Doğu Fen Bilimleri Dergisi / Journal of Natural & Applied Sciences of East 8(1): 1-15 (2025)

Araştırma Makalesi / Research Article

Bütünleşik Kodlama Modellemesi ile Karesel ve Üçgensel Sayılardan Algoritmik Şifreleme Oluşturulması

Bahar KULOĞLU[1*]

[1] Sivas Bilim ve Teknoloji Üniversitesi, Sivas, Türkiye
e-mail: bkuloglu@sivas.edu.tr

DOI: 10.57244/dfbd.1567632
Geliş tarihi/Received:15/10/2024 Kabul tarihi/Accepted:18/03/2025

Özet

Bu çalışmada 29 harfli Türk alfabesine karşılık gelen rakamlar boşluk (●) dahil "n "den "n+29 "a kadar yazılmıştır. Kodlanacak kelime veya herhangi bir verinin her bir harfine karşılık gelen sayılar harf sırasına göre yazılmış ve sayılar mod30'a göre yeniden düzenlenmiştir. Daha sonra mod30'a göre düzenlenen sayılara karşılık gelen harf kullanılarak oluşturulan metnin her harfini temsil eden bir kod oluşturulmuştur. Kodlanan metnin her türlü saldırı ve virüslere karşı korunması amacıyla $Z_{n+1}Z_{n-1} - Z_n^2 = -2n^2 + 1$ (Karesel sayılar için Cassini Özdeşliği) ile ikinci dereceden sayılardan oluşan matris formatının (Z_n) her bir elemanı belirli işlem ve yöntemlerden sonra çözülmüştür. Özellikle çalışmanın devamında yukarıda verilen şifreleme işlemlerine farklı bir boyut kazandırmak yani daha güçlü bir şifreleme ve şifre çözme algoritması oluşturarak geçerlilik ve güvenilirliğini arttırmak amacıyla i'nin tek veya çift olmasına göre hem karesel hem de üçgensel sayılar dikkate alınarak "Bütünleşik Kodlama" adını verdiğimiz yeni bir şifreleme modellemesi oluşturulmuştur.

Anahtar Kelimeler: Kriptoloji, Metin şifreleme, Karesel sayılar, Üçgensel sayılar

Generating Algorithmic Cipher from Quadratic and Triangular Numbers with Integrated Coding Modelling

Abstract

In this study, the numbers corresponding to the 29-letter Turkish alphabet were written from ‘n’ to ‘n+29’ including the space (●). The numbers corresponding to each letter of the word or any data to be coded were written in letter order and the numbers were rearranged according to mod30. Then, a code representing each letter of the text was created by using the letter corresponding to the numbers arranged according to mod30. In order to protect the encoded text against all kinds of attacks and viruses, $Z_{n+1}Z_{n-1} - Z_n^2 = -2n^2 + 1$ (Cassini Identity for quadratic numbers) and each element of the matrix format consisting of quadratic numbers (Z_n) was decoded after certain operations and methods. In the continuation of the study, to add a different dimension to the encryption processes given above, that is, to increase the validity and reliability by creating a stronger encryption and decryption algorithm, a new encryption modelling, which we call ‘Integrated Coding’, has been created by considering both quadratic and triangular numbers according to whether is odd or even.

Keywords: Cryptology, Text encryption, Quadratic numbers, Triangular numbers.

Giriş

Kriptoloji, bilgilerin gizlenmesi ve korunması için kullanılan matematiksel tekniklerin bir bütünüdür (Kriptografi, 2023). En basit tanımıyla şifreleme bilimi olarak da bilinen bu alan, bilginin istenmeyen kişiler tarafından okunamayacak şekilde yeniden farklı bir forma dönüştürülmesini sağlar.

Kriptolojinin tarihi, insanlığın bilgi güvenliğine duyduğu ihtiyaç kadar eskidir. Mısır hiyerogliflerinden Jül Sezar'ın kullandığı şifreleme yöntemine kadar uzanan bu tarih, günümüzde dijital dünyanın güvenliğini sağlamada da kritik rol oynamaktadır.
Yapılan literatür taramalarında sayı dizileri üzerinde birçok şifreleme ve şifre çözme algoritmalarına rastlamaktayız (Kuloğlu ve ark., 2023a; Kuloğluve ark., 2023b; Eser ve ark., 2023; Uçar ve ark., 2019; Stakhov, 1999; Dişkaya ve ark.; 2022; Stakhov, 2006; Basu ve ark., 2009; Wang ve ark., 2010; Prajapat ve ark., 2014).

Sayı dizilerini temel alan şifreleme ve şifre çözme algoritmaları, kriptolojinin temelini oluşturur. Teknolojinin gelişmesiyle birlikte dijital bilginin güvenli iletimi ve korunması daha da önem kazanmıştır. Bu bağlamda, karesel sayılar (Eric), matrisler ve determinantlar üzerine kurulu yeni bir kodlama ve kod çözme algoritması geliştirilmiştir.

Algoritmamızın temel özellikleri: Virüslere, frekans saldırılarına ve yetkisiz erişime karşı daha yüksek güvenlik, askeri, politik, ticari ve kişisel alanlarda kullanılabilirlik, akıllı kartlar, yazılım ve donanım uygulamaları, blok ve akan şifreler gibi geniş bir yelpazede uygulama imkânı, modern kripto analiz yöntemleriyle uyumluluk olup; çalışmanın amacı ise bilgi güvenliğine yönelik yeni ve daha güvenilir bir çözüm sunmak, farklı alanlarda kullanılabilecek esnek ve güçlü bir algoritma geliştirmek ve kriptoloji bilimine katkıda bulunmaktır.

Bütün bu çalışmalardan esinlenip üzerinde çalışılmış olan şifreleme ve şifre çözme sistemlerini göz önüne alarak daha önce çalışılmamış karesel sayılarla matris/determinant ilişkileriyle isimlendirdiğimiz Bütünleşik Kodlama modeliyle daha güçlü bir şifreleme yöntemi olarak oluşturuldu.
Fibonacci dizisi F_n, $F_0 = 0$ ve $F_1 = 1$ başlangıç şartları olmak üzere

$$F_{n+1} = F_{n-1} + F_n, n \geq 1, n \in N$$

bağıntısıyla verilir. Bu dizinin ilk birkaç terimi; 0,1,1,2,3,5,8,13,21,34, … şeklindedir.

