ISSN 2278-3091
Volume 9, No.3, May - June 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse198932020.pdf
https://doi.org/10.30534/ijatcse/2020/198932020

Polybius Square in Cryptography: A Brief Review of Literature

Jan Carlo T. Arroyo[1], Cristina E. Dumdumaya[2], Allemar Jhone P. Delima[3]
[1,3]College of Computing Education, University of Mindanao, Davao City, Davao del Sur, Philippines
[1,2]College of Information and Computing, University of Southeastern Philippines, Davao City, Davao del Sur, Philippines
[3]College of Engineering, Technology and Management, Cebu Technological University-Barili Campus, Cebu, Philippines
jancarlo_arroyo@umindanao.edu.ph[1], cedumdumaya@usep.edu.ph[2], allemardelima@umindanao.edu.ph[3]

ABSTRACT

Cryptography is a method to secure sensitive data for storage and communication in the presence of third parties called adversaries. One of the first recorded incidents of cryptography occurred in Ancient Rome, where the Polybius cipher, also known as Polybius square, was developed. The Polybius cipher has been used as an advantage in winning wars over enemies according to history and is also utilized as a medium of communication. Today, as there is a need for more secure communication, the Polybius cipher, despite its early discovery and usage, is still at par when it comes to serving its purpose; to encrypt a secret message to provide secure information. There is a need for a secure cryptographic performance, and Polybius cipher is being improved and is hybridized along with other algorithms in the quest to achieve better system performance. This paper shows a brief literature review on the use of Polybius square in cryptography.

Key words: Ciphertext, cryptography, encryption, decryption, Polybius square

1. INTRODUCTION

In today's modern world, one of the most vital assets an organization can have is its data and information [1]. Securing data has been a challenge in this digital age, with the widespread use of electronic communication systems [2]. For instance, Internet Banking systems must have a secure communication system to guarantee the confidentiality of data. Under no circumstances, the perpetrators must not penetrate the database where accessed data may be illegally used [2]–[4]. In defense systems, vital information must not be leaked as it can be disastrous [5]–[7]. A known technique used to safeguard data is cryptography [8], [9].

Cryptography [10] is one of the renowned approaches in IT security that is commonly used in educational systems [11], cybercrime prevention [12], business, and finance data protection [13], health care data security [14], and many more. It is one of the renowned methods in security that concerns data integrity, confidentiality, authentication to a wireless communication system, and several other security services where information transfer between different users takes place [10]–[12]. To protect the information, data are transformed into an unintelligible format using varied cipher technologies [15]. Maintaining data integrity and security is done through cipher whose bottleneck for an optimal implementation relies on the cipher used. A cipher is an algorithm responsible for both the encryption and decryption processes of a file being protected. Encryption takes place by transforming essential information, in the form of plaintext, into ciphertext that is unrecognizable by a human. Some ciphers require the key to produce various transformations and substitutions, depending on the cipher being used [16].

Some of the classical ciphers found in the literature that are still being used today are ADFGX cipher [17]–[19], Affine cipher [19]–[22], Atbash cipher [23], Auto-key cipher [24], Baconian cipher [19], [25], Base64 cipher [26]–[28], Beaufort cipher [19], Caesar cipher [29]–[31], Grille cipher [32], Hill cipher [33], Homophonic Substitution cipher [34], [35], Playfair cipher [36]–[38], Polybius cipher [39], Railfence cipher [40], [41] and more. Among these, the Polybius cipher is considered to be one of the most widely used ciphers. It is one of the first encryption systems recorded, which was developed by Polybius. The Polybius square is the first of the early systems developed for substituting numbers for letters through fractionating to obscure plaintext message [42]. To this date, cryptographers find the Polybius square extremely valuable. Its ability to convert letters sequences to numeric sequences, reduce the number of different characters, and allow encoding of plaintext into two separately manipulatable units are known to be its advantages [17], [43]. With this at hand, modern cryptographic systems have embedded the Polybius square as a fundamental component of the encipherment process, such as in the key generation procedures used by modern ciphers [44], [45].

The Polybius encryption, as one of the earliest ciphers developed in history, has paved the way to the development and processes of other classical cipher techniques that are still used today such as ADFGVX Cipher [19], [46]–[48], Bifid cipher [19], [49], Nihilist cipher [50], and Trifid cipher [51], [52]. Originally, the abovementioned classical ciphers were

first designed to allow ciphering and deciphering process by hand but are now being improved to cope up with the emerging computer technologies as they are still useful because of their sophisticated performance [19]. The Polybius-based ciphers, along with other classical ciphers are used to improve services for internet shopping [53], online banking, image encryption, chip operation, mobile cloud computing, and some mobile messaging service that requires text protection in digital media.

Classical ciphers, specifically, the Polybius square is still being integrated along with modern ciphers like the advance encryption standard (AES), data encryption standard (DES), and other algorithms for improved performance of the abovementioned services [16], [46], [47], [54]–[57].

