GEOMETRİK YAPILARDAKİ YÜZEY VE BİRLEŞİM NOKTALARINA GÖRE ŞİFRELEME

Encryption According to Surface and Junction Points in Geometric Structures

ANTALYA
İL MİLLÎ EĞİTİM MÜDÜRLÜĞÜ

Asya ŞİMŞEK[1] **Duygu Alyeşil Kabakçı**[2*]

[1,2*]İzmit Bilim ve Sanat Merkezi
[1,2*]İzmit Science and Art Center, Uşak, Türkiye

simsekasya16@gmail.com
orcid: 0000-0001-8695-2691

*matemaduygu@gmail.com
orcid: 0000-0002-7400-6363

MAKALE BİLGİSİ / ARTICLE INFORMATION

Geliş Tarihi / Date Received
01.04.2023

Kabul Tarihi / Date Accepted
31.12.2023

Yayın Tarihi / Date Published
Aralık / December 2023

Yayın Sezonu / Pub Date Season
Aralık - Temmuz / December - July

ATIF / CITE as

Şimşek, A., Alyeşil Kabakçı D., (2023). "Geometrik Yapılardaki Yüzey ve Birleşim Noktalarına Göre Şifreleme" / "Encryption According to Surface and Junction Points in Geometric Structures": Bilim Armonisi Dergisi, 6 (2): 42-50. doi: 10.37215/bilar.1275186

https://dergipark.org.tr/tr/pub/bilar

GEOMETRİK YAPILARDAKİ YÜZEY VE BİRLEŞİM NOKTALARINA GÖRE ŞİFRELEME

Encryption According to Surface and Junction Points in Geometric Structures

ANTALYA
İL MİLLÎ EĞİTİM MÜDÜRLÜĞÜ

ÖZET

Haberleşen iki veya daha fazla bireyin güvenli bir şekilde bilgi alışverişi yapabilmesi bilgilerin 3. şahısların ellerine geçmesinin engellenmesinde kriptoloji biliminden yararlanılmaktadır. Kriptoloji biliminin alt dalları olan kriptografi belgelerin şifrelenmesi ve şifresinin çözülmesi için kullanılan yöntemleri; kriptanaliz ise kriptolojik sistemlerin kurduğu sistemlerin incelenmesini ve şifrelerin kırılmasını araştıran alt alanlardır. Şifreleme olarak dallandırılan kriptoloji biliminde matematiksel formül ve algoritmalardan sıkça yararlanılmaktadır.

Yapılan araştırmalar incelendiğinde gerçek yaşamda yer alan yapılardan yararlanılarak geliştirilen formüller yardımıyla bir şifreleme yönteminin geliştirilmediği görülmüştür. Buradan yola çıkarak Barış Piramidi yapısından esinlenerek "mıknatıslı manyetik çubuklar ve toplar kullanılarak üçgensel yüzeylerle piramitler oluşturulmuş, tepe noktasından başlayarak saat yönünün tersine doğru yüzeyler ve toplar numaralandırılmış, kat ve sıra sayısına göre üçgensel yüzeylerin ve topların numarasını bulacak genel kurallar yardımıyla özgün bir şifreleme yöntemi geliştirilebilmesi amaçlanmıştır.

Proje nicel verilere dayalı uygulamalı bir araştırma olup tümevarım yöntemiyle oluşturulan piramit şeklinde yapılardaki top ve yüzey sayıları, kat ve sıra sayılarına göre yüzey ve top numaraları sırasıyla 1. kat 2. kat 3. kat şeklinde hesaplanmış ve genel kuralları çıkarılmıştır. Bulunan formüller Python programında kodlanmıştır.

Anahtar kelimeler: Şifreleme, piramit, modelleme, genel kural

ABSTRACT

The science of cryptology is being used to prevent third parties from accessing the information exchange of two or more individuals in terms of security. Cryptography is a sub-branch of cryptology which investigates the methods used for encryption and decryption of documents; Cryptanalysis, on the other hand, is the sub-fields that investigate the systems established by cryptological systems and the cracking of passwords. Mathematical formulas and algorithms are frequently used in the science of cryptography, which is branched as encryption.

When looking at the research on this topic, it is seen that no encryption method has been developed with the help of the formulas developed by using the structures in real life. Based on this, it is aimed to develop a unique encryption method with the help of general rules to find the number of triangular surfaces and balls according to the number of floors and rows, and the surfaces and balls are numbered counterclockwise starting from the apex, by using magnetic rods and balls with magnets inspired by the Peace Pyramid structure.

The project is applied research based on quantitative data. The number of balls and surfaces in the pyramid-shaped structures created by the inductive method, the surface, and ball numbers according to the number of floors and rows is calculated as the 1st floor, the 2nd floor, the 3rd floor, respectively, and the general rules are deduced. The formulas found are coded using the Python coding language.

Keywords: Encryption, Pyramid, Modeling, General Rule

1. GİRİŞ

Çevremizdeki dünyayı anlayabilme becerisine katkı sunan örüntü ve ilişkiler, belirli bir düzende kurallı bir şekilde devam eden sayı dizileridir. Bu örüntülerin incelenerek içerdiği ilişiklerin keşfettirilmesi, kuralların bulunması ve genelleştirilmesi dünyayı anlama yeteneğini geliştirmektedir. (MEB 2006).