Fibonacci matrisi,

$$Q = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$$

şeklinde tanımlanır. Burada dikkat edilirse Q matrisinin determinantı, $detQ = (-1)^n$dir. Örneğin $n = 5$ için

$$detQ = det\begin{pmatrix} F_6 & F_5 \\ F_5 & F_4 \end{pmatrix} = \begin{pmatrix} 8 & 5 \\ 5 & 3 \end{pmatrix} = 8.3 - 5.5 = (-1)^5 = -1$$

Fibonacci dizileri için Cassini özdeşliği (Beall)

$F_{n+1}F_{n-1} - F_n^2 = (-1)^n, n \geq 1$ bağıntısı ile verilir.

Sayı dizileri için de önemli bir eşitlik olan ve Curry paradoksunun çözümü gibi birçok yerde kullanıma sahip olan Cassini özdeşliği, her iki modellemede de kullanılmıştır. İlginç olan ve bizi kullanıma iten güç tabiki Fibonacci matrisinin determinant değerinin Cassini özdeşliğinin sağ tarafını vermesidir.
Yaptığımız bu şifreleme yöntemi, günümüzde bilgi güvenliği son yıllarda daha önemli bir sorun haline geldiğinden bu alanda yapılan kodlama ve kod çözme algoritmaları bu güvenliğin geliştirilmesine katkı sağlayabileceği düşünülmektedir.

Materyal ve Yöntem

Bu çalışmada yapılan literatür taraması ile matematiksel işlemlerde kullanılan mantıksal tasarım ve bilimsel metotlardan yararlanılmıştır.

Bu anlamda sayı dizilerine karşı artan ilgi de göz önüne alınarak ilk olarak yapılan çalışmalar üzerinde durduğumuzda Fibonacci sayıları ya da Pascal üçgeninin bağlantılı örnekleri incelenmiş olup bu sayıların doğada, bilimde özellikle "ALTIN ORAN" adı altında birçok uygulamasına rastlanılmıştır. Bu bağlamda ilham kaynağım bu şekilde bir örüntüye sahip olan Pascal üçgeni ile özdeşleştirmiş olduğumuz karesel sayılar olmuştur. Karesel sayılar ilk terimleri 1, 4, 9, 16, … olan ve genel terimi$Z_n = n^2$ şeklinde tanımlanmış bir sayı dizisidir ("Karesel sayı," 2023).

Çalışmanın devamında yukarıda verilen şifreleme işlemlerine farklı boyut kazandırmak amacıyla yani daha güçlü bir şifreleme ve şifre çözme algoritması oluşturularak geçerlilik ve güvenirliliğin artırılması için i nin tek ve çift olma durumuna göre hem karesel hem de üçgensel sayılar ele alınıp "Bütünleşik Kodlama" adını verdiğimiz yeni bir şifreleme modellemesi oluşturulmuştur.

Bu modelleme de şifrelerken karesel sayılar ve blok matrisler kullanılırken şifre çözmede ise matrisin determinantına karşılık gelen karesel sayılar için Cassini özdeşliği, $Z_{n+1}Z_{n-1} - Z_n^2 = -2n^2 + 1$, kullanılmıştır.

Bulgular

Bu kısımda şifreleme ve şifre çözmede sayı dizilerinden yararlanılmıştır. Matris yöntemi ile oluşturacağımız 4×4 mertebeli X matrisi, 2×2 mertebeli B_1, B_2, B_3 ve B_4blok matrislerine aşağıdaki gibi ayrılır. Yani

$$X = \begin{pmatrix} a & z & c & d \\ e & f & g & h \\ k & l & m & n \\ o & ö & p & r \end{pmatrix}$$

$B_1 = \begin{pmatrix} a & z \\ e & f \end{pmatrix}$, $B_2 = \begin{pmatrix} c & d \\ g & h \end{pmatrix}$, $B_3 = \begin{pmatrix} k & l \\ o & ö \end{pmatrix}$ ve $B_2 = \begin{pmatrix} m & n \\ p & r \end{pmatrix}$ matrisleri elde edilir.

Blok matris sayısını b ile gösterirsek; n' yi

$n = \begin{cases} 3, & b \leq 3 \\ b, & b > 3 \end{cases}$ şeklinde tanımlayabiliriz. Bu çalışmada karesel sayılar ve buna bağlı olarak elde edilen "Cassini özdeşliği" kullanılarak üretilen yeni kod ve kod çözme algoritmasını uyguluyoruz. 29 harfli Türkçe alfabeye ek olarak (●) boşluk dahil olacak şekilde 30 harfli A, B, C, …, (●) karakterlerine sırasıyla $n, n+1, n+2, n+3, \ldots, n+29$ karşılık gelecek şeklinde yerleştirilir.

Tablo 1. Harflere karşılık gelen kod sayıları

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

Tablo1'deki *n* sayısına bağlı olarak elde ettiğimiz veriler ile *X* matrisi oluşturulur. Sonra *X* matrisi $B_i$blok matrislerine ayrılır. Oluşan blok sayısına bağlı olarak n değeri belirlenir. Harflere karşılık gelen değerler. Yazılan değerlere karşılık oluşan blok matrislerin determinantları yazılır hesaplanır. Bu determinantlar 4×4 mertebeli aşağıdaki *S* matrisinin ilk sütununa yazılır. İkinci sütuna sırasıyla B_1, B_2, B_3 ve B_4 matrislerinin 1. Satır ve 1.sütundaki elamanları, üçüncü sütuna sırasıyla B_1, B_2, B_3 ve B_4 matrislerinin 1. satır ve 2. sütundaki elamanları ve son olarak dördüncü sütuna sırasıyla B_1, B_2, B_3 ve B_4 matrislerinin 2. Satır ve 2.sütundaki elamanları yazılır. 2. satır ve 2. sütundaki değerleri yazmamamızın sebebi şifre çözme yönteminin doğru çalışıp çalışmadığını kontrol etmek içindir. Eğer aşağıda verilen (1) eşitliğindeki x_i değerlerinin 2. satır ve 2. sütundaki değerleri veriyorsa bu durumunda şifre çözme algoritması doğru çalıyor demektir. Burada 2. satır ve 2. sütundaki değerler rastgele seçilmiş olup 2. satır ve 2. sütundaki değerler dışında diğer satır ve sütunlardan herhangi biri için de benzer işlemler yapılabilir. Böylece şifreleme algoritması sonlandırılır.