Despite being regarded as one of the first recorded cipher used for cryptography, there is a need for a review on its current performance and usability as its adaptations can be utilized along with other cryptographic algorithms in the future; thus, this study. This paper unravels the potential of Polybius cipher as it offers several security measures and lobby strength when modified [56] and used along with other cryptographic algorithms [58]. Further, this paper aims to answer the following research questions (RQ):

RQ1. What are the drawbacks of the cipher?
RQ2. What improvements have been made to address the drawbacks?
RQ3. What are the contributions of the Polybius square in the current cryptography?

2. METHODOLOGY

To identify relevant papers to be used for this study, a search on different research repositories such as ResearchGate, Semantic Scholar, Science Direct, Springer, and IEEE databases was conducted. Various documents from book sections, websites, journals, and conference papers were used with the time interval from 1996-2020. The search keywords used in the review are as follows:

1. “Polybius cipher” or “Polybius Square.”
2. “Polybius encryption” or “Polybius cryptography.”
3. “Cryptography.”
4. “Cipher.”
5. “Encryption.”
6. “Modified Polybius cipher.”
7. “Modified Polybius Square.”
8. “Enhanced Polybius Square”
9. “Hybrid Polybius Square.”

The research papers are filtered and are included in this study according to the following criteria:

1. title and abstract
2. keywords
3. methodology and its application
4. proposed methodology
5. results and discussion
6. conclusion and recommendation

Results were examined through peer-review by two of the authors in order to filter out which papers should qualify as sources of knowledge to be included in this study. Each author gave 1 point to each satisfied criterion that is deemed fit for the readership that matches the topic of interest. For the paper to be eligible as a reference, each cited reference gained at least 3 points.

Based on the criteria, 73 primary studies were found, and only 63 studies were cited in this paper. The other four papers were discarded as they are not written in English. The remaining six papers were also discarded as they do not contribute considerable knowledge to the research topic. Out of 63 cited papers, 54 studies are used for general backgrounds such as the application of the Polybius square and other ciphers in cryptography. Further, nine studies that focused on the modifications and hybridizations made specific on the Polybius Cipher are given emphasis. In order to address the research questions, 6, 9, and 7 research studies were used to answer RQ1, RQ2, and RQ3, respectively.

The graphical representation of the 63 indexed publication resources used in this study that are grouped by type and its equivalent percentage is shown in Figure 1.

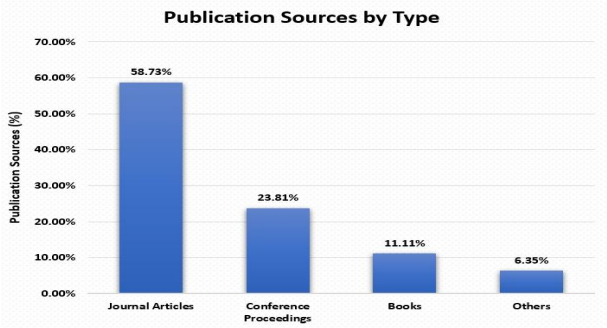

Figure 1: Publication sources grouped by type. Source: Authors

As to the document classification shown in Figure 1, most of the papers used in this study are from journal publications with 37 articles. 28% of the cited articles are from conference proceedings with 15 research articles, whereas seven citations are from book sections. Two citations were taken from the theses and the other two from web sources, which are categorized as others. This denotes that researches in relation to the selected topic are mostly published in journals followed by conference proceedings. The graphical representation of the distribution of the 63 research studies by year is presented in Figure 2.

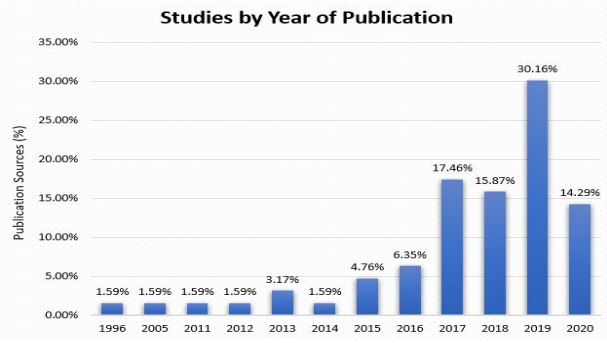

Figure 2: Selected documents by year of publication. Source: Authors

Figure 2 shows that most of the related and significant works in the Polybius Cipher are published between the years 2017-2019. The indexed graphical representation of the distribution of sources by year with its corresponding types is shown in Figure 3.

