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

REKÜRANS BAĞINTILARI VE KODLAMA YÖNTEMLERİ

DOKTORA TEZİ

SÜLEYMAN AYDINYÜZ

DENİZLİ, ŞUBAT - 2022

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

REKÜRANS BAĞINTILARI VE KODLAMA YÖNTEMLERİ

DOKTORA TEZİ

SÜLEYMAN AYDINYÜZ

DENİZLİ, ŞUBAT - 2022

Bu tez çalışması Pamukkale Üniversitesi Bilimsel Araştırma Projesi (BAP) tarafından 2020FEBE003 nolu proje ile desteklenmiştir.

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

Süleyman AYDINYÜZ

ÖZET

REKÜRANS BAĞINTILARI VE KODLAMA YÖNTEMLERİ
DOKTORA TEZİ
SÜLEYMAN AYDINYÜZ
PAMUKKALE ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

(TEZ DANIŞMANI:PROF. DR. MUSTAFA AŞCI)

DENİZLİ, ŞUBAT - 2022

Bu tezde; 2×2 tipindeki Fibonacci blok matrisleri ile tanımlanmış olan şifreleme algoritması yeniden tanımlandı ve $k\times k$ tipindeki matrislere genelleştirilerek Advanced Encryption Standard (AES) benzeri bir şifreleme algoritması tanımlandı. Bu algoritma ile ilgili örneklere yer verildi.

Birinci bölümde, rekürans bağıntıları hakkında temel tanımlara ve teoremlere yer verildi. Ayrıca Fibonacci ve Lucas sayılarının rekürans bağıntıları tanımlandı ve genelleştirilerek k. mertebeden Fibonacci sayılarının rekürans bağıntısı verildi. Bu tanımlamaların yanı sıra matris gösterimlerine yer verildi. Bu bölümde son olarak Fibonacci polinomunun tanımı verildi ve genelleştirilerek k. mertebeden Fibonacci polinomları tanımlandı ve matris gösterimleri verildi.

İkinci bölümde, modern kriptolojinin önemli terimlerinden bazıları tanımlandı ve bazı bilinen algoritmalar hakkında bilgiler verildi. Bu bölümde gelişmiş şifreleme algoritması (AES) hakkında bilgiler verilerek bu algoritmanın katmanları tanımlandı. Ayrıca AES katmanlarında çokça kullanılan sonlu cisimlerin varlığından bahsedildi ve Galois cismi olarak adlandırılan sonlu cismin özellikleri verildi.

Üçüncü bölümde, 2×2 tipindeki Fibonacci blok matrisleri ile tanımlanmış olan şifreleme algoritması yeniden tanımlandı ve $k\times k$ tipindeki matrislere genelleştirerek Advanced Encryption Standard (AES) benzeri bir şifreleme algoritması verildi. Algoritmanın tanımlanmasından sonra bu algoritma ile ilgili örneklere yer verildi.

ANAHTAR KELİMELER: Fibonacci Sayıları, Fibonacci Polinomları, k. mertebeden Fibonacci Polinomları, Fibonacci Matrisi, k. mertebeden Fibonacci Polinom Matrisi, Galois Cismi, AES, Kriptoloji

ABSTRACT

RECURRENCE RELATIONS AND CODING METHODS
PH.D THESIS
SÜLEYMAN AYDINYÜZ
PAMUKKALE UNIVERSITY INSTITUTE OF SCIENCE
MATHEMATICS

(SUPERVISOR:PROF. DR. MUSTAFA AŞCI)

DENİZLİ, FEBRUARY 2022

In this thesis; the encryption algorithm define by Fibonacci block matrices of type 2×2 has been redefined and an encryption algorithm similar to the Advanced Encryption Standard (AES) is defined by generalizing to $k\times k$ type matrices. Examples of this algorithm are given.

In the first chapter, basic definitions and theorems about recurrence relations are given. In addition, recurrence relations of Fibonacci and Lucas numbers are defined and generalized of the recurrence relation of $k-$ order Fibonacci numbers. In addition to these definitions, matrix representations are included. In this section, finally, the definition of Fibonacci polynomial is given and generalized $k-$ order Fibonacci polynomials and matrix representations are given.

In the second part, some of the important terms of modern cryptography are defined and some known algorithms are given. In this section, information about the advanced encryption algorithm (AES) is given and the layers of this algorithm are defined. In addition, the existence of finite objects, which are widely used in AES layers, is mentioned and the properties of the finite object called Galois field were given.

In the third chapter, the encryption algorithm define with Fibonacci block matrices of type 2×2 is redefined and generalized to matrices of type $k\times k$, an encryption algorithm similar to Advanced Encryption Standard (AES) is given. After the algorithm is defied, examples related to this algorithm are given.

KEYWORDS: Fibonacci Numbers, Fibonacci Polynomials, $k-$ Order Fibonacci Polynomials, Fibonacci Matrix, $k-$ Order Fibonacci Polynomials Matrix, Galois Field, AES, Cryptology.

İÇİNDEKİLER

Sayfa

ŞEKİL LİSTESİ

Sayfa

TABLO LİSTESİ

Sayfa

SEMBOL LİSTESİ

F_n	:	n. Fibonacci Sayısı
L_n	:	n. Lucas Sayısı
T_n	:	n. Tribonacci Sayısı
$g(k)_n$	:	k. Mertebeden Fibonacci Sayı Dizisi
$f_n(x)$	:	n. Fibonacci Polinomu
$J_n(x)$	:	Jacobsthal tarafından tanımlanan n. Fibonacci Polinomu
$g(x)$	:	Fibonacci Sayılarının Üreteç Fonksiyonu
$h(x)$	:	Lucas Sayılarının Üreteç Fonksiyonu
$F_n^{(k)}(x)$	:	k. Mertebeden Fibonacci Polinomu
Q_k	:	$k \times k$ Boyutlu $Q-$ matrisi
$F(k)_n$	:	k. Mertebeden Fibonacci Matrisi
AES	:	Gelişmiş Şifreleme Standardı
$GF(p)$	:	Galois Cismi

ÖNSÖZ

Çalışmalarım boyunca değerli katkılarıyla beni yönlendiren ve her safhasında bilgisine başvurduğum Sayın Hocam Prof. Dr. Mustafa AŞCI' ya teşekkürü borç bilirim. Yine bu çalışmanın hazırlanması aşamasında düşünce ve önerileriyle katkıda bulunan Tez izleme komitesi üyeleri Sayın Doç. Dr. Murat BEŞENK ve Sayın Doç. Dr. Ummahan MERDİNAZ ACAR hocalarıma da şükranlarımı sunarım. Tezi yazmamda uluslararası konferanslarda beni destekleyen, bana maddi olanak sağlayan PAUBAP' a teşekkür ederim. Manevi destekleriyle beni hiçbir zaman yalnız bırakmayan aileme, değerli eşim Fatma AYDINYÜZ'e ve oğluma teşekkür ederim.

1. GİRİŞ

On üçüncü yüzyılın matematiksel yenilikçisi Leonardo Fibonacci, orta çağ boyunca matematik biliminin önde gelen liderlerindendi. İtalya'nın Pisa kentinde doğdu ve bu durumdan dolayı Leonardo Pisano veya Pisa'lı Leonardo olarak da biliniyordu. Babası Afrika'nın kuzey kıyısındaki Bougie'de (Şimdi Cezayir sınırları içerisinde bulunuyor.) gümrük tahsildarı iken, Fibonacci'nin Mağribi (Fas'a ait bir topluluk) bir öğretmeni vardı ve onu Hindu-Arap sayı sistemi ve hesaplama yöntemleriyle tanıştırdı. Fibonacci'nin babasına yardım sebebiyle çok seyahat etmesi ve hesaplama sistemlerinin kapsamlı çalışmalarından sonra 1202'de Hindu-Arap rakamlarını ve bunların hesaplamada nasıl kullanıldığını açıkladığı "Liber Abaci" yi yazdı. Bu ünlü kitap sayesinde, Roma numaralandırma sistemini değiştirmede ve bugün günümüzde kullanılan sayı sistemini tanıtmada etkili olmuştur. Ayrıca bu kitap bazı geometri terimlerinin ve matematiğin cebir alanının temellerini oluşturmaktadır.

Fibonacci çeşitli matematik konuları üzerine çalışmalar yapmış olmasına rağmen, özellikle adının geçtiği

$$1,1,2,3,5,8,13,21,34,55\ldots,$$

sayı dizisiyle hatırlanır. Bu sayı dizisi, bugün bile, özellikle "The Fibonacci Quaterly" 'i yayınlayan "Fibonacci Derneği" tarafından devam eden araştırmaların konusudur.

Fibonacci sayıları o kadar ilginçtir ki doğada ve bilimde oldukça beklenmedik yerlerde ortaya çıkmaktadır. Bunların bazılarını aşağıdaki gibi listeleyebiliriz:

- Fibonacci ve Dünya
- Fibonacci ve Illinois (Amerika'da eyalet)
- Fibonacci ve Çiçekler
- Fibonacci ve Ağaçlar
- Fibonacci ve Ayçiçekler

- Fibonacci, Çam Kozalağı, Enginar ve Ananas
- Fibonacci ve Arılar
- Fibonacci ve Alt Küme
- Fibonacci ve Kanalizasyon Arıtma Sistemi
- Fibonacci ve Atom
- Fibonacci ve Balmer Serisi
- Fibonacci ve X-ışınları
- Fibonacci ve Gazyağı
- Fibonacci ve Müzik
- Fibonacci ve Şiir
- Fibonacci ve Sinir Fizyolojisi
- Fibonacci ve Elektrik Akımı
- Fibonacci ve Ekonomi
- Fibonacci ve Kriptoloji

Bu uygulamaların ve çalışmaların detayları Koshy (2017), Vajda (1989) ve Hoggatt (1969) incelenebilir.

Fransız matematikçi Edouard Lucas (1842-1891) tarafından Fibonacci sayı dizisine benzer bir tanımlama ile Lucas sayı dizisi tanımlanmıştır ve yapılan çalışmalar Lucas sayı dizisinin Fibonacci sayı dizisi ile bağlantısının oldukça fazla olduğunu göstermektedir. Dolayısıyla bu yapılan çalışmalar sayılar teorisinde özel sayılar olarak adlandırılan Pell, Pell-Lucas, Jacobsthal, Jacobsthal-Lucas gibi birçok sayı dizisini literatüre kazandırmıştır (Horadam, 1961, 1963).

Günden güne, iletişim kanalları üzerinden veri aktarımı konusunda bilgi güvenliğini sağlamak amacıyla bu konuda birçok çalışma yapıldı ve yapılmaya devam etmektedir. Bu nedenle kodlama/kod çözme algoritmaları bilgi güvenliğini sağlamada önemli rol oynar. Özellikle, Fibonacci dizisi kodlama teorisinde en çok tercih edilen sayı dizilerinden biridir. Yapılan birçok çalışmada bunların örneklerini görebiliriz. Örneğin; Stakhov (1999, 2006) Fibonacci $p-$sayıları ve Q_p-matrisleri için Cassini formülünün genelleştirilmesini kullanan bir kodlama teorisine yeni bir yaklaşım getirdi. 2009 yılında M. Basu ve M. Prasad Fibonacci kodlama teorisi için kod unsurları arasındaki genelleştirilmiş ilişkileri sundu (Basu ve Prasad, 2009).

Ayrıca M. Basu ve M. Das (2014) Tribonacci matrisleri için yeni bir kodlama teorisi tanıttı ve 2014 yılında Tribonacci sayıları için verilen kodlama teorisini genelleştirerek n. mertebeden Fibonacci sayıları için kodlama teorisini tanımlamıştır (Basu ve Das, 2014). Yapılan bu çalışmalar Asci ve Aydinyuz (2020) tarafından genelleştirilerek kompleks uzaya taşındı. k. mertebeden Gaussian Fibonacci polinomlarını tanımladılar ve bu polinomlar üzerinde kodlama teorisini verdiler.

Bu tezde, Dişkaya, Avaroğlu ve Manken (2020) de 2×2 tipindeki Fibonacci blok matrisleri ile tanımlamış oldukları şifreleme algoritması yeniden tanımlanarak $k\times k$ tipindeki matrislere genelleştirildi ve Advanced Encryption Standard (AES) benzeri bir şifreleme algoritması tanımlandı. Bu metot ile ilgili örneklere yer verildi.

1.1 Temel Tanım ve Teoremler

Çalışmanın bu bölümünde, daha sonraki kısımlarda kullanılacak temel tanım ve teoremlere yer verilmiştir.

Matematikte, bir indirgeme (rekürans) bağıntısı, bir dizinin n. terimini, bağıntının mertebesi olarak adlandırılan bazı sabit k (n'den bağımsız) değerleri için önceki k terimin bir fonksiyonu olarak ifade eden bir denklem olarak tanımlanır. Şimdi bu tanımı matematiksel bir dille verelim:

Tanım 1.1.1. $a_0, a_1, a_2, a_3, ..., a_n, ...$ sonsuz bir dizi, $k \in \mathbb{N}$ sabit ve $f : \mathbb{N} \times \mathbb{Z}^k \to \mathbb{R}$ bir fonksiyon olsun. $a_0, a_1, a_2, a_3, ..., a_{k-1}$ başlangıç değerleri olmak üzere ve $\forall n \geq k$ için

$$a_n = f\left(n, a_{n-1}, a_{n-2}, a_{n-3}, ..., a_{n-k}\right) \tag{1.1}$$

fonksiyonuna k. mertebeden indirgeme (rekürans) bağıntısı denir. Dizinin bütün elemanlarını (1.1) denklemi ve $a_0, a_1, a_2, a_3, ..., a_{k-1}$ başlangıç değerleri ile belirlenir. (Koshy, 2001)

Tanım 1.1.2. (a_n) sonsuz bir dizi, $k \in \mathbb{N}$sabit ve $f_0, f_1, f_2, ..., f_k$ $\mathbb{N}$'den $\mathbb{R}$' ye tanımlı fonksiyonlar ve $f_k(n) \neq 0$ olmak üzere $\forall n \geq k$ için

$$a_n = f_1(n)a_{n-1} + f_2(n)a_{n-2} + ... + f_k(n)a_{n-k} + f_0(n) \tag{1.2}$$

biçimindeki indirgeme bağıntısına k. mertebeden lineer indirgeme (rekürans) bağıntısı denir. (Koshy, 2001)

- (1.2) denklemindeki $f_1, f_2, ..., f_k$ fonksiyonları sabit fonksiyonlar ve $f_i(n) = b_i$ $(1 \leq i \leq k)$ biçiminde olmak üzere

$$a_n = b_1a_{n-1} + b_2a_{n-2} + ... + b_ka_{n-k} + f_0(n) \tag{1.3}$$

  indirgeme bağıntısına sabit katsayılı indirgeme bağıntısı denir.

