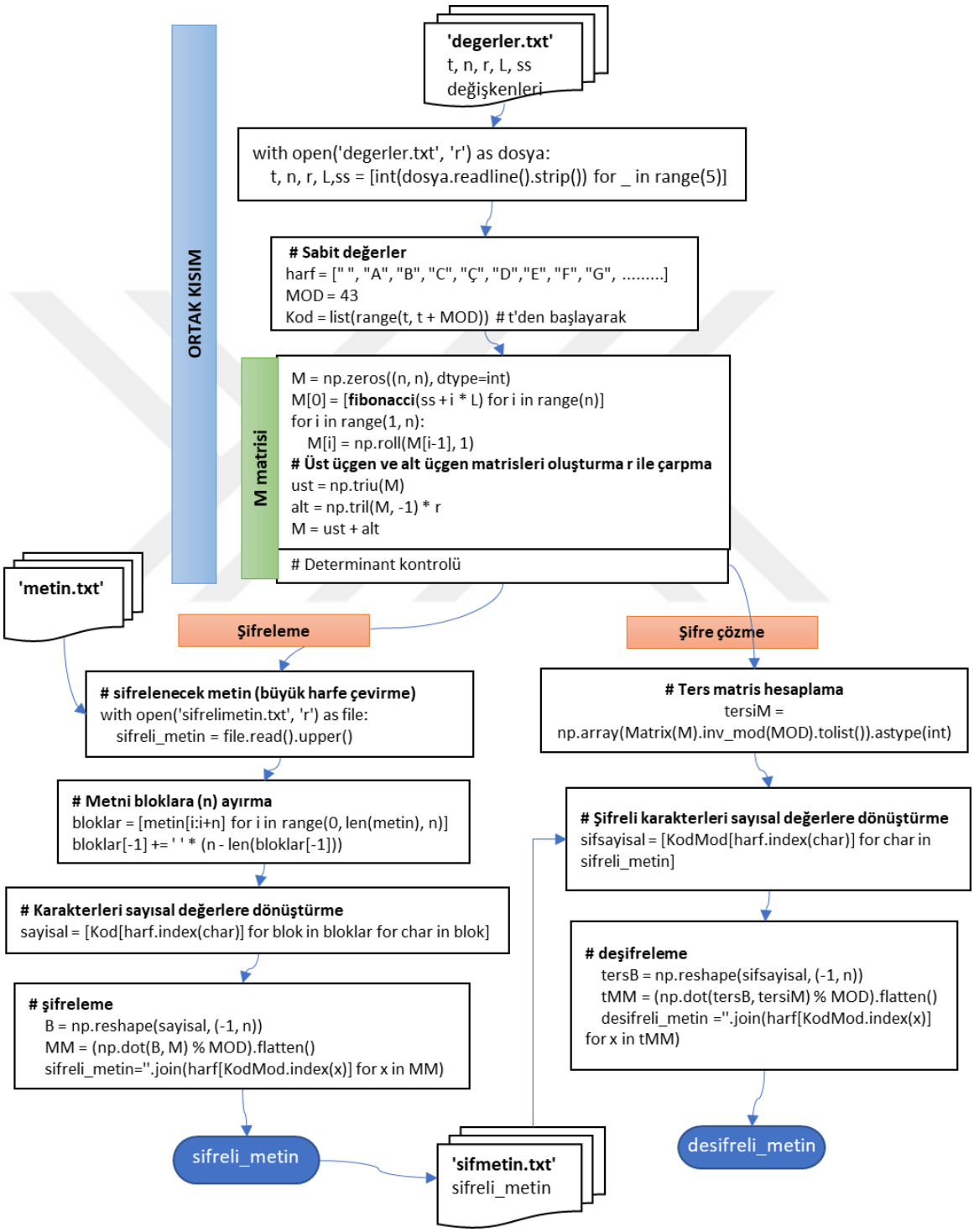
Bu karakterler boşluklarda dahil edilerek de yazıldığında

"MATEMATİKTE ZEKADAN ÖNCE SABIR GELİR"

şeklinde elde deşifrelenip düz metin elde edilir.

3.2 Uygulama Örnekleri

Şimdi, yukarı da anlatılan aynı örneği (t, n, r, s, l) değişkenlerine göre Fibonacci veya Lucas dizilerinden istenilen durumuna göre Şekil 3.5 verilen algoritma mantığında yazılan program içinde şifreleme ve deşifreleme incelemeleri yapılır.



Şekil 3.5 Affine Hill şifreleme ve deşifreleme yöntemi akış şeması

Şekil 3.5'te süreç açıkta görülmektedir.

(3.3) ve (3.6)'deki (t, n, r, s, l) verileri değiştirerek elde ettiğimiz (1.44)'deki

"MATEMATİKTE ZEKADAN ÖNCE SABIR GELİR"

metnin Tablo 3.1'deki sayı değerini (t'e göre değişiyor), bu değerlere karşılık gelen şifrelenmiş sayısal değerleri (n ve r göre değişiyor) ve şifrelenmiş metni (r, s ve l 'e göre değişiyor) aşağıdaki Tablo 3.6 verelim.

