Kadirli Uygulamalı Bilimler Fakültesi Dergisi
Cilt 4, Sayı 1, 48-59, 2024

Journal of Kadirli Faculty of Applied Sciences
Volume 4, Issue 1, 48-59, 2024

Kadirli Uygulamalı Bilimler Fakültesi Dergisi

Journal of Kadirli Faculty of Applied Sciences

An Affine-Hill Cipher Application with the p-Generalized Fibonacci Q matrices and Steganography

Gülçin ÇİVİ BİLİR[1*], İlayda ALTINKOL[2]

[1]İstanbul Teknik Üniversitesi Fen-Edebiyat Fakültesi Matematik Müh. Bölümü, İstanbul
[2]İstanbul Üniversitesi YÖK TEBİP Programı, Matematik Bölümü, İstanbul

[1]https://orcid.org/0000-0002-8375-980X
[2]https://orcid.org/0000-0002-9517-7874
*Corresponding author: civi@itu.edu.tr

Research Article

Article History
Received: 13.07.2023
Accepted: 20.09.2023
Avaliable online: 08.03.2024

Keywords:
Fibonacci Q matrices
Steganography
Affine-Hill cipher
Trellis
Symmetric key

ABSTRACT

Affine-Hill Cipher is a symmetric key cryptographic algorithm. There are many studies in the literature to overcome the disadvantages of the symmetric key which is called the secret key and used both for encryption and decryption. In this work, we proposed a secret key generated by using Fibonacci Q matrices and Trellis-based steganographic method. Our work includes iterative keys, one based on the generalized Fibonacci Q matrix and the other based on Trellis steganography method. What makes this work special is that knowing the secret key is not enough to decrypt it.

Genelleştirilmiş p-Fibonacci Q matrisleri ve Steganografi ile Bir Afin-Hill Şifreleme Uygulaması

Araştırma Makalesi

Makale Tarihçesi
Geliş Tarihi: 13.07.2023
Kabul Tarihi:20.09.2023
Online Yayınlanma: 08.03.2024

Anahtar Kelimeler
Fibonacci Q matrisleri
Steganografi
Affin-Hill şifresi
Kafes
Simetrik anahtar

ÖZ

Afin-Hill şifrelemesi simetrik anahtarlı kriptografik bir algoritmadır. Literatürde, gizli anahtar adı verilen ve hem şifreleme hem deşifreleme için kullanılan simetrik anahtarın dezavantajlarının üstesinden gelmek için önerilmiş birçok çalışma bulunmaktadır. Bu çalışmada, Fibonacci Q matrisleri ve Trellis tabanlı steganografik kullanılması ile üretilen bir gizli anahtar önerilmiştir. Çalışmamız biri Fibonacci Q matrislerine diğeri ise Trellis steganografi metoduna dayalı tekrarlı anahtarları içermektedir. Çalışmayı özel kılan şey, gizli anahtarın bilinmesinin deşifre için yeterli olmamasıdır.

To Cite: Çivi Bilir G, Altınkol İ., 2024. An affine-hill cipher application with the p-generalized fibonacci Q matrices and steganography. Kadirli Uygulamalı Bilimler Fakültesi Dergisi, 4(1): 48-59.

Introduction

Hill cipher was invented by Lester S. Hill in 1929, is the first polygraphic substitution based on Linear Algebra. In 1931, L.S. Hill extended Hill Cipher by using the affine transformation. In Hill encryption and decryption, the same invertible key matrix is used (Stallings, 2017). Therefore, it must be secured and protected. In many studies, the different

procedures have been applied to increase the security. Various researchers gave new forms to improve those that already exist results by using the principles of linear algebra. Viswanath and Kumar proposed a public key cryptosystem involving two digital signatures for Hill's cipher (Viswanath and Kumar, 2015). Then, Sundarayya and Prasad (2019) proposed a system involving two or more digital signatures under modulation of prime numbers. An algorithm for Affine-Hill cipher in which the key was taken as the reflection on a line $y = ax + b$ is used by Prasad et al. (2016). In the literature, there are also articles that use Fibonacci sequences for the Affine Hill Cipher, reducing time complexity and increasing security. One of these works was to exchange the order and the power of multinacci matrices instead of exchanging key matrix (Uçar et al., 2019; Prasad and Mahato, 2021). Finally, very recently, Billore and Patel (2023) proposed an extended generalized Fibonacci matrices and modified a public key for Affine-Hill Cipher by using extended generalized Fibonacci matrices).