- (1.2) denklemindeki $\forall n \in \mathbb{N}$ için $f_0(n) = 0$ ise

$$a_n = f_1(n)a_{n-1} + f_2(n)a_{n-2} + ... + f_k(n)a_{n-k} \tag{1.4}$$

  İndirgeme bağıntısına homojen indirgeme bağıntısı denir.

Teorem 1.1.1. $a_n = c_1a_{n-1} + c_2a_{n-2}$ indirgeme bağıntısı olsun. Bu durumda indirgeme bağıntısının karakteristik denklemi

$$r^2 - c_1r - c_2 = 0 \tag{1.5}$$

ve kökleri α ve β olmak üzere genel çözümü

$$a_n = c\alpha^n + d\beta^n \tag{1.6}$$

dir. Burada c ve d sabit sayılardır. (Koshy, 2001)

Teorem 1.1.2. p. dereceden homojen, lineer

$$a_n = b_1a_{n-1} + b_2a_{n-2} + ... + b_pa_{n-p} \tag{1.7}$$

indirgeme bağıntısının karakteristik denklemi

$$r^p - b_1 r^{p-1} - b_2 r^{p-2} - \ldots - b_{p-1} r - b_p = 0 \tag{1.8}$$

olsun. Bu karakteristik denklemin q_i katlı kökü r_i olmak üzere

$$k_{i_1} r_i^n + k_{i_2} n r_i^n + k_{i_3} n^2 r_i^n + \ldots + k_{i_{qi}} n^{q_i - 1} r_i^n \tag{1.9}$$

ifadesi a_n indirgeme bağıntısı için bir çözümdür. Burada $k_{i_1}, k_{i_2}, \ldots, k_{i_{qi}}$ keyfi sabitlerdir.

1.1.1 Fibonacci ve Lucas Sayıları

Tanım 1.1.1.1. Fibonacci sayı dizisi $\{F_n\}$ ve $\forall n \geq 2$ doğal sayısı için başlangıç koşulları $F_0 = 0$ ve $F_1 = 1$ olmak üzere

$$F_n = F_{n-1} + F_{n-2} \tag{1.10}$$

indirgeme (rekürans) bağıntısı ile tanımlanır. Burada F_n'e *n.* Fibonacci sayısı denir.

Tanım 1.1.1.2. Lucas sayı dizisi $\{L_n\}$ ve $\forall n \geq 2$ doğal sayısı için $L_0 = 2$ ve $L_1 = 1$ başlangıç koşulları olmak üzere

$$L_n = L_{n-1} + L_{n-2} \tag{1.11}$$

indirgeme (rekürans) bağıntısı ile tanımlanır. Burada L_n' e *n.* Lucas sayısı denir.

Tanım 1.1.1.3. Tribonacci sayı dizisi $\{T_n\}$ ve $\forall n \geq 3$ doğal sayısı için başlangıç koşulları $T_0 = 0, T_1 = 1$ ve $T_2 = 1$ olmak üzere

$$T_n = T_{n-1} + T_{n-2} + T_{n-3} \tag{1.12}$$

indirgeme bağıntısı ile tanımlanır. Burada T_n' e *n.* Tribonacci sayısı denir.

Teorem 1.1.1.1. F_n, *n.* Fibonacci sayısı ve L_n, *n.* Lucas sayısı olmak üzere, Fibonacci sayısının Binet formülü

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

olarak bulunur. Aynı şekilde Lucas indirgeme bağıntısı için Binet formülü

$$L_n = \alpha^n - \beta^n$$

olarak bulunur. Burada $\alpha = \frac{1+\sqrt{5}}{2}$ ve $\beta = \frac{1-\sqrt{5}}{2}$ dir.

Tanım 1.1.1.4. $a_0, a_1, a_2, \ldots$ bir reel sayı dizisi olsun.

$$g(x) = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n + \ldots$$

ifadesine $\{a_n\}$ sayı dizisinin üreteç fonksiyonu denir.

Teorem 1.1.1.2. Fibonacci sayı dizisi $\{F_n\}$ ve Lucas sayı dizisi $\{L_n\}$ olmak üzere Fibonacci sayı dizisinin üreteç fonksiyonu

$$g(x) = \frac{x}{1 - x - x^2}$$

ve Lucas sayı dizisinin üreteç fonksiyonu

$$h(x) = \frac{2 - x}{1 - x - x^2}$$

olarak bulunur.

Fibonacci ve Lucas sayı dizilerinin indirgeme bağıntılarının bir genellemesi ise k. mertebeden genellemeleridir. k. mertebeden Fibonacci sayıları $k \geq 2$ için aşağıdaki gibi tanımlanır.

Tanım 1.1.1.5. $k \geq 2$ bir pozitif tamsayı ve $n > k \geq 2$ olmak üzere $\{g(k)_n\}$ k. mertebeden Fibonacci sayı dizisi

$$g(k)_1 = ... = g(k)_{k-2} = 0, \quad g(k)_{k-1} = 1, \quad g(k)_k = 1 \tag{1.13}$$

başlangıç koşulları ile

$$g(k)_n = g(k)_{n-1} + g(k)_{n-2} + g(k)_{n-3} + ... + g(k)_{n-k}$$

indirgeme (rekürans) bağıntısı ile tanımlanır. (Lee ve Kim, 2003).

Matrisler ile indirgeme bağıntıları ilişkili sayı dizileri arasında bağlantıların kurulduğu ve bu ilişkiler ile sayı dizilerinin incelendiği çalışmalar matematik dünyasında oldukça fazla sayıda yer almaktadır. Charles H. King (1960) matrisler ile Fibonacci sayıları arasında oldukça ilginç bir ilişki kurdu ve bu çalışma matematik dünyasının ilgisini oldukça çekerek bu alanda birçok yeni çalışmanın önünü açtı.

Teorem 1.1.1.3. $n \geq 2$ ve $F_{n+1} = F_n + F_{n-1}$ indirgeme bağıntısı ile tanımlanan Fibonacci sayı dizisinin matris gösterimi

$$Q = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \tag{1.14}$$

ile verilir. Buna göre

$$Q^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} \tag{1.15}$$

dir. (Koshy, 2001)

Teorem 1.1.1.4. $\{F_n\}$ Fibonacci sayı dizisi ve $F_0 = 0, F_1 = 1$ başlangıç koşulları olmak üzere $n \geq 2$ için Q – matrisi aşağıdaki özellikleri sağlar:

1. $Q^n Q^m = Q^m Q^n = Q^{n+m}$

2. $Q^n = Q^{n-1} + Q^{n-2}$.

Teorem 1.1.1.5. $\{F_n\}$ Fibonacci sayı dizisi olmak üzere Cassini özdeşliği

$$\det\left(Q^n\right) = F_{n-1}F_{n+1} - F_n^2 = (-1)^n$$

olarak bulunur.

Teorem 1.1.1.6. Lee, (Lee ve ark., 2002) $F_n = \left[f_{ij} \right]$, $n \times n$ Fibonacci matrisi olmak üzere

$$f_{ij} = \begin{cases} F_{i-j+1} & , \quad i-j+1 \geq 0 \\ 0 & , \quad i-j+1 \leq 0 \end{cases}$$

şeklinde tanımladı. Bu matrisin yani Fibonacci matrisinin tersi ise

$$F_n^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ -1 & 1 & 0 & 0 & \cdots & 0 \\ -1 & -1 & 1 & 0 & \cdots & 0 \\ 0 & -1 & -1 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & -1 & -1 & 1 \end{bmatrix}$$

olarak verilmiştir.

Teorem 1.1.1.7. k. mertebeden Fibonacci matrisi $F(k)_n = \left[f(k)_{i,j} \right]_n$ olmak üzere $k \geq 2$ için

$$f(k)_{i,j} = \begin{cases} g_{i-j+1} & , \quad i-j+1 \geq 0 \\ 0 & , \quad i-j+1 < 0 \end{cases}$$

olarak tanımlanmıştır. Burada g_n ; (1.13) denklemdeki $g_n = g(k)_{n+k-2}$ 'dir. Bu matrisin tersi ise aşağıdaki gibi verilmiştir:

$$F(k)_n^{-1} = \begin{bmatrix} 1 & 0 & 0 & \cdots & \cdots & \cdots & 0 \\ -1 & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & & & \vdots \\ -1 & \cdots & \ddots & \ddots & \ddots & & \vdots \\ 0 & \ddots & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & -1 & \cdots & -1 & 1 \end{bmatrix}$$

1.1.2 Fibonacci Polinomları

Fibonacci polinomları matematikte büyük önem taşır. Bu büyük polinom sınıfları, Fibonacci sayı dizilerinde verilen indirgeme bağıntısı benzeri bir indirgeme (rekürans) bağıntısı ile tanımlanabilir ve özel değerler ile Fibonacci sayı dizisini vermektedir. Fibonacci polinomları olarak adlandırılan bu tür polinomlar, 1883'te Belçikalı matematikçi Eugene Charles Catalan ve Alman matematikçi E. Jacobsthal tarafından incelenmiş ve çalışmaları sayesinde Fibonacci polinomlarının birçok özelliği literatüre kazandırılmıştır. (Horadam, 1982), (Asci ve Gürel, 2013).

Tanım 1.1.2.1. Catalan tarafından tanımlanan Fibonacci polinomu $f_n(x)$, $f_1(x)=1, f_2(x)=x$ başlangıç koşulları olmak üzere $n \geq 3$ için

$$f_n(x) = xf_{n-1}(x) + f_{n-2}(x) \tag{1.16}$$

rekürans bağıntısı ile tanımlanır. Burada özel olarak $x=1$ alındığında $f_n(1)=F_n$ n. Fibonacci sayısı elde edilir.

Tablo 1.1: Fibonacci Polinomlarının Bazıları

n	Fibonacci Polinomları
1	1
2	x
3	x^2+1
4	x^3+2x
5	x^4+3x^2+1

6	x^5+4x^3+3x
7	$x^6+5x^4+6x^2+1$
⋮	⋮

Tanım 1.1.2.2. Jacobsthal tarafından tanımlanan ve çalışılan Fibonacci polinomu $J_n(x)$ olmak üzere, $J_1(x)=1=J_2(x)$ başlangıç koşulları ve $n\geq 3$ için

$$J_n(x)=J_{n-1}(x)+xJ_{n-2}(x)$$

indirgeme bağıntısı ile tanımlanır.

Teorem 1.1.2.1. $f_n(x)$ Fibonacci polinomu olmak üzere kapalı formülü $n\geq 0$ için

$$f_n(x)=\sum_{j=0}^{\lfloor n-1/2\rfloor}\binom{n-j-1}{j}x^{n-2j-1}$$

şeklinde tanımlanır.

Teorem 1.1.2.2. $f_n(x)$ Fibonacci polinomu olmak üzere

$$Q(x)=\begin{bmatrix} x & 1 \\ 1 & 0 \end{bmatrix} \tag{1.17}$$

ve $n\geq 1$ için

$$Q^n(x)=\begin{bmatrix} f_{n+1}(x) & f_n(x) \\ f_n(x) & f_{n-1}(x) \end{bmatrix} \tag{1.18}$$

elde edilir. $Q^n(x)$ matrisine Fibonacci polinom matrisi olarak adlandırılır.

Teorem 1.1.2.3. $Q^n(x)$ Fibonacci polinom matrisi olsun. Dolayısıyla Fibonacci polinom matrisinin determinantı

$$\left|Q^n(x)\right| = f_{n+1}(x)\,f_{n-1}(x) - f_n^2(x) = (-1)^n$$

olarak bulunur. Fibonacci polinom matrisinin tersi ise

$$\left(Q^n(x)\right)^{-1} = \begin{bmatrix} f_{n-1}(x) & -f_n(x) \\ -f_n(x) & f_{n+1}(x) \end{bmatrix}$$

olarak bulunur.

N. Philippou, C. Georghiou ve G. Philippou tarafından Fibonacci sayı dizisinde yapılmış olan genelleştirmeye benzer bir genelleştirme ile Fibonacci polinomlarını da k. mertebedene taşıdılar.

Tanım 1.1.2.3. $\left\{ f_n^{(k)}(x) \right\}_{n=0}^{\infty}$ k. mertebeden Fibonacci polinomları dizisi olmak üzere $f_0^{(k)}(x) = 0,\ f_1^{(k)}(x) = 1$ başlangıç koşulları için

$$f_n^{(k)}(x) = \begin{cases} \sum_{i=1}^{n} x^{k-i} f_{n-i}^{(k)}(x) & eğer \quad 2 \le n \le k \\ \sum_{i=1}^{k} x^{k-i} f_{n-i}^{(k)}(x) & eğer \quad n \ge k+1 \end{cases}$$

olarak tanımlanır.