Tablo 3.6 (t, n, r, s, l) değişkenlerine göre Fibonacci sayıları örneklemi

Fibonacci sayıları kullanılarak $(F_s, F_{s+l}, F_{s+2l}, \dots, F_{s+(n-1)l},)$	
$t = 8$ $n = 4$ $r = 1$ $s = 3$ $l = 2$	24 9 32 14 24 9 32 20 22 32 14 8 37 14 22 9 13 9 25 8 27 25 11 14 8 30 9 10 19 29 8 16 14 23 20 29
	23 32 37 3 10 24 26 15 21 23 15 3 21 3 41 20 9 5 20 12 42 10 28 36 42 20 10 39 4 31 6 20 11 12 33 30
	LTZ5BMOFJLF5J50İA7İÇ1BPY1İB,6Ş8İCÇUS
$t = 8$ $n = 4$ $r = 3$ $s = 7$ $l = 1$	24 9 32 14 24 9 32 20 22 32 14 8 37 14 22 9 13 9 25 8 27 25 11 14 8 30 9 10 19 29 8 16 14 23 20 29
	9 19 33 29 0 29 34 21 16 5 41 30 12 3 12 37 21 42 40 16 30 7 26 39 23 10 3 16 19 30 0 42 18 14 27 27
	AIUR2RÜJG70SÇ5ÇZJ1?GS9O,LB5GIS21HEÖÖ
$t = 8$ $n = 4$ $r = 0$ $s = 5$ $l = 3$	24 9 32 14 24 9 32 20 22 32 14 8 37 14 22 9 13 9 25 8 27 25 11 14 8 30 9 10 19 29 8 16 14 23 20 29
	34 33 34 13 34 33 34 0 24 20 34 38 13 30 42 7 22 17 9 32 6 4 16 20 40 17 11 34 9 28 18 16 27 22 23 21
	ÜUÜDÜUÜ2MİÜ.DS19KĞAT86Gİ?ĞCÜAPHGÖKLJ
$t = 17$ $n = 4$ $r = -1$ $s = 7$ $l = 1$	33 18 41 23 33 18 41 29 31 41 23 17 46 23 31 18 22 18 34 17 36 34 20 23 17 39 18 19 28 38 17 25 23 32 29 38
	13 40 37 18 16 8 8 10 19 29 32 19 8 23 41 26 19 11 31 5 15 4 30 28 32 2 27 5 9 28 37 31 23 33 42 16
	6ŞPA9113BİLB1ETĞB4K,8.JILYH,2IPKEMU9
$t = 17$ $n = 4$ $r = 1$ $s = 5$ $l = 3$	33 18 41 23 33 18 41 29 31 41 23 17 46 23 31 18 22 18 34 17 36 34 20 23 17 39 18 19 28 38 17 25 23 32 29 38
	32 12 22 12 29 30 5 42 42 32 39 37 41 8 37 6 2 5 14 31 39 21 4 19 19 42 39 33 35 38 29 15 35 37 33 20
	L5D5İJ,UULSPT1P?Y,7KSÇ.BBUSMORİ8OPMC
$t = 25$ $n = 4$ $r = 3$ $s = 4$	41 26 49 31 41 26 49 37 39 49 31 25 54 31 39 26 30 26 42 25 44 42 28 31 25 47 26 27 36 46 25 33 31 40 37 46
	31 38 10 18 3 29 11 36 5 11 11 14 16 41 27 12 15 8 15 27 24 42 9 7 11 11 16 28 3 8 22 20 23 40 29 12

$l=2$	EJY3RÇZIŞZZ?1MB.0Ü0B9NVUZZ1CRÜ758LÇ.
$t=25$ $n=4$ $r=-1$ $s=4$ $l=2$	41 26 49 31 41 26 49 37 39 49 31 25 54 31 39 26 30 26 42 25 44 42 28 31 25 47 26 27 36 46 25 33 31 40 37 46
	39 27 27 18 34 30 41 36 11 35 15 14 10 27 26 12 29 20 19 27 39 7 26 7 39 21 10 28 14 35 29 20 16 33 14 12
	KBB3ĞDMIZH0?YBA.Ç54BKUAUK6YC?HÇ51G?.

(3.3) ve (3.7) 'deki değerleri değiştirerek elde ettiğimiz

"MATEMATİKTE ZEKADAN ÖNCE SABIR GELİR"

metnin Tablo 3.1'deki sayı değerini (t'e göre değişiyor), bu değerlere karşılık gelen şifrelenmiş sayısal değerleri (n ve r göre değişiyor) ve şifrelenmiş metni (r, s ve l 'e göre değişiyor)

