KRİPTOLOJİYE GİRİŞ

2014
YÜKSEK LİSANS TEZİ
MATEMATİK

Çağla ÖZYILMAZ

KRİPTOLOJİYE GİRİŞ

Çağla ÖZYILMAZ

Karabük Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalında
Yüksek Lisans Tezi
Olarak Hazırlanmıştır

KARABÜK
Haziran 2014

Çağla ÖZYILMAZ tarafından hazırlanan "KRİPTOLOJİYE GİRİŞ" başlıklı bu tezin Yüksek Lisans Tezi olarak uygun olduğunu onaylarım.

Doç. Dr. Ayşe NALLI .....

Tez Danışmanı, Matematik Anabilim Dalı

Bu çalışma, jürimiz tarafından oy birliği ile Matematik Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir. 16 /06/ 2014

Ünvanı, Adı SOYADI (Kurumu)	İmzası
Başkan : Doç. Dr. Ayşe NALLI(KBÜ)	.....
Üye : Yrd.Doç.Dr.TufanTURACI(KBÜ)	.....
Üye: Doç. Dr. Ahmet DEMİR(KBÜ)	.....

11./08./2014

KBÜ Fen Bilimleri Enstitüsü Yönetim Kurulu, bu tez ile, Yüksek Lisans derecesini onamıştır.

Prof. Dr. Mustafa BOZ .....

Fen Bilimleri Enstitüsü Müdürü

"Bu tezdeki tüm bilgilerin akademik kurallara ve etik ilkelere uygun olarak elde edildiğini ve sunulduğunu; ayrıca bu kuralların ve ilkelerin gerektirdiği şekilde, bu çalışmadan kaynaklanmayan bütün atıfları yaptığımı beyan ederim."

Çağla ÖZYILMAZ

ÖZET

Yüksek Lisans Tezi

KRİPTOLOJİYE GİRİŞ

Çağla ÖZYILMAZ

Karabük Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Tez Danışmanı:
Doç. Dr. Ayşe NALLI
Haziran 2014, 87 sayfa

Tarih boyunca insanlar kendileri için özel saydıkları bilgilerin istemedikleri kişilerin eline geçmemesi için çabalamışlardır. Böylece ilkel sayılabilecek yöntemlerle şifrelemenin temelleri atılmıştır. Günümüzde ise teknolojinin inanılmaz hızı düşünüldüğünde, teknolojinin gelişmesiyle ortaya çıkan güvenlik açığının ne kadar önem taşıdığı görülmektedir.

Bu tezde, ilk olarak şifrelemeden ve bazı klasik şifreleme türlerinde bahsedilmiş, sonraki bölümlerde ise Fibonacci kodu ve Fibonacci kodunun bir varyasyonu olan *Gopala-Hemachandra (GH)* kodu çeşitli mertebelerden tanımlanmış, pozitif tamsayıların bazı mertebelerden *GH* kodları veya temsilleri elde edilmiştir. Bu temsiller veya bu kodlar kullanılarak bazı koşullar altında şifreleme örnekleri yapılmıştır.

Anahtar Sözcükler : Kriptoloji, Fibonacci kodu, *Gopala-Hemachandra* temsili, şifreleme, anahtar.

Bilim Kodu : 204.1.011

ABSTRACT

M. Sc. Thesis

ENTER TO CRYPTOLOGY

Çağla ÖZYILMAZ

Karabük University
Graduate School of Natural and Applied Sciences
Department of Mathematics

Thesis Advisor:
Assoc. Prof. Dr. Ayşe NALLI
June 2014, 87 pages

Throughout history, people try not to learn the others the information which is specific according to themselves. Thus, the foundations the cryptography are built by relatively primitive methods. Today, considering the incredible speed of technology, it is seen that the vulnerabilitiy emerging by the development of technology is very important.

In this thesis, firstly it is cited that cryptography and some simple cryptosystems, then it is defined that Fibonacci code and variations on the Fibonacci universal code which may also be called the *Gopala-Hemachandra* code and it is obtained the some ordered *GH* representations or *GH* codes of positive integer. Under the some circumsitances, it is done applications of *Gopala-Hemachandra (GH)* codes or *Gopala-Hemachandra (GH)* representations to cryptography by using this *GH* representations or *GH* codes.

Key Word : Cryptology, Fibonacci code, *Gopala-Hemachandra* representation, encryption, key.

Science Code : 204.1.011

TEŞEKKÜR

İlk olarak tezime bilgisiyle yön veren, bu tez çalışmasının oluşumunda ilgi ve desteğini esirgemeyen, engin bilgi ve tecrübelerinden yararlandığım, yönlendirme ve bilgilendirmeleriyle çalışmamı bilimsel temeller ışığında şekillendiren sayın hocam Doç. Dr. Ayşe NALLI'ya sonsuz teşekkürlerimi sunarım.

Ayrıca, tez çalışmam ve araştırmalarım sırasında bilgisayar ve programlama bilgileriyle bana destek olan Murat KORKMAZ'a teşekkür ederim.

Son olarak da hayatım boyunca hep yanımda olan ve maddi ve manevi olarak desteklerini hiçbir zaman benden esirgemeyen annem Kezban ÖZYILMAZ'a ve babam Osman ÖZYILMAZ'a sonsuz teşekkür ederim.

İÇİNDEKİLER

Sayfa

Sayfa

ŞEKİLLER DİZİNİ

Sayfa

ÇİZELGELER DİZİNİ

Sayfa

SİMGELER VE KISALTMALAR DİZİNİ

SİMGELER

$\mathbb{Z}$: Tamsayılar cümlesi

$\mathbb{R}$: Reel sayılar cümlesi

$\oplus$: XOR işlemi

E_e : Şifreleme dönüşümü

D_d : Deşifreleme dönüşümü

$F_n^{(m)}$: Pozitif n tamsayısının m .mertebeden Fibonacci kodu

$GH_a^{(m)}$: m .mertebeden *Gopala-Hemachandra* (*GH)* kodlarının ailesi

$VF_a^{(m)}$: m .mertebeden *Variant Fibonacci* kodlarının ailesi

$\sum$: Toplam sembolü

KISALTMALAR

GH : Gopala-Hemachandra Dizisi

DES : Data Encrption Standard (Veri Şifreleme Standardı)

AES : Advanced Encryption Standard (İleri Şifreleme Standardı)

IDEA : International Data Encryption Algorithm (Uluslararası Veri Şifreleme Algoritması)

GCD : Greatest Common Divisor (En Büyük Ortak Bölen)

N/A : Not Available (Ulaşılamayan Değer)

BÖLÜM 1

KRİPTOLOJİYE GENEL BAKIŞ

1.1. GİRİŞ

Yazının icadından günümüze kadar, insanlar haberleşmelerinde gizliliği her zaman ön planda tutmuşlardır. İnsanoğlu var olduğundan beri haberleşme için yeni yöntemler geliştirmiş ve iletilerini başka insanlardan saklama gerekliliği ortaya çıktığından beri de gizlilik, haberleşmedeki en önemli kıstas olmuştur. Bilgileri kodlama, binlerce yıl önce devletlerin ve imparatorlukların gizli ve önemli bilgileri düşmanın eline geçmeden iletebilmesi için ortaya çıkmıştır. İleti elden veya bir köleyle gönderilse de, günümüzdeki gibi postacılarla veya internet üzerinden gönderilse de her zaman başkalarının eline geçme ihtimali vardır. Bu sebeple iletiyi kodlama, yani başka bir deyişle bir sözcüğün veya cümlenin başka bir sözcük, sayı ya da sembol ile yerini değiştirerek gönderme, mesajın başkaları tarafından anlaşılmasını zorlaştırmaktadır [1].

Günümüzde kodların yerini şifreler almış, kod kelimesinin kullanımı azalmıştır. Sözcüklerin değil, harflerin yerlerini değiştirerek daha temel düzeyde işlev gören şifre, alternatif bir koddur. Eski zamanlara göre şifrelerin kullanım alanları değişiklik göstermiş, fakat kullanım amaçları eskisi gibi gizliliği sağlamak olmuştur. Bilgi günümüz rekabet ortamında gitgide daha değerli bir konu haline gelmektedir. İletişim tekniklerindeki gelişmeler de bilgiyi saklama ve iletme açısından işleri zorlaştırmakta, yeni teknikler geliştirmek için insanları zorlamaktadır. Telefon görüşmeleri uydudan yansımakta, internet üzerindeki haberleşmelerimiz de çeşitli bilgisayarlardan geçmektedir. Haberleşme ve bilişimin genel sorunu bilgi güvenliğidir. Özellikle son yıllarda artan internet üzerinden yapılan sanal alışverişler, bireysel bankacılık işlemleri ve e-posta trafiği interneti daha güvenli bir ortam olmaya zorlamaktadır. O halde sorun, bilgi ve haberleşme güvenliğinin yüksek

oranda sağlanmasının nasıl gerçekleşeceğine odaklanmaktır. Bunu sağlayacak olan da şifre biliminin ta kendisidir. Sonuç olarak haberleşmenin günümüzde yön değiştirmesi eski çağlardaki kodlamadan yola çıkan ve günümüzde disiplinlerarası bir bilim haline gelmiş kriptografinin ne denli önemli olduğunun altını çizmektedir [1].

Gizli haberleşme, bundan yaklaşık 4000 yıl önce kullanılmaya başlanmış; özellikle diplomasi ve askeri servislerde yer almış ve II .Dünya Savaşı gibi modern savaşlarda önemli rol oynamıştır. İlk olarak Eski Mısırlıların tarihi anıtlarındaki hiyeroglif yazıların bazılarında görülen şifreleme daha sonra İbranililerin kutsal kitaplarındaki belirli kelimelerde görülmüştür [2].

Kriptografi, köken olarak Yunanca gizli saklı anlamına gelen *kryptos* ve yazmak anlamına gelen *graphein* sözcüklerinden türetilmiştir. Kriptografi gizlilik, kimlik denetimi, bütünlük gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemler bütünüdür. Bu yöntemler, bir bilginin iletimi esnasında karşılaşılabilecek saldırılardan bilgiyi, bilgi göndericisini ve alıcısını koruma amacı taşır. Bir başka deyişle kriptografi, okunabilir durumdaki bir bilginin istenmeyen taraflarca okunamayacak bir hale dönüştürülmesinde kullanılan tekniklerin tümüdür [1].

Kriptanaliz ise ele geçen şifrelenmiş, yani anlamsız bir metinden bazı teknikleri kullanarak doğru metni bulma yöntemidir [1]. Analizcinin amacı herhangi bir algoritma kullanılarak kapatılmış metinlerin açık metin halini elde edebilmektir. Genellikle bu amaca algoritmada kullanılan gizli anahtarın tamamı veya belli bir kısmı elde edilerek ulaşılır [3].

Kriptoloji, matematiğin hem şifre bilimi (kriptografi), hem de şifre analizini (kriptanaliz) kapsayan dalıdır. Şifre biliminin amacı, ileti güvenliğini sağlamak, şifre analizinin amacı ise var olan şifreleri çözmektir. Kriptolojinin temel kavramlarından biri olan şifreleme bir düz metnin içeriğini okunamayacak hale getirme işlemidir. Şifrelemede esas olan, iletinin istenmeyen kişiler tarafından okunmasını engellemektir. Deşifreleme (şifre çözümü) ise şifrelemenin tam tersi olup şifreli

metnin düz metne çevrilmesi işlemidir. Bu işlem kısaca aşağıdaki gibi gösterilebilir [2].

Şekil 1.1. Bir düz metnin şifrelenmesi ve deşifrelenmesi [2].

Şimdi kriptografide kullandığımız bazı matematiksel terimleri tanımlayalım.

1.2. TEMEL MATEMATİKSEL KAVRAMLAR

Tanım 1.2.1.

Boş olmayan A ve B cümleleri verilsin. A cümlesinden B cümlesine bir f bağıntısı A'nın her x elemanını B'nin en az bir ve en çok bir elemanı ile eşliyorsa bu bağıntıya tanım cümlesi A, değer cümlesi B olan bir *fonksiyon* denir.
Bu tanıma göre, A'dan B' ye bir f bağıntısının bir fonksiyon olması için,

$$\forall x \in A, \exists y \in B, \quad (x,y) \in f$$

$$\forall x \in A, \exists y, y' \in B, \quad [(x,y) \in f \ ve \ (x,y') \in f] \Rightarrow y = y'$$

önermelerinin doğru olması gerekir ve yeter.

Tanım 1.2.2.

Tanım cümlesi A ve değer cümlesi B olan bir f fonksiyonunun verildiği,

$$f : A \to B$$

biçiminde yazılarak anlatılır. $(x,y)\in f$ ise y 'ye x 'in f fonksiyonundaki *görüntüsü* veya f 'nin x teki değeri denir. Bu değer çoğu kez $f(x)$ ile gösterilir.

Bu tanıma göre,

$$(x,y)\in f \Leftrightarrow y=f(x)$$

dir.

$$y=f(x)$$

eşitliğine f fonksiyonunun kuralı denir.

Tanım 1.2.3.

$f:A\to B$ bir fonksiyon olsun. $X\subseteq A$ olduğuna göre,

$$\{y:\ y\in B\wedge(\exists x\in X\,,\ y=f(x))\}$$

cümlesine yani,

$$f(X)=\{f(x)|x\in X\}$$

cümlesine X 'in f fonksiyonundaki *görüntüsü* denir.

Tanım 1.2.4.

$f:A\to B$ bir fonksiyon olsun. $y\in B$ verilsin. $y=f(x)$ olacak biçimde A 'nın bir x elemanı varsa bu x elemanına y 'nin bir *ters görüntüsü* denir. y 'nin tüm ters görüntülerinin cümlesi,

$f^{-1}(\{y\})$ veya $f^{-1}\{y\}$

biçiminde gösterilir.

Tanıma göre,

$f^{-1}\{y\} \subseteq A$ ve $f^{-1}\{y\}=\{x|x\in A \text{ ve } f(x)=y\}$

dir.

Tanım 1.2.5.

$f:A\to B$ bir fonksiyon olsun. A'nın farklı elemanlarının f fonksiyonundaki görüntüleri farklı ise, f fonksiyonuna *birebir fonksiyon* denir. Tanıma göre,

$(f \text{ birebirdir}) \Leftrightarrow [\forall x_1, x_2 \in A \text{ için}, x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)]$

dir.

Tanım 1.2.6.

$f:A\to B$ bir fonksiyon olsun. B'nin her elemanının en az bir ters görüntüsü varsa f fonksiyonuna *örten fonksiyon* denir. Tanıma göre,

$(f \text{ örtendir}) \Leftrightarrow \forall y\, [\forall y \in B \Rightarrow \exists x\in A \text{ için } f(x)=y]$

dir.

Tanım 1.2.7.

$f:A\to B$ bir fonksiyon olsun. Bu durumda f'nin tersine f fonksiyonunun tersi denir. f fonksiyonunun tersi bir fonksiyon ise buna f'nin *ters fonksiyonu* denir.

f 'nin tersi f^{-1} ile gösterilir.

$$(x,y)\in f \Leftrightarrow (y,x)\in f^{-1}$$

dir.

Teorem 1.2.1.

$f:A\to B$ fonksiyonunun tersinin bir fonksiyon olması için gerek ve yeter koşul f nin *birebir ve örten* olmasıdır.

Tanım 1.2.8.

Herhangi bir A cümlesinden A cümlesine birebir ve örten bir fonksiyona A'nın bir *permütasyonu* denir.

Tanım 1.2.9.

A cümlesinde tanımlanan bir β bağıntısı yansıyan, simetrik ve geçişli ise bu bağıntıya A cümlesinde tanımlı bir *denklik bağıntısı* denir.

Tanım 1.2.9.1.

A cümlesinde tanımlanan bir bağıntı β olsun.

$$\forall x(x\in A \Rightarrow (x,x)\in \beta)$$

önermesi doğru ise β bağıntısının *yansıma* özelliği vardır veya β *yansıyan* bir bağıntıdır, denir. Tanıma göre,

$\beta, A\ da\ yansıyandır \Leftrightarrow \forall x[x \in A \Rightarrow (x,x) \in \beta]$

dir.

Tanım 1.2.9.2.

A cümlesinde tanımlanan bir bağıntı β olsun.

$\forall (x,y)\ [(x,y) \in \beta \Rightarrow (y,x) \in \beta]$

önermesi doğru ise, β bağıntısının *simetri* özelliği vardır veya β *simetrik* bir bağıntıdır, denir. Tanıma göre,

$\beta\ simetriktir \Leftrightarrow \forall (x,y)\ [(x,y) \in \beta \Rightarrow (y,x) \in \beta]$

dir.

Tanım 1.2.9.3.

A cümlesinde tanımlanan bir bağıntı β olsun.

$\forall (x,y),\ \forall (y,z)\ [((x,y) \in \beta \wedge (y,z) \in \beta) \Rightarrow (x,z) \in \beta]$

önermesi doğru ise β bağıntısının *geçişme* özelliği vardır veya β *geçişli* bir bağıntıdır, denir.

Tanıma göre,

$\beta\ geçişlidir \Leftrightarrow \forall (x,y),\ \forall (y,z)\ [((x,y) \in \beta \wedge (y,z) \in \beta) \Rightarrow (x,z) \in \beta]$

dir .

Tanım 1.2.10.

a ve b tamsayılar olsun. Bu takdirde eğer $b=a.c$ olacak şekilde bir c tamsayısı mevcutsa a, b 'yi böler denir ve $a|b$ ile gösterilir [4].