In this article, a new key exchange model in which the determined key is first hidden by a Trellis-based steganography method, then iterated by using the p- generalized Fibonacci Q matrices and finally transmitted to the receiver as the secret key is proposed.

Steganography is the art of the concealing of confidential or non-confidential data within a message or a video or an object. It is originally derived from the ancient Greek words Steganos meaning secret, and graphia meaning writing. Therefore, it is sometimes compared to cryptography but in reality, they are different. In cryptography data is transmitted to the receiver after encrypted by using various ways. Whereas no encryption or decryption is used in steganography. So, it can be defined as "covered writing" and cryptology as "secret writing" (Kahn, D., 1996). In our paper we use one of the steganography method called Trellis.

Fibonacci Q Matrices

The sequence $\{F_n\}$ defined by the recurrence relation

$$F_n = F_{n-1} + F_{n-1} \ , \quad n \geq 2 \ , \tag{1}$$

where $F_0 = F_1 = 1$ is known as the second order Fibonacci sequence (Bruggles and Hoggat,1963), (Hoggat, 1969), (Koshy 2018). Thus, the Fibonacci sequence is the series of the numbers

$$0, 1, 1, 2, 3, 5, \dots, 8,13,21,34, \dots$$

Now, we consider the recurrence relation given by

$$f_{n+p} = f_n + f_{n+1} + \cdots + f_{n+p-1} \ , \quad p \in Z^+ \quad , \tag{2}$$

where $f_0 = f_1 = \cdots = f_{n-2} = 0$, $f_{n-1} = 1$.

Setting $p = 2$ we find the Fibonacci sequence given by (1).

Setting $p = 3$ we find the recurrence formula

$$f_{n+3} = f_n + f_{n+1} + f_{n+2} \ , \ f_0 = f_1 = 0, \ f_2 = 1,$$

which defines the Tribonacci sequence.

By setting $p = 4$, $p = 5$, $p = 6$, $p = 7$, $p = 8$, $p = 9$ in (2), we find Fibonacci sequences called Tetranacci, Pentanacci, Hexanacci, Heptanacci, Octanacci and Enneanacci sequences, respectively.

For any $p \in Z^+$, the sequence defined by (2) is called the p-generalized Fibonacci sequence or Multinacci sequence of order p. By rewriting (2) in the vectoral form found as follows:

$$\begin{bmatrix} f_{n+p} \\ f_{n+p-1} \\ \vdots \\ f_{n+2} \\ f_{n+1} \end{bmatrix} = \begin{bmatrix} f_n + f_{n+1} + \cdots + f_{n+p-1} \\ f_{n+p-1} \\ \vdots \\ f_{n+2} \\ f_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \ldots & 1 & 0 \end{bmatrix} . \begin{bmatrix} f_{n+p-1} \\ f_{n+p-2} \\ \vdots \\ f_{n+1} \\ f_n \end{bmatrix}, \tag{3}$$

where the matrix denoted by

$$Q_p = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \ldots & 1 & 0 \end{bmatrix}$$

is a pxp matrix and it is called the $p-$generalized Fibonacci Q matrix (Stakhov, 1999).

The sequence obtained by setting $p = 2$ in (3) gives the matrix defined as the Fibonacci Q matrix

$$Q = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} F_2 & F_1 \\ F_1 & F_0 \end{bmatrix}$$

The Fibonacci Q matrix was first used by Brenner (1951) and the basic properties of the matrix were given by King (1960).

In this article we used the Multinacci Q matrix of order p to exchange the secret key for Affine Hill-Cipher.

Trellis Steganography Method

One of the methods of steganography used in secret communication was to hide messages by writing them on stencils (Çivi Bilir, 2023). One such variation, called Trellis, which resembles a chessboard, was used by Sir Francis Walsingham (1530-1590) who was a spymaster in the Elizabethan (Kahn, 1996).

To conceal the letters of the plaintext to a Trellis stencil, the following steps are performed.

Step 1. Trellis board similar to the chessboard is taken in the wrong position**.**

Step 2. Each letter of the plaintext is written in a single white cell as vertically.

Step 3. After filling in 32 letters, the board is turned through in the clockwise direction by 90 degrees.

Step 4. Each of the remaining letters is written in a single white cell vertically.