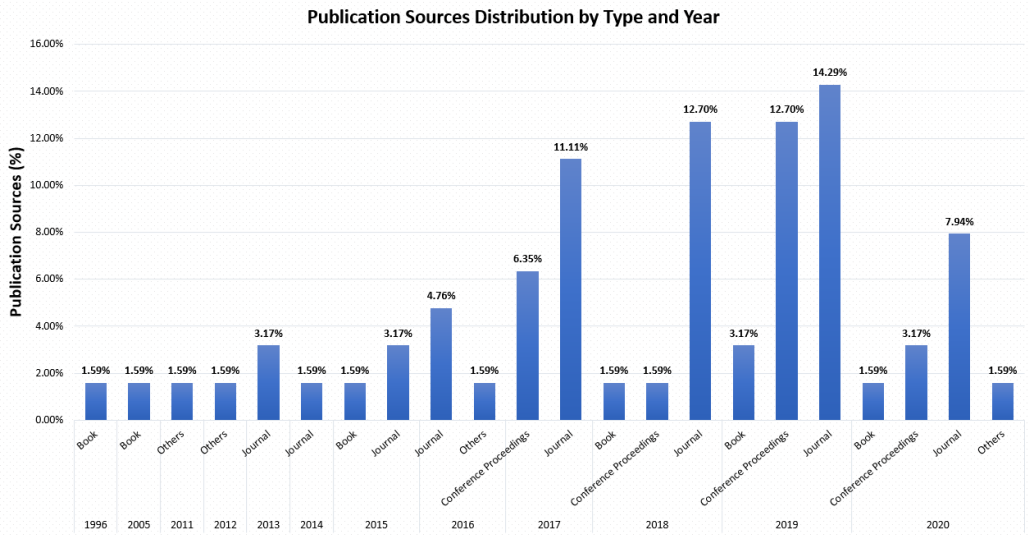

Figure 3: Documents by year with its corresponding publication type. Source: Authors

Figure 3 shows that most of the studies from the corpus of 63 relevant resources are published in the year 2019, where most of the papers are published in journals followed by conference proceedings with 14.29% and 12.70%, respectively.

3. POLYBIUS CIPHER

Polybius Square is a substitution cipher that fractionates the alphabet, arranging them into a square matrix consisting of five rows and five columns [42]. Since it is one of the first recorded ciphers, the Polybius cipher became an essential tool for the Roman Empire, giving them an advantage over enemies during wars [52].

Letters of the alphabet in the Polybius square are arranged in a 5x5 grid. Since there are only 24 characters in the Greek alphabet, the last cell is set as space. As seen in Table 1, the letters represent the plaintext while the combination of column and row numbers represent the ciphertext.

Table 1: Polybius square with the Greek alphabet

	1	2	3	4	5
1	Α	Β	Γ	Δ	Ε
2	Ζ	Η	Θ	Ι	Κ
3	Λ	Μ	Ν	Ξ	Ο
4	Π	Ρ	Σ	Τ	Υ
5	Φ	Χ	Ψ	Ω	

This coding scheme was used to transmit messages through holding and raising torches. Torches raised using the right hand indicate the row value, while the left hand denotes the column value. In the case of the modern English alphabet comprising 26 characters, the letters are spread throughout 25 cells in the matrix. The character 'J' is usually combined in a single cell with the character 'I,' hence sharing the same code [56] as shown in Table 2.

Table 2: Polybius square with the modern English alphabet

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

To encrypt plaintext, each letter is replaced with a corresponding pair number obtained through the intersection of the row and column value the letter is plotted. For example, the character 'E' is located at the 1st row, 5th column, hence, will be encrypted as the value 15. When a string is encrypted, each character is transformed respectively with or without spaces separating each ciphertext. For instance, the plaintext 'AJPD' may be represented as '11243514' or '11 24 35 14'.

Decrypting the ciphertext is done by matching each pair of numbers to the square matrix. For instance, the ciphertext '31344115' or '31 34 41 15' is easily decrypted as 'LOVE.' Even if the ciphertext is written with or without spaces between each character, it is relatively easy to decipher. Characters are always represented as a pair called bigram.

However, the Polybius cipher also has its limitations. The traditional Polybius cipher does not use the key for encryption and decryption process, thus, vulnerable to attacks [41], [59]. Moreover, having characters 'I' and 'J' share the same grid in the Polybius square distorts the original plaintext and, in turn, confuse the decoding process [42], [43], [56]. Also, the Polybius cipher, like other substitution ciphers, are prone to frequency analysis attacks. This happens when a cryptanalyst tries to break the ciphertext by analyzing character patterns [16], [17], [42], [43]. A plaintext with identical characters such as AABBAABB is translated with similar patterns as well, such as 11 11 12 12 11 11 12 12. Cracking 11 and 12 in this ciphertext allows the cryptanalyst to easily identify the whole sequence completely.

Polybius Cipher, being one of the commonly used cipher algorithms in the literature, are continuously being used and is modified to address problems and anomalies in IT and data security.

4. IMPROVEMENTS AND MODIFICATIONS

The literature in the use of Polybius Cipher is extensive. Over time, Polybius Cipher is being improved, and various models were developed and utilized in response to the problems the researchers sought to answer about the effectiveness of the cipher algorithm.