Şifre çözme algoritması başlatılır. Şifre çözme algoritmasında kullanacağımız terimlerden olan $\bar{Z}_n$ aşağıda verilen Z_n matrisinin her bir elemanını temsil etmektedir. Karesel sayılar matris formatı ile

$$Z_n = \begin{pmatrix} \bar{Z}_{n+1} & \bar{Z}_n \\ \bar{Z}_n & \bar{Z}_{n-1} \end{pmatrix} \text{ şeklinde gösterilir.}$$

Benzer şekilde üçgensel sayılar

$$T_n = \begin{pmatrix} \tilde{T}_{n+1} & \tilde{T}_n \\ \tilde{T}_n & \tilde{T}_{n-1} \end{pmatrix}$$

matris formatı ile gösterilir ve karesel sayılar için elde edilen ve şifre çözme esnasında kullanılan formül üçgensel sayılar içinde $T_{n-1}T_{n+1} - T_n^2 = -T_n$ şeklinde elde edililir. Daha sonra t_1^i , t_2^i değerleri hesaplanır ve

$$t_1^i = \bar{Z}_1 b_1^i + \bar{Z}_3 b_3^i$$
$$t_2^i = \bar{Z}_2 b_2^i + \bar{Z}_4 b_4^i$$

Şeklinde formüle edilir. Burada $b_k^i, k = 1,2,3,4$ değerleri verilen cümlelerden oluşturulan *X* kare matrisinin 2x2 kare matrislerine bölünmesinden sonra elde edilen B_k matrisinin elemanlarını temsil etmektedir.

Son olarak B_k matrisinin değerlerini bulmak için aşağıda bulunan formül kullanılarak şifre çözme algoritmasının doğru bir şekilde çalışıp çalışmadığı kontrol edilir. Bu formül

$$(-2n^2 + 1)d_i = s_1^i(\bar{Z}_2 x_i + \bar{Z}_4 b_4^i) - t_2^i(\bar{Z}_1 x_i + \bar{z}_3 b_4^i) \quad (1)$$

şeklinde ifade edilir.

Böylece şifre çözme algoritması sonlandırılır. Yukarıdaki işlemleri daha sistematik olması açısından algoritmik olarak aşağıdaki örneği göz önüne alalım.

Örnek:
"KAYBET VE ÖĞREN" kelimesini ele alalım.
İlk olarak X matrisini ve bloklara ayrılmış B_i matrislerini oluşturalım. X matrisi

$X=\begin{pmatrix} K & A & Y & B \\ E & T & \bullet & V \\ E & \bullet & \text{Ö} & \text{Ğ} \\ R & E & N & \bullet \end{pmatrix}$ şeklinde olur. Böylece,

$B_1=\begin{pmatrix} K & A \\ E & T \end{pmatrix}$ $B_2=\begin{pmatrix} Y & B \\ \bullet & V \end{pmatrix}$ $B_3=\begin{pmatrix} E & \bullet \\ R & E \end{pmatrix}$ $B_4=\begin{pmatrix} \text{Ö} & \text{Ğ} \\ \text{N} & \bullet \end{pmatrix}$

Blok matrisleri elde edilir. 4 adet 2×2 blok matris oluştuğu için $b = 4 > 3$ olur ve n' nin tanımından $n = 4$ elde edilir. O halde $mod30$'a göre değerleri yeniden yazarsak:

K	A	Y	B	E	T
17	4	1	5	9	27
V	Ö	Ğ	R	N	●
0	22	12	24	20	3

elde edilir.

Aşağıda $mod30$'a göre blok matris elemanlarının aldığı değerleri yerine yazılmıştır:

$B_1=\begin{pmatrix} 17 & 4 \\ 9 & 27 \end{pmatrix}$ $B_2=\begin{pmatrix} 1 & 5 \\ 3 & 0 \end{pmatrix}$ $B_3=\begin{pmatrix} 9 & 3 \\ 24 & 9 \end{pmatrix}$ $B_4=\begin{pmatrix} 22 & 12 \\ 20 & 3 \end{pmatrix}$

Blok matrisleri satır ve sütun sıralarına göre şu şekilde yazalım:

$b_1^1=17$ $b_1^2=1$ $b_1^3=9$ $b_1^4=22$
$b_2^1=4$ $b_2^2=5$ $b_2^3=3$ $b_2^4=12$ (2)
$b_3^1=9$ $b_3^2=3$ $b_3^3=24$ $b_3^4=20$
$b_4^1=27$ $b_4^2=0$ $b_4^3=9$ $b_4^4=3$

Şimdi $mod30$'a göre blok matrislerin determinant hesaplamalarını yapalım:

$\det(B_1) = d_1 = 459 - 36 = 423$
$\det(B_2) = d_2 = 0 - 15 = -15$ (3)
$\det(B_3) = d_3 = 81 - 72 = 9$
$\det(B_4) = d_4 = 66 - 240 = -174$

(2) ve (3)' ten S matrisi elde edilir:

$$S = \begin{pmatrix} 423 & 17 & 4 & 27 \\ -15 & 1 & 5 & 0 \\ 9 & 9 & 3 & 9 \\ -174 & 22 & 12 & 3 \end{pmatrix}$$

Böylece şifreleme algoritması sonlandırılır. Şifre çözme algoritması başlatılır.
Öncelikle karesel sayılardan oluşan matris gösteriminde bulmuş olduğumuz $n = 4$ değeri için aşağıdaki matrisi oluşturalım:

$Z_4=\begin{pmatrix} \bar{Z}_5 & \bar{Z}_4 \\ \bar{Z}_4 & \bar{Z}_3 \end{pmatrix}= \begin{pmatrix} 25 & 16 \\ 16 & 9 \end{pmatrix}$

Buradan $\bar{Z}_1 = 25$, $\bar{Z}_2 = 16$, $\bar{Z}_3 = 16$, $\bar{Z}_4 = 9$ olduğu görülür.
Şimdi t_1^i ve t_2^i değerlerini hesaplayalım:
$t_1^1=\bar{Z}_1 b_1^1 + \bar{Z}_3 b_2^1$ =25.17 + 16.4 = 489
$t_1^2=\bar{Z}_1 b_1^2 + \bar{Z}_3 b_2^2$ = 25.1 + 16.5 = 105
$t_1^3=\bar{Z}_1 b_1^3 + \bar{Z}_3 b_2^3$ =25.9 + 16.3 = 273
$t_1^4=\bar{Z}_1 b_1^4 + \bar{Z}_3 b_2^4$ =25.22 + 16.12 = 742
ve
$t_2^1=\bar{Z}_2 b_1^1 + \bar{Z}_4 b_2^1$ = 16.17 + 9.4 = 308
$t_2^2=\bar{Z}_2 b_1^2 + \bar{Z}_4 b_2^2$ =16.1 + 9.5 = 61
$t_2^3=\bar{Z}_2 b_1^3 + \bar{Z}_4 b_2^3$ = 16.9 + 9.3 = 171
$t_2^4=\bar{Z}_2 b_1^4 + \bar{Z}_4 b_2^4$ = 16.22 + 9.12 = 460
elde edilir.