Teorem 1.1.2.4. $k \ge 2$ için

$$Q_k(x) = \begin{bmatrix} x^{k-1} & x^{k-2} & x^{k-3} & \cdots & x & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{bmatrix}_{k\times k} \tag{1.19}$$

ve

$$Q_k^n(x)=\begin{bmatrix} F_{n+k-1}^{(k)}(x) & x^{k-2}F_{n+k-2}^{(k)}(x)+x^{k-3}F_{n+k-3}^{(k)}(x)+...+F_n^{(k)}(x) \\ F_{n+k-2}^{(k)}(x) & x^{k-2}F_{n+k-3}^{(k)}(x)+x^{k-3}F_{n+k-4}^{(k)}(x)+...+F_{n-1}^{(k)}(x) \\ \vdots & \vdots \\ F_{n+1}^{(k)}(x) & x^{k-2}F_n^{(k)}(x)+x^{k-3}F_{n+k-3}^{(k)}(x)+...+F_{n-k+2}^{(k)}(x) \\ F_n^{(k)}(x) & x^{k-2}F_{n-1}^{(k)}(x)+x^{k-3}F_{n-2}^{(k)}(x)+...+F_{n-k+1}^{(k)}(x) \end{bmatrix}$$

$$\begin{bmatrix} x^{k-3}F_{n+k-2}^{(k)}(x)+x^{k-4}F_{n+k-3}^{(k)}(x)+...+F_{n+1}^{(k)}(x) & \cdots & F_{n+k-2}^{(k)}(x) \\ x^{k-3}F_{n+k-3}^{(k)}(x)+x^{k-4}F_{n+k-4}^{(k)}(x)+...+F_n^{(k)}(x) & \cdots & F_{n+k-3}^{(k)}(x) \\ \vdots & \ddots & \vdots \\ x^{k-3}F_n^{(k)}(x)+x^{k-4}F_{n-1}^{(k)}(x)+...+F_{n-k+3}^{(k)}(x) & \cdots & F_n^{(k)}(x) \\ x^{k-3}F_{n-1}^{(k)}(x)+x^{k-4}F_{n-2}^{(k)}(x)+...+F_{n-k+2}^{(k)}(x) & \cdots & F_{n+k-1}^{(k)}(x) \end{bmatrix} \quad (1.20)$$

dır. Burada $F_n^{(k)}(x)$ $k.$ mertebeden Fibonacci polinomudur.

2. KRİPTOLOJİ

Bu bölümde, modern kriptolojinin önemli terimlerinden bazılarını tanıtacak ve bazı bilinen algoritmalar hakkında bilgi vereceğiz.

Kriptografi ve şifreleme algoritmaları ile ilgili ayrıntılı bilgiyi Paar ve Pelzl (2010) tarafından yazılan "Understanding Cryptography: A Textbook for Students and Practitioners" adlı kitapta bulunabilir.

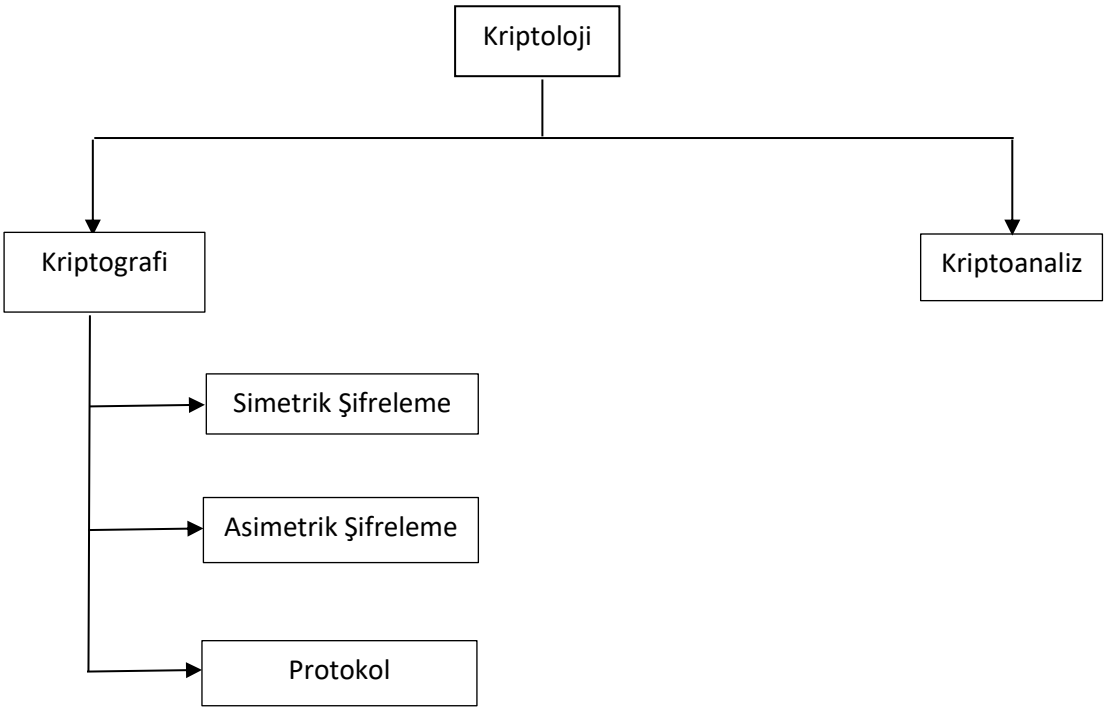
2.1 Kriptolojiye Genel Bakış

Kriptografi kelimesini ilk duyduğumuzda, genelde ilk ilişkilendirmelerimiz e-posta şifreleme, güvenli web sitesi erişimi, bankacılık uygulamaları için akıllı kartlar veya Alman Enigma şifreleme makinesine (Şekil 2.1) karşı ünlü saldırı gibi II. Dünya Savaşının gidişatını değiştiren olaylar dizisi aklımıza gelmektedir.

Şekil 2.1: Alman Enigma Şifreleme Makinası

Kriptografi, modern elektronik iletişiminde önemli yere sahiptir. Buna ek olarak, kriptografi, eski Mısır'da standart dışı "gizli" hiyerogliflerin kullanıldığı M.Ö. 2000 yıllarına dayanan ilk örnekleriyle oldukça eski bir iştir. Mısır günlerinden beri kriptografi, yazılı dili geliştiren kültürlerin çoğunda olmasa da pek çoğunda şu veya bu şekilde kullanılmıştır. Antik Yunanistan'da belgelenmiş gizli yazı vakaları vardır, yani Sparta scytale veya antik Roma'daki ünlü Sezar şifresi kriptografi örneklerinden bazılarıdır. Bu çalışma da daha çok modern kriptografinin terimleri üzerinde durulmuştur.

Kriptografi alanına genel bir bakış Şekil 2.2 de verilmiştir.



Şekil 2.2: Kriptoloji Alanına Genel Bakış

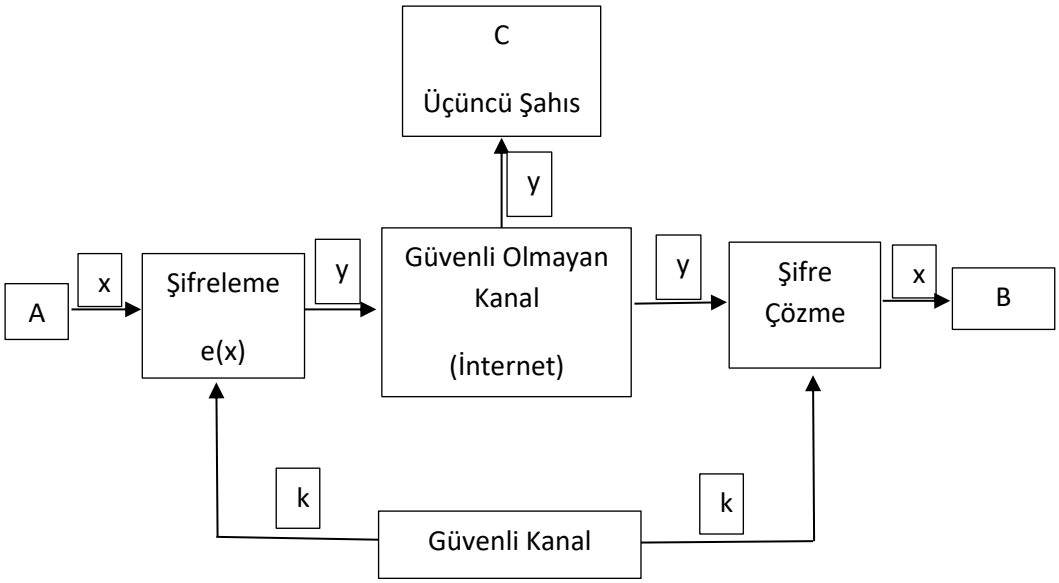
Burada fark ettiğimiz ilk şey, en genel terimin kriptografi değil kriptoloji olduğudur. Kriptoloji iki ana dala ayrılır:

- **Kriptografi;** Bir mesajın anlamını gizlemek amacıyla yapılan gizli yazma bilimidir. İletilen bilginin istenmeyen şahıslar tarafından anlaşılmayacak bir biçime dönüştürülmesinde kullanılan tekniklerin bütünüdür.
- **Kriptoanaliz;** Kriptosistemleri kırma bilimi veya kırma sanatı olarak adlandırabilir. Kriptolojinin, kriptografik sistemlerin şifrelenmiş metinlerini

çözebilmek için bu sistemlerin güvenliklerini inceleyen, zayıf yanlarını bulmaya çalışan dalıdır. Şifre kırmanın istihbarat topluluğu veya belki de organize suçlar için olduğunu ve ciddi bir bilimsel disiplin sınıflandırmasına dahil edilmemesi gerektiğini düşünebilirsiniz. Bununla birlikte, çoğu kriptoanaliz, günümüzde akademide saygın araştırmacılar tarafından yapılmaktadır. Kriptoanaliz, modern şifreleme sistemleri için merkezi bir öneme sahiptir. Kripto yöntemlerimizi kırmaya çalışan insanlar olmadan, gerçekten güvenli olup olmadıkları asla bilinemez.

Kriptoanaliz, bir kriptosistemin güvenli olduğundan emin olmanın tek yolu olduğundan, kriptolojinin ayrılmaz bir parçasıdır. Bununla birlikte; bu tezin odak noktası kriptografidir. Şekil 2.2 ye geri dönüş yaptığımızda kriptografinin kendisi üç ana dala ayrılır:

- **Simetrik Algoritmalar:** Birçok kişinin kriptografiyle ilgili olduğunu varsaydığı şeydir: İki taraf, gizli bir anahtarı paylaştığı bir şifreleme ve şifre çözme yöntemine sahiptir. Antik çağlardan 1976'ya kadar tüm kriptografi, yalnızca simetrik yöntemlere dayanıyordu. Simetrik şifreler, özellikle veri şifreleme ve mesajların bütünlük kontrolü için hala yaygın olarak kullanılmaktadır.



Şekil 2.3: Simetrik Anahtarlı Kriptosistem

- **Asimetrik (Açık Anahtar) Algoritmalar:** 1976 yılında Whitfield Diffie, Martin Hellman ve Ralp Merkle tarafından tamamen farklı bir şifreleme algoritması tanıtıldı. Açık anahtarlı bir şifrelemede, bir kullanıcı simetrik şifrelemede olduğu gibi bir gizli anahtara ama aynı zamanda da bir açık anahtara sahiptir. Asimetrik algoritmalar, dijital imzalar ve anahtar oluşturma gibi uygulamalar için ve ayrıca klasik veri şifreleme için kullanılabilirler.
- **Kriptografik Protokollar:** Kabaca konuşursak, kripto protokolleri kriptografik algoritmaların uygulaması ile ilgilenir. Simetrik ve asimetrik algoritmalar, güvenli internet iletişimi gibi uygulamaların gerçekleştirilebileceği yapı taşları olarak görülebilir. Her web tarayıcısında kullanılan Taşıma Katmanı Güvenliği (TLS) şeması, şifreleme protokolünün bir örneğidir.

Pratik sistemlerdeki kriptografik uygulamaların çoğunda, simetrik ve asimetrik algoritmalar (ve ayrıca genellikle özet fonksiyonları) birlikte kullanılır. Bu, bazen hibrit şemalar olarak anılır. Her iki algoritma ailesini de kullanmanın nedeni, her birinin belirli güçlü ve zayıf yönlerinin olmasıdır. Dolayısıyla birbirlerinin eksik yönlerini tamamlamak için hibrit algoritmalar kullanılmaktadır.

2.2 The Advanced Encryption Standard (AES)

Gelişmiş Şifreleme Standardı (AES), günümüzde en yaygın olarak kullanılan simetrik şifreleme algoritmasıdır. Adındaki “Standart” terimi yalnızca ABD hükümeti uygulamalarına atıfta bulunsa da AES blok şifresi de birçok endüstri standardında zorunludur ve birçok ticari sistemde kullanılmaktadır. AES’ i içeren ticari standartlar arasında internet güvenlik standardı IPsec, TLS, Wi-Fi şifrelemesi standart IEEE 802.11i, güvenlik kabuk ağ protokolü SSH (Secure Shell), internet telefonu Skype ve dünya çapında çok sayıda güvenlik ürünü bu şifreleme algoritmasını kullanmaktadır. Bugüne kadar, AES’ e karşı bilinen Brute-Force (Kaba Kuvvet Saldırısı)’ dan daha iyi bir saldırı yoktur.