BÖLÜM 2

TEMEL ŞİFRELEME YÖNTEMLERİ

Eski çağlardan beri gizlilik üzerinde önemle durulan bir sorundur. Gizlilikte amaç gönderilen bir mesajı ilgili alıcısından başka kimsenin anlamamasıdır [5]. Günümüz teknolojisinin inanılmaz hızı göz önüne alındığında, teknolojinin gelişmesiyle ortaya çıkan güvenlik açığının ne kadar önem taşıdığı görülmektedir. Kriptoloji, kişiler arası veya özel devlet kurumları arasındaki mesajlaşmalardan sistemlerin oluşumunda ve işleyişindeki güvenlik boşluklarına kadar her türlü dalla alakalıdır [2].

2.1. KRİPTOLOJİDE KULLANILAN TEMEL KAVRAMLAR

Kriptoloji: Şifre bilimidir.

Kriptografi: Kodunu yalnız alıcısının açabileceği şekilde düzenlenen mesajların içeriğini gizleme ve mesajı tekrar eski orijinal haline geri dönüştürme prensipleri ve yöntemlerini içeren gizli dönüşümler bilimidir.

Açık Metin(Plaintext): Gönderilen mesajın şifrelenmemiş halidir. Yani orijinal metindir. Düz metin de denir.

Şifreli Metin(Ciphertext): Gönderilen mesajın bazı dönüşümler uygulanmış halidir.

Anahtar(Key): Sadece gönderici ve alıcının bildiği, mesajı gönderen tarafından kullanılan önemli bilgilerdir.

Şifreleme(Encryption): Bir düz metnin içeriğinin anlaşılmaz hale getirilmesi işlemidir.

Deşifreleme(Decryption): Şifrelenmiş metnin tekrar anlaşılabilir hale getirilmesi işlemidir.

Kriptanaliz: Bir kriptografik sistemin girdi veya çıktılarını inceleyerek bilgi ve anahtar olmaksızın orijinal verilere ulaşmayı amaçlayan yasa dışı analizdir. Aynı zamanda kod kırma (codbreaking) olarak da adlandırılır.

Kriptanalist: Kriptanalizle uğraşanlara denir.

Kriptografik Algoritma: Şifreleme ve deşifreleme işlemlerinde kullanılan matematiksel işlemler bütünüdür.

Simetrik Algoritmalar: Şifreleme ve deşifreleme işlemlerinde aynı anahtarın kullanıldığı algoritmalardır. Gizli anahtarlı algoritmalar da denir.

Asimetrik Algoritmalar: Şifreleme ve deşifreleme işlemlerinde ayrı ayrı anahtarın kullanıldığı, deşifreleme anahtarının şifreleme anahtarından elde edilemediği algoritmalardır. Açık anahtarlı algoritmalar da denir.

Bir şahıs veya grup (entity): Bilgiyi kullanan, kabul eden ya da gönderen kişi veya araçtır.

Bir gönderici (sender): Bir haberleşmede bilgiyi meşru olarak gönderen kişidir.

Bir alıcı(receiver): Haberleşmede bilgiyi alan kişidir.

Saldırgan (Adversary): Taraflar arasındaki haberleşmede, mesajı alan veya gönderen kişi olmayıp güvenliği kırmaya çalışan zararlı kişidir.

Saldırı: Bir kriptosistemin bir kısmını veya tamamını kırmak için başarılı veya başarısız olarak yapılan girişimdir.

Kanal: Bilginin bir şahıstan diğerine taşınmasına yardımcı olan kişi veya araçtır.

$M:$ Mesaj uzayının cümlesi olarak adlandırılır. Tanım alfabesinin sembollerinden oluşur. M 'nin her bir elemanına *düz metin (plaintext)* denir ve P ile gösterilir.

$C:$ Şifreli metin uzayının cümlesidir. Tanım alfabesinin sembollerinden oluşur. C nin her bir elemanına *şifreli metin* denir.

$K:$ Anahtar uzayının bir cümlesini belirtir. K 'nin bir elemanı anahtar olarak adlandırılır. Her bir $e \in K$, M 'den C 'ye birebir örten bir eşlemeyi belirtir ve E_e ile gösterilir.

E_e : Şifreleme fonksiyonu veya şifreleme dönüşümüdür. Her bir $d \in K$, C'den M'ye yani $D_d : C \to M$ birebir-örten bir eşleme belirtir. Buradaki D_d ; deşifreleme fonksiyonu veya deşifreleme dönüşümüdür.

Bir Şifreleme Tasarısı: Her bir $e \in K$ için bir tek $d \in K$ olacak şekilde

$$D_d = E_e^{-1}$$

özelliğini sağlayan

$$\{E_e : e \in K\}$$

şifreleme dönüşümlerinin ve buna karşılık gelen

$$\{\mathrm{D}_d : d \in K\}$$

dönüşümlerinin bir cümlesidir. Burada bütün

$m \in M$ için $D_d(E_e(m)) = m$

dir.

Şifrelemede sıkça karşılaşacağımız bir başka kavram ise *bit* kavramıdır. Bilgisayar sistemlerinde bütün bilgiler, ikilik (binary) sistemde 0 ve 1 şeklinde ifade edilen karakterlerle depolanır. İkilik sistemde her bir basamağa *bit* denir. Örneğin 10010 sayısı beş bittir [2].

Kriptografideki temel bazı tanımları verdik. Şimdi ise konuyu kriptolojik bir yaklaşımla örnek üzerinde açıklayalım.

Kriptografinin amacı güvensiz bir kanal üzerinde genellikle Alice ve Bob olarak adlandırılan iki kişi arasında karşıt kişi Oscar'ın anlayamayacağı biçimde iletişim kurabilmeyi sağlamaktır. Örneğin bu kanal telefon hattı ya da bilgisayar ağı olabilir.

Alice'in Bob'a göndermek istediği bilgi yani açık metin(plaintext), düz bir metin, sayısal bir veri ya da herhangi bir şey olabilir. Yani açık metin tamamıyla keyfi olarak seçilir. Alice ve Bob arasındaki bu iletişim şu şekilde gerçekleşir.

Alice önceden belirlediği bir anahtar kullanarak göndermek istediği keyfi bilgiyi yani açık metni şifreler(encrypt) ve kanal üzerine şifre metin(ciphertext) olarak gönderir. Oscar, kanal üzerindeki bu şifrelenmiş metni gördüğü zaman bunun açık metin halini yani gönderilen halini anlayamaz fakat şifreleme anahtarını önceden bilen Bob şifrelenmiş metni deşifre eder (decrypt) ve açık metni yeniden yapılandırır.

Bu durum aşağıdaki matematiksel notasyonlar kullanılarak tanımlanır. Tanıma göre bir kriptosistem P, C, K, E, D öğeleri ile aşağıdaki şartları sağlamalıdır.

1. P, mümkün olan bütün açık metinleri bulunduran sonlu küme
2. C, mümkün olan bütün şifre metinleri bulunduran sonlu küme
3. K, mümkün olan bütün anahtarları bulunduran sonlu küme
4. Her $k \in K$ için $e_k \in E$ olan bir şifreleme kuralı ve $d_k \in D$ olan bir deşifreleme kuralı vardır. Açık metindeki her $x \in P$ için $d_k(e_k(x)) = x$ dir.

Burada $e_k : P \to C$ ve $d_k : C \to P$ fonksiyonlardır.

Burada temel özellik 4.özelliktir. Bu özellikle anlatılmak istenen e_k kullanılarak bir düz metin(x) şifrelenir ve elde edilen şifreli metin daha sonra d_k kullanılarak çözülür ve orijinal düz metin(x) elde edilir.

Alice ve Bob aşağıdaki protokolü belirli bir kriptosistem kullanarak çalıştıracaklardır. Öncelikle, rastgele bir anahtar seçerler($k \in K$). Anahtar seçme işlemi Alice ve Bob aynı yerdeyken ve Oscar tarafından gözetlenmiyorken ya da Alice ve Bob farklı yerlerde olup güvenli bir kanala eriştikleri zaman yapılabilir.

Daha sonra Alice'in Bob'a güvenli olmayan bir kanal üzerinden bir mesaj göndermek istediğini varsayalım ve bu mesaj örneğin şu şekilde olsun.

$n \geq 1$, $x_i \in P$,$1 \leq i \leq n$ için

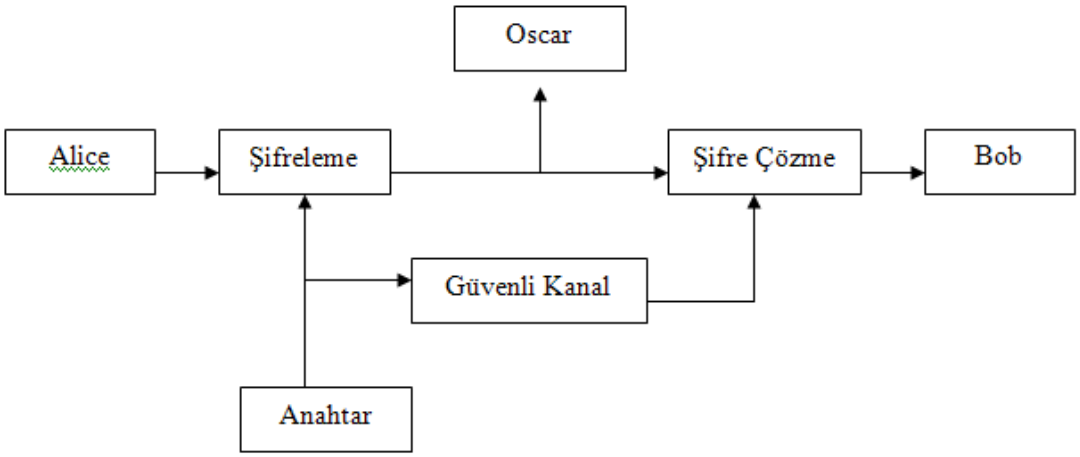
$x = x_1 x_2 \ldots x_n$.

Her x_i önceden belirlenen K anahtarı ile e_k şifreleme kuralı kullanılarak şifrelenir.

Alice, $y_i = e_k(x_i)$, $1 \leq i \leq n$ 'i hesaplar ve sonuç olarak şifreli metni

$y = y_1 y_2 \ldots y_n$

olarak elde ederek kanal üzerine gönderir. Bob $y = y_1 y_2 \ldots y_n$ 'i aldığı zaman d_k şifre çözme kuralını kullanarak şifreli metni çözer ve $x = x_1 x_2 \ldots x_n$ düz metnini elde eder. Bu haberleşme kanalı Şekil 2.1'de gösterilmektedir.



Şekil 2.1. Basit bir haberleşme sistemi [6].

Açıkça görüldüğü üzere, her şifreleme fonksiyonu e_k bire-bir fonksiyon olmalıdır. Aksi halde, şifre çözme belirli bir yöntem kullanılarak gerçekleştirilemez. Örneğin

$$y = e_k(x_1) = e_k(x_2)(x_1 \neq x_2)$$

olduğu bir durumda Bob, y 'nin x_1 ile mi yoksa x_2 ile mi çözüleceğini bilemez. Eğer $P = C$ ise, her şifreleme fonksiyonu bir permütasyondur. Yani, eğer düz metinlerin ve şifreli metinlerin kümesi özdeş ise, her şifreleme fonksiyonu bu kümenin elemanlarını tekrardan düzenler [6].

Bir şifre sistemi algoritmalardan, düz metinlerden, şifre metinlerden ve anahtarlardan oluşur. Kriptografik algoritma, şifreleme algoritması adı da verilen şifreleme ve şifre çözümü için kullanılan matematiksel işlemler topluluğudur.

2.2. KRİPTOGRAFİK ALGORİTMALAR

Tüm modern algoritmalar şifreleme ve şifre çözme işlemlerini kontrol etmek için bir anahtar kullanırlar ve bir mesaj sadece kullanılan anahtar şifreleme anahtarıyla uyuştuğunda çözülebilir. Şifreleme süresince anahtarlı ya da anahtarsız olmak üzere iki farklı yöntem kullanılabilir. Özet (Hash) fonksiyonları, sıkıştırma fonksiyonları

anahtarsız yöntemlere örnek olarak gösterilebilir. Anahtarlı kriptosistemler iki ana başlık altında incelenebilir.

1. Simetrik anahtarlı şifreleme (veya gizli-anahtarlı şifreleme)
2. Asimetrik şifreleme (veya açık-anahtarlı şifreleme)

2.2.1. Simetrik Şifreleme Algoritmaları

Simetrik şifreleme algoritmalarında mesajın şifrelenmesinde ve çözülmesinde tek bir gizli anahtar kullanılır. Şifreleme işlemlerini gerçekleştirdikten sonra şifreli metni alıcıya gönderirken şifreli metinle birlikte gizli anahtarın da alıcıya güvenli bir şekilde gönderilmesi gerekmektedir. Simetrik şifreleme algoritmaları çok hızlı şifreleme ve şifre çözme işlemleri gerçekleştirebildiğinden dolayı günümüzde çok yaygın olarak kullanılmaktadır.

Simetrik anahtarlı kriptosistemler, blok ve akan şifreleme olmak üzere ikiye ayrılır. Simetrik şifreleme algoritmaları şunlardır:

1. Blok şifreleme algoritmaları (AES, DES, IDEA, Skipjack, RC5 …)
2. Akan Şifreleme algoritmaları (RC2, RC4…)

2.2.2. Asimetrik Şifreleme Algoritmaları

Açık anahtarlı kriptosistemlerde ya da başka bir deyişle asitmerik şifrelemede her iki tarafın sahip olduğu açık (e) ve gizli (d) olarak adlandırılan bir anahtar çifti kullanılır. Şifreleme anahtarı olarak kullanılan e' nin gizli olması gerekmez. Açık anahtarlı şifrelemenin altında yatan temel düşünce açık anahtar, e, verildiği halde şifre çözme anahtarı olarak kullanılan d 'nin bulunmasının zor olmasıdır. Açık anahtarlı sistemler sayısal imza ve anahtar değişim protokolleri gibi uygulamalarda kullanılır.

Asimetrik şifreleme algoritmaları şunlardır:

1. RSA
2. El Gamal
3. Eliptik Eğri Sistemleri
4. Diffie-Hellman anahtar belirlemesi
5. Kod-tabanlı Kriptosistemler [7].

Biz bu tezde simetrik yani gizli anahtarlı şifreleme algoritmaları kullanarak çalışmalar yaptık.

Şimdi de bazı klasik simetrik şifreleme yöntemlerinden bahsedelim.

2.3. KLASİK KRİPTOGRAFİ

2.3.1. Kaydırma Şifresi (The Shift Cipher)

Burada, modüler aritmetiğe dayanan kaydırma şifresini tanımlanacaktır.

Tanım 2.3.1. Kaydırma Şifresi (Shift Cipher)

$P=C=K=Z_{29}$ olsun, $0\le k\le 28$ için

$$e_k(x)=(x+k)\bmod 29$$

ve

$$d_k(y)=(y-k)\bmod 29$$

$(x,y)\in Z_{29}$ olarak tanımlanır.

Özel olarak $k=3$ için kriptosistem Caesar şifresi olarak bilinir [6].

Burada kaydırma şifresi kullanarak şifreleme yapmak için kolaylık olması için $\bmod 29$ daki Türk alfabesini kullanacağız. Örneklerde kullanacağımız için bu yazılımı bir çizelge ile gösterelim.

Çizelge 2.1. Türk Alfabesinin $\bmod 29$ 'ya göre tamsayı karşılıkları.

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
15	16	17	18	19	20	21	22	23	24	25	26	27	28

Örnek 2.3.1.

Kaydırma şifresi için $k=11$ ve düz metin de YARIN GELECEĞİZ, olsun.
Öncelikle düz metindeki her harf Çizelge 2.1 kullanılarak tamsayılara çevrilir ve

Y	A	R	I	N	G	E	L	E	C	E	Ğ	İ	Z
27	*0*	*20*	*10*	*16*	*7*	*5*	*14*	*5*	*2*	*5*	*8*	*11*	*28*

elde edilir.

Daha sonra her birine $\bmod 29$ 'ya göre *11* eklenir;

9	*11*	*2*	*21*	*27*	*18*	*16*	*25*	*16*	*13*	*16*	*19*	*22*	*10*

elde edilir.

Elde edilen bu tamsayılar şifreli metni elde etmek üzere Çizelge 2.1 yardımıyla alfabetik karakterlere çevrilir ve

H İ C S Y Ö N Ü N K N P Ş I

şifre metni elde edilir.

H İ C S Y Ö N Ü N K N P Ş I

şifre metni tam sayılı ifadelere çevrilir.

9 11 2 21 27 18 16 25 16 13 16 19 22 10

Sonra mod 29 'ya göre sırayla her sayıdan *11* çıkarılınca

27 0 20 10 16 7 5 14 5 2 5 8 11 28

elde edilir. Tekrar Çizelge 2.1 yardımıyla tam sayılar alfabetik karakterlere çevrilerek

Y A R I N G E L E C E Ğ İ Z

mesajı elde edilir.

2.3.2. Yer Değiştirme Şifresi (The Substitution Cipher)

Diğer bilinen kriptosistemlerden bir tanesi de yer değiştirme şifresidir.

Tanım 2.3.2. Yer Değiştirme Şifresi

$P=C=Z_{29}$ olsun. K ; 29 sembolün yani $0,1,...,28$ in bütün olası permütasyonlarından oluşsun. Her $\pi \in K$ permütasyonu için,
π^{-1} , π 'nin ters permütasyonu olmak üzere;

$$e_{\pi}(x)=\pi(x)$$

ve

$$d_\pi(y) = \pi^{-1}(y)$$

olarak tanımlanır [6]. Düz metin karakterleri büyük harflerle ve şifreli metin karakterleri de küçük harflerle yazılmıştır. Bu durum Çizelge 2.2'de görülmektedir.

Çizelge 2.2. Örnek π fonksiyonu.

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L
c	a	z	u	v	ğ	ç	y	ü	b	d	h	s	ı	j

M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
i	k	n	E	o	p	g	ö	ş	f	m	t	l	r

Şifre çözme fonksiyonu alfabetik sıranın tersidir. Bu durum Çizelge 2.3'te görülmektedir.