Tablo 3.7 (t,n,r,s,l) değişkenlerine göre Lucas sayıları örneklemi

Lucas sayıları kullanılarak $(L_s, L_{s+l}, L_{s+2l}, \dots, L_{s+(n-1)l},)$	
$t=8$ $n=4$ $r=1$ $s=3$ $l=2$	24 9 32 14 24 9 32 20 22 32 14 8 37 14 22 9 13 9 25 8 27 25 11 14 8 30 9 10 19 29 8 16 14 23 20 29
	13 42 9 42 36 1 35 23 4 32 20 34 14 31 21 13 1 32 23 8 30 5 16 30 17 21 25 26 22 21 11 29 37 27 19 3
	D1A1Y3VL6TİÜEŞJD3TL S7GSĞJNOKJCRZÖI5
$t=8$ $n=4$ $r=3$ $s=7$ $l=1$	24 9 32 14 24 9 32 20 22 32 14 8 37 14 22 9 13 9 25 8 27 25 11 14 8 30 9 10 19 29 8 16 14 23 20 29
	0 6 42 42 29 41 20 1 39 8 41 8 11 17 33 30 34 10 14 35 42 0 26 38 15 10 35 21 24 35 42 6 41 9 10 5
	2811R0İ3, 0 CĞUSÜBEV12O.FBVJMV180AB7
$t=8$ $n=4$ $r=0$ $s=5$ $l=3$	24 9 32 14 24 9 32 20 22 32 14 8 37 14 22 9 13 9 25 8 27 25 11 14 8 30 9 10 19 29 8 16 14 23 20 29
	6 23 4 31 6 23 4 11 27 10 16 32 20 1 7 22 14 22 17 38 39 39 4 27 2 18 5 3 37 8 29 23 25 8 2 8
	8L6Ş8L6CÖBGTİ39KEKĞ.„6Ö4H75Z RLN 4
$t=17$ $n=4$ $r=-1$ $s=7$ $l=1$	33 18 41 23 33 18 41 29 31 41 23 17 46 23 31 18 22 18 34 17 36 34 20 23 17 39 18 19 28 38 17 25 23 32 29 38
	7 12 37 23 26 29 30 25 17 30 21 32 33 13 37 11 29 38 37 16 23 18 21 19 14 35 20 2 35 18 42 30 8 26 21 29
	05PEĞİJG JÇLM6P4İRP9EAÇB7OCYOAUJ1ĞÇİ
$t=17$	33 18 41 23 33 18 41 29 31 41 23 17 46 23 31 18 22 18 34 17 36 34 20 23 17 39 18 19 28 38 17 25 23 32 29 38

$n=4$ $r=1$ $s=5$ $l=3$	9 39 34 41 33 29 18 21 32 41 19 42 35 9 36 32 19 38 20 5 20 25 34 37 0 16 17 13 6 13 25 33 42 31 35 18
	2SNTMİAÇLTBUO2ÖLBRC,CGNPÜ9 6?6GMUKOA
$t=25$ $n=4$ $r=3$ $s=4$ $l=2$	41 26 49 31 41 26 49 37 39 49 31 25 54 31 39 26 30 26 42 25 44 42 28 31 25 47 26 27 36 46 25 33 31 40 37 46
	17 23 30 11 40 9 8 10 38 13 31 7 15 25 20 39 5 8 2 38 14 8 11 23 24 33 40 7 1 13 37 4 17 36 17 16
	28DZLVÜYJ,EU0 5KŞÜPJ?ÜZ89GLUÖ,İS2I21
$t=25$ $n=4$ $r=-1$ $s=4$ $l=2$	41 26 49 31 41 26 49 37 39 49 31 25 54 31 39 26 30 26 42 25 44 42 28 31 25 47 26 27 36 46 25 33 31 40 37 46
	33 15 0 11 11 34 36 10 36 13 29 7 26 29 42 39 6 14 0 38 19 12 24 23 39 10 0 7 6 42 12 4 40 16 3 16
	G0OZZĞIYI,ÇUAÇNKT?OJ4.98KYOUTN.SL1R1

Tablo 3.7'de görülüyor ki, $r=1$ alırsak, (1.35)'de tanımlanan gibi bir Circulant matris değerlendirmesi yapılmıştır.

$r=-1$ alınırsa (1.38) denkleminde verilen gibi bir SC_n Negacyclic Circulant matris değerlendirmesi yapılmıştır.

$r=0$ alırsa (1.40) denkleminde verilen gibi bir $C_{n,s}$ Semicirculant matris değerlendirmesi yapılmıştır.

Diğer değişkenler ve r değerlendirmeleri random olarak seçilmiştir. Matris boyunun önemi olmadığı için $n=4$ değerlendirilmiştir.

Metin uzunluğunun değerlendirmesi içinde amcam Ahmet ÖZMEN'e ait "Sen" isimli şiirini Fibonacci ve Lucas dizilerini kullanarak verilen diğer değişkenlere göre Ek-1 ve Ek-2 kısmında yöntemimize göre yapılan program ile değerlendirmesi yapıldı. Şiir olmasına rağmen, düz metin verileri ve değişkenler "duzmetin.tex" kutusundan veriler alındığı için Tablo 3.1'deki karaktere göre düzenlenerek "enter" boşlukları olmadan aşağıdaki gibi yazılmıştır.