Matematikte örüntülerin meydana getirdiği örneklerin tümevarım yöntemiyle teoremlerin formülleştirilmesine genellemeler öncülük eder (Sriraman 2004). Örüntülerin hayatımızdaki yerine farklı bir perspektiften bakıldığında örüntüler yaşamımızın pek çok yönünü tanımladığını fark ederiz. Matematiksel olarak örüntüler, sayıların veya geometrik şekillerin düzen içinde olan ilişkisidir (Karabel ve Tanışlı 2010). Geometrik pek çok yapıta örüntüler yer almakta bazı yapılarda da piramit, çok yüzlüler gibi geometrik cisimlerden oluşmaktadır. Paris'te yer alan Louvre Müzesi, Bursa'da bulunan Zafer Plaza, Kazakistan'ın Astana şehrinde bulunan üçgen yüzeylerle yapılmış Barış Piramidi de bunlara örnek verilebilir.

"Astana Barış piramidinin tabanı, bir kenarı 60 metre olan kare şeklindedir. Piramit yapısının taşıyıcı sistemi olarak çelik bir uzay kafes sistemi düşünülmüştür. Dış ve iç piramidin yan yüzleri diyagonal çubuklarla üçgenlere bölünerek güçlü bir taşıyıcı sistem elde edilmiştir. " Astana Barış Piramidi Şekil 1,c,d'de verilmiştir (Çeltikçi 2014).

Önemli bilgiler (devletler, bankalar vs.) içeren kurumlar arası iletişimin güvenli bir şekilde gerçekleşmesi oldukça önemlidir. Bu sebeple kriptoloji bilimi, teknoloji çağına geçişle birlikte geliştirilmesi için büyük bir çaba harcanan bilimlerden biridir (Ural ve Örenç 2019). Değişen çağ ile birlikte kriptoloji sanal dünyada güvenlik amacıyla kullanılmaya başlanmıştır (Stallings 2003).Kriptoloji (şifreleme), iletilen mesajlar için güvenlik sağlayan, göndericiyle alıcının arasındaki iletişime farklı kişilerin girmesini önleyerek bilgi iletiminin korunaklı bir şekilde olmasını sağlayan bir bilim dalıdır (Ural ve Örenç 2019). Kriptoloji biliminin temeli matematiksel problemlere, yöntemlere ve tekniklere dayanır. Kriptolojinin iki temel alt dalı bulunur. Bunlardan biri olan "kriptografi, belgelerin şifrelenmesi ve şifrenin çözünmesinde kullanılan yöntemleri araştırırken, kriptanaliz ise kriptolojik sistemlerin kurduğu mekanizmaları inceler ve kırmaya çalışır" (Paar 2010). "Yunan dilinde 'kryptos' (saklı – gizli) ve 'logos' (sözcük) kelimelerinden türetilmiş olan kriptoloji terimi, dilimizde 'gizli sözcük' anlamına gelmektedir. " Bu anlamdan yola çıkarak kriptoloji biliminin sözcüklerin anlamlarını gizlemek, güvenliklerini sağlayarak gizliliği korumak gibi temel amaçlara sahip olduğu söylenebilir (Oppliger R, 2005). Kriptoloji bilimi, cümlelerin şifrelenmesi ve şifrelenmiş cümlelerin anlaşılır hale getirilmesi için kullanılan metotlarla ilgilenir. Bugüne kadar farklı algoritmalar kullanılarak pek çok şifreleme yöntemi geliştirilmiştir (Saboncha vd. 2016). Tarihten günümüze pek çok şifreleme yöntemi geliştirilmiştir. Bunlardan en bilineni Sezar'ın savaşlarda devlet haberleşmesinde kullandığı Sezar şifrelemedir. Bu şifreleme yöntemi olarak normal alfabedeki harflerin yerini değiştirerek oluşturulan şifreleme yöntemiydi ve devlet işlerinde mesajlarının gizliliğinde kullanılırdı. Bu yöntemde alfabedeki her harfi belirli bir sayıda ileri kaydırarak şifreleme yapılmasına dayanırdı. Her harfi belirli bir sabit sayıda ileri kaydırarak farklı harflerle eşleştirilirdi. Bu yöntem açık metindeki her harfin alfabede kendisinden 3 harf sonraki harfle değiştirilmesine dayanıyordu. Bir başka şifreleme yöntemi ise, Vigenère şifreleme yöntemidir.

Bu yöntemde, her karakterin şifrelenmesi için farklı bir alfabeyi temsil eden bir anahtar kullanılır. Anahtar kelime veya dizi, şifrelenecek metin boyunca tekrarlanır ve her karakter için bir kaydırma miktarı olarak kullanılır. Şifrelenecek metindeki bir harf, anahtarın karşılık geldiği harfe göre bir kaydırma yapılarak şifrelenir.

Örneğin; Şifrelenecek kelime: ÖMER olsun. Anahtar kelime: NURİ ise şifrelemek için, Vigenère tablosunda "Ö" harfine karşılık gelen satır bulunarak tabloda satırda "N" harfine karşılık gelen sütun ile kesiştirilir. Bu kesişim noktasında bulunan harf, şifrelenmiş harf olur. Bunların dışında geometrideki doğru denklemlerinin kullanıldığı ve doğrusal denklemler yardımıyla şifrelemelerin yapıldığı şifreleme yöntemi de geliştirilmişti. Doğrusal şifreleme olarak bilinen bu şifreleme yönteminde veriyi şifrelemek için matematiksel bir işlem olan doğrusal bir fonksiyon kullanırdı (Ural ve Örenç 2019).