With the advent of the hybridization of various algorithms, Polybius cipher has become more effective and efficient in performing the job. The following modifications and hybridization of the Polybius Cipher are discussed in this section. The indexed modifications made in the Polybius cipher is shown in Table 3.

Table 3: Indexed Polybius cipher modifications

Title	Authors/ Year	Methods	Purpose	Significant Results
An Extended Version of the Polybius Cipher	Kondo & Mselle (2013)	Modified the Polybius cipher with the introduction of 8x8 Polybius square grid	To extend the traditional 5x5 grid Polybius square for an enhanced cipher capability	The extended Polybius square can now encrypt plaintext containing digits, special symbols, and alphabets. Further, the characters I and j are now separated, which inhibits ambiguity during the cipher process.
A Modified Version of Polybius Cipher Using Magic Square and Western Music Notes	Maity (2014)	Modified Polybius Cipher with the introduction of 6x6 magic square and musical notes	To introduce diversity in the substitution process of the traditional Polybius cipher following the magic square theory, and generate a music sequence out of ciphertext	The proposed method offers a unique substitution process since the arrangement of alphabets depends on the unique magic squares generated, making the cracking process difficult. In this study, no two characters share the same cell anymore.
A Hybrid Polybius-Playfair Music Cipher	C. Kumar, Dutta, & Chakraborty (2015)	Hybrid Polybius and Playfair ciphers with a secret key	To integrate music cryptography in generating ciphertext using a key matrix for secure encryption and decryption using a hybrid Polybius-Playfair method.	The study has paved the way for creating musical sequences using a dual encryption method. The result of using the hybrid process produces satisfactory musical sequences without compromising the security of the hidden message. Characters I and J still share the same cell in this proposed method.
Development of Modified Polybius Technique for Data Security	P. Kumar & Rana (2015)	Modified the Polybius cipher with the introduction of 6x6 Polybius square grid following a different arrangement of characters	To extend the capability of the cipher using a 6x6 Polybius square and introduce a new method of arranging alphabets	The study introduces a different sequencing of characters in the grid. With the addition of digits, the cipher can cater more characters to be encoded and decoded. Further, the characters I and J are also separated in different cells since there are already enough spaces for all letters and digits.
Design of a Modified AES algorithm for Data Security	P. Kumar & Rana (2016)	Modified the Polybius cipher with the introduction of 6x6 Polybius square grid	To extend Polybius square into a 6x6 matrix and use this for key generation process in another cryptographic system	The proposed modification allows all letters and numbers to be processed. As a result, the key generation process in the AES algorithm has been made more secure and sophisticated.
A Novel Structure of Advance Encryption Standard (AES) with 3-Dimensional S-box, RSA based Key Scheduling and modified 3- Dimensional Polybius Cube Encipherment	Rahman et al., (2017)	Modified the Polybius cipher with the introduction of 9x9x9 Polybius cube	To introduce a novel 3-dimensional Polybius cube for the key scheduling algorithm (KSA) accommodating letters, numbers and as well symbols	The study introduces a unique method of key generation process for the AES algorithm with the use of a 3D dynamic substitution box with a ciphertext output of a trigram instead of a bigram. With a bigger capacity, the cipher can process uppercase letters, lowercase letters, numbers, and most special characters.
A Modified Polybius Square Based Approach for Enhancing Data Security	Manikandan, Rajendiran, Balakrishnan, & Thangaselvan (2018)	Modified the ciphertext generation process of the 6x6 Polybius cipher through matrix transmutation	To introduce a series of transmutation methods for the Polybius square and the use of a key for a more secure cryptography	The modified Polybius cipher offers diverse ciphertext generation techniques with the introduction of square ring rotation, transpose, and reversal key generation schemes that increase the time complexity of breaking the encoded message.
Embedding Data Crypted With Extended Shifting Polybius Square Supporting Turkish Character Set	Macit, Koyun, & Yüksel (2019)	Modified the Polybius Cipher with the introduction of 10x7 Polybius square grid	To extend the traditional Polybius square grid to accommodate characters in the Turkish keyboard and shift elements in the table using a key	The proposed process allows encryption and decryption of more characters, particularly those appearing in the Turkish alphabet. With this study, matrix shifting is introduced, spaces can already be encrypted, while characters I and J are now separated in different cells. The proposed method was successfully implemented in the domain of image steganography.
Implementation of Nihilist Cipher Algorithm in Securing Text Data With Md5 Verification	Haryannto, Zulfadly, Daifiria, Akbar, & Lazuly (2019)	Altered the placement of the elements in the Polybius square grid	To use the Polybius square with varied character arrangements elements using the Nihilist cipher and MD5 technology for a more secured encryption and decryption	The proposed method produced a more secure ciphertext due to layers and diverse processes being conducted.