"SEN SEN MIRILDANIYOR DALGALAR SENİ FISILDIYOR GECE SENİNLE BAŞLIYOR SENİNLE BİTİYOR DİLİMDEN DÖKÜLEN HER HECE SENİNLE DOĞUYOR GÜN SENİNLE AĞLIYOR BULUTLAR SEN DİYE DÜŞÜP TOPRAĞIN BAĞRINA BİR DAHA SEN OLSUN DİYE UMUTLAR SEN LENİYOR MEHTAP AY DA SEN YILDIZDA SEN SEN LE DOLUYOR GÖNLÜMÜN DERYASI YAKAMOZUN TEBESSÜMÜNDE SEN"

Bu metni ve t, alfabedeki kaydırma, n matris boyutu ve r köşegen altı değeri ile Fibonacci ve Lucas dizilerine göre s ve l indis değişkenleri için değerler “tex” uzantılı dosyadan alınır, çıktı sonuçları Ek-1 ve Ek-2 kısımlarında verilir.

4. SONUÇLAR VE ÖNERİLER

4.1 Sonuçlar

Bu tez sayesinde, tamsayı dizileri ve matris dönüşümleri kullanılarak şifreleme ve deşifreleme yapan birkaç algoritmanın birleştirilmesiyle elde edilen melez bir yöntem öne çıkarılmıştır. Affine-Hill şifreleme yöntemi olarak bilinen bu yöntemin, gizli anahtarını belirlemede kullanılan r-Circulant matrisinin elemanları, Fibonacci ve Lucas sayı dizilerinden seçilmek suretiyle kapsamlı bir analiz gerçekleştirilmiştir.

Affine-Hill şifreleme yönteminin gizli anahtarını belirlerken, bazı parametrik değerler ($'t', 'n', 'r', 's'$ ve $'l'$) kullanılarak anahtarın gizliliği/güvenliği artırılmaya çalışılmıştır. Bu değişkenlerin oluşturduğu gizli anahtarın güvenliği için değişkenlerin RSA ve El-Gamal şifreleme yöntemleri ile şifrelenerek iletilmesi yöntemi denenmiştir.

Kullanılan beş değişken ($'t', 'n', 'r', 's'$ ve $'l'$) ve tez boyuncaki örneklerde kullanmak üzere belirlenen esas metin ("Matematikte zekadan önce sabır gelir") bağlamında, şifreleme parametrelerinin kullanılmasının şifreli mesaja nasıl etki ettiği Tablo 3.6 ve Tablo 3.7'deki veriler sayesinde açık bir biçimde görülmektedir.

Fibonacci ve Lucas sayı dizilerinin anahtar matris elemanlarını oluşturmak için kullanılması, RSA ve El-Gamal şifreleme yöntemi ile anahtar matrisin değişkenlerinin güvenli bir şekilde iletilmesi ile hibrit bir şifreleme sistemi oluşturularak yenilikçi bir yaklaşım sunulmuştur. Bu yaklaşımın, veri alışverişinin güvenli bir şekilde gerçekleştirilmesi sürecine katkı sağlandığı gözlenmiştir.

Sonuç olarak, bu tez, Affine Hill şifreleme yöntemi ve r-Circulant matrislerin kullanımı konusunda önemli bir katkı sağlamakta ve bu alandaki bilgi birikimini artırmıştır. Ayrıca, RSA ve El-Gamal şifrelemesi ile anahtar değerlerinin iletimi sağlanarak hibrit bir şifreleme sistemi oluşturulması gibi yenilikçi yaklaşımlar sunarak, kriptografi alanında yeni araştırma konuları açılması amaçlanmıştır.

4.2 Öneriler

Hill şifreleme algoritmasının ve onun varyasyonlarının kriptografideki potansiyeli ve sınırlılıklarını daha fazla çalışma yapılarak ortaya koyulabilir.

Anahtar matrisleri oluşturmak için Fibonacci ve Lucas dizilerinin kullanımı yerine, kullanılabilecek birçok farklı tam sayı dizisi eklenebilir. Bu dizilerin özellikleri, algoritmaların tahmin edilemezliğini artırabilir.

Şifreleme sisteminin uygulanabilirliğini artırmak için, anahtar matrisin oluşturulmasında kullanılan Fibonacci ve Lucas sayı dizilerinin yanı sıra diğer matematiksel dizilerin de incelenmesi önerilir.

Anahtar matrisin değişkenlerinin iletimi sırasında güvenlik açıklarını en aza indirmek için ek kriptografik önlemler alınabilir yada ek bir güvenlik katmanı daha verilebilir. RSA ve El-Gamal gibi asimetrik şifreleme yöntemleri ile Hill şifrelemesinin kombinasyonu, mesaj güvenliğini artırabilir. Her iki algoritmanın avantajlarını birleştirerek daha güçlü bir Hibrit şifreleme sistemi sunabilir.

Bu çalışmada verilen algoritma modern kriptografik ihtiyaçlara uygun olarak geliştirilebilir.

Hibrit şifreleme sisteminin etkinliğini ve güvenliğini değerlendirmek üzere daha kapsamlı bir sistem analizi yapılmalıdır.

Gerçek uygulamalarda kullanım öncesi, sistemin farklı senaryolarda test edilerek hata oranlarının minimize edilmesi sağlanmalıdır.

Önerilen şifreleme sistemi, güvenlik ve verimlilik açısından mevcut sistemlere alternatif bir çözüm olarak değerlendirilebilir.