Bir şifreleme algoritmasının performansı, şifreleme ve çözme işlemlerine harcanan zaman, ihtiyaç duyulan bellek miktarı, kırılabilme süresinin uzunluğu, bu algoritmaya dayalı şifreleme uygulamalarının esnekliği, algoritmaların standart hale getirilebilmesi gibi bileşenlere bağlıdır (Atay 2005; Yerlikaya 2006).

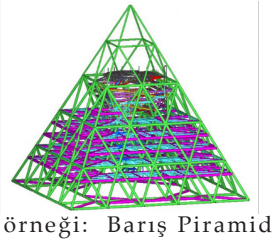
Yapılan araştırmalarda sihirli küpler yardımıyla şifreleme, geometrik örüntülerle şifreleme, Fibonacci sayı dizi ile şifreleme, tek veya çift bölen sayısına göre şifreleme, poincare disk modeli yardımıyla ile şifreleme, küme problemleri yardımıyla (TÜBİTAK 2019a; TÜBİTAK 2019b; TÜBİTAK 2020) gibi pek çok şifreleme yöntemine rastlanmıştır. Geliştirilen şifreleme yöntemleri incelendiğinde pek çok yöntemin geliştirildiği fakat geometrik yapılardan yola çıkılarak bir şifreleme yöntemi geliştirilmediği görülmüştür

Buradan yola çıkarak mıknatıslı manyetik çubuklar ve toplar kullanılarak üçgensel yüzeylerle piramitler oluşturulmuş, tepe noktasından başlayarak saat yönünün tersine doğru üçgensel yüzeyler ve toplar numaralandırılmıştır. Kat ve sıra sayısına göre üçgensel yüzeylerin ve topların numarasını bulacak genel kurallar yardımıyla özgün bir şifreleme yöntemi geliştirilebilir mi? sorusuna yanıt aranmış ve şifrelemede kullanılmak üzere bulunan kurallar python programlama dilinde kodlanmıştır.

2. MATERYAL ve METOT

Proje uygulamalı bir araştırma olup tümevarım yöntemiyle veriler toplanarak yorumlanmıştır. Araştırmada öncelikle literatür taraması yapılarak geometrik yapılar incelenmiş Şekil 1.a,b,c,d'de verilen örnekler incelenmiştir.


Şekil 1.a,b: Geometrik yapı örnekleri: Louvre Müzesi, Bursa Zafer Plaza (Wikipedia 2021)

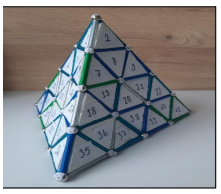
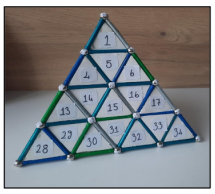
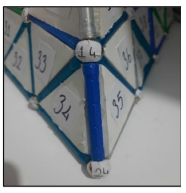



Şekil 1.c,d: Geometrik yapı örneği: Barış Piramidi (Çeltikçi 2014)

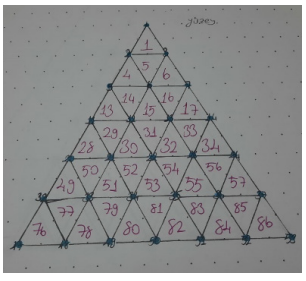
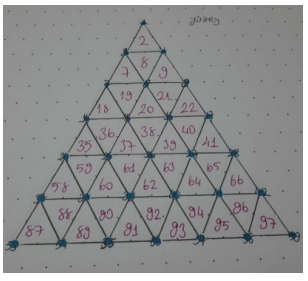
Şifrelemede kullanılmak üzere Barış Piramidinden esinlenerek mıknatıslı manyetik çubuklar ve toplar yardımıyla üçgen piramit şeklinde yapılar oluşturulmuştur. Şekil 2'de görüldüğü gibi modellenerek katlara göre 1. kat, 2. Kat, 3. kat olarak isimlendirilmiştir.

Şekil 1.c,d: Geometrik yapı örneği: Barış Piramidi (Çeltikçi 2014)

Modellerin yüzeylerinde yer alan üçgensel bölgeler ve toplar Şekil 3.a,b,c'de görüldüğü en üst tepeden itibaren sırasıyla saat yönünün tersinde yüzeyler ve taban olmak üzere sırasıyla numaralandırılmıştır. Sayılar kat ve sıra sayısına göre Şekil 4.a,b'deki gibi izometrik kâğıtlara yazılmıştır.

Şekil 3.a,b,c: Modeldeki topların ve yüzeylerin numaralandırılması.

Şekil 4 a.b: Modeldeki topların ve yüzeylerin sırasıyla izometrik kâğıtlarda numaralandırılması.

Kuralların çıkarılmasında aşağıdaki adımlar uygulanmıştır.

- Katlarda bulunan toplam top ve yüzey sayılarından oluşan sayı dizisi oluşturularak tablo 4'de bir araya getirilerek katlarda bulunan yüzey ve top sayılarının genel kuralı çıkarıldı.