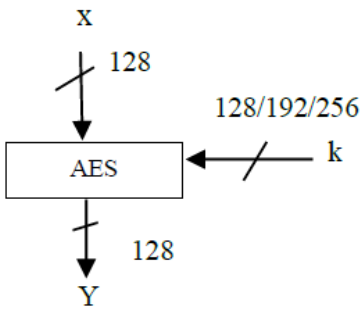
1999’da ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), DES’ in yalnızca eski sistemler için kullanılması gerektiğini ve bunun yerine üçlü Des (3DES) kullanılması gerektiğini belirtti. 3DES, günümüz teknolojisiyle Brute-Force

(Kaba kuvvet saldırısı) saldırılarına dirense de, onunla ilgili çeşitli sorunlar bulundurmaktadır. Bu sorunların ilki, yazılım uygulamaları açısından bu algoritma çok verimli değildir. DES, hali hazırda yazılım için özellikle uygun değildir ve 3DES, DES' ten üç kat daha yavaştır. Diğer bir dezavantajı 64 bitlik nispeten kısa boyutlu bir blok şifrelemesi bulunmaktadır ve bu da bize belirli uygulamalarda bir dezavantajın olduğunu göstermektedir. Son olarak, önümüzdeki yıllarda gelişmiş kuantum bilgisayarlarla yapılan saldırılar konusunda endişe duyulmaktadır. Çünkü yeni kuantum bilgisayarlarında 256 bitlik anahtar uzunlukları kullanılacağı düşünülmektedir. Tüm bu değerlendirmeler, NIST' in DES' in yerine tamamen yeni bir blok şifrelemenin gerekli olduğu sonucuna götürdü.

1997' de NIST, yeni bir Gelişmiş Şifreleme Standardı (AES) için teklif çağrısında bulundu. DES geliştirmesinden farklı olarak, AES için algoritma seçimi, NIST tarafından yönetilen açık bir süreçti. Sonraki 3 AES değerlendirme turunda, NIST ve uluslararası bilim topluluğu, sunulan şifrelerin avantajlarını ve dezavantajlarını tartıştı ve potansiyel adayların sayısını azalttı. 2001' de NIST, Rijndael blok şifresini yeni AES olarak ilan etti ve son bir standart olarak yayınladı (FIPS PUB 197). Bu standart Rijndael algoritması olarak adlandırılmaktadır. Bu algoritma, iki genç Belçikalı kriptograf tarafından tasarlanmıştır.

2.2.1 AES Algoritmasına Genel Bakış

AES şifresi, Rijndael blok şifresiyle neredeyse aynıdır. Rijndael bloğu ve anahtar boyutu 128, 192 ve 256 bit arasında değişir. Fakat, AES standardı yalnızca 128 bitlik bir blok boyutu gerektirir. Bu nedenle, yalnızca 128 bit blok uzunluğuna sahip Rijndael, AES algoritması olarak bilinir. Bu bölümün geri kalanında, yalnızca 128 bitlik blok uzunluğuna sahip standart Rijndael sürümü üzerinden işlem yapacağız.



Şekil 2.4: AES Giriş-Çıkış Parametreleri

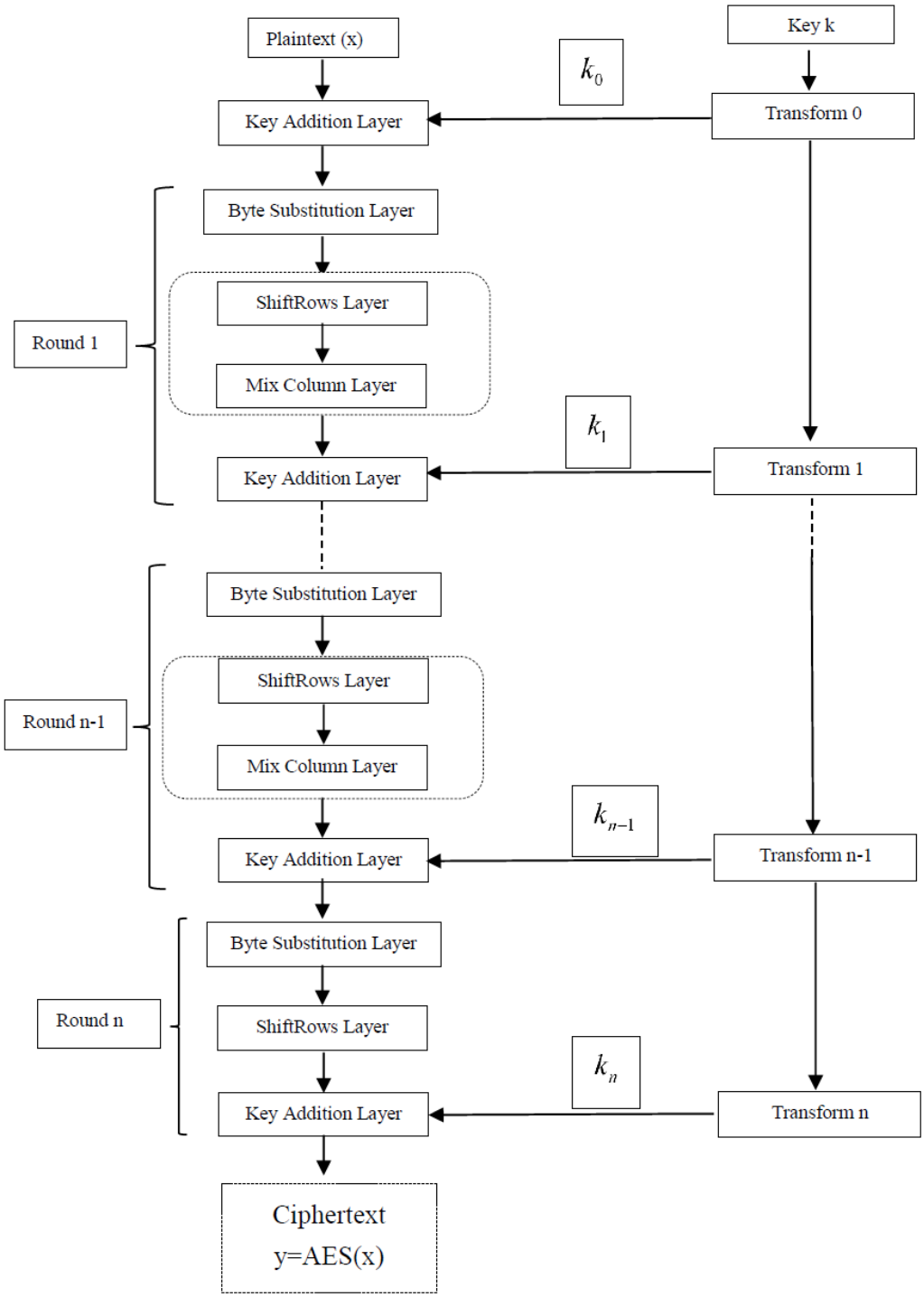
Daha önce belirtildiği gibi, bu bir NIST tasarım gereksinimi olduğundan Rijndael tarafından üç anahtar uzunluğu desteklenmelidir. Şifrenin dahili tur sayısı, Tablo 2.2' e göre anahtar uzunluğunun bir fonksiyonudur.

Tablo 2.2: AES için anahtar uzunlukları ve tur sayısı

Anahtar Uzunluğu	Tur Sayısı
128 bit	10
192 bit	12
256 bit	14

DES' in aksine AES, Feistel yapısına sahip değildir. Feistel ağları, her iterasyon için bir bloğun tamamını şifrelemez. Buna örnek olarak DES' te $\frac{64}{2} = 32$ bit bir turda şifrelenir. AES ise 128 bitin tamamını bir yineleme de şifreler. Bu ise, nispeten daha az sayıda tura sahip olmasının nedenidir.

AES, sözde katmanlardan oluşur. Her katman, veri yolunun tüm 128 bitini yönetir. Veri yolu, algoritmanın durumu olarak da adlandırılır. Yalnızca üç katman türü vardır. Birincisi hariç her tur, Şekil 2.5' de gösterildiği gibi üç katmandan oluşur: Düz metin x, şifreli metin y ve tur sayısı n olarak gösterilir. Ayrıca, son tur yani n. tur şifreleme ve şifre çözme şemasını simetrik yapan MixColoumn dönüşümünü kullanmaz.



Şekil 2.5: AES Şifreleme Blok Şeması

Katmanların kısa bir açıklamasını aşağıda görebiliriz:

Anahtar ekleme katmanı (Key Addition Layer); anahtar programında ana anahtardan türetilen 128 bitlik bir yuvarlak anahtar veya alt anahtar duruma XOR' lanır.

Bayt değiştirme katmanı (Byte Substitution Layer) (S-Box); Durumun her öğesi, özel matematiksel özelliklere sahip arama tabloları kullanılarak doğrusal olmayan bir şekilde dönüştürülür. Bu, verilerde karışıklık yaratır, yani, bireysel durum bitlerindeki değişikliklerin veri yolu boyunca hızlı bir şekilde yayılmasını sağlar.

Difüzyon katmanı (Diffusion Layer); tüm durum bitleri üzerinde difüzyon sağlar. Her ikisi de doğrusal işlemler gerçekleştiren iki alt katmandan oluşur:

- ShiftRows katmanı, verilere bayt düzeyinde izin verir.
- MixCloumn katmanı, dört baytlık blokları birleştiren (karıştıran) bir matris işlemidir.

DES' e benzer şekilde, anahtar zamanlama, orijinal AES anahtarından yuvarlak anahtarları veya alt anahtarları $(k_0, k_1, ..., k_n)$ hesaplar.

Bölümdeki katmanların iç fonksiyonlarını tanımlamadan önce Galois cismi olarak adlandırılan yeni bir matematiksel kavram tanıtmalıyız. AES katmanları içindeki tüm işlemler için Galois cismi hesaplamaları gereklidir.

2.2.2 Sonlu Cisimlerin Varlığı

AES' de Galois cisim aritmetiği çoğu katmanda, özellikle S-Box ve MixColumn katmanında kullanılır. Bu nedenle, AES' in içindekileri daha derinden anlamak için algoritmaya devam etmeden önce bu amaç için gerekli olan Galois cismine özet bir şekilde değineceğiz.

Galois cismi olarak da adlandırılan sonlu bir cisim, sonlu sayıda eleman içeren bir kümedir. Özetleyecek olursak, Bir Galois cismi, toplayabileceğimiz, çıkarabileceğimiz, çarpabileceğimiz ve tersini alabileceğimiz sonlu elemana sahip bir kümedir. Galois cisminin tanımını vermeden önce daha basit bir cebirsel yapı olan grup kavramına ihtiyacımız vardır.

Tanım 2.2.2.1. *Grup*

G boş olmayan bir küme ve bu küme üzerinde bir ikili işlem "$\circ$" olsun. Buna göre eğer aşağıdaki şartlar sağlanırsa $(G,\circ)$ cebirsel yapısına bir grup denir. (Tasci, 2018)

1. G kümesi "$\circ$" işlemine göre kapalıdır. Yani $\forall a,b \in G$ için $a \circ b \in G$ dir.
2. G kümesi "$\circ$" işlemi üzerinde birleşme özelliğine sahiptir. Yani $\forall a,b,c \in G$ için $(a \circ b) \circ c = a \circ (b \circ c)$ dir.
3. "$\circ$" işleminin birim elemanı vardır. Yani $\forall a \in G$ için $a \circ e = e \circ a = a$ olacak şekilde $e \in G$ vardır.
4. "$\circ$" işlemine göre G kümesinde her elemanın tersi vardır. Yani, $\forall a \in G$ için $a \circ a^{-1} = a^{-1} \circ a = e$ olacak şekilde $a^{-1} \in G$ vardır.

Eğer $\forall a,b \in G$ için $a \circ b = b \circ a$ sağlanıyorsa G grubu değişmelidir (abelyandır) denir.

Örnek 2.2.2.1. $\mathbb{Z}$ tamsayılar kümesinde çarpma işlemine göre her elemanın tersi olmadığından çarpma işlemine göre grup değildir. Fakat $\mathbb{Z}$ tamsayılar kümesi toplama işlemine göre bir gruptur.

Tanım 2.2.2.2. *Halka*

G boştan farklı bir küme ve G üzerinde tanımlı "$\circ$" ve "$*$" birer ikili işlem olsun. Eğer aşağıdaki şartlar sağlanıyorsa $(G,\circ,*)$ cebirsel yapısına halka denir.

1. $(G,\circ)$ cebirsel yapısı değişmeli bir grup olmalıdır.

2. G kümesi "*" işlemine göre kapalıdır. Yani, $\forall a,b \in G$ için $a*b \in G$ dir.
3. G kümesi "*" işlemi üzerinde birleşme özelliğine sahiptir. Yani, $\forall a,b,c \in G$ için $(a*b)*c = a*(b*c)$ dir.
4. "*" işleminin "$\circ$" işlemi üzerinde soldan ve sağdan dağılma özelliğine sahiptir. Yani $\forall a,b,c \in G$ için $a*(b \circ c) = (a*b) \circ (a*c)$ ve $(b \circ c)*a = (b*a) \circ (c*a)$ dir.

Eğer $\forall a,b \in G$ için $a*b = b*a$ sağlanıyorsa G halkası değişmelidir denir.

Eğer $\forall a \in G$ için $a*e' = e'*a = a$ olacak şekilde bir $e' \in G$ var ise G halkası birimlidir denir.

Örnek 2.2.2.3. Bilinen toplama ve çarpma işlemleri üzerinde tanımlı $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ve $\mathbb{C}$ kümeleri birer halkadır.

Tanım 2.2.2.3. *Cisim*

Birimli ve değişmeli bir halkanın sıfırdan farklı her elemanının "*" işlemine göre bir tersi varsa o zaman bu halkaya cisim denir ve genel olarak F ile gösterilir.