5. KAYNAKLAR

Adinarayana, R.K., Vishnuvardhan, B.M., Krishna A.V.N., 2012, A modified Hill cipher based on circulant matrices, *Procedia Technology*, 4, 114 – 118.

Altındis, H., 2011, Sayılar teorisi ve uygulamaları, *Lazer Ofset,* Ankara, 308 s.

Bayar, E., 2012, Modern kriptosistemlerle şifrelemenin modellenmesi ile veri güvenliğinin sağlanması, Yüksek Lisans Tezi*, Marmara Üniversitesi Fen Bilimleri Enstitüsü,* İstanbul.

Billore, V. and Patel, N. 2023, Cryptography utilizing the Affine-Hıll cipher and extended generalized Fibonacci matrices, Electronic Journal of Mathematical Analysis and Applications, Vol. 11(2), No. 4, 1-12.

Cangül, İ. N. Çelik, B., 2013, Sayılar teorisi problemleri, *Dora Basım Yayın*.

Çimen, C., Akyıldız, E. ve Akleylek, S., 2009, Şifrelerin matematiği: Kriptografi, *4. Baskı, Orta Doğu Teknik Üniversitesi Toplum ve Bilim Merkezi,* Ankara,131s.

Davis, P. J.,1979, Circulant matrices, *John Wiley and Sons,* New York.

Debnath, L., 2011, A short history of the Fibonacci and golden numbers with their applications, *International Journal of Mathematical Education in Science and Technology*,42(3), 337-367.

Demirtürk, B. 2010, Fibonacci and Lucas sums by matrix methods, *International Mathematical Forum*, 5, no. 3, 99–107.

Elgamal, T., 1985, A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory* 31, 4, 469–472.

Good, I. J., 1986, Skew circulants and the theory of numbers, *The Fibonacci Quarterly*, 24(2), 47-60.

Gray, R. M., 2006, Toeplitz and circulant matrices: A review, *Foundations and Trends in Communications and Information Theory*, 2(3), 155-239.

Grimaldi, R. P., 2011, Fibonacci and Catalan numbers, *John Wiley & Sons, Inc*. DOI:10.1002/9781118159743.

Gupta, I., Singh, J., and Chaudhary, R., 2007, Cryptanalysis of an extension of the Hill cipher, *Cryptologia*, 31, 3, 246–253.

Hill LS, 1929, Cryptography in an algebraic alphabet, *American Mathematical Monthly*, 36: 306-312.

Hill LS, 1931, Concerning certain linear transformation apparatus of cryptography, *American Mathematical Monthly*,38: 135-154.

Hoggatt, Jr. V. E. and Bicknell, M., 1964, Some new Fibonacci identities, *Fibonacci Quarterly*, 2, (1), 29-31.

Ismail IA, Amin M, Diab H., 2006, How to repair the Hill cipher, *Journal of Zhejiang University- Science A*, 7, 2022–2030.

Kalman D. and White J.E., 2001, Polynomial equations and circulant matrices, *Amer. Math. Monthly*, 108, 821–840.

Koken, F. and Bozkurt, D., 2010, On Lucas numbers by the matrix method, *Hacettepe Journal of Mathematics and Statistics*, 39(4), 471–475.

Koken, F., 2019, The Representations of the Fibonacci and Lucas matrices, *Iranian J. Sci. Tech., Trans. A: Sci*. 43 2443–2448.

Koshy, T., 2019, Fibonacci and Lucas numbers with applications, *Wiley–Blackwell; Volume II*, DOI:10.1002/9781118033067.

Kra, I., and Simanca, S. R., 2012, On circulant matrices, *Notices of the AMS*, 59(3), 368-377.

Li C., Zhang D., Chen G., 2008, Cryptanalysis of an image encryption scheme based on the Hill cipher, *Journal of Zhejiang University - Science A*, 9, 1118–1123.

Lin C.H., Lee C.Y., Lee C.Y., 2004, Comments on Saeednia's improved scheme for the Hill cipher, *Journal of the Chinese Institute of Engineers*, 27, 743–746.

Lüy, E., 2012, Abelyan olmayan sonlu gruplar kullanılarak elde edilen açık anahtar kriptosistem üzerine, Yüksek lisans tezi*, Erciyes Üniversitesi,* Kayseri, 74s.

Mahmoud, A. Y., and Chefranov, A. G., 2014, Hill cipher modification based on pseudo-random eigenvalues, *Applied Mathematics & Information Sciences*, 8, No. 2, 505-516.

Mahmoud A., Y., 2012, Development of matrix cipher modifications and key exchange protocol, doctor of philosophy in computer engineering, *Eastern Mediterranean University*, North Cyprus, 96s.

Maxrizal, I Gusti Nyoman Yudi Hartawan, Padrul Jana, Baiq Desy Aniska Prayanti, 2019, Modified public key cryptosystem based on circulant matrix, *International Conference on Mathematics and Natural Sciences* 2019, doi:10.1088/1742-6596/1503/1/012007.

Obaid, H.Z., 2016, Kriptoloji yöntemlerinin karşılaştırılması, Yüksek lisans tezi, *Erciyes Üniversitesi,* Kayseri, 84s.