Şimdi x_1, x_2, x_3 ve $x_4$elamanlarının değerlerini bulalım:
$(-2n^2 + 1)\, d_1 = t_1^1(\bar{Z}_2 x_1 + \bar{Z}_4 b_4^1) - t_2^1(\bar{Z}_1 x_1 + \bar{Z}_3 b_4^1)$
-31.423 = 489 (16.x_1 + 9.27) – 308 (25. x_1 + 16.27)
-13113 = 124x_1 – 14229
1116=124x_1
$x_1 = b_3^1$=9,
$(-2n^2 + 1)\, d_2 = t_1^2(\bar{Z}_2 x_2 + \bar{Z}_4 b_4^2) - t_2^2(\bar{Z}_1 x_2 + \bar{Z}_3 b_4^2)$
-31.-15 = 105 (16.x_2 + 9.0) – 61 (25. x_2 + 16.0)
465 = 1680x_2 – 1525x_2
465 = 155x_2
$x_2 = b_3^1$=3,
$(-2n^2 + 1) d_3 = t_1^3(\bar{Z}_2 x_3 + \bar{Z}_4 b_4^3) - t_2^3(\bar{Z}_1 x_3 + \bar{Z}_3 b_4^3)$
-31.9 = 273 (16.x_3 + 9.9) – 171 (25. x_3 + 16.9)
-279 = 93x_3 – 2511
2232=93x_3
$x_3 = b_3^1$=24,
$(-2n^2 + 1) d_4 = t_1^4(\bar{Z}_2 x_4 + \bar{Z}_4 b_4^4) - t_2^4(\bar{Z}_1 x_4 + \bar{Z}_3 b_4^4)$
-31.-174 = 742 (16.x_4 + 9.3) – 460 (25. x_4 + 16.3)
5394 = 372x_4 – 2046
7440=372x_4
$x_4 = b_3^1$=20.

Bulmuş olduğumuz x_1,x_2, x_3 ve x_4 değerleri aradığımız 2. satır ve 2. sütundaki değerleri yani $m_3^i, 1 \le i \le 4$ elemanlarına denk geldiğinden algoritmamızın doğru çalıştığı sonucuna varılmaktadır. Şimdi B_i matrislerini oluşturalım:

$B_1=\begin{pmatrix}17 & 4\\ 9 & 27\end{pmatrix}$ $B_2=\begin{pmatrix}1 & 5\\ 3 & 0\end{pmatrix}$ $B_3=\begin{pmatrix}9 & 3\\ 24 & 9\end{pmatrix}$ $B_4=\begin{pmatrix}22 & 12\\ 20 & 3\end{pmatrix}$

Buradan X matrisini oluşturursak;

$$X=\begin{pmatrix}17 & 4 & 1 & 5\\ 9 & 27 & 3 & 0\\ 9 & 3 & 22 & 12\\ 24 & 9 & 20 & 3\end{pmatrix} = \begin{pmatrix}K & A & Y & B\\ E & T & \bullet & V\\ E & \bullet & Ö & Ğ\\ R & E & N & \bullet\end{pmatrix}$$

elde ederiz böylece gönderdiğimiz mesaj cümlesine ulaşmış olduğumuz için şifreleme ve şifre çözme algoritmasının doğru çalıştığını ispat ederek işlemi sonlandırmış oluruz. Yukarıda ele almış olduğumuz adımlarda detaylı olarak karesel sayılarda kodlama işlemini gösterdikten sonra, yapılan kodlama işlemlerinde daha güçlü ve güvenilir bir kodlama oluşturmak için ikinci aşamaya geçtik. Bu aşamada hem üçgensel hem karesel sayıları kullanarak "Bütünleşik Kodlama" adını verdiğimiz bir şifreleme ve şifre çözme algoritması oluşturduk.

Bu kısımda ele alacağımız bu yeni yöntemde hem üçgensel hem de karesel sayılara ait matris formundan yola çıkılarak i nin tek olduğu durumlarda üçgensel matris formatı kullanılırken çift olduğu durumlarda ise karesel sayılardan oluşan matris formatı üzerinden işlemler yapılacaktır. Bu şekilde şifre çözme işlemi daha karmaşık ve güçlü hale gelecektir.

Bütünleşik Kodlama Modeli

Kodlama Algoritması:

Adım 1: K matrisini blok B_i matrislerine böl.
Adım 2: n sayısını bul.
Adım 3: b_j^i $(1 \le j \le 4)$ değerlerini bul.
Adım 4: B_i matrislerinin determinantlarını hesapla. $(det(B_i) = di)$
Adım 5: $F = [det(B_i), b_k^i]$ matrisini oluştur.
Adım 6: Algoritmayı sonlandır.

Kod Çözme Algoritması:

Adım 1: $T_n$matrisini oluştur.
Adım 2: Z_n matrisini oluştur.
Adım 3: $\check{T}_{n+1}b_1^i + \check{T}_n b_2^i \rightarrow e_1^i$ oluştur.
Adım 4: $\check{Z}_{n+1}.b_1^i + \check{Z}_n.b_2^i \rightarrow e_1^i$oluştur.
Adım 5: $\check{T}_n b_1^i + \check{T}_{n-1} b_2^i \rightarrow e_2^i$ oluştur.
Adım 6: $\check{Z}_n.b_1^i + \check{Z}_{n-1}.b_2^i \rightarrow e_2^i$ oluştur.
Adım 7: $-T_n.d_i = e_1^i(\check{T}_n b_3^i + \check{T}_{n-1}x_i) - e_2^i(\check{T}_{n+1}b_3^i + \check{T}_n x_i)$ çöz.
Adım8:$(-2n^2+1)d_i = e_1^i(\check{Z}_n b_3^i + \check{Z}_{n-1}x_i) - e_2^i(\check{Z}_{n+1}b_3^i + \check{Z}_n x_i)$ çöz.
Adım 9: $x_i = b_4^i$
Adım 10: Algoritmayı sonlandır.
Yukarıda adımları aşağıdaki örnek üzerinden gösterelim.