4.1 An Extended Version of the Polybius Cipher

In [56], the Polybius square was extended into an 8x8 matrix, also to include digits and symbols. This modification allows extensive coverage for encrypting messages with characters other than letters of the English alphabet. The study also introduces a keyword to variate the arrangement of characters in the matrix. The keyword is plotted from top to bottom and left to right without repetitions. Any remaining letters not used in the keyword are then filled in the remaining cells in alphabetical order. Next, digits are placed in ascending order, followed by the special symbols arranged according to their ASCII value. Table 4 shows how the extended Polybius square would appear using the keyword “POLY2013”.

Table 4: Extended Polybius square

	1	2	3	4	5	6	7	8
1	P	O	L	Y	2	0	1	3
2	A	B	C	D	E	F	G	H
3	I	J	K	M	N	Q	R	S
4	T	U	V	W	X	Z	4	5
5	6	7	8	9		!	“	#
6	$	%	&	‘	(	)	*	+
7	,	-	.	/	:	;	<	=
8	>	?	@	[	\	]	^	_

The study also proposed a unique way of encrypting the plaintext. Each character in the plaintext is identified according to its relative position in the string, whether odd or even. All odd positioned characters (1st, 3rd, 5th) are encrypted by combining the row number first, then the column number next. On the other hand, all even positioned characters (2nd, 4th, 6th) are encrypted by combining the column number first, then the row number next. With this approach, breaking the code using frequency analysis may be made difficult. For example, encrypting the plaintext “AJPDJCTA” will result in the ciphertext “2123114232324112,” as seen in Table 5.

Table 5: Encryption using extended Polybius square

Plaintext	A	J	P	D	J	C	T	A
Position	1	2	3	4	5	6	7	8
Ciphertext	21	23	11	42	32	32	41	12

Table 5 shows that although the characters ‘A’ and ‘J’ have appeared twice in the plaintext, its ciphertext is not the same as they appear in different positions. Looking at the ciphertext for the character ‘J’ at position five and character ‘C’ at position six may denote confusion and difficulty when decrypting as both have the same ciphertext values.

When decrypting a message, it is important to note the odd and even positioned characters first before matching the ciphertext to the extended Polybius matrix. For instance, decrypting the ciphertext “2123114232324112” results in ‘AJPDJCTA,’ as seen in Table 6.

Table 6: Decryption using extended Polybius square

Ciphertext	21	23	11	42	32	32	41	12
Position	1	2	3	4	5	6	7	8
Plaintext	A	J	P	D	J	C	T	A

4.2 A Modified Version of Polybius Cipher Using Magic Square and Western Music Notes

The proposed system of [39] introduced a novel way of implementing the Polybius cipher through the use of a unique 6x6 magic square and musical notes. To come up with a magic square, each cell is identified with an integer from 1 to 36 while ensuring that the sum of the numbers in any horizontal, vertical, or main diagonal line is always equal [60]. In the case of a 6x6 matrix, the sum should equal to 111. After, letters ‘a’ to ‘z’ are plotted in cells 1 to 26 based on their order in the alphabet. On the other hand, digits 0-9 are placed in cells 27 to 36 in ascending order. As the magic square uses music notes for the cipher, all rows and columns are denoted with the notes C-D-E-F-G-A. Table 7 shows a sample magic square with its corresponding elements.

Table 7: Magic square with music notes

	C	D	E	F	G	A
C	26 Z	35 8	1 A	19 S	6 F	24 X
D	17 Q	8 H	28 1	10 J	33 6	15 O
E	30 3	12 L	14 N	23 W	25 Y	7 G
F	3 C	21 U	5 E	32 5	34 7	16 P
G	31 4	22 V	27 0	9 I	2 B	20 T
A	4 D	13 M	36 9	18 R	11 K	29 2

Character ‘A,’ being the first in the alphabet, is placed in the cell with the value 1 located at the 1st row 3rd column. The digit 0, which is identified as 27th in the sequence, is placed at the 5th row 3rd column.

To encrypt the string ‘MARCH24’, each character is substituted using the magic square to retrieve the corresponding music note value, as shown in Table 8. To decrypt a given musical note sequence, match the pair of notes to the magic square to retrieve the equivalent plaintext.

Table 8: Encryption using the magic square

Plaintext	M	A	R	C	H	2	4
Ciphertext	AD	CE	AF	FC	DD	AA	GC

Each time the sequence of integers in the magic square changes, the arrangement of all elements will also shift. Thus, forming varied substitution values for every unique magic square.

4.3 A Hybrid Polybius-Playfair Music Cipher

The paper [61] presented a hybrid modification of the Polybius and Playfair cipher, which translates messages into a series of musical notes. First, the plaintext is converted into Playfair digraphs and then encrypted using a key matrix. Table 9 shows a sample Playfair key matrix in a Polybius square labeled with five major music chords ‘ABCDE.’ It can be observed that I/J share the same cells, which means that they use the same substitution value BA.