Çizelge 2.3. Örnek π^{-1} fonksiyonu.

a	b	c	ç	d	e	f	g	ğ	h	ı	i	j	k	l
B	H	A	F	I	O	U	S	E	İ	K	M	L	N	Y

m	n	o	Ö	p	r	s	ş	t	u	ü	v	y	z
U	O	P	Ş	R	Z	J	T	V	Ç	Ğ	D	G	C

Örnek olarak bu şifre fonksiyon kullanılarak 'afcıöciafjföczcüdr' metni deşifrelenebilir ve BU AKŞAM BULUŞACAĞIZ, düz metni elde edilir.

2.3.3. Affine Şifresi

Afin şifre öteleme şifresinin genel halidir.

Tanım 2.3.3. Affine Şifresi

$P=C=Z_{29}$

ve

$K=\{(a,\mathrm{b})\in Z_{29}\times Z_{29}\ ,\ \gcd(a,29)=1\}$

olsun. $k=(a,\mathrm{b})\in K$ için

$e_k(x)=(ax+\mathrm{b})\bmod 29$

ve

$\mathrm{d}_k(y)=a^{-1}(y-\mathrm{b})\bmod 29$

$(x,y\in Z_{29})$ olarak tanımlanır [6].

Örnek 2.3.3.

2.3.3'te verilen tanıma göre anahtar $k=(6,3)$ olsun. Buna göre,

$6^{-1}\bmod 29=5$

tir. Şifreleme fonksiyonu

$e_k(x)=6x+3$

ve buna bağlı olarak şifre çözme fonksiyonu da

$$d_k(y) = 5(y-3) = 5y - 15$$

olarak elde edilir.

$$\begin{aligned} d_k(e_k(x)) &= d_k(6x+3) \\ &= 5(6x+3) - 15 \\ &= x + 15 - 15 \\ &= x \end{aligned}$$

elde edilir.

2.3.4. Vigenere Şifresi

Vigenere şifresi çoklu alfabeli yer değiştirme şifresidir. Burada, düz metnin her bir harfi ayrı ayrı şifrelenir [8].

Tanım 2.3.4. Vigenere Şifresi

m, pozitif bir tamsayı olsun.

$P = C = K = (Z_{29})^m$ ve $k = (k_1, k_2, ..., k_m)$

anahtar olmak üzere

$$e_k(x_1, x_2, ..., x_m) = (x_1 + k_1, x_2 + k_2, ..., x_m + k_m)$$

ve

$$d_k(y_1, y_2, ..., y_m) = (y_1 - k_1, y_2 - k_2, ..., y_m - k_m)$$

olarak tanımlanır [6].

Örnek 2.3.4.

‘‘ GİZLİ ’’ kelimesini anahtar kelime olarak seçelim ve ‘‘ BU ZARFI AÇMAYINIZ’’ mesajını şifreleyelim. Önce mesajımızı anahtar kelimemizin uzunluğu kadar bloklara ayıralım.

BUZAR FIAÇM AYINI Z

İlk blok şifrelenirken

$$y \equiv x + k \pmod{29}$$

bağıntısı kullanılırsa $x_1 = 1$ (B) , $k_1 = 7$ (G) alınarak $y_1 = 8 \bmod 29$, $x_2 = 24$ (U), $k_2 = 11$ (İ) alınarak $y_2 = 6 \bmod 29$ elde edilir. Benzer olarak y_3, y_4, y_5 bulunursa ilk blok sayısal değerler olarak 8 6 27 14 2 şeklinde elde edilir. Aynı işlemler diğer bloklar için tekrarlanırsa şifre metnimiz sayısal değerler olarak

8 6 27 14 2 13 21 28 17 26 7 9 9 1 21 6

elde edilir. Bu sayılar da harflere dönüştürülürse şifre metni

ĞFYLC KSZOV GHHBS F

olarak ortaya çıkar. Deşifre ederken de

$$x \equiv y - k \pmod{29}$$

bağıntısı kullanılır ve gönderilen mesaj

BUZAR FIAÇM AYINI Z

olur. Yani BU ZARFI AÇMAYINIZ, olarak elde edilir [5].

2.3.5. Hill Şifresi (Blok Şifreler)

Simetrik anahtar blok şifreler kriptografik sistemlerin en önemli ve en iyi bilinen elemanlarıdır. Bir blok şifre açık metni çözebilen ve aynı anda bir bloğu şifreleyen şifreleme tasarısıdır. Başka bir ifadeyle bir blok şifre m blok uzunluğu olmak üzere m - bitlik bir açık metin bloğunu m - bitlik şifre metin bloğuna dönüştüren bir fonksiyondur [2].

Tanım 2.3.5. Hill Şifresi (Blok Şifreler)

$m \geq 2$ olan bir tamsayı olsun. $P = C = (Z_{29})^m$ ve

$$K = \{Z_{29} \text{ da } m \times m \text{ tipinde tersi alınabilen matrisler}\}$$

olsun. Bir k anahtarı için

$$e_k(x) = xk$$

ve

$$d_k(y) = yk^{-1}$$

olarak tanımlanır [6].

Örnek 2.3.5.

$$k = \begin{bmatrix} 11 & 2 & 19 \\ 5 & 23 & 25 \\ 20 & 7 & 1 \end{bmatrix}$$

matrisini kullanarak‘‘İYİ BAYRAMLAR’’mesajını şifreleyelim [5]. Burada k matrisi 3×3 lük olduğundan öncelikle düz metni üç harfli bloklara ayıralım.

İYİ BAY RAM LAR

Şimdi de mesajdaki her bir harfe karşılık gelen tamsayıyı Çizelge 2.1'den elde edelim.

İ	Y	İ	B	A	Y	R	A	M	L	A	R
11	*27*	*11*	*1*	*0*	*27*	*20*	*0*	*15*	*14*	*0*	*20*

Şimdi de k matrisini kullanarak şifreleme bağıntısını elde edelim.

$$C_1 \equiv 11P_1 + 2P_2 + 19P_3$$
$$C_2 \equiv 5P_1 + 23P_2 + 25P_3$$
$$C_3 \equiv 20P_1 + 7P_2 + P_3$$

Yukarıdaki her blok bu şifreleme bağıntısıyla şifrelenirse

7 23 14 *2 13 18* *12 11 9* *12 19 10*

elde edilir.

Son olarak her tamsayıya karşılık gelen harf Çizelge 2.1'den elde edilirse şifre metin

G T L C K Ö J İ H J P I

olarak elde edilir.

2.3.6. Permütasyon Şifresi

Buraya kadar bahsedilen bütün kriptosistemler kaydırmayı içeriyordu. Düz metin karakterleri yerine, farklı şifreli metin karakterleri konuluyordu. Permütasyon şifresinde ise düz metin karakterleri değiştirilmez; ancak, tekrardan düzenlenerek yerleri değiştirilir [9].

Tanım 2.3.6. Permütasyon Şifresi

m herhangi bir pozitif tamsayı olsun. $P=C=(Z_{29})^m$ ve K , $\{1,...,m\}$ 'in tüm permütasyonlarından oluşsun. Bir π anahtarı için,

$$e_\pi(x_1,...,x_m)=(x_\pi(1),\ ...,\ x_\pi(m))$$

$$d_\pi(y_1,...,y_m)=(y_{\pi^{-1}}(1),\ ...,\ y_{\pi^{-1}}(m))$$

Buradaki π^{-1}, π permütasyonunun tersidir [6].

Örnek 2.3.6.

$m=6$ ve anahtarda aşağıdaki gibi π permütasyonu olsun.

x	1	2	3	4	5	6
$\pi\ (x)$	3	5	1	6	4	2

Bu durumda π permütasyonunun tersi de π^{-1} permütasyonu ise $m=6$ için

x	1	2	3	4	5	6
$\pi^{-1}\ (x)$	3	6	1	5	2	4

olur. Göndereceğimiz mesaj BU KRİPTOSİSTEM ÇOK GÜVENLİ, olsun.

Öncelikle $m=6$ olduğu için mesajı 6 lı parçalara ayıralım.

BUKRİP TOSİST EMÇOKG ÜVENLİ

Şimdi de π permütasyonuna göre mesajı yeniden yapılandırırsak

KİBPRU SSTTİO ÇKEGOM ELÜİNV

olur. Yani şifre metin

KİBPRUSSTTİOÇKEGOMELÜİNV

olarak elde edilir. Şimdi şifrelenmiş metni deşifre edelim. Yine öncelikle şifre metni 6 lı parçalara ayıralım.

KİBPRU SSTTİO ÇKEGOM ELÜİNV

ve benzer şekilde π^{-1} permütasyonuyla şifrelenmiş metni deşifre edelim.

BUKRİP TOSİST EMÇOKG ÜVENLİ

Son olarak aradaki boşlukları atarsak gönderilen mesaj BU KRİPTOSİSTEM ÇOK GÜVENLİ, olarak elde edilir.

2.3.7. Akış Şifreleri (Stream Ciphers)

Simetrik anahtar şifreleme tasarılarının en önemli sınıflarından birini akış şifreleri oluşturur. Birbirine eş uzunlukta bloklara sahip çok basit blok şifreler oldukları da söylenebilir [2].

Tanım 2.3.7. Akış Şifreleri (Stream Ciphers)

Akış şifresi g fonksiyonu ve (P, C, K, L, E, D) öğeleri ile birlikte aşağıdaki şartları sağlamalıdır.

1. P, mümkün olan bütün açık metinleri bulunduran sonlu küme
2. C, mümkün olan bütün şifre metinleri bulunduran sonlu küme
3. K, mümkün olan bütün anahtarları bulunduran sonlu küme
4. L, anahtar akış alfabesi(keystream alphabet) olarak adlandırılan sonlu küme

5. g , anahtar akış üretecidir(keystream generator) g , girdi olarak bir K anahtarını alır ve her $i \geq 1$ için $z_i \in L$ olmak üzere anahtar akışı olarak adlandırılan z_1 ... sonsuz dizisini üretir.
6. Her $z \in L$ için, $e_z \in E$ olan bir şifreleme kuralı ve $d_z(e_z(x)) = x$ olan bir deşifreleme kuralı vardır. $e_z : P \to C$ ve $d_z : C \to P$ açık metindeki her $x \in P$ için $d_z(e_z(x)) = x$ olacak şekilde fonksiyonlardır [6].

En iyi bilinen akış şifresi Vernam Şifresidir.

2.3.7.1. Vernam Şifresi

Akan şifreler çoğunlukla ikili alfabelerle gösterilirler. Bu durumda özel olarak vernam şifresi olarak adlandırılırlar. Örneğin, $P = C = L = Z_2$. Bu durumda, şifreleme ve şifre çözme işlemleri:

$$e_z(x) = (x + \mathrm{z}) \bmod 2$$

ve

$$d_z(y) = (y + \mathrm{z}) \bmod 2$$

olur [6].

Akan şifre sistemleri, mesajın her karakterini (bitini) ayrı ayrı şifreler. Şifreleme işlemi mesaj uzunluğunda bir anahtar kullanılarak yapılır. Anahtarın her biti mesajın her bitiyle $\bmod 2$ de karşılıklı toplanır. Bu işleme XOR işlemi denir ve $\oplus$ ile gösterilir [3].

Eğer anahtar keyfi seçilmiş ve bir daha kullanılmaz ise Vernam Şifresi *tek kullanımlık şerit (One – Time - Pad)* veya *tek kullanımlık sistem* olarak adlandırılır. Tek kullanımlık şerit yollanacak mesaj kadar uzun olan bir anahtardır. Şeritteki her

harf rastgele seçilmiş olmalıdır. Mesajdaki her harf ve şeritteki o harfe karşılık gelen harf sayısal değerlerine çevrilip, toplanır. Şifreyi çözmek için aynı anahtar şeridi ile işlem tersinden yapılır; bu sefer şeritteki harfler mesajdaki harflerden çıkarılır. Toplama ve çıkarma işlemleri yine modüler aritmetiğe dayalı olarak mod 29 da yapılır [2].

Örnek 2.3.7.1.

Düz metin : ŞİFRELERGİZLİVEÖNEMLİİLETİLERTAŞIR

ve

Şerit : KSLDMELRKMMNDILSOLİMMBCPSFGKCNBÜPK

olsun.

O halde yukarıdaki tanımdan faydalanarak şifre metni

Şifre metin : FÇRURPPİRVLBMGPIDPVAVJNUMOSÖŞIBÖAD

olur.

BÖLÜM 3

FİBONACCİ KODLARI VE VARYASYONLARI

3.1. FİBONACCİ DİZİSİ VE FİBONACCİ KODLARI

Fibonacci kodu, pozitif tamsayıları sadece 0 ve 1 rakamlarını kullanmak suretiyle (ikili temsil) kodlayan, Fibonacci sayılarına dayalı evrensel bir kodlamadır. m, mertebe olmak üzere, $m \geq 2$ için Fibonacci sayıları $F_i^{(m)}$ ile gösterilir ve sınır koşulları $F_0^{(m)} = 1$ ve $-m < n < 0$ için $F_n^{(m)} = 0$ olmak üzere $n > 0$ için Fibonacci sayıları

$$F_n^{(m)} = F_{n-1}^{(m)} + F_{n-2}^{(m)} + ... + F_{n-m}^{(m)}$$

olarak tanımlanır [10]. Zeckhendorf Teoremi her pozitif tamsayının ard arda gelmeyen Fibonacci sayılarının toplamı olarak tek temsili olduğunu söyler [11]. Şimdi ilk olarak $2.$*mertebeden* Standart Fibonacci sayılarını oluşturalım.

B pozitif bir tamsayı olsun. B sayısı, $B = \sum_{i=1}^{r} c_i F_i^{(m)}$ olacak şekilde r uzunluğundaki $c_1 c_2 ... c_r$ dizisiyle temsil edilebilir. Bu temsil, şu şartlar kullanılırsa tektir: öncelikle B ye eşit ya da B den küçük, en büyük Fibonacci sayısı $F_r^{(m)}$ bulunur. Sonra, $B - F_r^{(m)}$ tekrarlanarak devam edilir. Örneğin $16 = 3 + 13$ olduğundan, 16 sayısının $2.$ *mertebeden* Fibonacci temsili 001001 olur. Bu durumun sonucu olarak bu toplamda ardışık Fibonacci sayıları kullanılmaz. Yani pozitif tamsayıların $2.$ *mertebeden* Fibonacci temsilinde ardışık 1 bit bulunmaz.

Şimdi de bu durumu daha yüksek mertebelere genelleştirelim. B sayısı, $B = \sum_{i=1}^{s} d_i F_i^{(m)}$ olacak şekilde yukarıdaki prosedür kullanılarak tanımlanırsa s uzunluğundaki $d_1 d_2 \ldots d_{s-1} d_s$ dizisiyle tek türlü temsil edilebilir. Bu durumun sonucunda da bu temsilde ardışık m tane 1 bit bulunmaz [10].

Çizelge 3.1. Bazı küçük sayıların standart Fibonacci temsili.

n	2 Zechendorf ($m = 2$ için Standart Fibonacci temsili)	3 Zechendorf ($m = 3$ için Standart Fibonacci temsili)
1	1	1
2	01	01
3	001	11
4	101	001
5	0001	101
6	1001	011
7	0101	0001
8	00001	1001
9	10001	0101
10	01001	1101
11	00101	0011
12	10101	1011
13	000001	00001
14	100001	10001
15	010001	01001

Mertebesi m olan n pozitif tamsayısının Fibonacci kodunu oluşturmak için n'in sonuna $(m-1)$ tane 1 eklenir.

Çizelge 3.2. Bazı küçük sayıların standart Fibonacci kodu.

n	$m = 2$ için Standart Fibonacci kodu	$m = 3$ için Standart Fibonacci kodu
1	11	111
2	011	0111
3	0011	1111
4	1011	00111
5	00011	10111
6	10011	01111
7	01011	000111
8	000011	100111
9	100011	010111
10	010011	110111
11	001011	001111
12	101011	101111
13	0000011	0000111
14	1000011	1000111
15	0100011	0100111

Pozitif tamsayıların Fibonacci kodunun şifrelemeye de uygulanabilen ve aynı zamanda *Gopala-Hemachandra (GH)* kodu olarak da adlandırılabilen çeşitli varyasyonları vardır. Şimdi de *Gopala-Hemachandra (GH)* dizisini tanımlayalım ve bu varyasyonları inceleyelim.

3.2. *GOPALA-HEMACHANDRA (GH)* DİZİSİ VE *GOPALA HEMACHANDRA (GH)* KODLARI

2. *mertebeden GH* dizisi; n pozitif tamsayı, a negatif tamsayı ve $b = 1-a$ olmak üzere

$$GH_a^{(2)}(n) = \{a, b, a+b, a+2b, 2a+3b, 3a+5b, \ ...\}$$

yani

$$GH_a^{(2)}(1) = a \ (a \in \square^-); \ GH_a^{(2)}(2) = 1-a$$

ve $n \geq 3$ için

$$GH_a^{(2)}(n) = GH_a^{(2)}(n-1) + GH_a^{(2)}(n-2)$$

olarak tanımlanmıştır. $a = -2$ için

$$\{-2, 3, 1, 4, 5, 9, 14, 23, \ldots\}$$

elde edilmiştir [12].

GH dizilerinde a 'nın farklı değerleri için farklı sıralamalar elde edilir. Daykin sadece Standart Fibonacci sıralamasında bütün pozitif tamsayıların bir tek Zeckendorf temsili olduğunu kanıtlamıştır [13]. Ne var ki bu durum, Fibonacci sıralamasının bir varyasyonu olan *GH* sıralaması için geçerli değildir. Yani *GH*

dizisine göre bazı pozitif tamsayıların birden fazla temsili olabilir. Örneğin hem $16=3+4+9$ hem de $16=-2+4+14$ olduğundan 16 sayısının 2. *mertebeden GH* temsili sırasıyla hem 010101 hem de 1001001 olur.