- Modellerde yer alan top numaraları, yüzey numaraları ve tabanlarda yer alan numaralar tablo 5 ve tablo 6 'da bir araya getirilmiştir. Tabanlar aynı zamanda yüzey olduğundan sıralama yapılırken tabanda yer alan üçgensel bölgeler, 3. yüzey son numarasından sonraki sayıdan başlanarak numaralandırılmıştır. Örneğin 1 model için, 1.2.3. yüzeyden sonra tabandaki üçgensel bölge 4. yüzey olarak, başka bir örnek olarak 3. modelde 3. yüzeyin son numarası 27 sayısından sonra, 4. yüzey olan tabana geçilerek tabandaki üçgensel bölgeler 28,29,30... şeklinde numaralandırılırmıştır).

1.Tablolarda bir araya getirilen veriler incelenerek sayılar arasındaki matematiksel ilişkiler ve örüntüler incelenmiş, oluşan sayılar dizi halinde ifade edilerek farklama yöntemiyle m, kat ve r sıra numarası olmak üzere üçgensel yüzeyin numarasını ve topun numarasını bulacak kurallar geliştirilmiştir.

2.Numaralandırmada taban da 4. yüzey olarak devam ettiğinden ve taban son katın devamı şeklinde yazıldığından sıra sayısı kattaki toplam üçgensel yüzey sayısına eşit veya büyük olunca numaralandırma tabana geçeceğinden formüller sıra sayısına göre parçalı fonksiyon şeklinde iki forma yazılmıştır.

3.Bulunan formüller Tablo 7'de yer aldığı gibi genel kurallar tablosu başlığında bir araya getirilmiştir.

Bu sayede herhangi bir modelin herhangi bir sırasındaki herhangi bir üçgensel yüzeyin numarasını ve topun numarasını bulacak genellemeler elde edilmiştir. İlişkiler irdelenerek, kurallar yardımıyla özgün bir şifreleme yöntemi geliştirilmiştir. Şifreleme için öncelikle 29 farklı harfin bulunduğu tablo 1 'deki gibi bir şifreleme harf tablosu hazırlanmıştır.

Çizelge 1. Şifrelemede kullanılacak harf tablosu

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

2.2. Şifreleme:

Şifreleme tek sayılı günlerde yüzey numarası çift sayılı günlerde top numarası formülü olmak üzere 2 şekilde olarak tasarlanmıştır. Bu işlem her kendi arasında her yeni mesajda yer şekilde değişir. Örneğin Ocak ayının 3'ünde şifre gönderiliyorsa yüzey numarasına göre 4'ünde gönderiliyorsa top numarasına göre şifreleme yapılır. Bir sonraki mesajda ise tam tersi uygulanarak tek sayılı günlerde top numarası çift sayılı günlerde yüzey numarası temel alınarak şifreleme yapılır. Şifrelemede çarpanlara ayırma, gönderilen tarih gibi pek çok değişken kullanılması ve iki farklı formülün olması da deşifre edilmesini de imkânsıza yakın derecede zorlaştıracaktır.

Şifreleme şu şekilde yapılacaktır;

Yüzey numarasına göre şifreleme

• Şifrelenecek harfin tablodaki sayı değeri bulunur.

• Şifrelemede piramidin kaçıncı katının kaçıncı sırasındaki yüzeyin kullanılacağı tespit edilir. Kullanılacak yüzey numarasının bulunması için bulunan formülde (tablo 5) kat ve sıra sayıları yerine koyularak hesaplanır.

• Bulunan yüzey sayısı çarpanlarına ayrılır. Çarpanlar arasından bir çift belli bir kriter belirlenerek. Bu şifrelemede tercihen toplamının en küçük değer alması kriteri belirlendiğinden çarpanları birbirine en yakın olan sayı çifti alınmıştır. Fakat bu kriter her mesajda değiştirilerek, (örneğin başka bir mesajda çarpan çift toplamı en büyük olacak şekilde) seçilecektir. Veya her bir şifrede bu kural belli bir algoritmayla değiştirilerek şifreleme yapılması tercih edilebilir. Bu da şifreli metnin çözülme ihtimalini zorlaştıracaktır.

• Bulunan toplam ile şifrelenecek harfin tablodaki sayı değeri, şifrenin gönderildiği tarih ayın kaçı ise o sayı toplanır.

• Elde edilen sayının mod 29'e göre sonucu bulunur ve harf tablosuyla eşleştirilerek hangi sayıya denk geldiği hesaplanarak ilk harfi temsilen yazılır.

• Şifrenin yazımında kat ve sıra sayıları şifrenin en başında yazılarak şifreleme yazılır, boşluklarda ve bir sonraki harfe geçmeden önce harfler arasına o gün ayın kaçı ise o sayı yazılır her harfte bu sayıya 1 eklenerek boşluklara yerleştirilir.

Örneğin nisan ayı ise ilk harfe karşılık gelen sayıdan sonra 4, 2. Harfe karşılık gelen sayıdan sonra 5,.... şeklinde devam eder.

Top numarasında göre şifrelemede de aynı uygulamalar yapılır farklı olarak top numarasının bulunması için kat ve sıra sayıları bulunan formülde (tablo 6) yerine koyularak hesaplanır.

2.2. Deşifreleme:

Deşifrelemede aşağıdaki adımlar izlenilecektir:

• Şifreli metnin başındaki sayılar aralarında o günün hangi ay olduğunun sayı değeri ile ayrılarak belirlenir. Örneğin Temmuz ayında gönderilen ve 1379 ile başlayan bir şifrelemede temmuz ayı ayın 7'i olduğundan kat sayısı 13 sıra sayısı 9 olarak bulunur.

• Şifrelenmiş olan harfin sayı değeri bulunur.