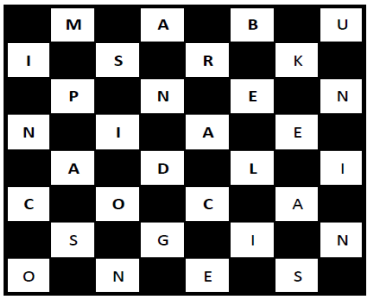
Step 5. If the plain text is shorter than 64, the remaining cells are filled up with null letters. If the plain text is longer than 64 letters, we require another turn of the board.

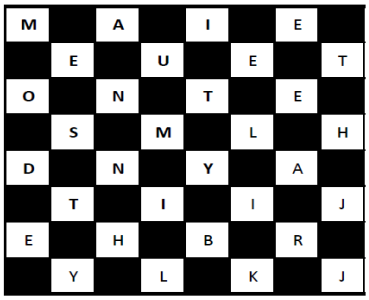
Step 6. The hiding process is completed by reading the 64 letters on the cells from left to right horizontally.

Example of Trellis Method

Let us consider the plaintext from Mevlana's wise words as

"In compassion and grace be like a sun, in modesty and humility be like earth"





M	M	A	A	I	B	E	U
I	E	S	U	R	E	K	T
O	P	N	N	T	E	E	N
N	S	I	M	A	L	E	H
D	A	N	D	Y	L	A	I
C	T	O	I	C	I	A	J
E	S	H	G	B	I	R	N
O	Y	N	L	E	K	S	J

After following the steps of the Trellis method, the ciphertext is obtained as "MMAAIBEUIESUREKTOPNNTEENNSIMALEHDANDYLAICTOICIAESHGBIR NOYNLEKSJ"

The Proposed Method

In this paper an application for Affine-Hill cipher with iterated keys is given. The main aim of our work is to transmit the key by exchanging it in two steps. We first applied the idea used in Trellis to conceal the key and then we constructed the exchanged key by using the multinacci Q matrices of order p.

Consider Alice's message as "Where are you?". Alice wants to send her message to Bob. Now, we explain our proposal in the following steps:

A. Encryption

Step 1. Alice chooses her key. Let it be "Hello everyone".

By using the following conversion table, the corresponding key matrix is constructed as

$$\mathrm{K} = \begin{bmatrix} 7 & 4 & 11 & 11 \\ 14 & 4 & 21 & 4 \\ 17 & 24 & 14 & 13 \\ 4 & 26 & 26 & 26 \end{bmatrix},$$

where the number 26 is used to represent the null character.

Step 2. Alice takes the shifting vector B as any column of the matrix K. Let it be

$$B = \begin{bmatrix} 7 \\ 14 \\ 17 \\ 4 \end{bmatrix}$$

Step 3. Alice encrypts her message by using the Affine Hill cipher algorithm. In encryption mode E with the key matrix, she finds the ciphertext C that converts the plaintext P, where $C = E(P, K)$.

By applying the Affine-Hill algorithm over Z_{27}, we use

$$C_i = KP_i + B \ (mod\ 27),$$

where

$$\mathrm{p}_1 = \begin{bmatrix} W \\ H \\ E \\ R \end{bmatrix},\ \mathrm{p}_2 = \begin{bmatrix} \mathrm{E} \\ \mathrm{A} \\ \mathrm{R} \\ \mathrm{E} \end{bmatrix},\ \mathrm{p}_3 = \begin{bmatrix} \mathrm{Y} \\ \mathrm{O} \\ \mathrm{U} \\ 9 \end{bmatrix}$$

and corresponding vectors are

$$P_1 = \begin{bmatrix} 22 \\ 7 \\ 4 \\ 17 \end{bmatrix},\ P_2 = \begin{bmatrix} 4 \\ 0 \\ 17 \\ 4 \end{bmatrix},\ P_3 = \begin{bmatrix} 24 \\ 14 \\ 20 \\ 26 \end{bmatrix}$$

according to the conversion table.