$a=-5$ için 2. *mertebeden GH* dizisi

$$GH_{-5}^{(2)}(n)=\{-5,6,1,7,8,15,23,38,\ldots\}$$

olarak elde edilmiş ve $n=5,12$ pozitif tamsayılarının *GH* kodunun mevcut olmadığı*(N/A)* gösterilmiştir [14].

Bu bölümde biz de 2. *mertebeden GH* dizisinin tanımından faydalanarak öncelikle 3. *mertebeden GH* dizisini ; n pozitif tamsayı, a negatif tamsayı ve $b=1-a$ olmak üzere

$$GH_a^{(3)}(n)=\{a,b,a+b,2a+2b,3a+4b,6a+7b,11a+13b,20a+24b,\ ...\}$$

yani

$$GH_a^{(3)}(1)=a\ (a\in\mathbb{Z}^-);\ GH_a^{(3)}(2)=1-a\ ;GH_a^{(3)}(3)\ =1$$

ve $n\geq 4$ için

$$GH_a^{(3)}(n)=GH_a^{(3)}(n-1)+GH_a^{(3)}(n-2)+GH_a^{(3)}(n-3)$$

olarak tanımladık. Örneğin $a=-2$ için

$$GH_{-2}^{(3)}(n)=\{-2,3,1,2,6,9,17,32,\ ...\}$$

elde ettik.

Daha sonra bu dizi yardımıyla pozitif tamsayıların *GH* kodlarını elde ettik.

Ayrıca biz $a=-11$ için 3. *mertebeden GH* dizisini

$$GH_{-11}^{(3)}(n)=\{-11,12,1,2,15,18,\ldots\}$$

olarak elde ettik ve $n=11$ pozitif tamsayısının *GH* kodunun mevcut olmadığı*(N/A)* sonucuna ulaştık.

Ayrıca M. Basu ve B. Prasad $-20\le a\le -2$ için $n=1,2,\ldots,100$ pozitif tamsayılarının 2. *mertebeden GH* kodlarını ya da ulaşılamayan değerleri*(N/A)* tablo ile göstermişler ve tablolardan sonuçlar elde etmişlerdir [12].

Biz de bu durumdan yola çıkarak bu çalışmada $-20\le a\le -2$ için $n=1,2,\ldots,100$ pozitif tamsayılarının 3. *mertebeden GH* kodlarını ya da ulaşılamayan değerleri*(N/A)* Çizelge 3.3-3.10'da gösterdik ve bu çizelgelerden sonuçlar elde ettik.

Çizelge 3.3. $1 \le n \le 50$ ve $-6 \le a \le -2$ için n pozitif tamsayılarının 3. *mertebeden* *GH* kodları.

	$GH_{-2}^{(3)}$	$GH_{-3}^{(3)}$	$GH_{-4}^{(3)}$	$GH_{-5}^{(3)}$	$GH_{-6}^{(3)}$
1	00111	00111	00111	00111	00111
2	000111	000111	000111	000111	000111
3	0111	001111	001111	001111	001111
4	1000111	0111	1000111	1000111	1000111
5	1010111	1010111	0111	1010111	1010111
6	0000111	1001111	1001111	0111	1001111
7	10000111	0000111	10000111	10000111	0111
8	10100111	10100111	0000111	10100111	10100111
9	00000111	10010111	10010111	0000111	10010111
10	11000111	00000111	10110111	10110111	0000111
11	00010111	11000111	00000111	0001111	1100111
12	11010111	00010111	11000111	00000111	0001111
13	10001111	11010111	00010111	11000111	00000111
14	10101111	10001111	11010111	00010111	11000111
15	100000111	10101111	10001111	11010111	00010111
16	101000111	100000111	10101111	10001111	11010111
17	000000111	101000111	100000111	10101111	10001111
18	110000111	100100111	101000111	100000111	10101111
19	000100111	000000111	100100111	101000111	100000111
20	110100111	110000111	101100111	100100111	101000111
21	100010111	000100111	000000111	101100111	100100111
22	101010111	110100111	110000111	11001111	101100111
23	100110111	100010111	000100111	000000111	00001111
24	100001111	101010111	110100111	110000111	11001111
25	101001111	100110111	100010111	000100111	000000111
26	100101111	100001111	101010111	110100111	110000111
27	110001111	101001111	100110111	100010111	000100111
28	000101111	100101111	100001111	101010111	110100111
29	110101111	101101111	101001111	100110111	100010111
30	1000000111	110001111	100101111	100001111	101010111
31	1010000111	000101111	101101111	101001111	100110111
32	0000000111	110101111	000001111	100101111	100001111
33	1100000111	1000000111	110001111	101101111	101001111
34	0001000111	1010000111	000101111	000110111	100101111
35	1101000111	1001000111	110101111	000001111	101101111
36	1000100111	0000000111	1000000111	110001111	001010111
37	1010100111	1100000111	1010000111	000101111	000110111
38	1001100111	0001000111	1001000111	110101111	000001111
39	1000010111	1101000111	1011000111	1000000111	110001111
40	1010010111	1000100111	0000000111	1010000111	000101111
41	1001010111	1010100111	1100000111	1001000111	110101111
42	1100010111	1001100111	0001000111	1011000111	1000000111
43	0001010111	1000010111	1101000111	010101111	1010000111
44	1101010111	1010010111	1000100111	0000000111	1001000111
45	1000110111	1001010111	1010100111	1100000111	1011000111
46	1010110111	1011010111	1001100111	0001000111	011001111
47	1000001111	1100010111	1000010111	1101000111	010101111
48	1010001111	0001010111	1010010111	1000100111	0000000111
49	1001001111	1101010111	1001010111	1010100111	1100000111
50	1100001111	1000110111	1011010111	1001100111	0001000111

Çizelge 3.4. $50 \le n \le 100$ ve $-6 \le a \le -2$ için n pozitif tamsayılarının 3. *mertebeden* *GH* kodları.

	$GH_{-2}^{(3)}$	$GH_{-3}^{(3)}$	$GH_{-4}^{(3)}$	$GH_{-5}^{(3)}$	$GH_{-6}^{(3)}$
51	0001001111	1010110111	0000010111	1000010111	1101000111
52	1101001111	1000001111	1100010111	1010010111	1000100111
53	1000101111	1010001111	0001010111	1001010111	1010100111
54	1010101111	1001001111	1101010111	1011010111	1001100111
55	1001101111	1011001111	1000110111	0001100111	1000010111
56	10000000111	1100001111	1010110111	0000010111	1010010111
57	10100000111	0001001111	1000001111	1100010111	1001010111
58	00000000111	1101001111	1010001111	0001010111	1011010111
59	11000000111	1000101111	1001001111	1101010111	0010100111
60	00010000111	1010101111	1011001111	1000110111	0001100111
61	11010000111	1001101111	0000001111	1010110111	0000010111
62	10001000111	10000000111	1100001111	1000001111	1100010111
63	10101000111	10100000111	0001001111	1010001111	0001010111
64	10011000111	10010000111	1101001111	1001001111	1101010111
65	10000100111	00000000111	1000101111	1011001111	1000110111
66	10100100111	11000000111	1010101111	0010110111	1010110111
67	10010100111	00010000111	1001101111	0000001111	1000001111
68	11000100111	11010000111	10000000111	1100001111	1010001111
69	00010100111	10001000111	10100000111	0001001111	1001001111
70	11010100111	10101000111	10010000111	1101001111	1011001111
71	10001100111	10011000111	10110000111	1000101111	0000110111
72	10101100111	10000100111	00000000111	1010101111	0010110111
73	10000010111	10100100111	11000000111	1001101111	0000001111
74	10100010111	10010100111	00010000111	10000000111	1100001111
75	10010010111	10110100111	11010000111	10100000111	0001001111
76	11000010111	11000100111	10001000111	10010000111	1101001111
77	00010010111	00010100111	10101000111	10110000111	1000101111
78	11010010111	11010100111	10011000111	0001101111	1010101111
79	10001010111	10001100111	10000100111	00000000111	1001101111
80	10101010111	10101100111	10100100111	11000000111	10000000111
81	10011010111	10000010111	10010100111	00010000111	10100000111
82	10000110111	10100010111	10110100111	11010000111	10010000111
83	10100110111	10010010111	00000100111	10001000111	10110000111
84	10010110111	10110010111	11000100111	10101000111	1100101111
85	11000110111	11000010111	00010100111	10011000111	0001101111
86	00010110111	00010010111	11010100111	10000100111	00000000111
87	11010110111	11010010111	10001100111	10100100111	11000000111
88	10000001111	10001010111	10101100111	10010100111	00010000111
89	10100001111	10101010111	10000010111	10110100111	11010000111
90	10010001111	10011010111	10100010111	00011000111	10001000111
91	11000001111	10000110111	10010010111	00000100111	10101000111
92	00010001111	10100110111	10110010111	11000100111	10011000111
93	11010001111	10010110111	00000010111	00010100111	10000100111
94	10001001111	10110110111	11000010111	11010100111	10100100111
95	10101001111	11000110111	00010010111	10001100111	10010100111
96	10011001111	00010110111	11010010111	10101100111	10110100111
97	10000101111	11010110111	10001010111	10000010111	00101000111
98	10100101111	10000001111	10101010111	10100010111	00011000111
99	10010101111	10100001111	10011010111	10010010111	00000100111
100	11000101111	10010001111	10000110111	10110010111	11000100111

Çizelge 3.5. $1 \le n \le 50$ ve $-10 \le a \le -7$ için n pozitif tamsayılarının 3. *mertebeden GH* kodları.

	$GH_{-7}^{(3)}$	$GH_{-8}^{(3)}$	$GH_{-9}^{(3)}$	$GH_{-10}^{(3)}$
1	00111	00111	00111	00111
2	000111	000111	000111	000111
3	001111	001111	001111	001111
4	1000111	1000111	1000111	1000111
5	1010111	1010111	1010111	1010111
6	1001111	1001111	1001111	1001111
7	10000111	10000111	10000111	10000111
8	0111	10100111	10100111	10100111
9	10010111	0111	10010111	10010111
10	10110111	10110111	0111	10110111
11	0000111	010111	01111	0111
12	1100111	0000111	010111	01111
13	0001111	1100111	0000111	010111
14	00000111	0001111	1100111	0000111
15	11000111	00000111	0001111	1100111
16	00010111	11000111	00000111	0001111
17	11010111	00010111	11000111	00000111
18	10001111	11010111	00010111	11000111
19	10101111	10001111	11010111	00010111
20	100000111	10101111	10001111	11010111
21	101000111	100000111	10101111	10001111
22	100100111	101000111	100000111	10101111
23	101100111	100100111	101000111	100000111
24	01010111	101100111	100100111	101000111
25	00001111	01100111	101100111	100100111
26	11001111	01010111	01000111	101100111
27	000000111	00001111	01100111	0101111
28	110000111	11001111	01010111	01000111
29	000100111	000000111	00001111	01100111
30	110100111	110000111	11001111	01010111
31	100010111	000100111	000000111	00001111
32	101010111	110100111	110000111	11001111
33	100110111	100010111	000100111	000000111
34	100001111	101010111	110100111	110000111
35	101001111	100110111	100010111	000100111
36	100101111	100001111	101010111	110100111
37	101101111	101001111	100110111	100010111
38	000010111	100101111	100001111	101010111
39	001010111	101101111	101001111	100110111
40	000110111	010100111	100101111	100001111
41	000001111	000010111	101101111	101001111
42	110001111	001010111	011000111	100101111
43	000101111	000110111	010100111	101101111
44	110101111	000001111	000010111	010000111
45	1000000111	110001111	001010111	011000111
46	1010000111	000101111	000110111	010100111
47	1001000111	110101111	000001111	000010111
48	1011000111	1000000111	110001111	001010111
49	010001111	1010000111	000101111	000110111
50	011001111	1001000111	110101111	000001111

Çizelge 3.6. $50 \le n \le 100$ ve $-10 \le a \le -7$ için n pozitif tamsayılarının 3. *mertebeden GH* kodları.

	$GH_{-7}^{(3)}$	$GH_{-8}^{(3)}$	$GH_{-9}^{(3)}$	$GH_{-10}^{(3)}$
51	010101111	1011000111	1000000111	110001111
52	0000000111	010110111	1010000111	000101111
53	1100000111	010001111	1001000111	110101111
54	0001000111	011001111	1011000111	1000000111
55	1101000111	010101111	011010111	1010000111
56	1000100111	0000000111	010110111	1001000111
57	1010100111	1100000111	010001111	1011000111
58	1001100111	0001000111	011001111	010010111
59	1000010111	1101000111	010101111	011010111
60	1010010111	1000100111	0000000111	010110111
61	1001010111	1010100111	1100000111	010001111
62	1011010111	1001100111	0001000111	011001111
63	0000100111	1000010111	1101000111	010101111
64	0010100111	1010010111	1000100111	0000000111
65	0001100111	1001010111	1010100111	1100000111
66	0000010111	1011010111	1001100111	0001000111
67	1100010111	0101000111	1000010111	1101000111
68	0001010111	0000100111	1010010111	1000100111
69	1101010111	0010100111	1001010111	1010100111
70	1000110111	0001100111	1011010111	1001100111
71	1010110111	0000010111	0110000111	1000010111
72	1000001111	1100010111	0101000111	1010010111
73	1010001111	0001010111	0000100111	1001010111
74	1001001111	1101010111	0010100111	1011010111
75	1011001111	1000110111	0001100111	0100000111
76	0101010111	1010110111	0000010111	0110000111
77	0000110111	1000001111	1100010111	0101000111
78	0010110111	1010001111	0001010111	0000100111
79	0000001111	1001001111	1101010111	0010100111
80	1100001111	1011001111	1000110111	0001100111
81	0001001111	0110010111	1010110111	0000010111
82	1101001111	0101010111	1000001111	1100010111
83	1000101111	0000110111	1010001111	0001010111
84	1010101111	0010110111	1001001111	1101010111
85	1001101111	0000001111	1011001111	1000110111
86	10000000111	1100001111	0100010111	1010110111
87	10100000111	0001001111	0110010111	1000001111
88	10010000111	1101001111	0101010111	1010001111
89	10110000111	1000101111	0000110111	1001001111
90	0000101111	1010101111	0010110111	1011001111
91	1100101111	1001101111	0000001111	0101100111
92	0001101111	10000000111	1100001111	0100010111
93	00000000111	10100000111	0001001111	0110010111
94	11000000111	10010000111	1101001111	0101010111
95	00010000111	10110000111	1000101111	0000110111
96	11010000111	0101001111	1010101111	0010110111
97	10001000111	0000101111	1001101111	0000001111
98	10101000111	1100101111	10000000111	1100001111
99	10011000111	0001101111	10100000111	0001001111
100	10000100111	00000000111	10010000111	1101001111

Çizelge 3.7. $1 \le n \le 50$ ve $-15 \le a \le -11$ için n pozitif tamsayılarının 3. *mertebeden GH* kodları.

	$GH_{-11}^{(3)}$	$GH_{-12}^{(3)}$	$GH_{-13}^{(3)}$	$GH_{-14}^{(3)}$	$GH_{-15}^{(3)}$
1	00111	00111	00111	00111	00111
2	000111	000111	000111	000111	000111
3	001111	001111	001111	001111	001111
4	1000111	1000111	1000111	1000111	1000111
5	1010111	1010111	1010111	1010111	1010111
6	1001111	1001111	1001111	1001111	1001111
7	10000111	10000111	10000111	10000111	10000111
8	10100111	10100111	10100111	10100111	10100111
9	10010111	10010111	10010111	10010111	10010111
10	10110111	10110111	10110111	10110111	10110111
11	N/A	N/A	N/A	N/A	N/A
12	0111	N/A	N/A	N/A	N/A
13	01111	0111	N/A	N/A	N/A
14	010111	01111	0111	N/A	N/A
15	0000111	010111	01111	0111	N/A
16	1100111	0000111	010111	01111	0111
17	0001111	1100111	0000111	010111	01111
18	00000111	0001111	1100111	0000111	010111
19	11000111	00000111	0001111	1100111	0000111
20	00010111	11000111	00000111	0001111	1100111
21	11010111	00010111	11000111	00000111	0001111
22	10001111	11010111	00010111	11000111	00000111
23	10101111	10001111	11010111	00010111	11000111
24	100000111	10101111	10001111	11010111	00010111
25	101000111	100000111	10101111	10001111	11010111
26	100100111	101000111	100000111	10101111	10001111
27	101100111	100100111	101000111	100000111	10101111
28	0110111	101100111	100100111	101000111	100000111
29	0101111	0100111	101100111	100100111	101000111
30	01000111	0110111	N/A	101100111	100100111
31	01100111	0101111	0100111	N/A	101100111
32	01010111	01000111	0110111	N/A	N/A
33	00001111	01100111	0101111	0100111	N/A
34	11001111	01010111	01000111	0110111	N/A
35	000000111	00001111	01100111	0101111	0100111
36	110000111	11001111	01010111	01000111	0110111
37	000100111	000000111	00001111	01100111	0101111
38	110100111	110000111	11001111	01010111	01000111
39	100010111	000100111	000000111	00001111	01100111
40	101010111	110100111	110000111	11001111	01010111
41	100110111	100010111	000100111	000000111	00001111
42	100001111	101010111	110100111	110000111	11001111
43	101001111	100110111	100010111	000100111	000000111
44	100101111	100001111	101010111	110100111	110000111
45	101101111	101001111	100110111	100010111	000100111
46	01101111	100101111	100001111	101010111	110100111
47	010000111	101101111	101001111	100110111	100010111
48	011000111	01001111	100101111	100001111	101010111
49	010100111	01101111	101101111	101001111	100110111
50	000010111	010000111	N/A	100101111	100001111

Çizelge 3.8. $50 \le n \le 100$ ve $-15 \le a \le -11$ için n pozitif tamsayılarının 3. *mertebeden GH* kodları.