Table 9: Hybrid Polybius-Playfair key matrix

	A	B	C	D	E
A	P	L	A	Y	F
B	I/J	R	B	C	D
C	E	G	H	K	M
D	N	O	Q	S	T
E	U	V	W	X	Z

The resulting Playfair ciphered text will be re-encrypted using the Polybius square of the same key matrix. The generated output will be musical equivalents of the Polybius cipher. Table 10 shows how the string ‘HELLO WORLD’ is encrypted using the hybrid technique. To decrypt a message, the process is done in reverse order by matching the chords with the generated matrix.

Table 10: Encryption using Polybius-Playfair cipher

Plaintext	HELLO WORLD					
Playfair Digraph	HE	LX	LO	WO	RL	DX
Playfair Cipher	KG	YV	RV	VQ	GR	ZC
Polybius Cipher	CDCB	ADEB	BBEB	EBDC	CBBB	EEBD

4.4 Development of Modified Polybius Technique for Data Security

The proposed Polybius Square in [44] uses a 6X6 matrix rather than a 5X5 matrix. In this study, the square now includes numbers instead of just letters. This allows more combinations of characters, thus increases its capacity. Moreover, two different characters do not hold the same cell, in the case of characters I and J. With this, there is no possibility of making mistakes in decrypting the ciphertext. The proposed matrix shown in Table 11 consists of both the alphabets and numerals filled without repetition from left to right of columns 1 to 4, then top to bottom of columns 5 to 6.

Table 11: Modified 6x6 Polybius square

	1	2	3	4	5	6
1	A	B	C	D	Y	4
2	E	F	G	H	Z	5
3	I	J	K	L	0	6
4	M	N	O	P	1	7
5	Q	R	S	T	2	8
6	U	V	W	X	3	9

Encrypting a plaintext using this proposed method still follows the traditional approach to the Polybius cipher. However, more characters can now be encoded and decoded with the extended matrix. To encrypt, each character from the plaintext is matched with the matrix to retrieve its respective bigram. For instance, the plaintext CIPHER is translated as 13 33 44 24 21 52, as presented in Table 12. With the varied arrangement of letters, this modified Polybius square allows the generation of a distinct ciphertext sequence as against the traditional method.

Table 12: Encryption of the plaintext CIPHER

Plaintext	C	I	P	H	E	R
Modified PS	13	33	44	24	21	52
Traditional PS	13	24	35	23	15	42

4.5 Development of a Modified AES algorithm for Data Security

This study proposes the use of the Polybius square in the key generation process as an integral component of the modified AES algorithm [44], as shown in Figure 4.

The Polybius square in this study is a 6x6 matrix composed of letters and numbers arranged in an extended but static layout, as presented in Table 13. Here, row and columns are identified by digits 0-5 instead of the traditional 1-6. Since the matrix is extended, no characters share the same cell any longer, and more characters can be processed.

Table 13: A 6x6 Polybius square

	1	2	3	4	5	6
1	A	B	C	D	E	F
2	G	H	I	J	K	L
3	M	N	O	P	Q	R
4	S	T	U	V	W	X
5	Y	Z	0	1	2	3
6	4	5	6	7	8	9

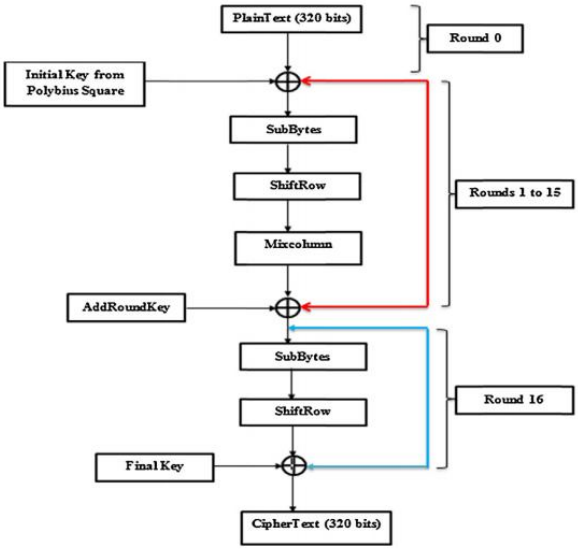

Figure 4: Modified AES with Polybius square [44]

The key generation process requires a string input that can be composed of letters A to Z and digits 0 to 9. Using the static matrix, characters are substituted as a bigram. The bigrams represent the combination of the row and column headings as value. For example, the plaintext SECURE is encoded into 30 04 02 30 25 04 as the equivalent ciphertext. The output from this process is then used as an input to their modified AES algorithm.

4.6 A Novel Structure of Advance Encryption Standard (AES) with 3-Dimensional S-box, RSA based Key Scheduling and modified 3- Dimensional Polybius Cube Encipherment

In this study, AES is strengthened by using a 3-dimensional Polybius square for key generation. The cube contains the Latin alphabet, numbers, and symbols in a 9x9x9 matrix [45], as presented in Figure 5. To be able to use the substitution method, the value must be located along the *x, y,* and *z*-axis. However, the study uses only two faces of the cube wherein the substituted value is retrieved using a row-column-position process. For instance, character P from the plaintext COMPUTER is encrypted using the proposed study. First, the row and column indices of P are identified based on the Polybius cube in Figure 5, wherein row = 4 and column = 2. Next, the character position is used to retrieve the substitution value from the other side of the cube, wherein position = 3. Therefore, the ciphertext equivalent of P is 42G, as shown in Table 14. In this modified method, ciphertext values are represented as a trigram instead of a bigram.