Okumuş, İ., 2012, RSA Kriptosisteminin hızını etkileyen faktörler, Doktora*, Atatürk Üniversitesi,* Erzurum, 68s.

Öztürkmenoğlu, c.ş., 2016, Matrislerle şifreleme üzerine, Yüksek lisans tezi, *Muğla Sıtkı Koçman Üniversitesi,* Muğla, 53s.

Prasad, K. and Mahato H., 2021, Cryptography using generalized Fibonacci matrices with Affine-Hill cipher, *Journal of Discrete Mathematical Sciences and Cryptography*, DOI: 10.1080/09720529.2020.1838744

Ramakrishna, V., Prasanna, T.V.N., 2013, Symmetric circulant matrices and publickey cryptography, *Int. J. Contemp. Math. Sciences*, Vol. 8, No. 12, 589 – 593.

Saeednia S., 2000, How to make the Hill cipher secure, *Cryptologia*, 24: 353-360.

Santoso, Y. S., 2021, Message security using a combination of Hill cipher and RSA algorithms, *Jurnal Matematika Dan Ilmu Pengetahuan Alam*, 1 (1) 20-28.

Stinson, D. R., 2005, Cryptography: Theory and practice, *3rd Ed. Chapman and Hall/CRC, Taylor & Francis Group*.

Strang, G., 2022, Introduction to linear algebra, *Wellesley-Cambridge Press*.

Sundarayya, P., and Vara Prasad, G., 2019, A public key cryptosystem using affine hill cipher under modulation of prime number, *Journal of Information and Optimization Sciences*, 40, 4, 919–930.

Tas, N., Uçar, S., and Özgür, N.Y. and Kaymak, Ö.Ö., 2018, A new coding/decoding algorithm using Fibonacci numbers, *Discrete Mathematics, Algorithms and Applications*, Vol. 10, No. 2. DOI: 10.1142/S1793830918500283

Tascı D., 2018, Lineer cebir, *Gazi Kitapevi*.

Thilaka, B., and Rajalakshmi, K., 2005, An extension of hill cipher using generalized inverses and mth residue modulo n, *Cryptologia* 29, 4, 367–376.

Toorani, M. Falahati, A., 2009, A secure variant of the Hill cipher, *IEEE*, 313–316.

Toorani, M. and Falahati, A., 2011, A secure cryptosystem based on affine transformation, *Journal of Security and Communication Networks*, 2:207–215.

Uçar, S. Taş N. and Özgür, Y. N., 2019, A new application to coding theory via Fibonacci and Lucas numbers, *Mathematical Sciences And Applications E-Notes*, 7 (1) 62-70.

Viswanath, M., and Kumar, M. R., 2015, A public key cryptosystem using Hill's cipher, *Journal of Discrete Mathematical Sciences and Cryptography 18*, 1-2, 129–138.

EKLER

EK-1 Yukardaki şiir metni için, (3.3)'de istenilen Tablo 3.1'in oluşturulası için gerekli $t = 8$, matris boyutu için $n = 6$ ve köşegen altı değeri $r = 2$ alınır. Ayrıca (3.4)'deki Fibonacci sayıları için $s = 4$ ve $l = 2$ değerleri alınarak oluşturulan Affine-Hill şifrelemedeki düz metne ait Tablo 3.1'deki sayısal değerler Tablo 5.1'de verilir.

Tablo 5.1 Tablo 3.1'de $t = 8$ değerine göre düz metnin sayısal değerleri

P_1	[30 14 25 8 30 14 25 8 24 19 29 19 23 13 9 25 19 36 26 29 8 13 9 23 16 9 23 9 29 8 30 14 25 20 8 15]
P_2	[19 30 19 23 13 19 36 26 29 8 16 14 11 14 8 30 14 25 20 25 23 14 8 10 9 31 23 19 36 26 29 8 30 14 25 20]
P_3	[25 23 14 8 10 20 32 20 36 26 29 8 13 20 23 20 24 13 14 25 8 13 27 22 34 23 14 25 8 18 14 29 8 18 14 11]
P_4	[14 8 30 14 25 20 25 23 14 8 13 26 17 33 36 26 29 8 16 34 25 8 30 14 25 20 25 23 14 8 9 17 23 19 36 26]
P_5	[29 8 10 33 23 33 32 23 9 29 8 30 14 25 8 13 20 36 14 8 13 34 31 34 28 8 32 26 28 29 9 17 19 25 8 10]
P_6	[9 17 29 19 25 9 8 10 20 29 8 13 9 18 9 8 30 14 25 8 26 23 30 33 25 8 13 20 36 14 8 33 24 33 32 23]
P_7	[9 29 8 30 14 25 8 23 14 25 20 36 26 29 8 24 14 18 32 9 28 8 9 36 8 13 9 8 30 14 25 8 36 19 23 13]
P_8	[19 37 13 9 8 30 14 25 8 30 14 25 8 23 14 8 13 26 23 33 36 26 29 8 16 27 25 23 34 24 34 25 8 13 14 29]
P_9	[36 9 30 19 8 36 9 22 9 24 26 37 33 25 8 32 14 10 14 30 30 34 24 34 25 13 14 8 30 14 25 8 8 8 8 8]

$n = 6$ seçildiği için sayısal değeri 36'lı bloklara ayırarak verilir. Diğer verilere oluşturulan matris kullanılarak (3.8)'deki işlemleri uygularsak Tablo 5.2'deki şifrelenmiş metne ait sayısal değer elde edilir.