Table 1. Conversion Table

Thus, the cipher blocks are obtained as

$$C_1 = \begin{bmatrix} 7 & 4 & 11 & 11 \\ 14 & 4 & 21 & 4 \\ 17 & 24 & 14 & 13 \\ 4 & 26 & 26 & 26 \end{bmatrix} \begin{bmatrix} 22 \\ 7 \\ 4 \\ 17 \end{bmatrix} + \begin{bmatrix} 7 \\ 14 \\ 17 \\ 4 \end{bmatrix} = \begin{bmatrix} 420 \\ 502 \\ 836 \\ 820 \end{bmatrix} (\text{mod } 27) = \begin{bmatrix} 15 \\ 16 \\ 26 \\ 10 \end{bmatrix},$$

$$C_2 = \begin{bmatrix} 7 & 4 & 11 & 11 \\ 14 & 4 & 21 & 4 \\ 17 & 24 & 14 & 13 \\ 4 & 26 & 26 & 26 \end{bmatrix} \begin{bmatrix} 4 \\ 0 \\ 17 \\ 4 \end{bmatrix} + \begin{bmatrix} 7 \\ 14 \\ 17 \\ 4 \end{bmatrix} = \begin{bmatrix} 266 \\ 443 \\ 375 \\ 566 \end{bmatrix} (\text{mod } 27) = \begin{bmatrix} 23 \\ 11 \\ 24 \\ 26 \end{bmatrix},$$

$$C_3 = \begin{bmatrix} 7 & 4 & 11 & 11 \\ 14 & 4 & 21 & 4 \\ 17 & 24 & 14 & 13 \\ 4 & 26 & 26 & 26 \end{bmatrix} \begin{bmatrix} 24 \\ 14 \\ 20 \\ 26 \end{bmatrix} + \begin{bmatrix} 7 \\ 14 \\ 17 \\ 4 \end{bmatrix} = \begin{bmatrix} 737 \\ 930 \\ 1379 \\ 1660 \end{bmatrix} (\text{mod } 27) = \begin{bmatrix} 8 \\ 12 \\ 2 \\ 13 \end{bmatrix},$$

which give the cipher blocks as

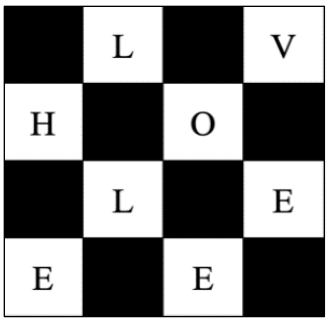
$$c_1 = \begin{bmatrix} P \\ Q \\ \vartheta \\ K \end{bmatrix},\ c_2 = \begin{bmatrix} X \\ L \\ Y \\ \vartheta \end{bmatrix} \text{ and } c_3 = \begin{bmatrix} I \\ M \\ C \\ N \end{bmatrix},$$

respectively. Finally, the plaintext is converted to the ciphertext “PQKXLYIMCN”.

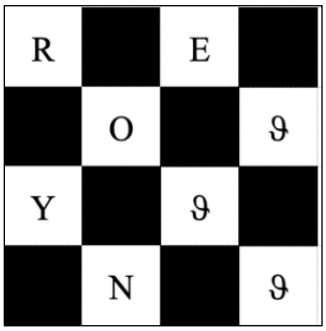
B. Key Exchange

Step 1. Determine the number n and construct a Trellis stencil sized $2mx2m$, where $n^2 = m + q$, m and q are the key length and the number of the null characters in the key matrix K, respectively.

Step 2. Construct a Trellis stencil and take it in the wrong position. Next, input $\frac{m+q}{2}$ letters of the key into the stencil, vertically.



Step 3. Rotate the stencil 90 degrees, clockwise and input the remaining letters, vertically. If the length of the key is less than $\frac{n}{2}$ choose a null character to fill up the squares.



Step 4. By reading from left to right, complete the steganography process.

R	L	E	V
H	O	O	
Y	L		E
E	N	E	

Step 5. Determine the corresponding matrix K_T by using Table 1.

$$\mathrm{K_T} = \begin{bmatrix} 17 & 11 & 4 & 21 \\ 7 & 14 & 14 & 26 \\ 24 & 11 & 26 & 4 \\ 4 & 13 & 4 & 26 \end{bmatrix}$$

Step 6. Consider the number $p = 2m$ and construct the multinacci matrix of order p as follows

$$Q_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Step 7. Calculate $K_F = K_T - Q_p$ as

$$K_F = K_T - Q_4 = \begin{bmatrix} 16 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Step 8. Find key text corresponding the matrix K_F

$$K_E : QKDUGOO\vartheta EEND\vartheta$$

Step 9. Transmit the pair $(C,\ K_E)$ to the receiver.