	$GH_{-11}^{(3)}$	$GH_{-12}^{(3)}$	$GH_{-13}^{(3)}$	$GH_{-14}^{(3)}$	$GH_{-15}^{(3)}$
51	001010111	011000111	01001111	101101111	101001111
52	000110111	010100111	01101111	N/A	100101111
53	000001111	000010111	010000111	N/A	101101111
54	110001111	001010111	011000111	01001111	N/A
55	000101111	000110111	010100111	01101111	N/A
56	110101111	000001111	000010111	010000111	N/A
57	1000000111	110001111	001010111	011000111	01001111
58	1010000111	000101111	000110111	010100111	01101111
59	1001000111	110101111	000001111	000010111	010000111
60	1011000111	1000000111	110001111	001010111	011000111
61	N/A	1010000111	000101111	000110111	010100111
62	010010111	1001000111	110101111	000001111	000010111
63	011010111	1011000111	1000000111	110001111	001010111
64	010110111	N/A	1010000111	000101111	000110111
65	010001111	N/A	1001000111	110101111	000001111
66	011001111	010010111	1011000111	1000000111	110001111
67	010101111	010110111	N/A	1010000111	000101111
68	0000000111	010110111	N/A	1001000111	110101111
69	1100000111	010001111	N/A	1011000111	1000000111
70	0001000111	011001111	010010111	N/A	1010000111
71	1101000111	010101111	011010111	N/A	1001000111
72	1000100111	0000000111	010110111	N/A	1011000111
73	1010100111	1100000111	010001111	N/A	N/A
74	1001100111	0001000111	011001111	010010111	N/A
75	1000010111	1101000111	010101111	011010111	N/A
76	1010010111	1000100111	0000000111	010110111	N/A
77	1001010111	1010100111	1100000111	010001111	N/A
78	1011010111	1001100111	0001000111	011001111	010010111
79	N/A	1000010111	1101000111	010101111	011010111
80	0100000111	1010010111	1000100111	0000000111	010110111
81	0110000111	1001010111	1010100111	1100000111	010001111
82	0101000111	1011010111	1001100111	0001000111	011001111
83	0000100111	N/A	1000010111	1101000111	010101111
84	0010100111	N/A	1010010111	1000100111	0000000111
85	0001100111	0100000111	1001010111	1010100111	1100000111
86	0000010111	0110000111	1011010111	1001100111	0001000111
87	1100010111	0101000111	N/A	1000010111	1101000111
88	0001010111	0000100111	N/A	1010010111	1000100111
89	1101010111	0010100111	N/A	1001010111	1010100111
90	1000110111	0001100111	0100000111	1011010111	1001100111
91	1010110111	0000010111	0110000111	N/A	1000010111
92	1000001111	1100010111	0101000111	N/A	1010010111
93	1010001111	0001010111	0000100111	N/A	1001010111
94	1001001111	1101010111	0010100111	N/A	1011010111
95	1011001111	1000110111	0001100111	0100000111	N/A
96	0110100111	1010110111	0000010111	0110000111	N/A
97	N/A	1000001111	1100010111	0101000111	N/A
98	0100010111	1010001111	0001010111	0000100111	N/A
99	0110010111	1001001111	1101010111	0010100111	N/A
100	0101010111	1011001111	1000110111	0001100111	0100000111

Çizelge 3.9. $1 \le n \le 50$ ve $-20 \le a \le -16$ için n pozitif tamsayılarının 3. *mertebeden* *GH* kodları.

	$GH_{-16}^{(3)}$	$GH_{-17}^{(3)}$	$GH_{-18}^{(3)}$	$GH_{-19}^{(3)}$	$GH_{-20}^{(3)}$
1	00111	00111	00111	00111	00111
2	000111	000111	000111	000111	000111
3	001111	001111	001111	001111	001111
4	1000111	1000111	1000111	1000111	1000111
5	1010111	1010111	1010111	1010111	1010111
6	1001111	1001111	1001111	1001111	1001111
7	10000111	10000111	10000111	10000111	10000111
8	10100111	10100111	10100111	10100111	10100111
9	10010111	10010111	10010111	10010111	10010111
10	10110111	10110111	10110111	10110111	10110111
11	N/A	N/A	N/A	N/A	N/A
12	N/A	N/A	N/A	N/A	N/A
13	N/A	N/A	N/A	N/A	N/A
14	N/A	N/A	N/A	N/A	N/A
15	N/A	N/A	N/A	N/A	N/A
16	N/A	N/A	N/A	N/A	N/A
17	0111	N/A	N/A	N/A	N/A
18	01111	0111	N/A	N/A	N/A
19	010111	01111	0111	N/A	N/A
20	0000111	010111	01111	0111	N/A
21	1100111	0000111	010111	01111	0111
22	0001111	1100111	0000111	010111	01111
23	00000111	0001111	1100111	0000111	010111
24	11000111	00000111	0001111	1100111	0000111
25	00010111	11000111	00000111	0001111	1100111
26	11010111	00010111	11000111	00000111	0001111
27	10001111	11010111	00010111	11000111	00000111
28	10101111	10001111	11010111	00010111	11000111
29	100000111	10101111	10001111	11010111	00010111
30	101000111	100000111	10101111	10001111	11010111
31	100100111	101000111	100000111	10101111	10001111
32	101100111	100100111	101000111	100000111	10101111
33	N/A	101100111	100100111	101000111	100000111
34	N/A	N/A	101100111	100100111	101000111
35	N/A	N/A	N/A	101100111	100100111
36	N/A	N/A	N/A	N/A	101100111
37	0100111	N/A	N/A	N/A	N/A
38	0110111	N/A	N/A	N/A	N/A
39	0101111	0100111	N/A	N/A	N/A
40	01000111	0110111	N/A	N/A	N/A
41	01100111	0101111	0100111	N/A	N/A
42	01010111	01000111	0110111	N/A	N/A
43	00001111	01100111	0101111	0100111	N/A
44	11001111	01010111	01000111	0110111	N/A
45	000000111	00001111	01100111	0101111	0100111
46	110000111	11001111	01010111	01000111	0110111
47	000100111	000000111	00001111	01100111	0101111
48	110100111	110000111	11001111	01010111	01000111
49	100010111	000100111	000000111	00001111	01100111
50	101010111	110100111	110000111	11001111	01010111

Çizelge 3.10. $50 \le n \le 100$ ve $-20 \le a \le -16$ için n pozitif tamsayılarının 3. *mertebeden GH* kodları.

	$GH_{-16}^{(3)}$	$GH_{-17}^{(3)}$	$GH_{-18}^{(3)}$	$GH_{-19}^{(3)}$	$GH_{-20}^{(3)}$
51	100110111	100010111	000100111	000000111	00001111
52	100001111	101010111	110100111	110000111	11001111
53	101001111	100110111	100010111	000100111	000000111
54	100101111	100001111	101010111	110100111	110000111
55	101101111	101001111	100110111	100010111	000100111
56	N/A	100101111	100001111	101010111	110100111
57	N/A	101101111	101001111	100110111	100010111
58	N/A	N/A	100101111	100001111	101010111
59	N/A	N/A	101101111	101001111	100110111
60	01001111	N/A	N/A	100101111	100001111
61	01101111	N/A	N/A	101101111	101001111
62	010000111	N/A	N/A	N/A	100101111
63	011000111	01001111	N/A	N/A	101101111
64	010100111	01101111	N/A	N/A	N/A
65	000010111	010000111	N/A	N/A	N/A
66	001010111	011000111	01001111	N/A	N/A
67	000110111	010100111	01101111	N/A	N/A
68	000001111	000010111	010000111	N/A	N/A
69	110001111	001010111	011000111	01001111	N/A
70	000101111	000110111	010100111	01101111	N/A
71	110101111	000001111	000010111	010000111	N/A
72	1000000111	110001111	001010111	011000111	01001111
73	1010000111	000101111	000110111	010100111	01101111
74	1001000111	110101111	000001111	000010111	010000111
75	1011000111	1000000111	110001111	001010111	011000111
76	N/A	1010000111	000101111	000110111	010100111
77	N/A	1001000111	110101111	000001111	000010111
78	N/A	1011000111	1000000111	110001111	001010111
79	N/A	N/A	1010000111	000101111	000110111
80	N/A	N/A	1001000111	110101111	000001111
81	N/A	N/A	1011000111	1000000111	110001111
82	010010111	N/A	N/A	1010000111	000101111
83	011010111	N/A	N/A	1001000111	110101111
84	010110111	N/A	N/A	1011000111	1000000111
85	010001111	N/A	N/A	N/A	1010000111
86	011001111	010010111	N/A	N/A	1001000111
87	010101111	011010111	N/A	N/A	1011000111
88	0000000111	010110111	N/A	N/A	N/A
89	1100000111	010001111	N/A	N/A	N/A
90	0001000111	011001111	010010111	N/A	N/A
91	1101000111	010101111	011010111	N/A	N/A
92	1000100111	0000000111	010110111	N/A	N/A
93	1010100111	1100000111	010001111	N/A	N/A
94	1001100111	0001000111	011001111	010010111	N/A
95	1000010111	1101000111	010101111	011010111	N/A
96	1010010111	1000100111	0000000111	010110111	N/A
97	1001010111	1010100111	1100000111	010001111	N/A
98	1011010111	1001100111	0001000111	011001111	010010111
99	N/A	1000010111	1101000111	010101111	011010111
100	N/A	1010010111	1000100111	0000000111	010110111

Çizelgelerden Elde Edilen Sonuçlar

1. $n = 1,2,3,4,5,6,7,8,9,10$ ve $a = -2,-3,\ldots,-20$ için bütün pozitif tamsayıların *GH* kodu mevcuttur.
2. $1 \le n \le 100$ için, $1 \le k \le 10$ olmak üzere $GH^{(3)}_{-(10+\mathrm{k})}(n)$ sütunundaki *GH* kodlarında en fazla k tane ardışık ulaşılamayan değer*(N/A)* vardır.
3. $1 \le n \le 100$ için, $1 \le k \le 10$ olmak üzere k arttıkça $GH^{(3)}_{-(10+\mathrm{k})}(n)$ sütunundaki *GH* kodlarının ulaşılabilirliği azalır.

2. *mertebeden GH* dizisinde n pozitif tamsayılarının bazı değerleri için $GH^{(2)}_{-5}(n), GH^{(2)}_{-6}(n), ..., GH^{(2)}_{-20}(n)$ sütunları kodlama yeteneğine sahip değilken, 3. *mertebeden GH* dizisinde n pozitif tamsayılarının bazı değerleri için $GH^{(3)}_{-11}(n), GH^{(3)}_{-12}(n), ..., GH^{(3)}_{-20}(n)$ sütunları kodlama yeteneğine sahip değildir. Dolayısıyla şifreleme açısından 3. *mertebeden GH* kodlarının 2. *mertebeden GH* kodlarına göre daha avantajlı olduğu ve aynı zamanda mertebe arttıkça şifreleme açısından sağlanan avantajın da artacağı söylenebilir.

Biz [12]'ye baktığımızda ilk olarak $n=5$ ve $a=-5$ için 2. *mertebeden Gopala-Hemachandra (GH)* kodunun mevcut olmadığını*(N/A)* gördük. Ardından kendi yaptığımız Çizelge 3.7'e baktığımızda ise ilk olarak $n=11$ ve $a=-11$ için 3. *mertebeden GH* kodunun mevcut olmadığı sonucuna ulaştık.

Burada aklımıza şöyle bir soru geldi: Acaba pozitif tamsayıların daha yüksek mertebelerden *GH* kodlarında ilk olarak hangi pozitif tamsayının *GH* kodu mevcut değildir? Bu sorudan yola çıkarak ve 2. *mertebeden GH* dizisinin tanımından faydalanarak 4., 5. ve 6. *mertebeden GH* dizilerini aşağıdaki gibi tanımladık.

4. *mertebeden GH* dizisini ; n pozitif tamsayı, a negatif tamsayı ve $b=1-a$ olmak üzere

$$GH^{(4)}_{a}(n) = \{a, b, a+b, 2a+2b, 4a+4b, 7a+8b, 14a+15b, 27a+29b, \ldots\}$$

yani

$GH_a^{(4)}(1) = a\ (a \in \mathbb{Z}^-);\ GH_a^{(4)}(2) = 1-a\ ; GH_a^{(4)}(3) = 1, GH_a^{(4)}(4) = 2$

ve $n \geq 5$ için

$$GH_a^{(4)}(n) = GH_a^{(4)}(n-1) + GH_a^{(4)}(n-2) + GH_a^{(4)}(n-3) + GH_a^{(4)}(n-4)$$

olarak tanımladık. Örneğin $a = -2$ için

$$GH_{-2}^{(4)}(n) = \{-2, 3, 1, 2, 4, 10, 17, 33, \ ...\}$$

elde ettik.

Ardından 5. *mertebeden GH* dizisini ; n pozitif tamsayı, a negatif tamsayı ve $b = 1-a$ olmak üzere

$$GH_a^{(5)}(n) = \{a, b, a+b, 2a+2b, 4a+4b, 8a+8b, 15a+16b, 30a+31b, \ ...\}$$

yani

$GH_a^{(5)}(1) = a\ (a \in \mathbb{Z}^-);\ GH_a^{(5)}(2) = 1-a\ ; GH_a^{(5)}(3) = 1, GH_a^{(5)}(4) = 2,$
$GH_a^{(5)}(5) = 4$

ve $n \geq 6$ için

$GH_a^{(5)}(n) = GH_a^{(5)}(n-1) + GH_a^{(5)}(n-2) + GH_a^{(5)}(n-3) + GH_a^{(5)}(n-4) +$
$GH_a^{(5)}(n-5)$

olarak tanımladık.

Örneğin $a=-2$ için

$$GH_{-2}^{(5)}(n)=\{-2,3,1,2,4,8,18,33,\ ...\}$$

elde ettik.

Son olarak biz 6. *mertebeden GH* dizisini ; n pozitif tamsayı, a negatif tamsayı ve $b=1-a$ olmak üzere

$$GH_a^{(6)}(n)=\{a,b,a+b,2a+2b,4a+4b,8a+8b,16a+16b,31a+32b,\ ...\}$$

yani

$$GH_a^{(6)}(1)=a\ (a\in\mathbb{Z}^-);\ GH_a^{(6)}(2)=1-a\ ;GH_a^{(6)}(3)\ =1,GH_a^{(6)}(4)\ =2,$$
$$GH_a^{(6)}(5)=4\ \ ,\ GH_a^{(6)}(6)=8$$

ve $n\geq 7$ için

$$GH_a^{(6)}(n)=GH_a^{(6)}(n-1)+GH_a^{(6)}(n-2)+GH_a^{(6)}(n-3)+GH_a^{(6)}(n-4)+$$
$$GH_a^{(6)}(n-5)+GH_a^{(6)}(n-6)$$

olarak tanımladık. Örneğin $a=-2$ için

$$GH_{-2}^{(6)}(n)=\{-2,3,1,2,4,8,16,34,\ ...\}$$

elde ettik.

Bu dizi tanımlarından faydalanarak araştırma yaptığımızda pozitif tamsayıların 4. *mertebeden Gopala-Hemachandra (GH)* kodunun ilk olarak $n=23$ ve $a=-23$ için mevcut olmadığını*(N/A),* 5. *mertebeden Gopala-Hemachandra (GH)* kodunun

ilk olarak $n=47$ ve $a=-47$ için mevcut olmadığını ve 6. *mertebeden Gopala-Hemachandra (GH)* kodunun ilk olarak $n=95$ ve $a=-95$ için mevcut olmadığını elde ettik.

Bu durumdan yola çıkarak, pozitif tamsayıların m. mertebeden *GH* kodu için ilk olarak $n=(3.2^{(m-1)}-1)$ ve $a=-(3.2^{(m-1)}-1)$ için mevcut olmayacağı sonucuna ulaştık. Yani pozitif tamsayıların m. *mertebeden GH* kodu için ilk mevcut olmayan değer*(N/A)* $n=(3.2^{(m-1)}-1)$ pozitif tamsayısı için $GH^{(m)}_{-(3.2^{(m-1)}-1)}$ sütunundadır.

Ayrıca ulaştığımız başka bir sonuç ise şudur: *GH* dizisinin tanımından dolayı, bazı a değerleri için aynı elemanın dizinin içinde tekrar ettiği görülür. Dolayısıyla bu durumdaki *GH* dizileri yardımıyla pozitif tamsayıların *GH* kodları bulunamaz ve aynı zamanda bu sütunlar şifrelemede kullanılamaz. Örneğin 4. *mertebeden GH* dizisinde

$a=-3$ için

$$GH^{(4)}_{-3}(n)=\{-3,4,1,2,4,11,18,...\}$$

elde edilir.

5. *mertebeden GH* dizisinde

hem $a=-3$ için

$$GH^{(5)}_{-3}(n)=\{-3,4,1,2,4,8,19,...\}$$

hem de $a=-7$ için

$GH_{-7}^{(5)}(n)=\{-7,8,1,2,4,8,23,...\}$

elde edilir.

6. *mertebeden GH* dizisinde

hem $a=-3$ için

$GH_{-3}^{(6)}(n)=\{-3,4,1,2,4,8,16,35,...\}$

hem $a=-7$ için

$GH_{-7}^{(6)}(n)=\{-7,8,1,2,4,8,16,39,...\}$

hem de $a=-15$ için

$GH_{-15}^{(6)}(n)=\{-15,16,1,2,4,8,16,47,...\}$

elde edilir. Bu durumdan yola çıkarak m. *mertebeden GH* temsili için de $a=-3$, $a=-7$, $a=-15$, $a=-31$,…, ve son olarak da $a=-(2^{(m-2)}-1)$ için $GH_a^{(m)}$ dizisinde aynı elemanların dizinin içinde tekrar edeceği sonucuna ulaştık. Dolayısıyla bu sütunlar şifrelemede kullanılamayacaktır.