Not 2.2.2.1. Bir cismi aşağıdaki gibi tanımlamak da mümkündür. $(F,+,.)$ halkasına $(F \setminus \{0\},.)$ değişmeli bir grup olmak şartıyla bir cisim denir. Yani $(F,+)$ toplamaya göre değişmeli bir grup ve $(F \setminus \{0\},.)$ çarpmaya göre bir değişmeli grup ise o taktirde $(F,+,.)$ cebirsel yapısına cisim denir.

Sonlu cisim olarak ta bilinen Evarista Galois'in adını taşıyan Galois cismi, içinde sonlu sayıda öğenin bulunduğu bir cismi ifade eder. İkili formlarda temsil edildikleri için bilgisayar verilerinin çevrilmesinde özellikle yararlıdır. Yani bilgisayar verileri, eleman sayısı iki olan Galois cismindeki bileşenler olan 0 ve 1 sayılarının birleşiminden oluşur. Verileri bir Galois cisminde bir vektör olarak temsil etmek, matematiksel işlemlerin verileri kolay ve etkili bir şekilde karıştırmasını sağlar.

Tanım 2.2.2.4. *Galois Cismi*

$p \in \mathbb{P}$ ve $n \in \mathbb{Z}^+$ olmak üzere $GF\left(p^n\right)$ Galois cismi

$$GF\left(p^n\right) = (0,1,2,...,p-1) \cup (p, p+1, p+2,..., p+p-1) \cup$$
$$\left(p^2, p^2+1, p^2+2,..., p^2+p-1\right) \cup ... \cup$$
$$\left(p^{n-1}, p^{n-1}+1, p^{n-1}+2,..., p^{n-1}+p-1\right)$$

olarak tanımlanır.

Kriptografide, hemen hemen her zaman, sonlu cisimler veya Galois cisimleri dediğimiz, elemanları sonlu sayıda olan cisimlerle ilgileniriz. Sonlu cismin eleman sayısı cismin mertebesi veya kardinalitesi (karakteristiği) olarak adlandırılır. Kriptoloji için temel öneme sahip teorem aşağıdaki gibidir:

Teorem 2.2.2.1. Her p asal sayısı ve her $n \in \mathbb{N}$ için $m = p^n$ mertebeli bir sonlu cisim vardır.

Bu teoreme göre şu örnekleri verebiliriz: 11 elemanlı sonlu bir cisim $11^1 = 11$ dir. 81 elemanlı sonlu bir cisim $3^4 = 81$ şeklinde yazabiliriz veya $2^8 = 256$ elemanlı sonlu bir cisim vardır. Fakat $12 = 2^2.3$ olarak yazıldığından 12 elemanlı sonlu bir cisim yoktur.

2.2.3 Asal Cisimler

Sonlu cisimlerin en sezgisel örnekleri, asal dereceli cisimlerdir. Yani, $n = 1$ dir. $GF(p)$ cisminin elemanları $0,1,...,p-1$ ' dir. Cismin iki işlemi tamsayılarda $\bmod p$ ye göre toplama ve çarpmadır.

Teorem 2.2.3.1. p asal sayı olsun. $\mathbb{Z}_p$ tamsayı halkası, $GF(p)$ olarak gösterilir ve asal cisim veya asal sayıda eleman içeren bir Galois cismi diye

adlandırılır. $GF(p)$ Galois cisminde sıfır olmayan tüm elemanların tersi vardır ve $GF(p)$ deki işlemler (aritmetik) mod p ye göre yapılır.

Örnek 2.2.3.1. $GF(5)$ sonlu cismini ele alalım. $GF(5)=\{0,1,2,3,4\}$ Galois cisminin elemanlarını ele alalım.

Tablo 2.3: Toplama İşlemi

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Tablo 2.4: Çarpma İşlemi

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Var olan en küçük sonlu cisim $GF(2)$ Galois cismidir.

Örnek 2.2.3.2. $GF(2)=\{0,1\}$ Galois cismini ele alalım

Tablo 2.5: Toplama İşlemi

+	0	1
0	0	1
1	1	0

Tablo 2.6: Çarpma İşlemi

×	0	1
0	0	0
1	0	1

AES şifreleme algoritmasında XOR' lama işlemi $\mathrm{mod}\,2$ ' ye göre toplama işlemine karşılık gelmektedir. AND işlemi ise $GF(2)$ üzerindeki çarpma işlemine karşılık gelmektedir.

2.2.4 Cisim Genişlemeleri $GF(2^m)$

AES şifreleme algoritmasında kullanılan sonlu cisim 256 eleman içerir ve $GF(2^8)$ olarak gösterilir. 256 elemanlı bir cisim seçilmesi her elemanın bir byte (1 byte) karşılık gelmesinden dolayıdır. AES şifreleme algoritmalarının içinde olan S-Box ve MixColumn dönüşümleri için her bir eleman yani her bir byte $GF(2^8)$ Galois cisminin bir elemanı olarak alınır ve işlemler bu cisim üzerinde yapılır.

Fakat sonlu bir cismin mertebesi (derecesi) asal değil ise (2^8 'in derecesi 8 asal olmadığından) toplama ve çarpma işlemleri $\mathrm{mod}\left(2^8\right)$ üzerinde toplama ve çarpma işlemleri olarak gösterilemez. Dolayısıyla $m>1$ şeklindeki cisimlere cisim genişlemeleri denir. Dolayısıyla burada farklı notasyonlara ve işlemlere ihtiyaç duyulmaktadır. Bir sonraki bölümde cisim genişlemelerinin elemanlarının polinom olarak temsil edilebileceğini ve cisim genişlemesindeki işlemlerin polinomlar üzerinden gösterilebileceğini göreceğiz. $GF(2^m)$ cisim genişlemesindeki elemanları tamsayılar olarak değil katsayıları $GF(2)$ de olan polinomlar olarak temsil edeceğiz. Polinomların maksimum derecesi $m-1$ 'dir ve toplamda m katsayı vardır. AES' te kullanılan $GF(2^8)$ cisminde, her bir $A \in GF\left(2^8\right)$ elemanını aşağıdaki gibi temsil edebiliriz:

$$A(x) = a_7 x^7 + \ldots + a_1 x + a_0, \quad a_i \in GF\left(2\right) = \{0,1\}.$$

Dolayısıyla $GF\left(2^8\right)$ cisminde $2^8 = 256$ adet polinom olduğunu görebiliriz. Yani bu şifreleme algoritmasında her bir polinomun dijital biçimde 8 bitlik bir vektör olarak basitçe saklanabileceğini gözlemleyebiliriz.

$$A = \left(a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0\right).$$

2.2.5 $GF(2^m)$ Galois Cisminde Toplama ve Çıkarma

Şimdi cisim genişlemelerinde toplama ve çıkarma işlemlerine bakalım. Anahtar ekleme katmanında (key addition layer) AES şifreleme algoritmasında toplama işlemi kullanılır. Yani bu katmandaki işlemler polinomlar üzerinde standart toplama ve çıkarma işlemidir ve kolayca yapılabilir. Şimdi bu işlemlere bir göz atalım:

Tanım 2.2.5.1. $A(x), B(x) \in GF\left(2^m\right)$ olsun.

$$C(x) = A(x) + B(x) = \sum_{i=0}^{m-1} c_i x^i, \quad c_i = a_i + b_i \mod(2)$$

$$C(x) = A(x) - B(x) = \sum_{i=0}^{m-1} c_i x^i, \quad c_i = a_i - b_i \equiv a_i + b_i \mod(2)$$

Örnek 2.2.5.1. AES şifreleme algoritmasında kullanılan $GF\left(2^8\right)$ Galois cismi üzerinde tanımlı bir örneği ele alalım:

$A(x) = x^7 + x^6 + x^4 + 1 \in GF\left(2^8\right)$ ve $B(x) = x^4 + x^2 + 1 \in GF\left(2^8\right)$ olsun. Dolayısıyla $C(x) = A(x) + B(x) = x^7 + x^6 + x^2$ olarak bulunur.

2.2.6 $GF(2^m)$ Galois Cisminde Çarpma

$GF\left(2^8\right)$ Galois cisminde çarpma işlemi, AES' in MixColumn dönüşümünün temel işlemidir. İlk adımda $GF\left(2^m\right)$ sonlu cismi üzerinde alınan iki eleman (polinom) standart polinom çarpma kuralı kullanılarak çarpılır:

$$A(x).B(x)=\left(a_{m-1}x^{m-1}+...+a_0\right).\left(b_{m-1}x^{m-1}+...+b_0\right)$$

$$c'_0 = a_0 b_0 \mod 2$$

$$c'_1 = a_0 b_1 + a_1 b_0 \mod 2$$

$$\vdots$$

$$c'_{2m-2} = a_{m-1} b_{m-1} \mod 2$$

olmak üzere

$$C'(x)=c'_{2m-2}x^{2m-2}+...+c'_0$$

elde ederiz. Burada tüm a_i, b_i ve c_i katsayılarının $GF\left(2\right)$ Galois cisminin elemanları olduğu ve işlemlerin $GF\left(2\right)$ de gerçekleştiğini görebiliriz. Dolayısıyla, burada $C\left(x\right)$ polinomunun derecesinin $m-1$' den daha yüksek bir dereceye sahip olduğu görülür. Bundan dolayı bu polinomun indirgenmesi gerekir. Buradaki temel fikir, asal cisimlerde çarpma durumuna benzer bir yaklaşımdır: $GF\left(p\right)$' de iki tamsayıyı çarpar, sonucu bir asal sayıya böler ve yalnızca kalanını dikkate alırız. Cisim genişlemelerinde de yaptığımız şey şudur: Çarpmanın ürünü belirli bir polinoma bölünür ve biz sadece polinom bölünmesinden sonra kalanını ele alırız. Bundan dolayı modül indirgemesi için indirgenemez polinomlara ihtiyacımız vardır. Şimdi indirgenemez polinomunun tanımına bakalım:

Tanım 2.2.6.1. $A(x), B(x) \in GF\left(2^m\right)$ ve $P(x) \equiv \sum_{i=0}^{m} p_i x_i$, $p_i \in GF(2)$ indirgenemez bir polinom olsun. Dolayısıyla, $C(x) \equiv A(x).B(x) \mod P(x)$ ' dir.

Dolayısyla, her $GF\left(2^m\right)$ cismi, $GF(2)$ ' den katsayılarla m derecesinde indirgenemez bir $P(x)$ polinomu gerektirir. Fakat burada dikkat etmemiz gereken şey tüm polinomların indirgenemez olmadığıdır. Örneğin; x^4+x^3+x+1 polinomu indirgenebilirdir. Çünkü $x^4+x^3+x+1=\left(x^2+x+1\right)\left(x^2+1\right)$ şeklinde yazabiliriz. Dolayısıyla $GF\left(2^4\right)$ cisim genişletmesini oluşturmak için kullanamayız. İlkel polinomlar özel bir indirgenemez polinom türü olduğundan, şekil 2.6' daki polinomlar $GF\left(2^m\right)$ cisim genişlemelerini oluşturmak için kullanılabilir.

(0,1,2)	(0,1,3,4,24)	(0,1,46)	(0,1,5,7,68)	(0,2,3,5,90)	(0,3,4,5,112)
(0,1,3)	(0,3,25)	(0,5,47)	(0,2,5,6,69)	(0,1,5,8,91)	(0,2,3,5,113)
(0,1,4)	(0,1,3,4,26)	(0,2,3,5,48)	(0,1,3,5,70)	(0,2,5,6,92)	(0,2,3,5,114)
(0,2,5)	(0,1,2,5,27)	(0,4,5,6,49)	(0,1,3,5,71)	(0,2,93)	(0,5,7,8,115)
(0,1,6)	(0,1,28)	(0,2,3,4,50)	(0,3,9,10,72)	(0,1,5,6,94)	(0,1,2,4,116)
(0,1,7)	(0,2,29)	(0,1,3,6,51)	(0,2,3,4,73)	(0,11,95)	(0,1,2,5,117)
(0,1,3,4,8)	(0,1,30)	(0,3,52)	(0,1,2,6,74)	(0,6,9,10,96)	(0,2,5,6,118)
(0,1,9)	(0,3,31)	(0,1,2,6,53)	(0,1,3,6,75)	(0,6,97)	(0,8,119)
(0,3,10)	(0,2,3,7,32)	(0,3,6,8,54)	(0,2,4,5,76)	(0,3,4,7,98)	(0,1,3,4,120)
(0,2,11)	(0,1,3,6,33)	(0,1,2,6,55)	(0,2,5,6,77)	(0,1,3,6,99)	(0,1,5,8,121)
(0,3,12)	(0,1,3,4,34)	(0,2,4,7,56)	(0,1,2,7,78)	(0,2,5,6,100)	(0,1,2,6,122)
(0,1,3,4,13)	(0,2,35)	(0,4,57)	(0,2,3,4,79)	(0,1,6,7,101)	(0,2,123)
(0,5,14)	(0,2,4,5,36)	(0,1,5,6,58)	(0,2,4,9,80)	(0,3,5,6,102)	(0,37,124)
(0,1,15)	(0,1,4,6,37)	(0,2,4,7,59)	(0,4,81)	(0,9,103)	(0,5,6,7,125)
(0,1,3,5,16)	(0,1,5,6,38)	(0,1,60)	(0,4,6,9,82)	(0,1,3,4,104)	(0,2,4,7,126)
(0,3,17)	(0,4,39)	(0,1,2,5,61)	(0,2,4,7,83)	(0,4,105)	(0,1,127)
(0,3,18)	(0,3,4,5,40)	(0,3,5,6,62)	(0,5,84)	(0,1,5,6,106)	(0,1,2,7,128)
(0,1,2,5,19)	(0,3,41)	(0,1,63)	(0,1,2,8,85)	(0,4,7,9,107)	
(0,3,20)	(0,1,2,5,42)	(0,1,3,4,64)	(0,2,5,6,86)	(0,1,4,6,108)	
(0,2,21)	(0,3,4,6,43)	(0,1,3,4,65)	(0,1,5,7,87)	(0,2,4,5,109)	
(0,1,22)	(0,5,44)	(0,3,66)	(0,8,9,11,88)	(0,1,4,6,110)	
(0,5,23)	(0,1,3,4,45)	(0,1,2,5,67)	(0,3,5,6,89)	(0,2,4,7,111)	

Şekil 2.6: İlkel Polinomlardan Bazıları

AES şifreleme algoritması indirgenemez polinom olarak

$$P(x) = x^8 + x^4 + x^3 + x + 1$$

polinomunu kullanır. AES spesifikasyonunun bir parçasıdır.