• Kullanılan yüzey numarasının bulunması için kat ve sıra sayıları bulunan formülde (tablo 5) yerine konularak hesaplanır.

• Bulunan yüzey sayısı çarpanları birbirine en yakın olacak şekilde çarpanlarına ayrılır ve bu çarpanların toplamı bulunur. (Bu örnek için bu kriter alınmıştır kriter her şifrede değiştirilecektir. Çarpanları toplamı en büyük çarpanları oranı ¾ olacak şekilde gibi)

• Bu toplam şifrenin gönderildiği tarih ayın kaçı ise bu sayı ile toplanarak bulunan sayı harfin eşleştiği sayıdan çıkarılır.

• Bulunan sonuca modüler toplama ile pozitif olana kadar 29 eklenir elde edilen sonuç harfin eşleşeceği sayı değerini verir.

• Bulunan sayı harf tablosundaki sayı ile eşleştirilerek harf değeri bulunur.

Top numarasında göre deşifrelemesinde de aynı uygulamalar yapılır, farklı olarak top numarasının bulunması için kat ve sıra sayıları bulunan formülde (tablo 6) yerine koyularak hesaplanır. Şifrelemede aynı harf olsa bile her seferinde farklı sayılara ulaşacağından, aynı harf birden çok sayıya denk geleceğinden ve tarihler değiştikçe aynı kelimeler farklı harflerle eşleşeceğinden şifrenin kırılma olasılığı en aza indirilmiştir.

Şifrelemenin yapılmasında işlem hatası riskini ortadan kaldırmak amacıyla şifreler python dilinde kodlanmıştır. Kodlar Tablo 2'de verilmiştir.

Çizelge 2. Bulunan formülün python dilinde kodlanması

Python Programında Formülün Kodlanması

```
a=int(input("Hangisini seçiyorsunuz 1/2 : "))
if a==1:
 m=int(input("m sayısını giriniz : "))
 r=int(input("r sayısını giriniz : "))
 if r<=(6*m-3):
   print(3*(m**2)-6*m+r+3)
 elif r>6*m-3:
    print(3*(m**2)+r)
 elif a==2:
   m=int(input("m sayısını giriniz : "))
   r=int(input("r sayısını giriniz : "))
   if r<=(3*m*(m-1))/2:
      print(((3*(m**2)-9*m+10)/2)+r-1)
   elif r>(3*m*(m-1))/2:
      print(((3*(m**2)-3*m+4)/2)+r-1)
```

3. BULGULAR

Çizelge 4. Herhangi bir modeldeki katlarda yer alan toplam top sayıları

Modellere göre bir model için m=kat sayısı olmak üzere

Kat	Toplam top sayıları	Katlardaki yüzey sayıları
1. kat	1	3
2. kat	3	9
3. kat	9	15
4. kat	18	21
5. kat	30	27
6. kat	45	33
7. kat	63	39
. . .	. . .	. . .
m. kat	m≠1 için , 3m(m-1)/2 m=1 için, 1	6m-3

Her bir kattaki toplam top sayıları genel kuralı 3m(m-1)/2 olarak bulundu.

Her bir kattaki yüzey sayıları genel kuralı (6m-3) olarak bulundu.

Çizelge 5. Herhangi bir modeldeki üçgensel bölgelerin yüzeylerinde yer alan sayılar

Herhangi bir model. için m=kat r=sıra

Kat	Yüzeydeki Sayılar	Tabandaki Sayılar
1. kat	1	3
2. kat	3	9
3. kat	9	15
4. kat	18	21
5. kat	30	27
. . .	. . .	. . .
m. kat	Katlardaki üçgensel bölgelerin 1.2.3.....r. sırasındaki numaraların genel kuralları $(3m^2-6m+4),(3m^2-6m+5),$ $(3m^2-6m+6)...(3m^2-6m+(r+3))$ $f:Z^+ x Z^+ \rightarrow Z^+$ $f(m,r)=(3m^2-6m+(r+3))$	Piramitlerin tabanında yer alan üçgensel bölgelerin 1.2.3.....r. sırasındaki numaraların genel kuralları $(3m^2+1),(3m^2+2),(3m^2+3)...$ $(3m^2+r)$ $f:Z^+ x Z^+ \rightarrow Z^+$ $f(m,r)=(3m^2+r)$

Katlarda yer alan üçgensel yüzeylerdeki ilk sayıların genel kuralı;

f(m) = 1 - 4 - 13 - 28 - 49 - 76 ... $(3m^2-6m+4)$ olarak bulundu.

Her kattaki üçgensel yüzeylerin numaraları birer birer artarak devam ettiğinden herhangi bir katın(m) herhangi bir sırasındaki(r) üçgensel yüzeyin numarasını bulacak genel kural $f(m,r)=(3m^2-6m+(r+3))$ olarak bulundu

Tabanlardaki üçgensel yüzeylerinde yer alan numaraların herhangi bir katın(m) herhangi bir sırasındaki(r) üçgensel yüzeyin numarasını bulacak genel kuralı $f(m,r)=(3m^2+r)$ bulundu.