3.3. *İKİNCİ VE ÜÇÜNCÜ MERTEBEDEN GOPALA-HEMACHANDRA (GH)* KODLARININ ŞİFRELEMEYE UYGULAMASI

Bu bölümde şifreleme yaparken özel olarak akış şifresi kullanacağız. Ayrıca biz bu bölümde pozitif tamsayıların *GH* kodunun şifrelemeye uygulamasını yapmak için bir yöntem oluşturduk. Şimdi, bu yöntemi açıklayalım.

Göndereceğimiz mesajı şifrelerken ilk olarak, mesajın içindeki her bir harfi bir sayıyla eşleştireceğiz. Bunu yapmak için de kolaylık olması için Türk alfabesini kullanacağız. Örneklerde kullanacağımız için bu yazılımı bir çizelge ile gösterelim.

Çizelge 3.11. Türk alfabesindeki harflerin pozitif tamsayı karşılıkları.

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
16	17	18	19	20	21	22	23	24	25	26	27	28	29

Sonra mesajdaki harflere karşılık gelen her bir sayının *GH* kodunu [12]'den ($m=2$ ise) ya da Çizelge 3.3 veya Çizelge 3.5'ten ($m=3$ ise)elde edeceğiz. Ardından mesajdaki her sayının *GH* kodunun uzunluğu mesajdaki en uzun *GH* kod uzunluğuna eşit olacak şekilde her sayının *GH* kodunun sonuna sıfır (ya da sıfırlar) ekleyeceğiz. Böylece P 'yi yani açık metni elde etmiş olacağız.

Ardından K 'yi yani anahtarı elde edeceğiz. Bunu yapmak için mesajı şifrelerken kullandığımız *GH* kod ailesindeki ($GH_a^{(m)}$) a 'yı eksiyle çarpıp $-a$ 'nın Standart Fibonacci kodunu Çizelge 3.2'den elde edeceğiz. Daha sonra bu kodun uzunluğu mesajdaki en uzun *GH* kod uzunluğuna eşit olacak şekilde sonuna sıfır (ya da sıfırlar) ekleyeceğiz. Böylece K 'yi elde etmiş olacağız. K yardımıyla akış anahtarını da elde ettikten sonra son olarak şifreleme anahtarına göre mesajı şifreleyeceğiz ve C 'yi yani şifreli metni elde etmiş olacağız.

Mesajı alan kişi Bob olsun. Bob mesajı deşifreleme anahtarına göre deşifreleyecek ve açık metni yeniden yapılandıracak. Şimdi sıra bu metni anlamlandırmaya geldi. Bunu yapmak için ilk olarak her bir parçanın uzunluğu K 'nin uzunluğuna eşit olacak şekilde açık metni parçalara ayıracak. İkinci olarak, K dahil her parçanın sonundaki sıfır ya da sıfırları silecek. Sonra, mesajın hangi *GH* koduyla gönderildiğini anlamak için Çizelge 3.2'den anahtar koda karşılık gelen sayıyı elde edecek. Bu sayıyı eksiyle çarptığında mesajın hangi *GH* koduyla gönderildiğini anlamış olacak. Böylece o ayırdığı her bir parçaya karşılık gelen sayıyı [12]'den ($m=2$ ise) ya da Çizelge 3.3

veya Çizelge 3.5'ten ($m=3$ ise) elde edecek ve son olarak da bu sayıları Çizelge 3.11'den alfabetik karakterlere dönüştürecek. Böylece gönderilen mesajı elde etmiş olacak. Bu yöntemle birkaç şifreleme örneği yapalım.

Örnek 3.3.1.

İlk örneğimizde $a=-2$ için pozitif tamsayıların 2. *mertebeden GH* kodunu $GH_{-2}^{(2)}$ kullanalım. Göndereceğimiz mesaj, BU MESAJ ÇOK ÖNEMLİDİR olsun. Mesajı şifrelemek için ilk olarak Çizelge 3.11'e göre mesajdaki her harfi bir sayıyla eşleştirelim.

B	U	M	E	S
2	*25*	*16*	*6*	*22*
A	J	Ç	O	K
1	*13*	*4*	*18*	*14*
Ö	N	E	M	L
19	*17*	*6*	*16*	*15*
İ	D	İ	R	
12	*5*	*12*	*21*	

Şimdi de mesajdaki her bir harfe karşılık gelen sayının *GH* kodunu bu örnek için mertebe 2 olduğundan, [12]'den elde edelim.

10011	100100011	10010011	001011	101000011
0011	10100011	00011	10101011	00000011

00001011 01000011 001011 10010011 00100011

0100011 000011 0100011 01010011

En uzun GH kodunun uzunluğu 9 olduğundan, her bir kod uzunluğu 9 olacak şekilde sonuna sıfır (ya da sıfırlar) ekleyelim.

100110000 100100011 100100110 001011000 101000011

001100000 101000110 000110000 101010110 000000110

000010110 010000110 001011000 100100110 001000110

010001100 000011000 010001100 010100110

Böylece P'yi

100110000100100011100100110001011000101000011001100000101000110000110000010101011000000011000001011001000011000101100010010011000100011001000110000001100001000110001010011

olarak elde etmiş olduk.

Şimdi de K'yi elde edelim. Burada şifreleme yaparken $GH_{-2}^{(2)}$ kodunu kullandığımız için Çizelge 3.2'den 2'nin Standart Fibonacci kodunu 011 olarak elde ederiz. En uzun kod uzunluğu 9 olduğu için K'yi 011000000 olarak elde ederiz. O halde akış anahtarı

011000000011000000011000000011000000011000000011000000011000000001100000001100000001100000001100000001100000001100000001100000001100000001100000001100000001100000011000000

olur.

Şimdi $e_z(x)=(x+z) \bmod 2$, $x=(x_1, x_2, ..., x_d) \in P$ denklemine göre P 'yi şifreleyeceğiz ve C 'yi

111110000111100011111100110010011000110000011010100000110000110011110000011001011001100011001101011000100011001001100011110011001000011000100110000110110000010011000011001101

olarak elde edeceğiz.

Şimdi de mesajı alan kişinin C 'yi nasıl deşifre edeceğine bakalım. Mesajı alan kişi C 'yi

111110000111100011111100110010011000110000011010100000110000110011110000011001011001100011001101011000100011001001100011110011001000011000100110000110110000010011000011001101

ve K 'yi 011000000 bildiği için akış anahtarını

011000000011000000001100000000110000000011000000001100000000110000000011000000001100000000110000000011000000001100000000110000000011000000

olarak elde eder ve $d_z(y)=(y+z) \bmod 2, y=(y_1, y_2, ..., y_d) \in C$ denklemine göre P 'yi

100110000100100011100100110001011000101000011001100000101000110000110000101011000000011000001011001000110010011000100011000100011000010001100010100110

olarak bulur.

Şimdi ise sıra bu metni anlamlandırmaya geldi. Bunun için öncelikle K 'nin uzunluğu 9 olduğu için P 'yi 9 li parçalara ayırır ve

100110000 100100011 100100110 001011000 101000011

001100000 101000110 000110000 101010110 000000110

000010110 010000110 001011000 100100110 001000110

010001100 000011000 010001100 010100110

olarak elde eder. Şimdi de K dahil her parçanın sonundaki sıfırı (ya da sıfırları) siler

10011 100100011 10010011 001011 101000011

0011 10100011 00011 10101011 00000011

00001011 01000011 001011 10010011 00100011

0100011 000011 0100011 01010011

ve K 'yi 011 olarak elde eder.

Şimdi ise mesajın hangi *GH* koduyla gönderildiğini anlamak için 011 in Çizelge 3.2'den karşılığına bakar ve 2 elde eder. 2 'yi eksiyle çarptığında da mesajın $GH_{-2}^{(2)}$ kodu ile gönderildiğini anlar. Dolayısıyla artık [12]'den her bir parçadaki *GH* koduna karşılık gelen sayıyı

2 *25* *16* *6* *22*

1 *13* *4* *18* *14*

19 *17* *6* *16* *15*

12 *5* *12* *21*

olarak elde eder. Son olarak da bunların karşılık geldiği harfe Çizelge 3.11'den bakar ve

B	U	M	E	S
A	J	Ç	O	K
Ö	N	E	M	L
İ	D	İ	R	

Yani BU MESAJ ÇOK ÖNEMLİDİR, mesajını elde eder.

Örnek 3.3.2.

İkinci örneğimizde $a=-4$ için pozitif tamsayıların 2. *mertebeden GH* kodunu $GH_{-4}^{(2)}$ kullanalım. Göndereceğimiz mesaj, GİZLİLİK HABERLEŞMEDE EN ÖNEMLİ KISTASTIR olsun. Mesajı şifrelemek için ilk olarak Çizelge 3.11'e göre mesajdaki her harfi bir sayıyla eşleştirelim.

G	İ	Z	L	İ
8	*12*	*29*	*15*	*12*
L	İ	K	H	A
15	*12*	*14*	*10*	*1*

B	E	R	L	E
2	*6*	*21*	*15*	*6*
Ş	M	E	D	E
23	*16*	*6*	*5*	*6*
K	İ	E	N	Ö
14	*12*	*6*	*17*	*19*
N	E	M	L	İ
17	*6*	*16*	*15*	*12*
K	I	S	T	A
14	*11*	*22*	*24*	*1*
S	T	I	R	
22	*24*	*11*	*21*	

Şimdi de mesajdaki her bir harfe karşılık gelen sayının *GH* kodunu [12]'den elde edelim.

001011	010011	100000011	1001011	010011
1001011	010011	0010011	1010011	0011
10011	00011	00100011	1001011	00011

10001011 10000011 00011 011 00011

0010011 010011 00011 10100011 0001011

10100011 00011 10000011 1001011 010011

0010011 01011 10010011 0101011 0011

10010011 0101011 01011 00100011

En uzun *GH* kod uzunluğu 9 olduğundan, her bir kod uzunluğu 9 olacak şekilde sonuna sıfır (ya da sıfırlar) ekleyelim.

001011000 010011000 100000011 100101100 010011000

100101100 010011000 001001100 101001100 001100000

100110000 000110000 001000110 100101100 000110000

100010110 100000110 000110000 011000000 000110000

001001100 010011000 000110000 101000110 000101100

101000110 000110000 100000110 100101100 010011000

001001100 010110000 100100110 010101100 001100000

100100110 010101100 010110000 001000110

Böylece *P* 'yi

001011000010011000100000011100101100010011000100101100010011000001001100100110000110000010011000000011000000100011010010110000011000011

0001011010000011000011000001100000000011000000100110001001100000110
00010100011000010110010100011000011000010000011010010110001001100000
10011000101100001001001100101011000011000001001001100101011000101100
00001000110
olarak elde etmiş olduk.

Şimdi de K ’yi elde edelim. Burada şifreleme yaparken $GH_{-4}^{(2)}$ kodunu kullandığımız için Çizelge 3.2’den 4 in Standart Fibonacci kodunu 1011 olarak elde ederiz. En uzun kod uzunluğu 9 olduğu için K ’yi 101100000 olarak elde ederiz.

O halde akış anahtarı

10110000010110000010110000010110000010110000010110000010110000010110
00001011000001011000001011000001011000001011000001011000001011000001
01100000101100000101100000101100000101100000101100000101100000101100
00010110000010110000010110000010110000010110000010110000010110000010
11000001011000001011000001011000001011000001011000001011000001011000
00101100000

olur.

Şimdi $e_z(x) = (x + z) \bmod 2$, $x = (x_1, x_2, ..., x_d) \in P$ denklemine göre P ’yi şifreleyeceğiz ve C ’yi

10011100011111100000110001100100110011111100000100110011111100010010
110000010110010000000000010100001010100001001001100010011001010100000
01110110001100110101010000110100000101010000100101100111111000101010
00000010011010100110000010011010101000000110011000100110011111100010
010110011101000000010001101110011001000000000010001101110011001110100
00100100110

olarak elde edeceğiz.

Şimdi de mesajı alan kişinin C 'yi nasıl deşifre edeceğine bakalım. Mesajı alan kişi C 'yi

10011100011111100000110001100100110011111100000100110011111100010010
11000001011001000000000001010000101010000100100110001001100101010 0000
01110110001100110101010000110100000101010000100101100111111000101010
00000010011010100110000001001101010100000011001100010011001111100010
01011001110100000010001101110011001000000000001000110111001100111010 0
00100100110

ve K 'yi 101100000 bildiği için akış anahtarını

10110000010110000010110000010110000010110000010110000010110000010110
00001011000001011000001011000001011000001011000001011000001011000001
01100000101100000101100000101100000101100000101100000101100000101100
00010110000010110000010110000010110000010110000010110000010110000010
11000001011000001011000001011000001011000001011000001011000001011000
00101100000

olarak elde eder ve $d_z(y)=(y+z)\bmod 2, y=(y_1, y_2, ..., y_d)\in C$ denklemine göre P 'yi

00101100001001100010000001110010110001001100010010110001001100000100
11001010011000011000000100110000000011000000010001101001011000000 1100001
0001011010000001100001100000110000000000110000000100110001001100000 0110
00010100011000010110010100011000011000010000001101001011000100110000 0
10011000101100001001001100101011000011000000100100110010101100010 1100
00001000110

olarak bulur.

Şimdi ise sıra bu metni anlamlandırmaya geldi. Bunun için öncelikle K 'nin uzunluğu 9 olduğu için P 'yi 9 li parçalara ayırır ve

001011000 010011000 100000011 100101100 010011000

100101100 010011000 001001100 101001100 001100000

100110000 000110000 001000110 100101100 000110000

100010110 100000110 000110000 011000000 000110000

001001100 010011000 000110000 101000110 000101100

101000110 000110000 100000110 100101100 010011000

001001100 010110000 100100110 010101100 001100000

100100110 010101100 010110000 001000110

olarak elde eder.

Şimdi de K dahil her parçanın sonundaki sıfırı (ya da sıfırları) siler ve

001011 010011 100000011 1001011 010011

1001011 010011 0010011 1010011 0011

10011 00011 00100011 1001011 00011

10001011 10000011 00011 011 00011

0010011 010011 00011 10100011 0001011

10100011 00011 10000011 1001011 010011

0010011 01011 10010011 0101011 0011
10010011 0101011 01011 00100011

ve K 'yi 1011 olarak elde eder.

Şimdi ise mesajın hangi *GH* koduyla gönderildiğini anlamak için 1011 in Çizelge 3.2'den karşılığına bakar ve 4 elde eder. 4 'ü eksiyle çarptığında da mesajın $GH_{-4}^{(2)}$ koduyla gönderildiğini anlar. Dolayısıyla artık [12]'den her bir parçadaki *GH* koduna karşılık gelen sayıyı

8 12 29 15 12

15 12 14 10 1

2 6 21 15 6

23 16 6 5 6

14 12 6 17 19

17 6 16 15 12

14 11 22 24 1

22 24 11 21

olarak elde eder. Son olarak da bunların karşılık geldiği harfe Çizelge 3.11'den bakar ve

G İ Z L İ

L İ K H A

B	E	R	L	E
Ş	M	E	D	E
K	İ	E	N	Ö
N	E	M	L	İ
K	I	S	T	A
S	T	I	R	

Yani GİZLİLİK HABERLEŞMEDEKİ EN ÖNEMLİ KISTASTIR, mesajını elde eder.

Örnek 3.3.3.

Bu örneğimizde de $a=-2$ için pozitif tamsayıların 3. *mertebeden GH* kodunu $GH_{-2}^{(3)}$ kullanalım. Göndereceğimiz mesaj, ŞİFRELEME UZUN BİR TARİHE SAHİPTİR olsun. Mesajı şifrelemek için ilk olarak Çizelge 3.11'e göre mesajdaki her harfi bir sayıyla eşleştirelim.

Ş	İ	F	R	E
23	*12*	*7*	*21*	*6*
L	E	M	E	U
15	*6*	*16*	*6*	*25*
Z	U	N	B	İ

29	*25*	*17*	*2*	*12*
R	T	A	R	İ
21	*24*	*1*	*21*	*12*
H	E	S	A	H
10	*6*	*22*	*1*	*10*
İ	P	T	İ	R
12	*20*	*24*	*12*	*21*

Şimdi de mesajdaki her bir harfe karşılık gelen sayının *GH* kodunu Çizelge 3.3'ten elde edelim.

100110111	11010111	10000111	100010111	0000111
100000111	0000111	101000111	0000111	101001111
110101111	101001111	000000111	000111	11010111
100010111	100001111	00111	100010111	11010111
11000111	0000111	101010111	00111	11000111
11010111	110100111	100001111	11010111	100010111

En uzun *GH* kod uzunluğu 9 olduğundan, her bir kod uzunluğu 9 olacak şekilde sonuna sıfır (ya da sıfırlar) ekleyelim.

100110111	110101110	100001110	100010111	000011100

100000111	000011100	101000111	000011100	101001111
110101111	101001111	000000111	000111000	110101110
100010111	100001111	001110000	100010111	110101110
110001110	000011100	101010111	001110000	110001110
110101110	110100111	100001111	110101110	100010111

Böylece P 'yi

10011011111010111010000111010001011100001110010000011100001110010100
011100000111001010011111101011111010011110000001110001110001101011101
0001011110000111100111000010001011111010111011000111000001110010101 0
1110011100001100011101101011101101001111000011111101011101000 10111

olarak elde etmiş olduk.