Table 14: Encryption using modified AES with Polybius

Plaintext	C	O	M	P	U	T	E	R
Position	0	1	2	3	4	5	6	7
Ciphertext				42G				

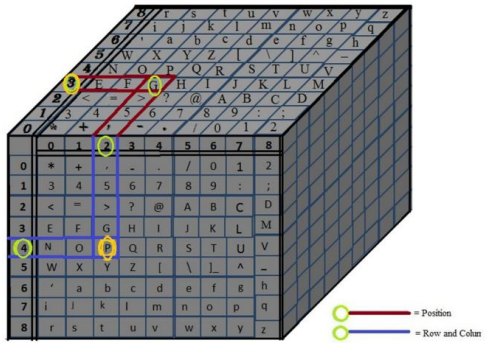

Figure 5: 3-Dimensional Polybius square [45]

4.7 A Modified Polybius Square Based Approach for Enhancing Data Security

A 6x6 Polybius matrix is introduced in [62], as shown in Table 15, which is composed of the English alphabet and numerals 0-9. The digits are first added in the matrix in ascending order, then followed by adding in the letters 'a' to 'z.'

Table 15: Polybius square with elements

0	1	2	3	4	5
6	7	8	9	a	b
c	d	e	f	g	h
i	j	k	l	m	n
o	p	q	r	s	t
u	v	w	x	y	z

The study proposes the use of the plaintext as a key to transmute the matrix through ring rotation, transposition, and row reversal. First, the matrix undergoes row reversal by swapping the values in the row such that the 1st element becomes the 5th element, and the 5th element becomes the 1st element. The same is applied for each remaining element in the row. For instance, row 1 consisting elements '0|1|2|3|4|5' becomes '5|4|3|2|1.' Table 16 shows the new matrix after applying row reversal.

Table 16: Row reversed Polybius square

5	4	3	2	1	0
b	a	9	8	7	6
h	g	f	e	d	c
n	m	l	k	j	i
t	s	r	q	p	o
z	t	x	w	v	u

In the next step, the transposition is done wherein each corresponding row will be rewritten as columns. For example, row 1 consisting of elements '5|4|3|2|1' becomes column 1 with the same values. The new matrix after transposition is shown in Table 17.

Table 17: Transposed Polybius square

5	b	h	n	t	z
4	a	g	m	s	y
3	9	f	l	r	x
2	8	e	k	q	w
1	7	d	j	p	v
0	6	c	i	o	u

Lastly, the matrix undergoes a ring rotation based on a given key. In this case, the given key is 'sastra.' The key is used to retrieve the number of rotations by finding the sum of its ASCII values modulo length of the ring. With the total ASCII sum of 654, the outermost ring is rotated clockwise by 14 times (654%20=14). The second outermost ring and the inner ring is rotated 6 (654%12=6) and 2 (654%4=2) times, respectively. The new matrix after ring rotation is shown in Table 18.

Table 18: Ring rotated Polybius square

y	x	w	v	u	o
z	p	j	d	7	i
t	q	k	e	8	c
n	r	l	f	9	6
h	s	m	g	a	0
b	5	4	3	2	1

Presented in Table 19 is the encryption of the given key 'sastra.' Each character must be identified with their relative coordinate in the new matrix and then matched with the corresponding value in the original matrix using its coordinates. For instance, the character 'a' in the new matrix is located at position (5,5) and therefore replaced with 's' based on the given value in the same position from the original matrix.

Table 19: Encryption using the modified Polybius square

Plaintext	s	a	s	t	r	a
Coordinates	(5,2)	(5,5)	(5,2)	(3,1)	(4,2)	(5,5)
Ciphertext	p	s	p	c	j	s

4.8 Embedding Data Crypted with Extended Shifting Polybius Square Supporting Turkish Character Set

The paper [63] presented an extended Polybius Square by incorporating Turkish characters in a 10x7 grid. This improved version also introduced a process of shifting elements based on a given key; therefore, it creates unique substitution values every time the matrix components shift. The elements of the extended matrix are shown in Table 20.

Table 20: Polybius square with Turkish characters

	01	02	03	04	05	06	07
01	A	B	C	Ç	D	E	F
02	G	Ğ	H	I	İ	J	K
03	L	M	N	O	Ö	P	R
04	S	Ş	T	U	Ü	V	Y
05	Z	Q	X	W	1	2	3
06	4	5	6	7	8	9	0
07	.	,	:	;	+	-	*
08	/		!	"	#	$	%
09	&	=	<	>	?	@	[
10	]	\	_	(	)	{	}

In order to encrypt plaintext 'AZ GİT,' a shifting value must be selected to generate a new square. For instance, the shift value is '0052', thus, creating a new square, as shown in Table 21.