Örnek 2.2.6.1. $GF\left(2^4\right)$ cisminde $A(x)=x^3+x^2+1$ ve $B(x)=x^2+x$ iki polinomu çarpalım. Galois cisminin indirgenemez polinomu

$$P(x)=x^4+x+1$$

olarak verilsin. Dolayısıyla,

$$C'(x)=A(x).B(x)=x^5+x^3+x^2+x$$

olarak bulunur. Klasik polinom bölme yöntemini kullanarak $C'(x)$ 'i indirgeyebiliriz.

$$x^4=1.P(x)+(x+1)$$

$$x^4\equiv x+1 \mod P(x)$$

$$x^5\equiv x^2+x \mod P(x)$$

Şimdi, yalnızca x^5 için indirgenmiş ifadeyi $C'(x)$ ara sonucuna eklememiz gerekiyor:

$$C(x)\equiv x^5+x^3+x^2+x \mod P(x)$$

$$C(x)\equiv\left(x^2+x\right)+\left(x^3+x^2+x\right)=x^3$$

$$A(x).B(x)\equiv x^3.$$

Özellikle Galois cisimlerinin yazılım uygulamalarıyla ilgileniyorsak $GF\left(2^m\right)$ 'de çarpma ile tamsayı çarpmasını karıştırmamak önemlidir. Polinomların, yani cisim elemanlarının normalde bilgisayarlarda bit vektörleri olarak depolandığını hatırlayalım. Bir önceki örnekteki çarpma işlemine bakacak olursak, bit düzeyinde şu çok alışılmamış işlem yapılıyor:

$$A.B=C$$

$$\left(x^3+x^2+1\right).\left(x^2+x\right)=x^3$$

$$(1101).(0110)=(1000)$$

Bu hesaplama tamsayı aritmetiği ile aynı değildir. Polinomlar tamsayılar olarak yorumlanırsa, yani $(1101)_2=13_{10}$ ve $(0110)_2=6_{10}$, sonuç $(1001110)_2=78_{10}$ olurdu ve buradan açıkça görülür ki Galois cismi üzerindeki çarpma işlemi ile aynı değildir. Bu nedenle, cisim öğelerini tamsayı verileri olarak görebilsekte türler, sağlanan tamsayı aritmetiğini kullanamayız.

2.2.7 $GF(2^m)$ Galois Cisminde Ters Alma

$GF\left(2^8\right)$ Galois cisminde ters alma, AES şifreleme algoritmasında S-Box' ları içeren Byte değiştirme (Byte Substitution) dönüşümünün temel işlemidir. $GF\left(2^m\right)$ sonlu bir cisim ve bu sonlu cisimde indirgenemez polinom $P(x)$ olmak üzere $A\in GF\left(2^m\right)$ sıfırdan farklı eleman için A' nın tersi A^{-1} şu şekilde tanımlanır:

$$A^{-1}(x).A(x)=1 \mod P(x)$$

Küçük cisimler için (pratikte bu genellikle 2^{16} veya daha az elemanlı cisimler için anlamına gelir) tüm cisim elemanlarının önceden hesaplanmış tersini içeren arama tabloları sıklıkla kullanılır. Şekil 2.7'de AES' in S-Box' ında kullanılan değerleri göstermektedir.

		Y														
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
	0	00	01	8D	F6	CB	52	7B	D1	E8	4F	29	C0	B0	E1	E5	C7
	1	74	B4	AA	4B	99	2B	60	5F	58	3F	FD	CC	FF	40	EE	B2
	2	3A	6E	5A	F1	55	4D	A8	C9	C1	0A	98	15	30	44	A2	C2
	3	2C	45	92	6C	F3	39	66	42	F2	35	20	6F	77	BB	59	19
	4	1D	FE	37	67	2D	31	F5	69	A7	64	AB	13	54	25	E9	09
	5	ED	5C	05	CA	4C	24	87	BF	18	3E	22	F0	51	EC	61	17
	6	16	5E	AF	D3	49	A6	36	43	F4	47	91	DF	33	93	21	3B
	7	79	B7	97	85	10	B5	BA	3C	B6	70	D0	06	A1	FA	81	82
X	8	83	7E	7F	80	96	73	BE	56	9B	9E	95	D9	F7	02	B9	A4
	9	DE	6A	32	6D	D8	8A	84	72	2A	14	9F	88	F9	DC	89	9A
	A	FB	7C	2E	C3	8F	B8	65	48	26	C8	12	4A	CE	E7	D2	62
	B	0C	E0	1F	EF	11	75	78	71	A5	8E	76	3D	BD	BC	86	57
	C	0B	28	2F	A3	DA	D4	E4	0F	A9	27	53	04	1B	FC	AC	E6
	D	7A	07	AE	63	C5	DB	E2	EA	94	8B	C4	D5	9D	F8	90	6B
	E	B1	0D	D6	EB	C6	0E	CF	AD	08	4E	D7	E3	5D	50	1E	B3
	F	5B	23	38	34	68	46	03	8C	DD	9C	7D	A0	CD	1A	41	1C

Şekil 2.7:AES S-Box içinde kullanılan xy byte' ları için çarpımsal ters tablo

Yukarıdaki tablo $GF\left(2^8\right)$ Galois cismindeki $\bmod P(x)=x^8+x^4+x^3+x+1$ içindeki tüm tersleri gösterir. Burada özel bir durum söz konusudur: "0" elemanın tersi olmadığından "0" elemanı cismin giriş öğesidir. Fakat AES S-Box için olası her giriş için tanımlanmış bir ikame tablosuna ihtiyaç vardır. Bu nedenle, tasarımcılar S-Box' ı giriş değeri "0" ile çıkış değeri "0" ile eşleşecek şekilde tanımladılar.

Örnek 2.2.7.1. Şekil 2.7' den

$$x^7+x^6+x=\left(11000010\right)_2=\left(C2\right)_{hex}=\left(xy\right)$$

polinomunun tersi C satırı 2. Sütundaki eleman tarafından verilir.

$$\left(2F\right)_{hex}=\left(00101111\right)_2=x^5+x^3+x^2+x+1$$

Bu işlemin sağlamasını şu çarpma ile doğrulayabiliriz:

$$\left(x^7+x^6+x\right).\left(x^5+x^3+x^2+x+1\right)\equiv 1 \mod P(x).$$

AES şifreleme algoritması ile ilgili daha fazla ayrıntıyı ve tüm katmanlar ile ilgili işlemleri Paar ve Pelzl (2010) tarafından yazılan “Understanding Cryptography: A Textbook for Students and Practitioners” adlı kitapta bulunabilir.

Dişkaya, Avaroğlu ve Menken (2020) AES benzeri şiflemeyi 2×2 tipinde blok matrisler üzerinden yeniden tanımladı. Bu tezin bir sonraki bölümünde Dişkaya, Avaroğlu ve Manken (2020) de 2×2 tipindeki Fibonacci blok matrisleri ile tanımlamış oldukları şifreleme algoritmasını yeniden tanımlandı ve $k\times k$ tipindeki matrislere genelleştirerek Advanced Encryption Standard (AES) benzeri bir şifreleme algoritması tanımlandı ve bu metot ile ilgili örneklere yer verildi.

3. K. MERTEBEDEN FİBONACCİ POLİNOMLARI İÇİN AES BENZERİ KRİPTOLOJİ

Bu bölümde indirgenemez polinomları kullanarak k. mertebeden Fibonacci polinomlarının elemanları yeniden tanımlandı. $GF\left(2^m\right)$ Galois cisminin elemanları sadece tamsayılardan oluşmamaktadır. Bu Galois cismi tamsayılarla birlikte polinomları da içermektedir. Bu çalışma boyunca $m=5$ seçilerek $GF\left(2^5\right)$ Galois cismi üzerinde çalışılmıştır. $GF\left(2^5\right)$ 32 eleman içeren Galois cismi üzerinde AES benzeri şifrelememizi yapılmıştır. Bu polinomların her bir öğesi, alfabemizdeki her bir harfe karşılık gelmektedir.

$GF\left(2^5\right)$ Galois cisminde tanımlı indirgenemez polinomlar şöyledir:

$$x^5+x^2+1$$

$$x^5+x^3+1$$

$$x^5+x^3+x^2+x+1$$

$$x^5+x^4+x^3+x+1$$

$$x^5+x^4+x^3+x^2+1$$

$$x^5+x^4+x^2+x+1$$

AES şifreleme algoritması da bir önceki bölümde verilmiş olan indirgenemez polinomlar üzerinde çalışmaktadır. AES şifreleme sisteminde kullanılan indirgenemez polinom

$$P\left(x\right)=x^8+x^4+x^3+x+1$$

olarak verilmiştir. Bu çalışma boyunca indirgenemez polinom olarak

$$P(x) = x^5 + x^2 + 1$$

Polinomu kullanılmıştır. $GF(2^5)$ Galois cisminde farklı indirgenemez polinomlar seçilerek farklı şifreleme algoritmaları elde edilebilir.

Daha sonra kullanılmak üzere ilk birkaç Fibonacci polinomu aşağıdaki Tablo 3.7' de gösterilmiştir:

Tablo 3.7: İlk Birkaç Fibonacci Polinomu

n	0	1	2	3	4	5	⋯
$f_n(x)$	0	1	x	x^2+1	x^3+2x	x^4+3x^2+1	⋯

İleri de kullanmak üzere indirgenemez Fibonacci polinomlarını Tablo 3.8' de gösterilmiştir:

Tablo 3.8: İndirgenemez Fibonacci polinomları

n	$f_n(x)$	Z_2
0	0	$\bmod 2$
1	1	$\bmod 2$
2	x	$\bmod 2$
3	x^2+1	$\bmod 2$
4	x^3	$\bmod 2$
5	x^4+x^2+1	$\bmod 2$
6	x^2+x+1	$\bmod 2$
7	x^4+x^3+x+1	$\bmod 2$
8	x^4+x^2	$\bmod 2$
9	x^4+x^2+x	$\bmod 2$
⋮	⋮	⋮

$GF(2^5)$ Galois cismi üzerinde tanımlı polinomlar Tablo 3.9' de gösterilmiştir ve bunların alfabe tablosundaki karşılıkları verilmiştir.

Tablo 3.9: Galois cismi üzerinde tanımlı polinomlar ve alfabe tablosu

No	Bit	Polinom	Alfabe
0	00000	0	A
1	00001	1	B
2	00010	x	C
3	00011	$x+1$	Ç
4	00100	x^2	D
5	00101	x^2+1	E
6	00110	x^2+x	F
7	00111	x^2+x+1	G
8	01000	x^3	Ğ
9	01001	x^3+1	H
10	01010	x^3+x	I
11	01011	x^3+x+1	İ
12	01100	x^3+x^2	J
13	01101	x^3+x^2+1	K
14	01110	x^3+x^2+x	L
15	01111	x^3+x^2+x+1	M
16	10000	x^4	N
17	10001	x^4+1	O
18	10010	x^4+x	Ö
19	10011	x^4+x+1	P
20	10100	x^4+x^2	R
21	10101	x^4+x^2+1	S
22	10110	x^4+x^2+x	Ş
23	10111	x^4+x^2+x+1	T
24	11000	x^4+x^3	U
25	11001	x^4+x^3+1	Ü

26	11010	$x^4 + x^3 + x$	V
27	11011	$x^4 + x^3 + x + 1$	W
28	11100	$x^4 + x^3 + x^2$	X
29	11101	$x^4 + x^3 + x^2 + 1$	Y
30	11110	$x^4 + x^3 + x^2 + x$	Z
31	11111	$x^4 + x^3 + x^2 + x + 1$	Q

Verilmiş olan ön bilgiler doğrultusunda şifreleme algoritması aşağıdaki gibi oluşturulmuştur:

3.1 Kodlama Algoritması

- **Adım 1:** n uzunluğundaki mesaj metnini ele alalım. Burada seçilen her harf bir uzunluğu temsil etmektedir.
- **Adım 2:** Keyfi k ve n değerleri seçilir. Seçilen bu keyfi k değeri hangi mertebeden Fibonacci polinomlarının kullanılacağını belirleyecektir.
- **Adım 3:** Seçilen k ve n değerlerine göre (1.20) denkleminden $Q_k^n(x)$ matrisi oluşturulur.
- **Adım 4:** Mesaj metni seçilen k değerine göre bloklara ayrılır. Dolayısıyla $k \times 1$ tipinde blok matrisler elde edilir. $Q_k^n(x)$ matrisi ile $k \times 1$ tipindeki matris çarpılarak yeni bir matris elde edilir. Bu matris alfabe tablosuna göre doldurarak ilk katmandaki yeni şifreli mesaj elde edilmiş olur.
- **Adım 5:** 4. Adımda elde edilmiş olan mesaj matrisi ile 1. anahtar matrisi çarpılır:

$$1.\,Anahtar\ Matrisi = \begin{bmatrix} B & B & C \\ Ç & E & Ğ \\ K & E & Y \end{bmatrix} = \begin{bmatrix} 1 & 1 & 2 \\ 3 & 5 & 8 \\ 13 & 5 & 29 \end{bmatrix}$$