Şimdi de K 'yi elde edelim. Burada şifreleme yaparken $GH_{-2}^{(3)}$ kodunu kullandığımız için Çizelge 3.2'den 2 'nin 3.*mertebeden* Standart Fibonacci kodunu 0111 olarak elde ederiz. En uzun kod uzunluğu 9 olduğu için K 'yi 011100000 olarak elde ederiz. O halde akış anahtarı

01110000001110000001110000001110000001110000001110000001110000001110
00000111000000111000000111000000111000000111000000111000000111000000
11100000011100000011100000011100000011100000011100000011100000011100
000011100000011100000011100000011100000011100000011100000011100000

olur.

Şimdi $e_z(x)=(x+z) \bmod 2$, $x=(x_1, x_2, ..., x_d) \in P$ denklemine göre P yi şifreleyeceğiz ve C ’yi

1110101111010011101111011101111101110111111001111001110111111110011010
01110111111001101011111010011111101011110111001110110110001010011101
11110111111101111010010000111110111101001110101101110011111100110110
1110100100001011011101010011101010001111111011111010011101111110111

olarak elde edeceğiz.

Şimdi de mesajı alan kişinin C ’yi nasıl deşifre edeceğine bakalım. Mesajı alan kişi C ’yi

1110101111010011101111011101111101110111111001111001110111111110011010
01110111111001101011111010011111101011110111001110110110001010011101
11110111111101111010010000111110111101001110101101110011111100110110
1110100100001011011101010011101010001111111011111010011101111110111

ve K ’yi 011100000 bildiği için akış anahtarını

01110000001110000001110000001110000001110000001110000001110000001110
00000111000000111000000111000000111000000111000000111000000111000000
111000000011100000011100000011100000011100000011100000011100000011100
0000111000000111000000111000000111000000111000000111000000111000000

olarak elde eder ve $d_z(y)=(y+z) \bmod 2, y=(y_1, y_2, ..., y_d) \in C$ denklemine göre P ’yi

100110111110101110100001110100010111000011100100000011100001110010100
01110000111001010011111101011111010011110000001110001110001101011101
000101111000011110011100001000101111101011101100011100000011100101010
111001110000110001110110101110110100111100001111110101110100010111

olarak bulur.

Şimdi ise sıra bu metni anlamlandırmaya geldi. Bunun için öncelikle K 'nin uzunluğu 9 olduğu için P 'yi 9 li parçalara ayırır ve

100110111	110101110	100001110	100010111	000011100
100000111	000011100	101000111	000011100	101001111
110101111	101001111	000000111	000111000	110101110
100010111	100001111	001110000	100010111	110101110
110001110	000011100	101010111	001110000	110001110
110101110	110100111	100001111	110101110	100010111

olarak elde eder. Şimdi de K dahil her parçanın sonundaki sıfırı (ya da sıfırları) siler ve

100110111	11010111	10000111	100010111	0000111
100000111	0000111	101000111	0000111	101001111
110101111	101001111	000000111	000111	11010111
100010111	100001111	00111	100010111	11010111
11000111	0000111	101010111	00111	11000111
11010111	110100111	100001111	11010111	100010111

ve K 'yi 0111 olarak elde eder.

Şimdi ise mesajın hangi *GH* koduyla gönderildiğini anlamak için 0111 in Çizelge 3.2'den karşılığına bakar ve 2 elde eder. 2 'yi eksiyle çarptığında da mesajın $GH_{-2}^{(3)}$ koduyla gönderildiğini anlar. Dolayısıyla artık Çizelge 3.3'ten her bir parçadaki *GH* koduna karşılık gelen sayıyı

23	*12*	*7*	*21*	*6*
15	*6*	*16*	*6*	*25*
29	*25*	*17*	*2*	*12*
21	*24*	*1*	*21*	*12*
10	*6*	*22*	*1*	*10*
12	*20*	*24*	*12*	*21*

olarak elde eder.

Son olarak da bunların karşılık geldiği harfe Çizelge 3.11'den bakar ve

Ş	İ	F	R	E
L	E	M	E	U
Z	U	N	B	İ
R	T	A	R	İ
H	E	S	A	H
İ	P	T	İ	R

Yani ŞİFRELEME UZUN BİR TARİHE SAHİPTİR, mesajını elde eder.

Örnek 3.3.4.

Bu örneğimizde de $a=-10$ için pozitif tamsayıların 3. *mertebeden GH* kodunu $GH_{-10}^{(3)}$ kullanalım. Göndereceğimiz mesaj, YARDIMA İHTİYACIMIZ VAR olsun. Mesajı şifrelemek için ilk olarak Çizelge 3.11'e göre mesajdaki her harfi bir sayıyla eşleştirelim.

Y	A	R	D	I
28	*1*	*21*	*5*	*11*
M	A	İ	H	T
16	*1*	*12*	*10*	*24*
İ	Y	A	C	I
12	*28*	*1*	*3*	*11*
M	I	Z	V	A
16	*11*	*29*	*27*	*1*

R
21

Şimdi de mesajdaki her bir harfe karşılık gelen sayının *GH* kodunu Çizelge 3.5'ten elde edelim.

01000111	00111	10001111	1010111	0111

0001111 00111 01111 10110111 101000111

01111 01000111 00111 001111 0111

0001111 0111 01100111 0101111 00111

10001111

En uzun *GH* kod uzunluğu 9 olduğundan, her bir kod uzunluğu 9 olacak şekilde sonuna sıfır (ya da sıfırlar) ekleyelim.

010001110 001110000 100011110 101011100 011100000

000111100 001110000 011110000 101101110 101000111

011110000 010001110 001110000 001111000 011100000

000111100 011100000 011001110 010111100 001110000

100011110

Böylece P'yi

010001110001110000100011110101011100011100000000011110000111000001111
000010110111010100011101111000010001110001110000000111100001110000000
001111000111000000110011100101111000011100001000111 10

olarak elde etmiş olduk.

Şimdi de K'yi elde edelim. Burada şifreleme yaparken $GH_{-10}^{(3)}$ kodunu kullandığımız için Çizelge 3.2'den 10'un 3*.mertebeden* Standart Fibonacci kodunu 110111 olarak

elde ederiz. En uzun kod uzunluğu 9 olduğu için K 'yi 110111000 olarak elde ederiz. O halde akış anahtarı

110111000110111000110111000110111000110111000110111000110111000110111
100011011100011011100011011100011011100011011100011011100011011100011
101110001101110001101110001101110001101110001101110001101110001101110

olur.

Şimdi $e_z(x)=(x+z) \bmod 2$, $x=(x_1, x_2, ..., x_d) \in P$ denklemine göre P 'yi şifreleyeceğiz ve C 'yi

100110110111001000010100110011100100101011000110000100111001000101000
100001101011001111111111010010001001101101110010001110000001010110001
100001001010110001011101101000001001110010000101001100

olarak elde edeceğiz.

Şimdi de mesajı alan kişinin C 'yi nasıl deşifre edeceğine bakalım. Mesajı alan kişi C 'yi

100110110111001000010100110011100100101011000110000100111001000101000
100001101011001111111111010010001001101101110010001110000001010110001
100001001010110001011101101000001001110010000101001100

ve K 'yi 110111000 bildiği için akış anahtarını

110111000110111000110111000110111000110111000110111000110111000110111
100011011100011011100011011100011011100011011100011011100011011100011
101110001101110001101110001101110001101110001101110001101110001101110

olarak elde eder ve $d_z(y)=(y+z)\bmod 2, y=(y_1, y_2, ..., y_d)\in C$ denklemine göre P 'yi

0100011100011100001000111101010111000111000000001111000011100000111
0000101101110101000111011110000010001110001110000001111000011100000
0011110001110000001100111001011110000111000010001111 0

olarak bulur.

Şimdi ise sıra bu metni anlamlandırmaya geldi. Bunun için öncelikle K 'nin uzunlugu 9 olduğu için P 'yi 9 li parçalara ayırır ve

010001110 001110000 100011110 101011100 011100000

000111100 001110000 011110000 101101110 101000111

011110000 010001110 001110000 001111000 011100000

000111100 011100000 011001110 010111100 001110000

100011110

olarak elde eder. Şimdi de K dahil her parçanın sonundaki sıfırı (ya da sıfırları) siler ve

01000111 00111 10001111 1010111 0111

0001111 00111 01111 10110111 101000111

01111 01000111 00111 001111 0111

0001111 0111 01100111 0101111 00111

10001111

ve K 'yi 110111 olarak elde eder.

Şimdi ise mesajın hangi *GH* koduyla gönderildiğini anlamak için 110111 in Çizelge 3.2'den karşılığına bakar ve 10 elde eder. 10 'u eksiyle çarptığında da mesajın $GH_{-10}^{(3)}$ koduyla gönderildiğini anlar. Dolayısıyla artık Çizelge 3.5'ten her bir parçadaki *GH* koduna karşılık gelen sayıyı

27	*1*	*21*	*5*	*11*
16	*1*	*12*	*10*	*24*
12	*27*	*1*	*3*	*11*
16	*11*	*29*	*27*	*1*
21				

olarak elde eder.

Son olarak da bunların karşılık geldiği harfe Çizelge 3.11'den bakar ve

Y	A	R	D	I
M	A	İ	H	T
İ	Y	A	C	I
M	I	Z	V	A
R				

Yani YARDIMA İHTİYACIMIZ VAR, mesajını elde eder.

BÖLÜM 4

POZİTİF TAMSAYILARIN *BEŞİNCİ VE ALTINCI MERTEBEDEN GOPALA – HEMACHANDRA (GH)* TEMSİLİNİN ŞİFRELEMEYE BİR UYGULAMASI

*3.bölüm*de Fibonacci kodunu tanımlayıp pozitif tamsayıların Fibonacci temsilinin şifrelemeye de uygulanabilen ve aynı zamanda *Gopala-Hemachandra (GH)* temsili olarak da adlandırılabilen çeşitli varyasyonları olduğunu söylemiştik. Ayrıca *3.bölüm*de Zeckhendorf Teoremine göre her pozitif tamsayının ard arda gelmeyen Fibonacci sayılarının toplamı olarak tek Fibonacci yani Zeckhendorf temsili olduğunu, ne var ki bu durumun, pozitif tamsayıların *GH* temsili için geçerli olmadığına da değinmiştik. Yani *GH* temsiline göre bazı pozitif tamsayıların birden fazla temsili olabilir ya da bazı pozitif tamsayıların *GH* temsili mevcut olmayabilir. Bu haliyle pozitif tamsayıların *GH* temsili kullanılarak şifreleme yapılamaz. Ancak *GH* temsiline bazı koşullar eklenerek ya da bazı sınırlandırmalar getirilerek pozitif tamsayıların sadece o koşullar altındaki *GH* temsili kullanılırsa bu temsil bir fonksiyon haline getirilmiş olur.

Bu bölümde pozitif tamsayıların 5. *ve* 6. *mertebeden GH* temsilleri yardımıyla şifreleme yapmak için biz Türk alfabesindeki harf sayısı kadar *n* tamsayısının her $a \in \square^{-}$ için *GH* dizisine göre aynı temsille var olması koşulunu ekleyerek kendi oluşturduğumuz şifreleme yöntemiyle *GH* temsilinin şifrelemeye birkaç uygulamasını yaptık.

4.1. *BEŞİNCİ VE ALTINCI MERTEBEDEN GOPALA-HEMACHANDRA (GH)* SIRALAMASI VE TEMSİLİ

Pozitif tamsayıların 3. *mertebeden Gopala-Hemachandra (GH)* temsilinin ilk olarak $n=11$ ve $a=-11$ için mevcut olmadığını, 4. *mertebeden Gopala-Hemachandra*

(GH) temsilinin ilk olarak $n=23$ ve $a=-23$ için mevcut olmadığını ve 5. *mertebeden Gopala-Hemachandra (GH)* temsilinin ilk olarak $n=47$ ve $a=-47$ için mevcut olmadığını *3.bölüm*de söylemiştik. Ayrıca aynı bölümde bu durumdan yola çıkarak, m . *mertebeden GH* temsili için ilk olarak $n=(3.2^{(m-1)}-1)$ ve $a=-(3.2^{(m-1)}-1)$ için mevcut olmayacağı sonucuna da ulaşmıştık.

Bu bölümde pozitif tamsayıların *GH* temsiliyle şifreleme yapabilmek için eklediğimiz koşul Türk alfabesindeki harf sayısı kadar n tamsayısının her $a \in Z^-$ için *GH* dizisine göre aynı temsille var olmasıydı. Bu da aslında Türk alfabesindeki harf sayısı kadar yani 29 tane pozitif n tamsayısının her $a \in Z^-$ için *GH* dizisine göre aynı temsille var olması anlamına gelir. O halde bu koşulla şifreleme yapabilmemiz için ilk kullanabileceğimiz mertebe 5. mertebedir. Çünkü 2. 3. ve 4. mertebelerden *GH* dizisine göre 29 'dan daha küçük sayılarda mevcut olmayan değer bulunur. Bu yüzden biz bu bölümde pozitif tamsayıların 5. ve 6. *mertebeden GH* temsillerini kullanarak şifreleme örnekleri yaptık.

4.2. POZİTİF TAMSAYILARIN *BEŞİNCİ VE ALTINCI MERTEBEDEN GOPALA-HEMACHANDRA (GH)* TEMSİLİNİN ŞİFRELEMEYE UYGULAMASI

Bu bölümde, biz pozitif tamsayıların *GH* temsilinin şifrelemeye uygulamasını yapmak için *3.bölüm*dekine benzer bir yöntem oluşturduk. Şimdi, bu yöntemi açıklayalım.

Göndereceğimiz mesajı şifrelerken ilk olarak, mesajın içindeki her bir harfi bir sayıyla eşleştireceğiz. Bunu yapmak için de kolaylık olması için Türk alfabesini kullanacağız. Bu durumu *3.bölüm*de çizelge 3.11 ile göstermiştik. Ardından da ilk 29 pozitif tamsayının koyduğumuz kuralla birlikteki *GH* temsillerini bir çizelge ile gösterelim.

Çizelge 4.1. $1 \le n \le 29$ için n pozitif tamsayılarının 5. *ve* 6. *mertebeden GH* temsilleri.

n	5. *mertebeden GH* temsili	6. *mertebeden GH* temsili
1	001	001
2	0001	0001
3	0011	0011
4	00001	00001
5	00101	00101
6	00011	00011
7	00111	00111
8	000001	000001
9	001001	001001
10	000101	000101
11	001101	001101
12	000011	000011
13	001011	001011
14	000111	000111
15	001111	001111
16	1000001	0000001
17	1010001	0010001
18	1001001	0001001
19	1011001	0011001
20	1000101	0000101
21	1010101	0010101
22	1001101	0001101
23	1011101	0011101
24	1000011	0000011
25	1010011	0010011
26	1001011	0001011
27	1011011	0011011
28	1000111	0000111
29	1010111	0010111

Sonra mesajdaki harflere karşılık gelen her bir sayının *GH* temsilini Çizelge 4.1'den elde edeceğiz. Ardından mesajdaki her sayının *GH* temsilinin uzunluğu mesajdaki en uzun *GH* temsil uzunluğuna eşit olacak şekilde her sayının *GH* temsilinin sonuna sıfır (ya da sıfırlar) ekleyeceğiz. Böylece P'yi yani açık metni elde etmiş olacağız.

Sonra K'yi yani anahtarı elde edeceğiz. Bunu yapmak için $GH_a^{(m)}$ ailesindeki m'nin 2.*mertebeden* Standart Fibonacci temsiline Çizelge 3.1'den bakacağız. Ardından m nin Standart Fibonacci temsilinin mesajdaki en uzun *GH* temsil uzunluğuna eşit olacak şekilde sonuna sıfır (ya da sıfırlar) ekleyeceğiz. Böylece K'yi elde etmiş olacağız. Son olarak şifreleme anahtarına göre mesajı şifreleyeceğiz ve C'yi yani şifreli metni elde etmiş olacağız.

Mesajı alan kişi Bob olsun. Bob mesajı deşifreleme anahtarına göre deşifreleyecek ve açık metni yeniden yapılandıracak. Şimdi sıra bu metni anlamlandırmaya geldi. Bunu yapmak için ilk olarak her bir parçanın uzunluğu K 'nin uzunluğuna eşit olacak şekilde açık metni parçalara ayıracak. İkinci olarak, K anahtarı dahil her parçanın sonundaki sıfır ya da sıfırları silecek. Sonra, mesajın hangi *GH* temsiliyle gönderildiğini anlamak için K anahtarına karşılık gelen sayıya Çizelge 3.1'den bakacak. Mesajın hangi *GH* temsiliyle gönderildiğini anladığı için artık Çizelge 4.1'den açık metni ayırdığı her bir parçaya karşılık gelen sayıyı elde edebilecek ve son olarak da bu sayıları Çizelge 3.11'den alfabetik karakterlere dönüştürecek. Böylece gönderilen mesajı elde etmiş olacak. Şimdi bu yöntemle birkaç örnek yapalım.

Örnek 4.2.1.

İlk örneğimizde pozitif tamsayıların 5. *mertebeden GH* temsilini ($GH_a^{(5)}$) kullanalım. Göndereceğimiz mesaj, ACİL DURUM olsun. Mesajı şifrelemek için ilk olarak Çizelge 3.11'e göre mesajdaki her harfi bir sayıyla eşleştirelim.

A	C	İ	L	D
1	*3*	*12*	*15*	*5*
U	R	U	M	
25	*21*	*25*	*16*	

Şimdi de mesajdaki her bir harfe karşılık gelen sayının *GH* temsilini Çizelge 4.1'den elde edelim.

001	0011	000011	001111	00101
1010011	1010101	1010011	1000001	

En uzun *GH* temsilinin uzunluğu 7 olduğundan, her bir temsil uzunluğu 7 olacak şekilde sonuna sıfır (ya da sıfırlar) ekleyelim.