Tablo 5.2 Şifrelenmiş metne ait sayısal değerler

S_1	[0 40 1 10 28 15 33 2 16 19 17 29 32 9 0 20 12 41 22 30 31 29 18 40 13 8 26 37 13 8 25 0 28 0 38 8]
S_2	[10 28 7 13 27 14 41 9 30 1 3 28 24 20 13 18 25 24 7 33 29 13 30 22 30 38 24 28 42 40 39 11 36 38 2 13]
S_3	[21 19 38 29 37 12 37 32 20 13 20 10 4 7 16 42 30 22 32 11 5 13 36 26 39 39 37 39 41 42 38 1 14 42 4 11]
S_4	[37 20 22 30 35 34 28 42 14 20 12 11 33 37 24 20 37 11 31 31 39 4 15 25 16 4 9 3 2 23 9 39 41 35 3 2]
S_5	[19 17 20 21 27 23 42 16 16 3 42 36 5 1 2 14 36 12 10 15 1 39 6 39 9 42 1 30 40 6 20 30 18 15 31 23]

S_6	[14 16 9 8 6 21 30 12 22 9 11 33 22 32 17 15 27 7 25 6 7 17 29 15 27 38 10 31 1 2 8 42 23 12 17 1]
S_7	[19 6 5 8 3 11 22 15 25 27 15 22 29 12 13 27 6 38 10 14 39 1 31 26 33 9 42 27 38 28 2 11 29 12 27 21]
S_8	[8 5 9 27 25 4 28 34 35 27 30 30 20 35 1 31 15 9 8 42 21 6 41 37 42 30 0 36 35 39 2 24 31 35 28 1]
S_9	[3 11 8 32 3 18 10 18 32 14 32 10 22 3 34 26 29 9 1 3 18 3 4 1 19 2 27 13 11 4 37 15 25 34 8 7]

Tablo 5.2'deki sayısal verileri Tablo 3.1'deki harf değerine dönüştürerek Tablo 5.3'deki 36'lı bloklar şeklindeki şifrelenmiş metni elde edelim.

Tablo 5.3 Şifrelenmiş metnin 36'lı blok hali

2?3BPFU4GIĞRTA2İÇ0KSŞRH?D OZD N2P2.
BP9DÖE0AS35PMİDHNM9URDSKS.MP1?,CY.4D
JI.RZÇZTİDİB69G1SKTC7DYO,,Z,01.3E16C
ZİKSVÜP1EİÇCUZMİZCŞŞ,6FNG6A54LA,0V54
IĞİJÖL1GG51Y734EYÇBF3,8,A13S?8İSHFŞL
EGA 8JSÇKACUKTĞFÖ9N89ĞRFÖ.BŞ34 1LÇĞ3
I87 5CKFNÖFKRÇDÖ8.BE,3ŞOUA1Ö.P4CRÇÖJ
7AÖN6PÜVÖSSİV3ŞFA 1J80Z1S2YV,4MŞVP3
5C T5HBHTETBK5ÜORA35H563I4ÖDC6ZFNÜ 9

Tablo 5.3'deki metnin Tablo 5.2'deki sayısal karşılıkları ile (3.10)'daki işlemleri uygularsak düz metne ait Tablo 5.1'deki sayısal değer elde edilir ki bu değerler Tablo 3.1'deki harf değeri ile Tablo 5.4'de düz metin 36'lı bloklar ile elde edilir.

Tablo 5.4 Düz metnin 36'lı blok hali

SEN SEN MIRILDANIYOR DALGALAR SENİ F
ISILDIYOR GECE SENİNLE BAŞLIYOR SENİ
NLE BİTİYOR DİLİMDEN DÖKÜLEN HER HEC
E SENİNLE DOĞUYOR GÜN SENİNLE AĞLIYO
R BULUTLAR SEN DİYE DÜŞÜP TOPRAĞIN B
AĞRINA BİR DAHA SEN OLSUN DİYE UMUTL
AR SEN LENİYOR MEHTAP AY DA SEN YILD
IZDA SEN SEN LE DOLUYOR GÖNLÜMÜN DER
YASI YAKAMOZUN TEBESSÜMÜNDE SEN

EK-2 Yukardaki şiir metni için, (3.3)'de istenilen Tablo 3.1'in oluşturulası için gerekli $t = 8$, matris boyutu için $n = 6$ ve köşegen altı değeri $r = 2$ alınır. Ayrıca (3.5)'deki Lucas sayıları için $s = 4$ ve $l = 2$ değerleri alınarak oluşturulan Affine-Hill şifrelemedeki düz metne ait Tablo 3.1'deki sayısal değerler Tablo 5.1'de verilir. Aynı t değeri kullanılarak yapıdığı için yeniden bir tabla ile verilmedi. Yine, $n = 6$ seçildiği için sayısal değeri 36'lı bloklar şeklinde verilir. Diğer verilere oluşturulan matris kullanılarak (3.8)'deki işlemleri uygularsak Tablo 5.2'deki şifrelenmiş metne ait sayısal değer elde edilir.