Çizelge 6. Katlara göre Üçgen piramitlerin üçgensel bölge köşelerindeki toplarda yer alan sayılar

n. model için m=kat r=sıra

Kat	Sırasıyla modelde yer alan top numaraları m-1. kata kadar olan formüller	Tabanda yer alan top numaraları m. kat
1. kat	1	-
2. kat	2,3,4	-
3. kat	5,6,7,8,9,10	-
4. kat	11,12,13,14,15,16,17,18,19	20
5. kat	20,21,22,23,24,25,26,27,28, 29,30,31	32,33,34
. . .	. . . .	. . .
m. kat	$\left(\frac{3m^2-9m+10}{2}\right),\left(\frac{3m^2-9m+10}{2}+1\right),$ $\left(\frac{3m^2-9m+10}{2}+2\right)....\left(\frac{3m^2-9m+10}{2}+(r-1)\right)$ $f: Z^+ x Z^+ \rightarrow Z^+$ $f(m,r)=\left(\frac{3m^2-9m+10}{2}+(r-1)\right)$ m>1 m=1 için f(1,1)=1	$\left(\frac{3m^2-3m+4}{2}\right),\left(\frac{3m^2-3m+4}{2}+1\right),$ $\left(\frac{3m^2-3m+4}{2}+2\right),\left(\frac{3m^2-3m+4}{2}+3\right)...$ $\left(\frac{3m^2-3m+4}{2}+(r-1)\right)$ $f: Z^+ x Z^+ \rightarrow Z^+$ $f(m,r)=\left(\frac{3m^2-3m+4}{2}+(r-1)\right)$ m>3

f(m)=1-2-5-11-20-32-47-65...$((3m^2-9m+10)/2)$ olarak bulundu.

Her kattaki top numaraları birer birer artarak devam ettiğinden herhangi bir katın(m) herhangi bir sırasındaki(r) topun numarasını bulacak genel kural $f(m,r)= (3m^2-9m+10)/2+(r-1)$ olarak bulundu.

Çizelge 7. Bulunan Genel Kurallar

Katlardaki toplam yüzey sayıları	6m-3
Üçgensel bölgelerin yüzeylerinde yer alan yüzeydeki sayılar	$f(m,r)=(3m^2-6m+(r+3))$
Üçgensel bölgelerin yüzeylerinde yer alan tabandaki sayılar	$f(m,r)=(3m^2+r)$
Üçgensel bölge köşelerindeki toplarda yer alan yüzeydeki sayılar	$(m,r)=((3m^2-9m+10)/2+(r-1))$
Üçgensel bölge köşelerindeki toplarda yer alan tabandaki sayılar	$f(m,r)=((3m^2-3m+4)/2+(r-1))$

Yüzey numaralarına şifreleme formülü; Taban son katın devamı şeklinde yazıldığından sıra sayısı kattaki toplam üçgensel yüzey sayısına eşit veya büyük olunca numaralandırma tabana geçeceğinden genel formül r sıra sayısının tabana geçeceği duruma göre;

$$f(m,r)=\begin{cases}3m^2-6m+(r+3), & r\le 6m-3\\ 3m^2+r, & r>6m-3\end{cases}$$

olarak yazıldı.

Top numaralarına şifreleme formülü; Taban son katın devamı şeklinde yazıldığından sıra sayısı kattaki toplam top sayısına eşit veya büyük olunca numaralandırma tabana geçeceğinden r sıra sayısının tabana geçeceği duruma göre;

$$f(m,r)=\begin{cases}\frac{3m^2-9m+10}{2}+(r-1), & r\le\frac{3m(m-1)}{2}\\ \frac{3m^2-3m+4}{2}+(r-1), & r>\frac{3m(m-1)}{2}\\ f(1,1)=1\end{cases}$$ olarak yazıldı.

Örnek olarak 23.03.2022 tarihinde göndereceğimiz ''BİLİMSEL'' kelimesini piramitteki 52. katın 21. sırasındaki top veya yüzey numarasına göre şifrelemesini ve deşifrelenmesi yapalım.

Şifrenin gönderileceği tarih 3. ay ve ayın 23'ü olduğundan Mart ayı 3. ay ve 3 de tek sayı olduğundan yüzey numarasına göre şifreleme yapılır.

İlk harf olan B için;

• B harfinin tablodaki sayı değeri 1 olarak bulunur.

• Şifrelemede 52. katın 21 sırasındaki üçgensel yüzeyin numarası

$f(m,r)=\{3m^2-6m+(r+3),\ r\le 6m-3$

$3m^2+r,\ r>6m-3\}$

formülünde yerine koyularak hesaplanır.

m = 52, r = 21

$r\le 6m-3$ için yerine koyarsak $21\le 309$ olacağından $3m^2-6m+(r+3)$ formülünü kullanırız.

$3.52^2-6.52+(21+3)=8112-312+24=7824$

Üçgensel yüzeyin numarasını 7824 olarak buluruz

• Bulunan yüzey sayısı çarpanları birbirine en yakın olacak şekilde çarpanlarına ayrılır ve bu çarpanların toplamı bulunur.

$7824=48.163$ $163+48=211$

• Bulunan toplam ile şifrelenecek harfin tablodaki sayı değeri ve şifrenin gönderildiği tarih ayın kaçı ise o sayı toplanır.

$211+1+23=235$

• Elde edilen sayının mod 29'e göre sonucu bulunur ve bulunan sayının günün harf tablosundaki değeri ile eşleştirilerek hangi sayıya denk geldiği hesaplanır. İlk harfi temsilen yazılır.

$235\equiv 3\ (mod29)$

3 harf tablosunda D harfine denk geldiğinden ''D'' olarak şifrelenir.