Örnek:

"İNSANI SADECE BİLİM SANAT YÜCELTİR" cümlesini aşağıdaki şekilde X matrisinin içerisine yerleştirelim.

$$X = \begin{bmatrix} \text{İ} & N & S & A & N & I \\ . & S & A & D & E & C \\ E & . & B & \text{İ} & L & \text{İ} \\ M & . & S & A & N & A \\ T & . & Y & \text{Ü} & C & E \\ L & T & \text{İ} & R & . & . \end{bmatrix}$$

Kodlama Algoritması:

Adım 1: X matrisini blok (2x2) mertebeli B_i matrislerine böl.

$$B_1 = \begin{bmatrix} \text{İ} & N \\ . & S \end{bmatrix}, \quad B_2 = \begin{bmatrix} S & A \\ A & D \end{bmatrix}, \quad B_3 = \begin{bmatrix} N & I \\ E & C \end{bmatrix}$$
$$B_4 = \begin{bmatrix} E & . \\ M & . \end{bmatrix}, \quad B_5 = \begin{bmatrix} B & \text{İ} \\ S & A \end{bmatrix}, \quad B_6 = \begin{bmatrix} L & \text{İ} \\ N & A \end{bmatrix}$$
$$B_7 = \begin{bmatrix} T & . \\ L & T \end{bmatrix}, \quad B_8 = \begin{bmatrix} Y & \text{Ü} \\ \text{İ} & R \end{bmatrix}, \quad B_9 = \begin{bmatrix} C & E \\ . & . \end{bmatrix}$$

Adım 2: $b > 3$ için $n = b$ olduğundan $b = 9 = n$ olur. $n = 9$ için karakter tablosundan X matrisindeki harfleri yerleştirirsek;

$$\begin{array}{cccccccccccccccccccccccc} & & & & & & & & \text{İ} & N & S & A & N & I & . & S & A & D & E & C & E & . \\ & & & & & & & & 20 & 25 & 0 & 9 & 25 & 19 & 8 & 0 & 9 & 13 & 14 & 11 & 14 & 8 \\ B & \text{İ} & L & \text{İ} & M & . & S & A & N & A & T & . & Y & \text{Ü} & C & E & L & T & \text{İ} & R & . & . \\ 10 & 20 & 23 & 20 & 24 & 8 & 0 & 9 & 25 & 9 & 2 & 8 & 6 & 4 & 11 & 14 & 23 & 2 & 20 & 29 & 8 & 8 \end{array}$$

Adım 3:

$$b_1^1 = 20 \quad b_2^1 = 25 \quad b_3^1 = 8 \quad b_4^1 = 0$$
$$b_1^2 = 0 \quad b_2^2 = 9 \quad b_3^2 = 9 \quad b_4^2 = 13$$
$$b_1^3 = 25 \quad b_2^3 = 19 \quad b_3^3 = 14 \quad b_4^3 = 11$$
$$b_1^4 = 14 \quad b_2^4 = 8 \quad b_3^4 = 24 \quad b_4^4 = 8$$
$$b_1^5 = 10 \quad b_2^5 = 20 \quad b_3^5 = 0 \quad b_4^5 = 9$$
$$b_1^6 = 23 \quad b_2^6 = 20 \quad b_3^6 = 25 \quad b_4^6 = 9$$
$$b_1^7 = 2 \quad b_2^7 = 8 \quad b_3^7 = 23 \quad b_4^7 = 29$$
$$b_1^8 = 6 \quad b_2^8 = 4 \quad b_3^8 = 20 \quad b_4^8 = 29$$
$$b_1^9 = 11 \quad b_2^9 = 14 \quad b_3^9 = 8 \quad b_4^9 = 8$$

Adım 4: Şimdi B_i matrislerinin d_i determinantlarını hesapla.

$$det(B_1) = \begin{vmatrix} 20 & 25 \\ 8 & 0 \end{vmatrix} = d_1 = -200$$
$$det(B_2) = \begin{vmatrix} 0 & 9 \\ 9 & 13 \end{vmatrix} = d_2 = -81$$
$$det(B_3) = \begin{vmatrix} 25 & 19 \\ 14 & 11 \end{vmatrix} = d_3 = 275 - 266 = 9$$
$$det(B_4) = \begin{vmatrix} 14 & 8 \\ 24 & 8 \end{vmatrix} = d_4 = 112 - 192 = -80$$
$$det(B_5) = \begin{vmatrix} 10 & 20 \\ 0 & 9 \end{vmatrix} = d_5 = 90$$

$$det(B_6) = \begin{vmatrix} 23 & 20 \\ 25 & 9 \end{vmatrix} = d_6 = 207 - 500 = -293$$
$$det(B_7) = \begin{vmatrix} 2 & 8 \\ 23 & 2 \end{vmatrix} = d_7 = 4 - 184 = -180$$
$$det(B_8) = \begin{vmatrix} 6 & 4 \\ 20 & 29 \end{vmatrix} = d_8 = 174 - 80 = 94$$
$$det(B_9) = \begin{vmatrix} 11 & 14 \\ 8 & 8 \end{vmatrix} = d_9 = 88 - 112 = 24$$

Adım 5: Adım 3 ve Adım 4 ten *F* matrisi oluşturuldu. Burada, b_4^i i=1,2,3,4,5,6,7,8,9 değerleri aranan değerler olduğu için yazılmamıştır.

$$F = \begin{bmatrix} -200 & 20 & 25 & 8 \\ -81 & 0 & 9 & 9 \\ 9 & 25 & 19 & 14 \\ -80 & 14 & 8 & 24 \\ 90 & 10 & 20 & 0 \\ -293 & 23 & 20 & 25 \\ -180 & 2 & 8 & 23 \\ 94 & 6 & 4 & 20 \\ -24 & 11 & 14 & 8 \end{bmatrix}$$

Adım 6: Algoritmayı sonlandır.