Eğer mesaj metninde artan 2 karakter varsa bu elde edilen mesaj matrisi de 2. anahtar matrisi ile çarpılır:

$$2.\,Anahtar\ Matrisi = \begin{bmatrix} E & A \\ O & D \end{bmatrix} = \begin{bmatrix} 5 & 0 \\ 17 & 4 \end{bmatrix}$$

- **Adım 6:** 5. Adımda elde edilen mesaj metni k. mertebeden Fibonacci polinomları ile toplanarak şifreli mesaj oluşturulur.

$$\sum_{i=1}^{n} F_i^{(k)}(x) = F_1^{(k)}(x) + F_2^{(k)}(x) + ... + F_n^{(k)}(x)$$

3.2 Geri Çözme Algoritması

- **Adım 1:** n karakterli şifreli mesajı ele alalım. Her bir karakter bir uzunluk olarak kabul edilir.
- **Adım 2:** Oluşturulan mesaj metni k. mertebeden Fibonacci polinomları ile toplanarak yeni mesaj metni elde edilir.

$$\sum_{i=1}^{n} F_i^{(k)}(x) = F_1^{(k)}(x) + F_2^{(k)}(x) + ... + F_n^{(k)}(x)$$

- **Adım 3:** 2. Adımda elde edilen mesaj matrisi 1. anahtar matrisinin tersi olan matris ile çarpılır.

$$1.\,Anahtar\ Matrisinin\ Tersi = \begin{bmatrix} F & Ç & Z \\ S & Ğ & N \\ V & T & G \end{bmatrix} = \begin{bmatrix} 6 & 3 & 30 \\ 21 & 8 & 16 \\ 26 & 23 & 7 \end{bmatrix}$$

Eğer mesaj metninde artan 2 karakter varsa bu kalan matriste 2. anahtar matrisinin tersi ile çarpılır:

$$2.\,Anahtar\ Matrisinin\ Tersi = \begin{bmatrix} T & A \\ Ğ & H \end{bmatrix} = \begin{bmatrix} 23 & 0 \\ 8 & 9 \end{bmatrix}$$

- **Adım 4:** Seçilen k ve n değerlerine göre $\left(Q_k^n(x)\right)^{-1}$ matrisi oluşturulur.

- **Adım 5:** Seçilen k değerine göre mesaj metni bloklara ayrılıp $k \times 1$ tipinde blok matrisler elde edilir. Bu oluşturulan blok matrisler $\left(Q_k^n(x)\right)^{-1}$ matrisi ile çarpılarak yeni mesaj metni elde edilir.
- **Adım 6:** Sonuç olarak elde edilen mesaj metni şifrelenmiş mesajdır.

3.3 Kodlama/Geri Çözme Algoritması ile İlgili Örnekler

Örnek 3.3.1. Mesaj metnini ele alalım:

"HELLO"

Kodlama Teorisine Uygulaması

- **Adım 1:** "HELLO" kelimesi 5 harflidir. Verilen kodlama algoritmasına göre n 'i keyfi olarak seçilebilir. Bu örnekte $n = 5$ seçilerek şifreleme algoritmasına devam edelim.
- **Adım 2:** $k = 3$ ve $n = 5$ seçelim. Dolayısıyla burada kullanılacak olan polinomlar Tribonacci polinomu ve Fibonacci polinomu olacaktır.
- **Adım 3:** $Q_k^n(x)$ matrisini oluşturalım:

$$Q_3^5(x) = \begin{bmatrix} x^2 & x & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}^5 = \begin{bmatrix} x^4+1 & x^4+x+1 & x^3+x^2 \\ x^3+x^2 & x^2 & x^3+x+1 \\ x^3+x+1 & x^2+1 & x^4+x \end{bmatrix}$$

- **Adım 4:**

$$9 = (01001) = x^3 + 1 = H$$

$$5 = (00101) = x^2 + 1 = E$$

$$14 = (01110) = x^3 + x^2 + x = L$$

$$17 = (10001) = x^4 + 1 = O$$

Dolayısıyla;

$$Q_3^5(x).\begin{bmatrix} H \\ E \\ L \end{bmatrix} = \begin{bmatrix} x^4+1 & x^4+x+1 & x^3+x^2 \\ x^3+x^2 & x^2 & x^3+x+1 \\ x^3+x+1 & x^2+1 & x^4+x \end{bmatrix}\begin{bmatrix} x^3+1 \\ x^2+1 \\ x^3+x^2+x \end{bmatrix}$$

$$= \begin{bmatrix} x^4+x^3+x \\ x^4+x^3+x \\ x^3+x^2+x+1 \end{bmatrix} = \begin{bmatrix} V \\ V \\ M \end{bmatrix}$$

"HELLO" kelimesi 5 harfli olduğu için 3×1 ve 2×1 şeklinde iki blok matris oluşturalım. O halde geriye kalan 2 harf için Fibonacci polinomlarını ele alalım.

$$Q_2^5(x) = \begin{bmatrix} x & 1 \\ 1 & 0 \end{bmatrix}^5 = \begin{bmatrix} x^2+x+1 & x^4+x^2+1 \\ x^4+x^2+1 & x^3 \end{bmatrix}$$

Dolayısıyla;

$$Q_2^5(x).\begin{bmatrix} L \\ O \end{bmatrix} = \begin{bmatrix} x^2+x+1 & x^4+x^2+1 \\ x^4+x^2+1 & x^3 \end{bmatrix}\begin{bmatrix} x^3+x^2+x \\ x^4+1 \end{bmatrix}$$

$$= \begin{bmatrix} x^3+x^2+1 \\ x^4+x^2 \end{bmatrix} = \begin{bmatrix} K \\ R \end{bmatrix}$$

İlk şifreli mesaj:

$$\text{“}HELLO \rightarrow VVMKR\text{”}$$

dir.

- **Adım 5:** 4. Adımda elde edilen mesaj matrisi 1. anahtar matrisi ile çarpalım:

$$\begin{bmatrix} B & B & C \\ Ç & E & \breve{G} \\ K & E & Y \end{bmatrix}\begin{bmatrix} V \\ V \\ M \end{bmatrix} = \begin{bmatrix} 1 & 1 & x \\ x+1 & x^2+1 & x^3 \\ x^3+x^2+1 & x^2+1 & x^4+x^3+x^2+1 \end{bmatrix}\begin{bmatrix} x^4+x^3+x \\ x^4+x^3+x \\ x^3+x^2+x+1 \end{bmatrix}$$

$$= \begin{bmatrix} x^4+x^3+x^2+x \\ 1 \\ x^2 \end{bmatrix} = \begin{bmatrix} Z \\ B \\ D \end{bmatrix}$$

Şimdi de geri kalan 2 harf için oluşturulan blok matrisini 2. Anahtar matrisi ile çarpalım:

$$\begin{bmatrix} E & A \\ O & D \end{bmatrix}\begin{bmatrix} K \\ R \end{bmatrix} = \begin{bmatrix} x^2+1 & 0 \\ x^4+1 & x^2 \end{bmatrix}\begin{bmatrix} x^3+x^2+1 \\ x^4+x^2 \end{bmatrix}$$

$$= \begin{bmatrix} x^4+x^3+x^2 \\ x^4+x^3+1 \end{bmatrix} = \begin{bmatrix} X \\ \ddot{U} \end{bmatrix}$$

Dolayısıyla; elde edilen ikinci şifreli mesaj:

$$\text{“}VVMKR \rightarrow ZBDX\ddot{U}\text{”}$$

dir.

- **Adım 6:**

$$Z + T_1(x) = x^4 + x^3 + x^2 + x + 1 = Q$$

$$B + T_2(x) = 1 + x^2 = E$$

$$D + T_3(x) = x^4 + x^2 + x = \text{Ş}$$

$$X + T_4(x) = x^4 + x^2 + x + 1 = T$$

$$\ddot{U} + T_5(x) = x^4 + x^2 + 1 = S$$

Burada $T_n(x)$ Tribonacci polinomlarıdır.

Sonuç olarak karşı tarafa gönderilen şifreli mesaj:

$$\text{“ } ZBDX\ddot{U} \rightarrow QE\c{S}TS \text{ ”}$$

dir.

Geri Çözme Algoritmasına Uygulaması

- **Adım 1:**

$$Q + T_1(x) = x^4 + x^3 + x^2 + x = Z$$

$$E + T_2(x) = 1 = B$$

$$\c{S} + T_3(x) = x^2 = D$$

$$T + T_4(x) = x^4 + x^3 + x^2 = X$$

$$S + T_5(x) = x^4 + x^3 + 1 = \ddot{U}$$

Burada $T_n(x)$, n. Tribonacci polinomudur.

Dolayısıyla;

$$\text{"}QE\c{S}TS \rightarrow ZBDX\ddot{U}\text{"}$$

dür.

- **Adım 2:** Elde edilen mesaj matrisi 1. anahtar matrisinin tersi ile çarpalım.

$$\begin{bmatrix} F & \c{C} & Z \\ S & \breve{G} & N \\ V & T & G \end{bmatrix} \begin{bmatrix} Z \\ B \\ D \end{bmatrix} = \begin{bmatrix} V \\ V \\ M \end{bmatrix}$$

Geri kalan 2 harf için oluşturulan 2×1 tipindeki blok matrisi de 2. anahtar matrisinin tersi ile çarpalım.

$$\begin{bmatrix} T & A \\ \check{G} & H \end{bmatrix}\begin{bmatrix} X \\ \ddot{U} \end{bmatrix}=\begin{bmatrix} K \\ R \end{bmatrix}$$

Dolayısıyla şifreli geri çözme mesajı:

$$"ZBDX\ddot{U} \rightarrow VVMKR"$$

olarak elde edilir.

- **Adım 3:** Seçilen $k=3$ ve $n=5$ değerleri için $\left(Q_k^n(x)\right)^{-1}$ matrisini elde edelim.

$$\left(Q_3^5(x)\right)^{-1}=\begin{bmatrix} 0 & x & x^3+1 \\ x^3+1 & 1 & x^4 \\ x^4 & x+1 & x^2 \end{bmatrix}=\begin{bmatrix} A & C & H \\ H & B & N \\ N & \text{Ç} & D \end{bmatrix}$$

Dolayısıyla;

$$\left(Q_3^5(x)\right)^{-1}.\begin{bmatrix} V \\ V \\ M \end{bmatrix}=\begin{bmatrix} 0 & x & x^3+1 \\ x^3+1 & 1 & x^4 \\ x^4 & x+1 & x^2 \end{bmatrix}.\begin{bmatrix} x^4+x^3+x \\ x^4+x^3+x \\ x^3+x^2+x+1 \end{bmatrix}$$

Geri kalan 2 harf içinde $k=2$ ve $n=5$ olmak üzere;

$$\left(Q_2^5(x)\right)^{-1}=\begin{bmatrix} x^3 & x^4+x^2+1 \\ x^4+x^2+1 & x^2+x+1 \end{bmatrix}=\begin{bmatrix} \check{G} & S \\ S & I \end{bmatrix}$$

dir. Dolayısıyla;

$$\left(Q_2^5(x)\right)^{-1}.\begin{bmatrix} K \\ R \end{bmatrix}=\begin{bmatrix} x^3 & x^4+x^2+1 \\ x^4+x^2+1 & x^2+x+1 \end{bmatrix}\begin{bmatrix} x^3+x^2+1 \\ x^4+x^2 \end{bmatrix}$$

$$= \begin{bmatrix} x^3 + x^2 + x \\ x^4 + 1 \end{bmatrix} = \begin{bmatrix} L \\ O \end{bmatrix}$$

Sonuç olarak şifrelenmiş mesaj:

$$"VVMKR \rightarrow HELLO"$$

olarak elde edilir.

Örnek 3.3.2. Mesaj metnini ele alalım:

"PUBLIC"

Kodlama Algoritmasına Uygulaması

- **Adım 1:** $n = 6$ ve $k = 4$ seçelim.
- **Adım 2:** $k = 4$ seçildiği için bu örnekte kullanılacak olan polinomlar Tetranacci polinomları ve Fibonacci polinomları olacaktır.
- **Adım 3:**

$$Q_4^6(x) = \begin{bmatrix} x^3 & x^2 & x & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}^6$$

$$= \begin{bmatrix} x^4 + x^3 + x & x^3 + x & x^3 + 1 & x^4 + x^3 + x^2 + x + 1 \\ x^4 + x^3 + x^2 + x + 1 & x^4 + x^3 + 1 & x^4 + x^3 + 1 & x^4 + x \\ x^4 + x & x^4 + x^3 + x + 1 & x^4 + x^3 + x + 1 & x^4 + x^3 \\ x^4 + x^3 & x^3 + x^2 & x^4 + x^2 & x^3 + x^2 + x \end{bmatrix}$$

- **Adım 4:**

$$19 = (10011) = x^4 + x + 1 = P$$

$$24 = (11000) = x^4 + x^3 = U$$

$$1 = (00001) = 1 = B$$

$$14 = (01110) = x^3 + x^2 + x = L$$

$$10 = (01010) = x^3 + x = I$$

$$2 = (00010) = x = C$$

Dolayısıyla;

$$Q_4^6(x).\begin{bmatrix} P \\ U \\ B \\ L \end{bmatrix} = Q_4^6(x)\begin{bmatrix} x^4 + x + 1 \\ x^4 + x^3 \\ 1 \\ x^3 + x^2 + x \end{bmatrix}$$

$$= \begin{bmatrix} x^4 + x^3 + x^2 + x \\ x + 1 \\ x^3 + x^2 + x \\ x^3 + x^2 + x + 1 \end{bmatrix} = \begin{bmatrix} Z \\ Ç \\ L \\ M \end{bmatrix}$$

"PUBLIC" 6 harfli olduğundan blok matrisleri 4×1 ve 2×1 şeklinde alınacaktır.

$$Q_2^6(x).\begin{bmatrix} I \\ C \end{bmatrix} = \begin{bmatrix} x^4 + x^3 + x + 1 & x^2 + x + 1 \\ x^2 + x + 1 & x^4 + x^2 + 1 \end{bmatrix}\begin{bmatrix} x^3 + x \\ x \end{bmatrix}$$

$$= \begin{bmatrix} x^4 + x^3 + x + 1 \\ x^4 + x^3 + x^2 \end{bmatrix} = \begin{bmatrix} W \\ X \end{bmatrix}$$

İlk mesaj metni:

$$"\ PUBLIC \rightarrow ZÇ\ LMWX\ "$$

olarak bulunur.