Tablo 5.5 Şifrelenmiş metne ait sayısal değerler

S_1	[13 5 34 36 8 3 8 34 25 1 42 29 41 19 34 42 15 6 18 32 41 38 5 21 23 7 42 25 37 6 30 7 23 7 36 6]
S_2	[36 8 27 5 25 7 4 14 15 37 23 6 30 26 7 15 10 4 39 24 1 38 29 16 25 42 19 12 20 19 8 6 30 13 41 12]
S_3	[40 38 4 19 20 25 17 42 32 25 20 41 23 33 14 28 30 19 6 37 1 42 23 28 26 19 4 25 10 19 41 42 5 30 28 36]
S_4	[32 37 13 17 27 9 22 7 15 40 9 35 29 35 34 38 14 10 9 22 37 28 24 16 24 0 1 14 14 30 28 30 25 42 18 26]
S_5	[37 21 36 13 19 5 14 30 25 6 42 11 24 18 12 8 14 0 17 33 29 20 14 10 31 30 37 28 2 10 20 24 13 34 28 17]
S_6	[10 37 24 25 27 17 9 29 19 12 23 4 4 27 39 19 38 24 40 19 35 17 40 20 12 25 10 7 20 18 28 14 9 23 16 35]
S_7	[22 9 11 1 7 9 29 24 16 13 11 29 4 7 23 36 21 34 1 31 31 19 14 9 38 17 31 5 4 22 33 37 15 40 37 22]
S_8	[27 36 30 29 29 35 21 28 2 41 7 12 32 2 33 13 39 23 28 14 15 2 11 37 29 33 8 2 24 28 36 7 10 13 28 19]
S_9	[16 36 32 13 39 41 42 13 26 2 8 3 20 33 18 42 6 22 13 37 35 7 30 29 23 24 5 36 37 4 22 22 10 17 7 13]

Tablo 5.5'deki sayısal verileri Tablo 3.1'deki harf değerine dönüştürerek Tablo 5.6'daki 36'lı bloklar şeklindeki şifrelenmiş metni elde edelim.

Tablo 5.6 Şifrelenmiş metnin 36'lı blok hali

D7ÜY 5 ÜN31R0IÜ1F8HT0.7JL91NZ8S9L9Y8
Y Ö7N96EFZL8SO9FB6,M3.RGN1IÇİI 8SD0Ç
?.6IİNĞ1TNİ0LUEPSI8Z31LPOI6NBI017SPY
TZDĞÖAK9F?AVRVÜ.EBAKZPMGM23EESPSN1HO
ZJYDI7ESN81CMHÇ E2ĞURİEBŞSZP4BİMDÜPĞ
BZMNÖĞARIÇL66Ö,I.M?IVĞ?İÇNB9İHPEALGV

KAC39ARMGDCR69LYJÜ3ŞŞIEA.ĞŞ76KUZF?ZK
ÖYSRRVJP409ÇT4UD,LPEF4CZRU 4MPY9BDPI
GYTD,01DO4 5İUH18KDZV9SRLM7YZ6KKBĞ9D

Tablo 5.6'deki metnin Tablo 5.5'deki sayısal karşılıkları ile (3.10)'daki işlemleri uygularsak düz metne ait Tablo 5.1'deki sayısal değer elde edilir ki bu değerler Tablo 3.1'deki harf değeri ile Tablo 5.7'de düz metin 36'lı bloklar ile elde edilir.

Tablo 5.7 Düz metnin 36'lı blok hali

SEN SEN MIRILDANIYOR DALGALAR SENİ F
ISILDIYOR GECE SENİNLE BAŞLIYOR SENİ
NLE BİTİYOR DİLİMDEN DÖKÜLEN HER HEC
E SENİNLE DOĞUYOR GÜN SENİNLE AĞLIYO
R BULUTLAR SEN DİYE DÜŞÜP TOPRAĞIN B
AĞRINA BİR DAHA SEN OLSUN DİYE UMUTL
AR SEN LENİYOR MEHTAP AY DA SEN YILD
IZDA SEN SEN LE DOLUYOR GÖNLÜMÜN DER
YASI YAKAMOZUN TEBESSÜMÜNDE SEN

Not: Kullandığımız Tablo 3.1'de boşluk karakterine ait bir değer (t) olduğu için kelimeler arasındaki boşluk değerlendirmeye alınıyor ve işlemler içerinde de boşluk karakterine ait aynı değer gelirse şifrelemede boşluk karakterini bırakmaktadır. Çıktı üzerinde fark edilmeye bilir. Fakat Tablo 5.3 Şifrelenmiş metnin 36'lı blok hali'deki ilk satırın sonunda boşluk karakteri 36'ıncı karakterdir veya 8.satırın başındaki boşluk 1.karakterdir. Her bir satır 36 karaktere sahip olmalıdır, baştaki ve sondaki karakterler çıktıda fark edilmeyebilir.