Kod Çözme Algoritması

Adım 1:

$$T_9 = \begin{bmatrix} \check{T}_{10} & \check{T}_9 \\ \check{T}_9 & \check{T}_8 \end{bmatrix} = \begin{bmatrix} 55 & 45 \\ 45 & 36 \end{bmatrix}$$

Adım 2:

$$Z_9 = \begin{bmatrix} \check{Z}_{10} & \check{Z}_9 \\ \check{Z}_9 & \check{Z}_8 \end{bmatrix} = \begin{bmatrix} 100 & 81 \\ 81 & 64 \end{bmatrix}$$

Adım 3: Eğer i tek sayı ise biz T_n matrisini kullanacağız.
Şimdi e_1^i değerlerini i = 1, 3, 5, 7, 9 için hesaplayalım.
$e_1^1 = 55.20 + 45.25 = 2225$
$e_1^3 = 55.25 + 45.19 = 2230$
$e_1^5 = 55.10 + 45.20 = 1450$
$e_1^7 = 55.2 + 45.8 = 470$
$e_1^9 = 55.11 + 45.14 = 1235.$

Adım 4: Eğer i çift sayı ise biz Z_n matrisini kullanacağız. Şimdi e_1^i değerlerini $i =$ 2,4,6,8 için hesaplayalım.
$e_1^2 = 100.0 + 81.9 = 729$
$e_1^4 = 100.14 + 81.8 = 2048$
$e_1^6 = 100.23 + 81.20 = 3920$
$e_1^8 = 100.6 + 81.4 = 920$

Adım 5: i'nin tek sayı değerleri için benzer şekilde T_n matrisini kullanalım.
$e_2^1 = 45.20 + 36.25 = 1800$
$e_2^3 = 45.25 + 36.19 = 1809$
$e_2^5 = 45.10 + 36.20 = 1170$
$e_2^7 = 45.2 + 36.8 = 378$
$e_2^9 = 45.11 + 36.14 = 999$

Adım 6: i'nin çift sayı değerleri için benzer şekilde Z_n matrisini kullanalım.
$e_2^2 = 81.0 + 64.9 = 576$
$e_2^4 = 81.14 + 64.8 = 1646$
$e_2^6 = 81.23 + 64.20 = 3143$
$e_2^8 = 81.6 + 64.4 = 742$

Adım 7: Eğer tek sayı ise- $T_9.d_i$ değerini kullanacağız ($i = 1,3,5,7,9$)
$-45.(-200) = 2225.(45.8 + 36.14) - 1800(55.8 + 45.\ x_1)$
$9000 = 9000 - 900\ x_1$
$x_1 = 0,$
$-45.(9) = 2230(45.14 + 36\ x_3)$
$-405 = 1.404.900 + 80.280\ x_3 - 1.392.930 - 81.405\ x_3$
$-405 = 11970 - 1125$
$x_3 = 11,$
$-45.90 = 1450.(45.0 + 36\ x_5) - 1170(55.0 + 45\ x_5)$
$-4050 = 52.200\ x_5 - 52.650\ x_5$
$-4050 = -450\ x_5$
$-\ x_5 = 9,$
$-45.(-180) = 470.(45.23 + 36\ x_7) - 378.(55.23 + 45.\ x_7)$
$8100 = 486450 + 16.920\ x_7 - 478.170 - 17010\ x_7$
$8100 = 8.280 - 90\ x_7$
$180 = 90\ x_7$
$x_7 = 2,$
$-45.(-24) = (45.8 + 36\ x_9) - 999.(55.8 + 45\ x_9)$
$1080 = 444600 + 44460\ x_9 - 439560 - 44.955\ x_9$
$1080 = 5040 - 495\ x_9$
$3960 = 495\ x_9$
$x_9 = 8,$

Adım 8: Eğer i çift sayı ise $(-2n^2 + 1).d_i$ değerini kullanacağız. ($i = 2,4,6,8$)
$(-2.81 + 1).(-81) = 4729.(81.9 + 46.656\ x_2) - 576.(100.9 + 81\ x_2)$
$13041 = 531.441 + 46.656\ x_2 - 518400 - 46656\ x_2$
$13041 = 13041$
$x_2\ \epsilon\ R$
$(-161).(-80) = 2048.(81.24 + 64\ x_4) - 1646.(100.24 + 81\ x_4)$
$12880 = 3981312 + 131072\ x_4 - 3950400 - 133326\ x_4$
$18032 = 2254\ x_4$
$x_4 = 8,$
$(-161).(-293) = 3920.(81.25 + 64\ x_6) - 3143.(100.25 + 81\ x_6)$
$47173 = 7938000 + 250880\ x_6 - 7857500 - 254583\ x_6$

$47173 = 85000 - 3703\, x_6$
$33347 = 3703\, x_6$
$x_6 = 9,$
$(-161).(94) = 924.(81.20 + 64\, x_8) - 742.(100.20 + 81\, x_8)$
$-15134 = 1496880 + 59136\, x_8 - 1484000 - 60102\, x_8$
$-15134 = 12880 - 966\, x_8$
$28014 = 966\, x_8$
$x_8 = 29,$

Adım 9:

$x_1=b_4^1=0,$ $x_2=b_4^2=\mathrm{R},$ $x_3=b_4^3=11$
$x_4=b_4^4=8,$ $x_5=b_4^5=9,$ $x_6=b_4^6=9$
$x_7=b_4^7=2$ $x_8=b_4^8=29$ $x_9=b_4^9=8.$

Böylece, aranan bütün $x_i = b_4^i$, $i = 1,2,3,4,5,6,7,8,9$ değerleri bulunmuş olur.

Adım 10: Algoritmayı sonlandır.