C. Decryption

Step1. Define the key length as p and construct the generalized Fibonacci matrix of order p as follows

$$Q_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

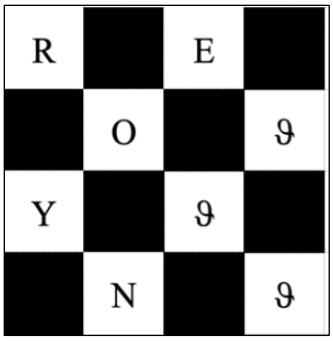
Step 2. Calculate $K_T = K_F + Q_p$ as

$$K_T = K_F + Q_4 = \begin{bmatrix} 17 & 11 & 4 & 21 \\ 7 & 14 & 14 & 26 \\ 24 & 11 & 26 & 4 \\ 4 & 13 & 4 & 26 \end{bmatrix}$$

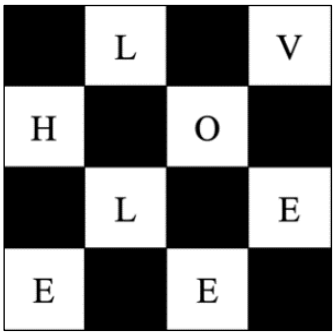
Step 3. Find the corresponding matrix as follows

R	L	E	V
H	O	O	ϑ
Y	L	ϑ	E
E	N	E	ϑ

Step 4. Construct a Trellis stencil with n^2 −cells. Then, input the $\frac{n^2}{2}$ letters corresponding to the white squares of the stencil, horizontally.



Step 5. Rotate the Trellis stencil 90 degrees, counter clockwise and input the remaining letters, to the white squares of the stencil, horizontally.



Step 6. Determine the secret key by using the Step 5 and Step 6:

"HELLO EVERYONE"

Step 7. Write the corresponding key matrix as

$$\mathrm{K} = \begin{bmatrix} 7 & 4 & 11 & 11 \\ 14 & 4 & 21 & 4 \\ 17 & 24 & 14 & 13 \\ 4 & 26 & 26 & 26 \end{bmatrix}$$

Step 8. Decrypt the ciphertext using the Affine-Hill algorithm. In decryption mode D with key K to recover P use $P = D(C, K) = K^{-1}\mathrm{C} \pmod{27}$.

Thus, we solve the message as "WHERE ARE YOU?"

In the following Figure we give the encryption algorithm with iterated keys.