İkinci harf İ için;

• Şifrelenecek harfin tablodaki sayı değeri 11 olarak bulunur.

• Şifrelemede 52. katın 21 sırasındaki üçgensel yüzeyin numarası 7824 olarak buluruz

• Bulunan yüzey sayısı çarpanları birbirine en yakın olacak şekilde çarpanlarına ayrılır ve bu çarpanların toplamı 211 olarak bulunur bulunur.

• Bulunan toplam ile şifrelenecek harfin tablodaki sayı değeri ve şifrenin gönderildiği tarih ayın kaçı ise o sayı toplanır.

$211+23+11=245$

• Elde edilen sayının mod 29'e göre sonucu bulunur ve bulunan sayının günün harf tablosundaki değeri ile eşleştirilerek hangi sayıya denk geldiği hesaplanır. İlk harfi temsilen yazılır.

$245\equiv 13\ (mod29)$

13 harf tablosunda K harfine denk geldiğinden ''K'' olarak şifrelenir.

Benzer şekilde devam ettirilerek "BİLİMSEL" kelimesi "DKNKOTGN" olarak şifrelenir.

• Şifrenin yazımında kat ve sıra sayıları arasına şifrenin gönderildiği ayın sayısal değeri yazılarak başlanır. Boşluklarda ve bir sonraki harfe geçmeden önce harfler arasına o gün ayın kaçı ise o sayı yazılır her harfte bu sayıya 1 eklenerek boşluklara yerleştirilir.

BİLİMSEL = 52321"DKNKOTGN"

Şifrenin çözümü

Şifrenin gönderileceği tarih ayın 3'ü ve 23 olduğundan Mart ayı ayın 3ü ve 3 sayısına de tek sayı olduğundan yüzey numarasına göre deşifreleme yapılır.

• Şifreli metinin başındaki sayılar aralarında o günün hangi ay olduğunun sayı değeri ile ayrılarak belirlenir. Şifre Mart ayında (3) gönderildiğinden şifrenin başındaki 52321 ifadesinde 3 ile sayısının solundaki ve sağındaki sayılar olan m=52 kat sayısı r=21 sıra sayısı olarak belirlenir.

• Kullanılan yüzey numarasının bulunması için kat ve sıra sayılarına göre bulunan formülde

$f(m,r)=\{\ 3m^2-6m+(r+3),\quad r\le 6m-3$

$3m^2+r,\quad r>6m-3\}$

$r\le 6m-3$ için $21\le 309$ olduğundan $3m^2-6m+(r+3)$ formülünde yerine koyularak hesaplanır.

$3.52^2-6.52+(21+3)=8112-312+24=7824$

Bulunan yüzey sayısı çarpanları birbirine en yakın olacak şekilde çarpanlarına ayrılır ve bu çarpanların toplamı bulunur.

$7824=48.163$ $163+48=211$

• Bu toplam şifrenin gönderildiği tarih ayın kaçı ise bu sayı ile toplanarak, bulunan sayı harfin eşleştiği sayıdan çıkarılır. Bulunan sonuca modüler toplama ile pozitif olana kadar 29 eklenir elde edilen sonuç harfin eşleşeceği sayı değerini verir.

211+23=234

3-234≡-211 ≡1(mod29)

Bulunan 1 sayısı sayı harf tablosundaki B harfine denk gelir.

Benzer şekilde devam ettirildiğinde BİLİMSEL olarak deşifrelenir.

Geliştirilen şifreleme kriptoanaliz yöntemlerinden olan metnin bölümlere ayrılarak çözümlenmesi yoluyla analiz edilen düz metin saldırısına karşı formülün çok değişkenlerce sürekli değişen değerlerle oluşturulması nedeniyle ve bir harf için her seferinde farklı harfler eşleştiğinden harf analizi metoduyla ve diğer metodlarla çözülmesiyle de çözülmesi zor bir kriptoloji yöntemidir. Bu şifreleme yöntemi şifrenin kırılması açısından değerlendirildiğinde, basit bir hesaplama ile yaklaşık olarak belirlemek gerekirse:

Yüzey numarasına göre oluşturulmuş ve tek basamaklı bir ayda gönderilmiş olduğu bilinen bir şifre için, şifrede verilen sayıdaki sıra ve kat sayılarını, seçilen ayın sayı değeri ile ayırıyorduk. Bu sayının hangi ay olacağının bulunma ihtimali şifreli sayının basamak sayısına göre değişecektir örneğin 20 basamaklı bir sayı ve tek basamaklı bir ay (örneğin mart (3)) için tek basamaklı ay sayısı 9 olduğundan, ay sayısına göre ayrıldığı bilindiğinde $(1/9)^{20}$ olacaktır. Bu değer bulunduğunda bulunan iki sayının birinin kat diğerinin sıra sayısını oluşturduğu düşünüldüğünde bunların tahmin edilme olasılığıyla birlikte $(1/9)^{20}.1/2$ olacaktır.

Bu sayılar bulunan genel formülde yerleştirileceğinden dolayı bu genel formül bilinse dahi, sayılar formülde yerine konulduğunda bulunan sayının çarpanlarına ayrılması sayının basamak sayısına göre değişecektir. Bir sayıyı asal çarpanlarına ayırmak için sayıyı tek tek asal sayılara bölerek bütün temel işlem sonuçlarını değerlendirmesi gerekir. Bu ise bilgisayar programlarıyla bile zaman alan bir süreç olacaktır. Örnek olarak 20 basamaklı bir şifrede yüzey, kat ve sıra sayısına göre bulunan sonuç m olsun ve bu sayının p adet çarpan çifti bulunsun. Bu da seçilen çarpan çiftinin hangisi olacağının bulunma ihtimalinin 1/p olması demektir.