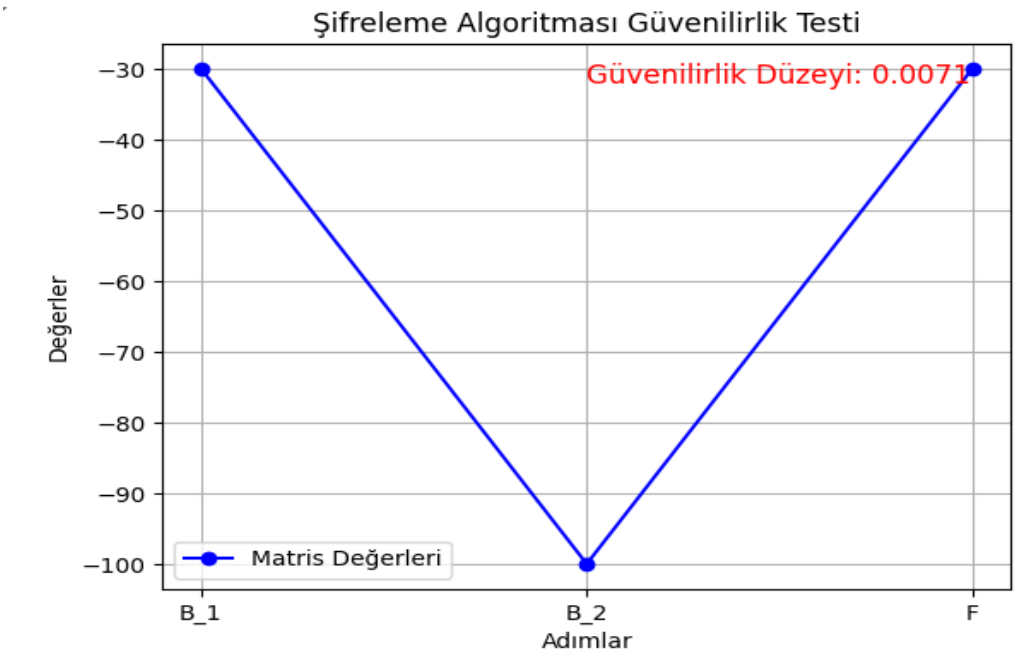
Böylece daha karma model olan ve Bütünleşik Kodlama Modeli olarak adlandırdığımız işlemlerin aşamalarını örnek ile açıklamış olduk. Bu sistemde iki sayı dizi kullanıldığı için yapılan şifre çözme işlemleri sadece bir sayı dizisine göre güvenirliğinin daha yüksek olacağı açıktır.

Aşağıda python da örnek olarak oluşturulan herhangi bir matris ve yukarda bahsedilen algoritmik işlemlerle kodlamanın güvenirliği sayısal olarak ele alınmıştır:

Python Kodu:

```
import numpy as np
import matplotlib.pyplot as plt
# Örnek bir matris K oluştur
K = np.array([[5, 8, 9, 12],
              [15, 18, 20, 25],
              [30, 32, 35, 40],
              [45, 50, 55, 60]])
# B_1 ve B_2 matrisleri oluştur
B_1 = K[:2, :2]  # İlk iki satır ve iki sütun
B_2 = K[2:, 2:]  # Son iki satır ve iki sütun
# Matrislerin determinantlarını hesapla
det_B1 = np.linalg.det(B_1)
det_B2 = np.linalg.det(B_2)
# Rastgele b_j^i değerleri
b_1 = np.random.randint(10, 20, size=(4,))
b_2 = np.random.randint(10, 20, size=(4,))
b_3 = np.random.randint(10, 20, size=(4,))
b_4 = np.random.randint(10, 20, size=(4,))
# F matrisini oluştur (det(B_i), b_k^i)
F = np.array([det_B1, *b_1])
# Değişim oranlarını hesaplamak için belirli adımları kullan
```

```
determinants = [det_B1, det_B2, F[0]]
# Değişim oranlarını hesapla
change_rate = [abs(determinants[i+1]- determinants[i]) for i in range(len(determinants)-1)]
# Güvenilirlik hesaplaması
# Güvenilirlik, değişim oranlarının tersine orantılıdır, daha küçük değişimler daha yüksek güvenilirlik anlamına gelir
reliability = 1 / (1 + sum(change_rate))  # Daha düşük değişim daha yüksek güvenilirlik
# Grafiksel gösterim
steps = ['B_1', 'B_2', 'F'] det_values = determinants  # det(B1), det(B2), F[0] (det(B1))
# Grafik çizimi
plt.plot(steps, det_values, marker='o', linestyle='-', color='b', label='Matris Değerleri')
plt.title('Şifreleme Algoritması Güvenilirlik Testi')
plt.xlabel('Adımlar')
plt.ylabel('Değerler')
plt.grid(True)
plt.legend()
# Güvenilirlik düzeyini yazdıralım
plt.text(1, max(det_values) - 2, f'Güvenilirlik Düzeyi: {reliability:.4f}', fontsize=12, color='red')
# Grafik gösterimi
plt.show()
# Güvenilirlik düzeyini konsolda yazdıralım
print(f"Güvenilirlik Düzeyi: {reliability:.4f}")
```




```
Güvenilirlik Düzeyi: 0.0071
```

Şekil 1. Şifreleme algoritması güvenirlik testi

Şekil 1 de elde edilen 0.0071'lik güvenilirlik düzeyi, şifreleme algoritmanızın oldukça güvenli ve karmaşık olduğunu, ancak çözülmesinin zor olduğunu gösteriyor. Bu

durum, algoritmanızın güçlü bir şekilde korunmuş olduğu ve şifre çözme işleminin yüksek hesaplama gücü gerektirdiği anlamına gelir.

Değişkenlik: Güvenilirlik düzeyinin 0.0071 olması, algoritmanın her bir adımındaki determinantların ve matris değerlerinin büyük değişimlere uğradığını gösterir. Bu, şifrelemenin oldukça dinamik ve istikrarsız olduğunu, yani her adımda belirgin değişiklikler yaşandığını belirtir.

Güvenlik: Düşük güvenilirlik genellikle daha yüksek güvenlik anlamına gelir. Çünkü sistemdeki değişkenlik ve dalgalanma, şifrenin çözülmesini daha zor hale getirebilir. Şifrelenecek veriler arasında büyük farklar olduğu için, potansiyel bir saldırganın çözümleme yapması oldukça güçleşir.

Çok Karışık Yapı: Algoritmanızda belirgin dalgalanmalar ve değişiklikler olduğunda, bu şifrelemenin daha karmaşık olduğu anlamına gelir. Bu tür şifreleme algoritmaları, genellikle daha güvenli kabul edilir çünkü çözülmesi için çok sayıda olasılık ve yol vardır.

Tartışma ve Sonuç

Kriptoloji Günlük hayatımızın her alanında, internet alışverişinden banka işlemlerine kadar, kriptoloji sessiz bir kahraman gibi bilgi güvenliğimizi koruyor. Kredi kartı çiplerimizden kimlik numaralarımıza kadar uzanan geniş bir yelpazede, hassas bilgilerimizi korumak için kriptolojiye güveniyoruz.