0010000 0011000 0000110 0011110 0010100

1010011 1010101 1010011 1000001

Böylece P

00100000011000000011000111100010100101001110101011010011100000 1

olarak elde etmiş olduk.

Şimdi de K 'yi elde edelim. Burada şifreleme yaparken $GH_a^{(5)}$ temsilini kullandığımız için Çizelge 3.1'den 5 'in 2. *mertebeden* Standart Fibonacci temsilini 0001 olarak elde ederiz. En uzun kod uzunluğu 7 olduğu için K 'yi 0001000 olarak elde ederiz. O halde akış anahtarı

0001000000100000010000001000000100000010000001000000100000001000

olur.

Şimdi $e_z(x)=(x+z) \bmod 2$, $x=(x_1, x_2, ..., x_d) \in P$ denklemine göre P 'yi şifreleyeceğiz ve C 'yi

0011000001000000011100010110001110010110111011101101101110011001

olarak elde edeceğiz.

Şimdi de mesajı alan kişinin C 'yi nasıl deşifre edeceğine bakalım. Mesajı alan kişi C 'yi

00110000010000000111000101100011100101101110111011010110111001001

ve K 'yi 0001000 bildiği için akış anahtarını

00010000001000000100000010000000100000001000000010000000100000001000

olarak elde eder.

Daha sonra $d_z(y)=(y+z) \bmod 2, y=(y_1, y_2, ..., y_d) \in C$ denklemine göre P 'yi

00100000011000000011000111100010100101001110101011010011100000 1

olarak bulur. Şimdi ise sıra bu metni anlamlandırmaya geldi. Bunun için öncelikle K nin uzunluğu 7 olduğu için P 'yi 7 li parçalara ayırır ve

0010000 0011000 0000110 0011110 0010100

1010011 1010101 1010011 1000001

olarak elde eder. Şimdi de K dahil her parçanın sonundaki sıfırı (ya da sıfırları) siler ve

001 0011 000011 001111 00101

1010011 1010101 1010011 1000001

ve K 'yi 0001 olarak elde eder.

Şimdi ise mesajın hangi *GH* temsiliyle gönderildiğini anlamak için 0001 in Çizelge 3.1'den karşılığına bakar ve 5 elde eder. Yani mesajın $GH_a^{(5)}$ temsiliyle gönderildiğini anlar. Dolayısıyla artık Çizelge 4.1'den her bir parçadaki *GH* temsiline karşılık gelen sayıyı

1	*3*	*12*	*15*	*5*
25	*21*	*25*	*16*	

olarak elde eder. Son olarak da bunların karşılık geldiği harfe Çizelge 3.11'den bakar ve

A	C	İ	L	D
U	R	U	M	

mesajını elde eder.

Örnek 4.2.2.

Bu örneğimizde de pozitif tamsayıların 6. *mertebeden GH* temsilini $GH_a^{(6)}$ kullanalım. Göndereceğimiz mesaj, ŞİFRELEME GÜVENLİ İLETİŞİM SAĞLAR olsun. Mesajı şifrelemek için ilk olarak Çizelge 3.11'e göre mesajdaki her harfi bir sayıyla eşleştirelim.

Ş	İ	F	R	E
23	*12*	*7*	*21*	*6*
L	E	M	E	G
15	*6*	*16*	*6*	*8*
Ü	V	E	N	L
26	*27*	*6*	*17*	*15*

İ	İ	L	E	T
12	*12*	*15*	*6*	*24*
İ	Ş	İ	M	S
12	*23*	*12*	*16*	*22*
A	Ğ	L	A	R
1	*9*	*15*	*1*	*21*

Şimdi de mesajdaki her bir harfe karşılık gelen sayının *GH* temsilini Çizelge 4.1'den elde edelim.

0011101	000011	00111	0010101	00011
001111	00011	0000001	00011	000001
0001011	0011011	00011	0010001	001111
000011	000011	001111	00011	0000011
000011	0011101	000011	0000001	0001101
001	001001	001111	001	0010101

En uzun *GH* temsilinin uzunluğu 7 olduğundan, her bir temsil uzunluğu 7 olacak şekilde sonuna sıfır (ya da sıfırlar) ekleyelim.

0011101	0000110	0011100	0010101	0001100
0011110	0001100	0000001	0001100	0000010

0001011 0011011 0001100 0010001 0011110

0000110 0000110 0011110 0001100 0000011

0000110 0011101 0000110 0000001 0001101

0010000 0010010 0011110 0010000 0010101

Böylece P 'yi

00111010000110001110000101010001100001111000011000000001000110000000
10000101100110110001100001000100111100000110000011000111100001100000
00110000110001110100001100000000100011010010000001001000111100010000
010101

olarak elde etmiş olduk.

Şimdi de K 'yi elde edelim. Burada şifreleme yaparken $GH_a^{(6)}$ temsilini kullandığımız için Çizelge 3.1'den 6 'nın 2.*mertebeden* Standart Fibonacci temsilini 1001 olarak elde ederiz. En uzun kod uzunluğu 7 olduğu için K 'yi 1001000 olarak elde ederiz. O halde akış anahtarı

10010001001000100100010010001001000100100010010001001000100100010010
00100100010010001001000100100010010001001000100100010010001001000100
10001001000100100010010001001000100100010010001001000100100010010001
001000

olur. Şimdi $e_z(x)=(x+z) \bmod 2$, $x=(x_1, x_2, ..., x_d) \in P$ denklemine göre P 'yi şifreleyeceğiz ve C 'yi

10101011001110101010010111011000100101011010001001001001100010010010
10100001110100111000100101100110101101001110100111010101101000100100

101110011101010101100111010010011000101101100010110101010110101100010
11101

olarak elde edeceğiz. Şimdi de mesajı alan kişinin C 'yi nasıl deşifre edeceğine bakalım. Mesajı alan kişi C 'yi

101010110011101010100101110110001001010110100010010010011000100100101
010000111010011100010010110011010110100111010011101010110100010010010
101110011101010101100111010010011000101101100010110101010110101100010
11101

ve K 'yi 1001000 bildiği için akış anahtarını

100100010010001001000100100010010001001000100100010010001001000100100010010
001001000100100010010001001000100100010010001001000100100010010001001000100
100010010001001000100100010010001001000100100010010001001000100100010010001
001000

olarak elde eder.

Daha sonra $d_z(y)=(y+z) \bmod 2, y=(y_1, y_2, ..., y_d) \in C$ denklemine göre P 'yi

001110100001100011100001010100011000011110000110000000010001100000001000010
110011011000110000100010011110000011000001100011110000110000001100000100001
100000110001110100001100000000100011010010000001001000111100010000001010101

olarak bulur. Şimdi ise sıra bu metni anlamlandırmaya geldi. Bunun için öncelikle K nin uzunluğu 7 olduğu için P 'yi 7 li parçalara ayırır ve

0011101 0000110 0011100 0010101 0001100

0011110 0001100 0000001 0001100 0000010

0001011	0011011	0001100	0010001	0011110
0000110	0000110	0011110	0001100	0000011
0000110	0011101	0000110	0000001	0001101
0010000	0010010	0011110	0010000	0010101

olarak elde eder. Şimdi de K dahil her parçanın sonundaki sıfırı (ya da sıfırları) siler ve

0011101	000011	00111	0010101	00011
001111	00011	0000001	00011	000001
0001011	0011011	00011	0010001	001111
000011	000011	001111	00011	0000011
000011	001111	001	0010101	0011101
000011	0000001	0001101	001	001001

ve K 'yi 1001 olarak elde eder.

Şimdi ise mesajın hangi *GH* koduyla gönderildiğini anlamak için 1001 in Çizelge 3.1'den 2. *mertebeden* karşılığına bakar ve 6 elde eder. Yani mesajın $GH_a^{(6)}$ temsiliyle gönderildiğini anlar. Dolayısıyla artık Çizelge 4.1'den her bir parçadaki *GH* temsiline karşılık gelen sayıyı

23	*12*	*7*	*21*	*6*
15	*6*	*16*	*6*	*8*

26	*27*	*6*	*17*	*15*
12	*12*	*15*	*6*	*24*
12	*23*	*12*	*16*	*22*
1	*9*	*15*	*1*	*21*

olarak elde eder. Son olarak da bunların karşılık geldiği harfe Çizelge 3.11'den bakar ve

Ş	İ	F	R	E
L	E	M	E	G
Ü	V	E	N	L
İ	İ	L	E	T
İ	Ş	İ	M	S
A	Ğ	L	A	R

Yani ŞİFRELEME GÜVENLİ İLETİŞİM SAĞLAR, mesajını elde eder.

BÖLÜM 5

SONUÇ

Günümüzde haberleşme sistemlerinin güvenliğinin sağlanması için kullanılan en önemli işlem, verilerin şifrelenerek anlamsız hale getirilip hedefe gönderilmesi ve hedefte tersi işlem yapılarak yani deşifrelenerek tekrar eski haline getirilmesidir. Kriptografi bilimi aracılığıyla verilerin güvenli bir şekilde şifrelenip gönderilmesi ve tekrar deşifre edilebilmesi için şifreleme algoritmaları oluşturulmaktadır [15]. Kriptoloji, kişiler arası veya özel devlet kurumları arasındaki mesajlaşmalardan sistemlerin oluşumunda ve işleyişindeki güvenlik boşluklarına kadar her türlü dalla alakalıdır [2].

Bu çalışmada ilk olarak kriptolojiye kısa bir giriş yapılarak kriptolojinin terminolojisinden ve kısaca kriptolojinin tarihinden bahsedilmiştir. Daha sonra kriptolojinin içinde yer alan kriptografi için gerekli olabilecek matematiksel alt yapıya değinilmiş ve bazı basit kriptosistemlerden bahsedilmiştir. Ayrıca günümüzde yaygın olarak kullanılan simetrik(gizli anahtarlı) ve asimetrik(açık anahtarlı) şifreleme algoritmaları tanımlanmış ve simetrik şifreleme uygulamaları yapılmıştır.

İlerleyen bölümlerde ise pozitif tamsayıların Fibonacci kodu tanımlanmış ve bazı pozitif tamsayıların Fibonacci temsilleri ve Fibonacci kodları çizelgeler halinde gösterilmiştir. Ayrıca Fibonacci kodlarının varyasyonlarından biri olan *Gopala-Hemachandra (GH)* kodu çeşitli mertebelerden tanımlanmış ve bazı pozitif tamsayıların çeşitli mertebelerden *GH* temsilleri veya *GH* kodları da çizelgeler halinde gösterilmiştir.

Zeckendorf teoremine göre her pozitif tamsayının ard arda gelmeyen Fibonacci sayılarının toplamı olarak tek Fibonacci temsili olduğuna fakat bu durumun pozitif tamsayıların *GH* temsili veya *GH* kodu için geçerli olmadığına değinilmiştir. Yani

GH dizisine göre bazı pozitif tamsayıların birden fazla temsili olabilir ya da bazı pozitif tamsayıların *GH* temsili mevcut olmayabilir*(N/A)* sonucuna ulaşılmıştır. Ayrıca bu çalışmada pozitif tamsayıların *GH* temsilleri veya *GH* kodları kullanılarak şifreleme yapıldığı için hangi değerlerin mevcut olmadığı*(N/A)* son derece önemlidir. Çünkü mevcut olmayan değerlerin bulunduğu sütunlar şifrelemede kullanılamayacaktır. Bu yüzden bu çalışmada öncelikle hangi değerlerin mevcut olmadığı araştırılmış ulaşılan sonuçlar açıklanmıştır. Ayrıca bazı pozitif tamsayıların birden fazla *GH* temsili olduğu için bu temsilin bir fonksiyon olmadığı belirtilmiştir. Bu yüzden pozitif tamsayıların *GH* temsillerine veya *GH* kodlarına bazı sınırlandırmalar getirilerek veya bazı koşullar eklenerek bu temsiller veya kodlar bir fonksiyon haline getirilmiştir. Sonrasında ise pozitif tamsayıların bazı mertebelerden *GH* temsilleri veya *GH* kodları kullanılarak kendi oluşturduğumuz bir yöntemle şifreleme örnekleri yapılmıştır.

TEZ SIRASINDA YAPILAN ÇALIŞMALAR

Uluslararası Kongre Ve Sempozyum Bildirileri

1. Özyılmaz Ç., Nallı A., ‘‘ The Third Order Variations On The Fibonacci Universal Code And An Application To Cryptography’’ 2 nd International Symposium On Innovation Technologies In Engineering And Science, 1792-1801 pp., Karabük, Türkiye, Haziran-2014

Ulusal Kongre Ve Sempozyum Bildirileri

1. Özyılmaz Ç., Nallı A., ‘‘ Gopala-Hemachandra (GH) Kodunun Şifrelemeye Bir Uygulaması’’ , 13. Matematik Sempozyumu, 77-78 pp., Karabük, Türkiye, Mayıs-2014

KAYNAKLAR

1. Çimen, C., Akleylek, S. ve Akyıldız, E. , "Şifrelerin Matematiği Kriptografi", ***ODTÜ Yayıncılık***, Ankara, 1: 5-10 (2007).

2. Soyalıç, S. , "Kriptografik Hash fonksiyonları ve uygulamaları", Yüksek Lisans Tezi, ***Erciyes Üniversitesi Fen Bilimleri Enstitüsü***, Kayseri, 1-3, 15-18, 24-26 (2004).

3. Altan, K., Kaşkaloğlu, K., Kındap, N., Özakın, Ç., Saygı, Z., Yıldırım, E., Yıldırım, M. ve Yıldız, S., "Akan Şifreler, Kriptolojiye Giriş Ders Notları", ***ODTÜ Yayıncılık***, Ankara, 32,33 (2004).

4. Akkaş, S., Hacısalihoğlu H. H., Özel, Z. ve Sabuncuoğlu, A., "Fonksiyon, Soyut Matematik", ***Gazi Üniversitesi Yayınları,*** Yayın No: 43, Ankara, 3: 90-96, 121-138 (1984).

5. İnternet: Altındiş, H., "Kriptoloji", **http://www.matematikdunyasi.org/arsiv/ PDF_eskisayilar,** 5: 17-21 (1993).

6. Stinson, D. R., "Classical Cryptograph, Cryptography Theory and Practice", Ed: Rosen, K. H., ***Chapman & Hall / CRC***, New York, 2: 1- 20 (2002).

7. Arda, D., "Kodlama teorisinin kriptografik açıdan incelenmesi", Doktara Tezi, ***Trakya Üniversitesi Fen Bilimleri Enstitüsü,*** Edirne, 30-32 (2011).

8. Kendirli, B., "Kriptografi, Sayılar Kuramı", ***Yalın Yayıncılık***, İstanbul, 1: 66,67 (2009).

9. Tuncal, T., "Bilgisayar güvenliği üzerine bir araştırma ve şifreleme- deşifreleme üzerine uygulama", Yüksek Lisans Tezi, ***Marmara Üniversitesi Fen Bilimleri Enstitüsü***, İstanbul, 16- 41 (2008).

10. Klein, S. T. and Ben-Nissan, M. K, "On the usefulness of Fibonacci Compression Codes", ***The Computer Journal***, 53 (6): 701 – 716 (2010).

11. Zeckendorf, E., "Representation des nombres naturels par une somme des nombres de Fibonacci ou de nombres de Lucas", ***Bull. Soc. Roy . Sci. Liege,*** 41: 179-182 (1972).

12. Basu, M. and Prasad B., "Long range variations on the Fibonacci universal Code", ***Journal of Number Theory***, 130: 1925 – 1931 (2010).

13. Daykin, D. E., ''Representation of natural numbers as sums of generalized Fibonacci numbers'', ***J. Lond. Math. Soc.*** , 35: 143-160 (1960).

14. Thomas, J. H., "Variation on the Fibonacci universal code", ***CoRR***, arxiv:cs/0701085v2 (2007).

15. Yerlikaya, T. , "Yeni şifreleme algoritmalarının analizi", Doktara Tezi, ***Trakya Üniversitesi Fen Bilimleri Enstitüsü,*** Edirne, 126,127 (2006).

16. Apostolico, A. and Fraenkel, A., ''Robust transmission of strings using Fibonacci representations", ***IEEE Trans. On Information Theory***, 33: 238- 245 (1987).

17. Kak, S., "Aristotle and Gautama on logic and physics", ***History and Philosophy of Physics***, arxiv:physics/0505172 (2005).

18. Kak, S., "Greek and Indian cosmology: Review of early history", Ed: G. C. Pande, ***The Golden Chain, CSC,*** New Delhi, arxiv: physics/0303001 (2005).

19. Kak, S., "The golden mean and the physics of aesthetics", ***Foarm Magazine,*** 5: 73-81, arxiv:physics/0411195 (2006).

20. İnternet: Pearce, I. G., "Indian Mathematics: Redressing The Balance", **http://www.history.mcs.st–andrews.ac.uk/history/projects/pearce/index. html** (2002).

ÖZGEÇMİŞ

Çağla ÖZYILMAZ 1988 yılında Karabük'te doğdu; ilk ve orta öğrenimini aynı şehirde tamamladı. 2006 yılında Uludağ Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü'nde öğrenime başladı. 2009-2011 yılında Uludağ Üniversitesi Fen Bilimleri Enstitüsü Matematik öğretmenliği tezsiz yüksek lisansını tamamladı. 2011 yılında Uludağ Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü'nden mezun oldu. Aynı yıl Karabük Üniversitesi Fen Bilimleri Enstitüsü Matematik Bölümü'nde yüksek lisans eğitimine başladı ve halen devam etmektedir.

ADRES BİLGİLERİ

Adres : Karabük Üniversitesi
Fen Bilimleri Enstitüsü
Balıklarkayası Mevkii/ KARABÜK

Tel : (532) 1738795
E-posta : casevfesey@hotmail.com