Şifrelemede şifrenin gönderildiği tarih veya seçilen özel bir tarih belirleneceğinden bir ayda 30 gün olduğundan 1/30 ihtimalle belirlenen gün bulunabilecek, tüm bu olasılıklar çarpıldığında yani 20 basamaklı bir şifreli sayı ile belirtilen bir metinde genel formül bilindiği varsayıldığında şifrelenmiş harfin bulunma ihtimali;

$\frac{1}{p}.\left(\frac{1}{9}\right)^{20}.\frac{1}{30}.\frac{1}{2} == \frac{1}{p.729459928.10^{23}}$ 'dir. 30 basamak olduğunda ise $\frac{1}{p.25434695.\ 10^{30}}$ olacaktır. Basamak sayısına n dersek $\frac{1}{p}.\left(\frac{1}{9}\right)^{n}.\frac{1}{30}.\frac{1}{2}$

Bu ihtimal şifrenin basamak sayısı arttıkça kuvvet değeri kadar artacağından formülün bulunma ihtimali de düşünüldüğünde yapılan şifreleme kırılması zor bir şifrelemedir denilebilir.

4. SONUÇ ve TARTIŞMA

Sonuç olarak bu projede mıknatıslı manyetik çubuklar ve toplar kullanılarak üçgensel yüzeylerle piramitler oluşturulmuş ve tepe noktasından başlayarak saat yönünün tersine doğru üçgensel yüzeyler ve toplar numaralandırılmıştır. Kat ve sıra sayısına göre üçgensel yüzeylerin ve topların numarasını bulacak genel kurallar bulunmuştur ve bu kurallar yardımıyla özgün bir şifreleme yöntemi geliştirilmiştir. Bu şifreleme yönteminde iki farklı formül ve şifrelemede çarpanlara ayırma, gönderilen tarih gibi pek çok değişken kullanılmıştır.

Bu sayede deşifre edilmesi de imkânsıza yakın derecede zor olan bir şifreleme yöntemi elde edilmiştir. Bu proje, numara sayısına göre konumu bulunacak şekilde de araştırılabilir. Farklı geometrik modellerde uygulanabilir. Modellemede eşkenar üçgenler yerine eşkenar dörtgenler kullanılarak kurallar bulunabilir. Topların etrafında bulunan yüzeyleri bulacak genel kural bulunup şifrelemede kullanılabilir.

KAYNAKLAR

Atay, S. (2005). "Eliptik Eğri Tabanlı Kriptografik Protokol ve Akıllı Kart Üzerinde Bir Uygulama". Ağ ve Bilgi Güvenliği Sempozyumu.

Çeltikçi, N. (2014). "Kazakistanda Bir Anıt Proje: Barış Piramidi". Erişim Adresi: https://www.tucsa.org/tr/proje.aspx?proje=36 Erişim tarihi: 11.12.2021.

Kabael, T. U., Tanışlı, D. (2010). "Cebirsel Düşünme Sürecinde Örüntüden Fonksiyona Öğretim". İlköğretim Online, 9(1): 213-228.

[MEB] (2006). "Ortaöğretim Matematik Dersi Öğretim Programı ve Kılavuzu". Ankara-Türkiye. Erişim Adresi: https://mufredat.meb.gov.tr/ProgramDetay.aspx?PID=329 Erişim Tarihi: 11.12.2021.

Oppliger, R.(2005). Contemporary Cryptology. Artec House. Norwood, MA- USA.

Paar, C., & Pelzl, J. (2009). Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media. Berlin-Almanya.

Sabonchı, A., Obaıd, Z., Akay, B. (2016). "Klasik Kriptoloji Yöntemlerinin Karşılaştırılması". Engineering Sciences,11 (4): 100-108.

Sriraman, B. (2004). "Reflective abstraction, uniframes and the formulation of generalizations". Journal of Mathematical Behavior, 23 (2): 205-222.doi: https://doi.org/10.1016/j.jmathb.2004.03.005.

Stallings, W. (2003). "Cryptography And Network Security, Third Edition". New Jersey.

[TÜBİTAK] (2019a). "13. Ortaokul Öğrencileri Araştırma Projeleri Yarışması Final 2019 Kitapçığı".

[TÜBİTAK] (2019b). "50. Lise Öğrencileri Araştırma Projeleri Yarışması Final 2019 Kitapçığı".

[TÜBİTAK] (2020). "51. Lise Öğrencileri Araştırma Projeleri Yarışması Final 2020 Kitapçığı".

Ural, N., Örenç, Ö. (2019). Şifreleme ve Şifre Çözme Yöntemleri: Pusula Yayınevi. İstanbul-Türkiye.

Yerlikaya, T.(2006). "Şifreleme Algoritmalarının Analizi". Yayınlanmamış Doktora Tezi, Trakya Üniversitesi. Edirne-Türkiye.

Wikipedia. (2021). Wikipedia web sitesi: https://tr.wikipedia.org/wiki/Louvre_M%C3%BCzesi adresinden alındı.

Wikipedia. (2021). Wikipedia web sitesi: https://tr.wikipedia.org/wiki/Zafer_Plaza adresinden alındı.