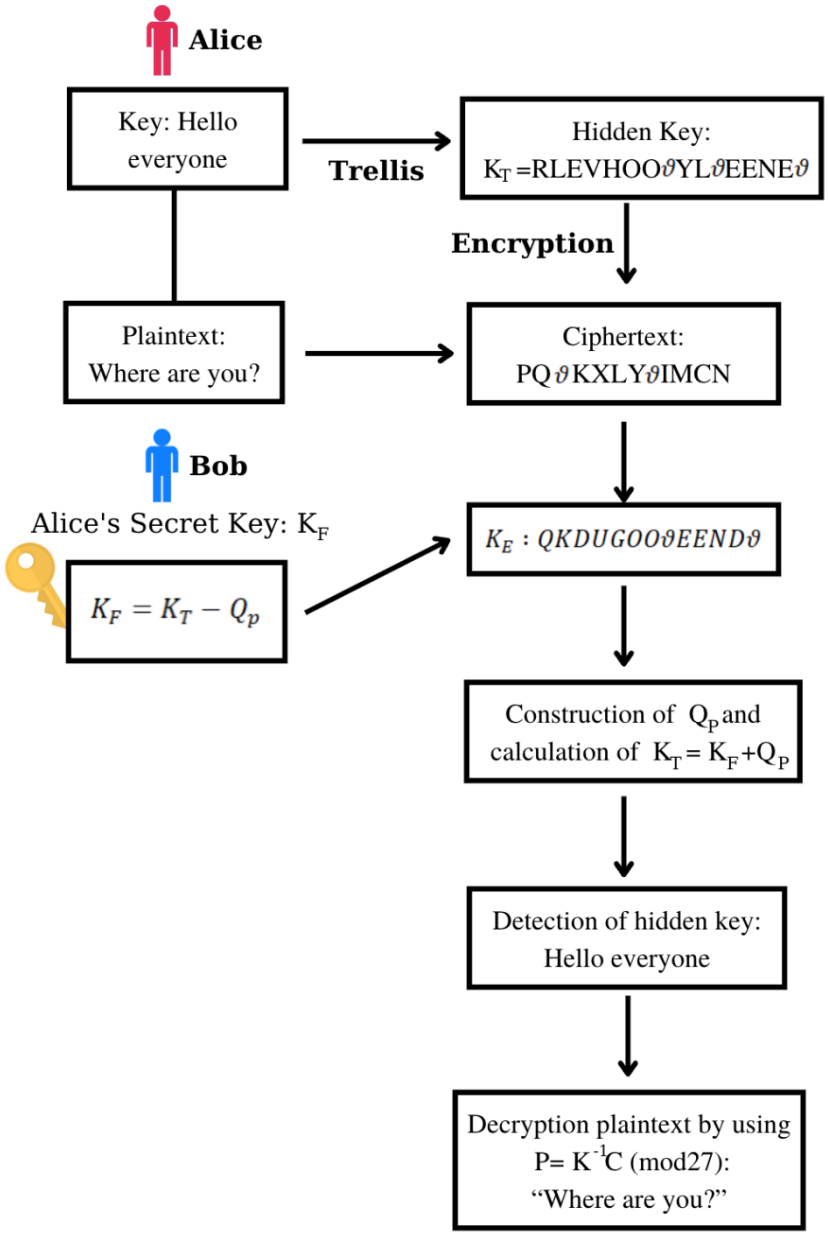


Figure1. The Proposed Algorithm with Iterated Keys

Comparisons and Conclusion

In the original form of the Affine-Hill's cipher, Alice and Bob agree on a common shared key used to encrypt and decrypt, but the main difficulty of the symmetric key is a problem of key transmission. For this reason, in recent decades Affine-Hill cipher are not limited to symmetric key. There are many articles based on public key cryptosystem.

The main result of the present article can be summarized as a new proposal for Affine-Hill cipher involving exchanged key via firstly with Trellis-based steganography method and multinacci Q matrices of order p.

Statement of Conflict Interest

Authors had no conflict of interest

Author's Contributions

All authors have contributed equally

References

Billore V, Patel N., 2023. Cryptography utilizing the affine hill cipher and extended generalized fibonacci matrices. Electronic Journal of Mathematical Analysis and Applications, 11(2): 1-12.

Brenner JL., 1951. 1. Lucas matrix. June Meeting of Pasific Nortwest Section. The American Mathematical Monthly, 58(3): 220-221.

Bruggles ID, Hoggat VE., 1963. A primer for the fibonacci numbers part IV. Fibonacci Q1, 4: 65-71.

Çivi Bilir G., 2023. Caesar'ın anahtarı-geçmişten günümüze klasik şifreleme yöntemleri. İTÜ Yayınevi, ISSBN 978-975-561-567-7.

Hoggat VE., 1969. Fibonacci and Lucas numbers. Palo Alto, CA, Houghton -Mifflin, ISBN 9789991205311.

Kahn D., 1996. The codebreakers the comprehensive history of secret communication from ancient times to the internet. 1996. ISBN 0-684-83130-9.

King CH., 1960. Some further properties of the fibonacci numbers. Master's Thesis, San Jose, CA.

Koshy T., 2018., Fibonacci and Lucas numbers with applications. John Wiley&Sons, New Jersey, 1: ISBN: 9781118742082.

Vara Prasad MG, Pari Purna Chari P, Pydi Satyam K., 2016. Affine hill cipher key generation matrix of order 3 by using reflects in an arbitrary line y=ax+ b. International Journal of Science, Technology and Manajemen, 5(8): 268-272.

Prasad K., Mahato H., 2021, Cryptography using generalized Fibonacci matrices with an Affine hill cipher. Journal of Discrete Mathematical Sciences and Cryptography, 25(8): 2341-2352.

Stakhov AP., 1999. A generalization of the fibonacci q-matrix. Reports of the National Academy of Sciences of Ukraine, 9: 46-49.

Stallings W., 2017. Cryptography and network security. Pearson, ISSBN 978-9332585225

Sundaraya P, Prasad V., 2019. A public key cryptosystem using affine hill cipher under modulation of prime number. Journal of Information and Optimization Sciences, 40(4): 919-930.

Uçar S., Taş N., Yılmaz Özgür N., 2019. A new application to coding theory via fibonacci and lucas numbers. Mathematical Sciences and Applications E-Notes, 7(1): 62-70.

Viswanath M, Kumar MR., 2015. A public key cryptosystem using Hill's cipher. Journal of Discrete mathematical Sciences and Cryptography, 18(1-2): 129-138.