İnternetin ve veri üretiminin hızla büyümesi, şifreleme ve şifre çözme işlemlerinin de daha hızlı ve güvenli hale gelmesini gerekli kılıyor. Bu amaçla, bilgisayarsız veya programlanabilir şifreleme yöntemlerine ihtiyaç duyulmaktadır.

Çalışmamız, mesaj kelimelerini 2x2 kare matrislere bölerek ve matris ve determinant işlemleri ile şifreleme/çözme algoritması oluşturarak bu alana yeni bir bakış açısı getiriyor. Algoritmamız, esnek yapısı ve yüksek performansı ile geniş bir kullanıcı kitlesine hitap ediyor. Geliştirilen şifreleme algoritmasını kullanan bir mobil uygulama, Flutter uygulama çatısı ile geliştirilerek hem Android hem de IOS cihazlarda çalışabilmesi sağlanabilir.

Burada kullanılan Cassini özdeşliğinin yerine daha genel hali olan Catalan özdeşliği (“Catalan özdeşliği”, 2023),

$F_n^2 - F_{n+r}F_{n-r} = (-1)^{n-r}F_r^2, n \geq 1$

alınarak şifre çözme algoritmasın da r sayısına bağlı olarak r tane farklı formül üzerinden şifre çözme algoritması uygulanabilir.

Etik Standartlar Bildirgesi

Bu makalenin sunulmasıyla birlikte beyan ederim ki: Bu araştırma makalesinin yazarı, bu çalışmanın planlanmasına, yürütülmesine veya analizine doğrudan katılmıştır. Bu makalenin yazarları gönderilen son versiyonu okumuş ve onaylamıştır. Bu makalenin içeriği başka bir yerde sunulmamış, telif hakkı alınmamış veya yayınlanmamıştır. Bu makalenin içeriği, dergi tarafından kabulü değerlendirilirken telif hakkı alınmayacak, sunulmayacak veya başka bir yerde yayınlanmayacaktır.

Yazarlık Katkı Beyanı

Yazar 1: Yazar çalışmanın konsept ve tasarımına katkıda bulunmuştur. Materyal hazırlama, veri toplama ve analiz Bahar KULOĞLU tarafından gerçekleştirilmiştir. Makalenin ilk taslağı Bahar KULOĞLU tarafından yazılmış ve yazar makalenin son halini okuyup onaylamıştır.

Çıkar Çatışması Beyanı

Finansman: Herhangi bir fon, hibe veya diğer destekler alınmamıştır. Çıkar çatışmaları / Rekabet eden çıkarlar: Yazarlar, bu makalede tartışılan konu veya materyallerle ilgili herhangi bir mali çıkarı veya mali olmayan çıkarı olan herhangi bir kuruluş veya kuruluşla bağlantıları veya katılımları olmadığını onaylar.
Veri ve materyallerin mevcudiyeti: Geçerli değil.
Kod kullanılabilirliği: Geçerli değil.
İnsanları ve/veya hayvanları içeren çalışmaların sonuçlarını bildiren yaşam bilimleri dergilerindeki makaleler için ek beyanlar: Geçerli değil.
Etik onayı: Geçerli değil
Katılım onayı: Kabul ediyorum
Yayın için onay: Kabul edildi.

Verilerin Kullanılabilirliği

Bu çalışma sırasında oluşturulan veya analiz edilen tüm veriler, yayınlanan bu makaleye dahil edilmiştir.

Teşekkür

TÜBİTAK Bilim İnsanı Destek Programı Başkanlığı tarafından 2023 yılında düzenlenen araştırma projeleri bölge finali yarışmasında 3. lük ödülüne layık gören bütün jüri ekibine yapıcı eleştirileri ile çalışmamızın geliştirilmesine olan destek ve katkılarından dolayı teşekkür ederiz.

Kaynaklar

Beall, J. C. Curry's paradox. In Zalta, Edward N. (ed.). Stanford Encyclopedia of Philosophy.

Basu, M. & Prasad, B. (2009). The generalized relations among the code elements forFibonacci coding theory. Chaos Solitons Fractals, 5, 2517-2525.

Dişkaya, O., Avaroğlu, E., Menken, H., & Emsal, A. (2022). A new Encryption Algorithm Based on Fibonacci Polynomials and Matrices. International Information and Engineering Technology Association, 39 (5), 1453-1462.

Eric W. Weisstein, Catalan's Constant (MathWorld)

Eric W. Weisstein. Square Triangular Number. MathWorld.

Eser E., Kuloğlu B.& Özkan E. (2023). An Encoding –Decoding Algorithm Based On Narayana Numbers. 9th International Conference on IFS and Contemporary Mathematics and Engineering (IFSCOM 2023), Mersin, Türkiye, 177-187.

Kriptografi, Bilginin Anahtarı, *https://bilimgenc.tubitak.gov.tr/makale/kriptografi-bilginin-anahtari*, (23.05.2023).

Kuloğlu B. & Özkan E. (2023a). Creating Encryption and Decryption Algorithm Using Pell Numbers. EYFOR14, Antalya, Türkiye, 505-515.

Kuloglu, B. & Özkan, E. (2023b). Applications of Jacobsthal and Jacobsthal-Lucas Numbers in Coding Theory, Mathematica Montisnigri, Lvii, 54–64.

Kuloğlu B. (2024). Creating a New Coding and Decoding Algorithm Based on Violin Notes, Research & Revıews: Dıscrete Mathematıcal Structures, 10 (3).

Prajapat, S, Jain, A. & Thakur, R. S. (2014) A novel approach for information security with automatic variable key using Fibonacci Q-matrix, International Journal of Computer and Communication Technology, 5(4), 295-299.

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

Stakhov, A. P. (2006).Fibonacci matrices, a generalization of the Cassini formula, and a new coding theory,Chaos Solitons Fractals, 30, 56-66.

Uçar, S., Taş, N. & Özgür, N. H. (2019). A New Application to Coding Theory via Fibonacci and Lucas Numbers. Mathematical Sciences and Application E-Notes, 7 (1), 62-70.

Wang, F., Ding, J., Dai, Z., and Peng, Y. (2010). An application of mobile phoneencryption based on Fibonacci structure of chaos. Second WRI World Congress onSoftware Engineering