- **Adım 5:** 4. Adımda elde edilen mesaj matrisini 1. anahtar matrisi ile çarpalım:

$$\begin{bmatrix} B & B & C \\ Ç & E & \breve{G} \\ K & E & Y \end{bmatrix}\begin{bmatrix} Z \\ Ç \\ L \end{bmatrix}=\begin{bmatrix} 1 & 1 & x \\ x+1 & x^2+1 & x^3 \\ x^3+x^2+1 & x^2+1 & x^4+x^3+x^2+1 \end{bmatrix}\begin{bmatrix} x^4+x^3+x^2+x \\ x+1 \\ x^3+x^2+x \end{bmatrix}$$

$$=\begin{bmatrix} 1 \\ x^4+x^2+x+1 \\ x^4+x^3+x \end{bmatrix}=\begin{bmatrix} B \\ T \\ V \end{bmatrix}$$

Geri kalan 3 harf için oluşturulan blok matrisi 3×1 tipinde olduğundan tekrar 1. anahtar matrisi ile çarpılır.

$$\begin{bmatrix} B & B & C \\ Ç & E & \breve{G} \\ K & E & Y \end{bmatrix}\begin{bmatrix} M \\ W \\ X \end{bmatrix}=\begin{bmatrix} 1 & 1 & x \\ x+1 & x^2+1 & x^3 \\ x^3+x^2+1 & x^2+1 & x^4+x^3+x^2+1 \end{bmatrix}\begin{bmatrix} x^3+x^2+x+1 \\ x^4+x^3+x+1 \\ x^4+x^3+x^2 \end{bmatrix}$$

$$=\begin{bmatrix} x^3+1 \\ x^4+x \\ x^4+x \end{bmatrix}=\begin{bmatrix} H \\ Ö \\ Ö \end{bmatrix}$$

Dolayısıyla;

$$" \; ZÇ\,LMWX \rightarrow BTVHÖ\,Ö \; "$$

dir.

- **Adım 6:**

$$B+F_1^{(4)}(x)=1=B$$

$$T+F_2^{(4)}(x)=x^4+x^2+x+1=T$$

$$V+F_3^{(4)}(x)=x^4+x^3+x+1=W$$

$$H+F_4^{(4)}(x)=1=B$$

$$Ö+F_5^{(4)}(x)=x^4+x^3+x^2=X$$

$$\ddot{O} + F_6^{(4)}(x) = x^3 + x = I$$

Burada $F_n^{(4)}(x)$, n. Tetranacci polinomudur.

Dolayısıyla, karşı tarafa gönderilen şifreli mesaj:

$$"\ BTVH\ddot{O}\ \ddot{O} \rightarrow BTWBXI"$$

dir.

Geri Çözme Algoritmasına Uygulaması

- **Adım 1:**

$$B + F_1^{(4)}(x) = 1 = B$$

$$T + F_2^{(4)}(x) = x^4 + x^2 + x + 1 = T$$

$$W + F_3^{(4)}(x) = x^4 + x^3 + x = V$$

$$B + F_4^{(4)}(x) = 1 + x^3 = H$$

$$X + F_5^{(4)}(x) = x^4 + x = \ddot{O}$$

$$I + F_6^{(4)}(x) = x^4 + x = \ddot{O}$$

Burada $F_n^{(4)}(x)$, n. Tetranacci polinomudur. Dolayısıyla;

$$"\ BTWBXI \rightarrow BTVH\ddot{O}\ \ddot{O}\ "$$

dir.

- **Adım 2:** Elde edilen mesaj metnine ait matris ile 1. anahtar matrisinin tersi çarpılır:

$$\begin{bmatrix} F & Ç & Z \\ S & Ğ & N \\ V & T & G \end{bmatrix}\begin{bmatrix} B \\ T \\ V \end{bmatrix}=\begin{bmatrix} Z \\ Ç \\ L \end{bmatrix}$$

Şimdi geri kalan 3 harf için elde edilen 3×1 tipindeki blok matris ile 1. anahtar matrisinin tersi çarpılır:

$$\begin{bmatrix} F & Ç & Z \\ S & Ğ & N \\ V & T & G \end{bmatrix}\begin{bmatrix} H \\ Ö \\ Ö \end{bmatrix}=\begin{bmatrix} M \\ W \\ X \end{bmatrix}$$

Dolayısıyla; şifreli mesaj

$$"BTVHÖÖ \rightarrow ZÇLMWX"$$

dir.

- **Adım 3:** Seçilen $k=4$ ve $n=6$ için

$$\left(Q_4^6(x)\right)^{-1}.\begin{bmatrix} Z \\ Ç \\ L \\ M \end{bmatrix}=\begin{bmatrix} P \\ U \\ B \\ L \end{bmatrix}$$

Ve geri kalan 2 harf için elde edilen blok matrisini

$$\left(Q_2^6(x)\right)^{-1}.\begin{bmatrix} W \\ X \end{bmatrix}=\begin{bmatrix} I \\ C \end{bmatrix}$$

elde ederiz. Dolayısıyla; mesaj metni

$$"ZÇLMWX \rightarrow PUBLIC"$$

olarak bulunur.

4. SONUÇ VE ÖNERİLER

AES (Gelişmiş Şifreleme Algoritması), elektronik verilerin şifrelenmesi için sunulan bir standarttır. AES şifreleme algoritması Rijndael bloklama şifresiyle neredeyse aynıdır. Rijndael bloğu ve anahtar boyutu 128, 192 ve 256 bit arasında değişir. Ancak, AES standardı yalnızca 128 bitlik bir blok boyutu gerektirir. Bu nedenle, yalnızca 128 bitlik blok uzunluğuna sahip Rijndael, AES algoritması olarak bilinir. Dolayısıyla, biz bu tezimizde blok uzunluğu 128 bit olan Rijndael' in yalnızca standart sürümü üzerinde çalışmalar yaptık.

Rijndael algoritması, Galois cisimlerinde polinomlar yardımıyla şifreleme gerçekleştirir. Biz bu tezimizde, daha önce yapılan çalışmaları genelleştirerek yeni bir şifreleme algoritması elde ettik. Bu çalışmada, Dişkaya, Avaroğlu ve Menken (2020) tarafından verilen şifreleme algoritmasını genelleştirdik ve 2×2 tipinde blok matris işlemi ile yapılan şifrelemeyi Galois cismi üzerinde $k\times k$ tipinde blok matrislere taşıyarak çalışmamızı yaptık. Kriptoloji algoritmamızda belirli bir indirgenemez polinom kullanarak k. mertebeden Fibonacci polinomları için yeniden tanımladık. Tanımlamış olduğumuz algoritma, AES benzeri şifreleme algoritmasında olduğu gibi dört adımdan oluşmaktadır. Bu algoritmada tanımlanan şifreleme algoritması, şifrelenmiş metnin hem şifrelenmesinde hem de şifresinin çözülmesinde kullanılan anahtarların birbiriyle ilişkili olduğu simetrik-anahtar algoritmasıdır. Şifreleme ve şifre çözme AES anahtarları ile aynıdır. Bu nedenle, bu kriptoloji algoritmasını k. mertebeden Fibonacci polinomları üzerinde AES-benzeri kriptoloji algoritması olarak adlandırdık. Bu şekilde, araştırmacılar keyfi seçimlere dayalı olarak şifreleme işlemini gerçekleştirebilirler.

Bu tezimizde, tasarım mantığını anlamak için matematiksel temelli ve açıklamanın kendisini takip eden özellikleri sunuyoruz. Ardından şifreleme yöntemini ve uygulamasını vererek AES-benzeri şifreleme algoritmamızı tanımlıyoruz.

Sonuç olarak; günümüzde teknolojinin gelişmesiyle birlikte bilgi güvenliği çok önemli bir hal aldı. Hızlı ve güçlü bilgisayarlar hayatımıza girdi. Bu bilgisayarlar

bize birçok yönden fayda sağlıyor. Fakat bilgisayarların gelişmesinin avantajlarının yanı sıra dezavantajları da bulunmaktadır. Kriptografi bu alanda ön plana çıkmaktadır. Hızlı ve gelişmiş bilgisayarlar bilgi güvenliğini sağlamada dezavantaj oluşturmaktadır. Dolayısıyla şifreleme algoritmaları da bilgisayarların gelişimiyle birlikte aynı ölçüde geliştirilmesi gerekmektedir. AES şifreleme algoritması donanımsal olarak çok iyi bir performans vermektedir. Dolayısıyla bizim oluşturmuş olduğumuz AES benzeri şifreleme algoritması da performans bakımından iyi sonuç vermektedir. Çünkü bizim bu tezde vermiş olduğumuz şifreleme algoritmasının temeli Rijndael algoritmasına dayanmaktadır.

Vermiş olduğumuz AES benzeri şifreleme algoritması $GF\left(2^5\right)$ Galois cisminde indirgenemez polinomlarından bir tanesi seçilerek oluşturulmuştur. Galois cisminde tek indirgenemez polinom bu olmadığından diğer indirgenemez polinomlar seçilerek yeni şifreleme algoritmaları oluşturulabilir. Bunun yanı sıra anahtar uzunluğumuzun boyutunu arttırarak döngü sayılarımızı arttırabilir ve bu da bilgi güvenliğini sağlamakta önemli ölçüde fayda sağlamaktadır.

Biz bu tezimizde AES benzeri şifreleme algoritmasını verirken k. mertebeden Fibonacci polinomlarını kullanmıştık. Aynı şekilde k. mertebeden Fibonacci polinomlarının yerine k. mertebeden Pell, Pell-Lucas, Jacobsthal, Jacobsthal-Lucas, Mersenne gibi diğer özel polinomlar kullanılarak yeni şifreleme algoritmaları tanımlanabilir. Bu ise bize kriptoloji de yeni bir çalışma alanı yaratmaktadır. Özel polinomlar sayesinde çeşitli şifreleme algoritmaları tanımlanabilir ve uygulanabilir.

5. KAYNAKLAR

Asci, M., Aydinyuz, S., “k-order Gaussian Fibonacci polynomials and applications to the coding/decoding theory”, *Journal of Discrete Mathematical Sciences and Cryptography*, (in press), DOI: 10.1080/09720529.2020.1816917.

Asci, M., Gurel, E., “Bivariate Gaussian Fibonacci and Lucas Polynomials”, *Ars Combin.*, 109, 461-472, (2013).

Basu, M., Prasad, B., “The generalized relations among the code elements for Fibonacci Coding Theory*", Chaos, Solitons and Fractals*, 41(5), 2517-2525, (2009).

Basu, M., Das, M., “Tribonacci matrices and a new coding theory”, *Discrete Math. Algorithms Appl.*, 6(1), article ID: 1450008, (2014).

Basu M., Das M., "Coding theory on Fibonacci n-step numbers", *Discrete Math. Algorithms Appl.*, 6(2), article ID: 145008, (2014).

Diskaya, O., Avaroglu, E., Menken, H., “The classical AES-like cryptology via the Fibonacci polynomial matrix”, *Turkish Journal of Engineering*, 4(3), 123–128, DOI 10.31127/tuje.646926, (2020).

Hoggatt, V.E, “Fibonacci and Lucas Numbers,” A publication of the Fibonacci Association. University of Santa Clara, Santa Clara, Houghton Mifflin Company, (1969).

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

Horadam, A. F., "Complex Fibonacci Numbers and Fibonacci Quaternions", *American Math. Monthly*, 70, 289-291, (1963).

Horadam, A. F., Horadam, E. M., “Roots of Recurrence-Generated Polynomials”, *Fibonacci Quart.*, 20(3), 219-226, (1982).

Kilic, E., Tasci,D., "On the generalized order-k Fibonacci and Lucas numbers", *Rocky Mountain J. Math.*, 36(6), 1915-1926, (2006).

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

Koshy, T., "*Fibonacci and Lucas Numbers with Applications*", A Wiley-Interscience Publication, (2017).

Lee, G. Y., Kim, J. S., “The linear algebra of the k-Fibonacci matrix”, *Linear Algebra Appl.,* 373:75-87, (2003).

Paar, C., Pelzl, J., “*Understanding cryptography: a textbook for students and practitioners*”, London: Springer Science, Business Media, (2009).

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

Stakhov, A. P., "*Fibonacci matrices, a generalization of the Cassini formula and a new coding theory*", Chaos, Solitions and Fractals, 30, no. 1, 56-66, (2006).

Tasci, D., “*Soyut Cebir*”, Ankara: Gazi Kitapevi, (2018).

Vajda, S., "*Fibonacci and Lucas Numbers, and the Golden SectionTheory and Applications*", Ellis Harwood Limitted, (1989).