Table 21: Shifted Polybius square

	01	02	03	04	05	06	07
01	"	#	$	%	&	=	<
02	>	?	@	[	]	\	_
03	(	)	{	}	A	B	C
04	Ç	D	E	F	G	Ğ	H
05	I	İ	J	K	L	M	N
06	O	Ö	P	R	S	Ş	T
07	U	Ü	V	Y	Z	Q	X
08	W	1	2	3	4	5	6
09	7	8	9	0	.	,	:
10	;	+	-	*	/		!

After a new square is created, each character from the plaintext is translated to the ciphertext in a 4-digit format. In the given example, 'AZ GİT' is converted into '030507051006040505020607', as shown in Table 22. Providing that the shifting key is known, the decryption process can be done by taking 4-digit numbers each time and matching it with the matrix.

Table 22: Encryption using shifting Polybius square

Plaintext	A	Z	(space)	G	İ	T
Ciphertext	0305	0705	1006	0405	0502	0607

The proposed method was successfully tested by implementing it in a steganographic algorithm. Since ciphertext value for every character falls into the range of 0101 to 1007, it can be used to alter the least-significant bit of an image to carry encrypted messages without causing distortion in the file.

4.9 Implementation of Nihilist Cipher Algorithm in Securing Text Data with Md5 Verification

The study [50] proposed the use of Polybius Square in encrypting messages. Though the study uses the traditional 5x5 Polybius matrix, the arrangement of the characters differs. Based on the given example in [50], letters are placed top to bottom per column instead, as shown in Table 23. The study also proposed the use of a key to further enhance security in encrypting and decrypting messages.

Table 23: Polybius square used in Nihilist cipher

	1	2	3	4	5
1	A	F	L	Q	V
2	B	G	M	R	W
3	C	H	N	S	X
4	D	I	O	T	Y
5	E	K	P	U	Z

For encryption, the plaintext and the key are converted into its equivalent ciphertext based on the given matrix. Each character's converted values will then be added together to come up with the final ciphertext. Table 24 shows how the plaintext 'KASKUS' is encrypted using the key 'CENDOL.' For instance, the character 'K' from the plaintext is converted as 52. The character 'C' from the key is turned to 31. The value for the final ciphertext will be 83 (52+31=83).

Table 24: Encryption using Nihilist cipher

Plaintext	K	A	S	K	U	S
Ciphertext	52	11	34	52	54	34
Key	C	E	N	D	O	L
Ciphertext	31	51	33	41	43	13
Final Ciphertext	83	62	67	93	97	47

To decrypt a message, the key must be known. The key is converted to ciphertext using the matrix, and then it is subtracted from the encrypted message. The result will be matched to the given Polybius Square to retrieve the original message.

Table 25: Indexed features and methodology

Study	Extended / More characters / No sharing of cells	Use of a secret key	New encryption and decryption process	Modified character arrangement in the grid	Used along with other cryptographic systems	Modified the generated ciphertext
1	✓	X	X	X	X	X
2	✓	X	X	✓	X	✓
3	✓	X	✓	✓	✓	X
4	✓	X	X	✓	X	X
5	✓	X	X	X	✓	X
6	✓	X	✓	✓	✓	✓
7	✓	✓	X	✓	X	X
8	✓	✓	✓	✓	✓	X
9	X	✓	✓	X	✓	X

5. CONCLUSION

In this paper, a brief review of the usage, problems, and improvements made to the Polybius Square along with its hybridization paired with other cryptographic algorithms has been done.

It is concluded that the Polybius encryption, despite being a classical technique, is still relevant up to this day. The Polybius cipher is still very effective in performing its task in securing data, especially when added to other cryptographic algorithms, as proposed in the studies of [44], [45], leading to reduced vulnerability from attackers. With the status quo, the Polybius cipher, together with other classical ciphers, remain significant regardless of the existence of modern cipher technologies. This study shows that current cryptographic methods continue to use the Polybius-based ciphers and other classical ciphers, such as in cipher process integrations and hybridizations [44], [45], [61].

Problems such as the limited number of characters in the square grid, the sharing of a cell for letters I and J, and the absence on the use of the secret key for encryption, has been addressed on the recent works on the Polybius square [41]–[43], [56], [59], [63].

To overcome the abovementioned drawbacks, improvements and modifications were done by introducing the concept of the secret key [61]–[63] and increasing the capacity of the cipher by extending the grid to a bigger matrix, allowing more characters to be encoded. The extension of the Polybius square ensures no two characters share the same cell [39], [44], [45], [56], [59], [62], [63]. The indexed improvements made on the Polybius cipher is shown in Table 25.

However, the risk of attacks through frequency analysis has not yet been fully addressed even by existing modifications. An attempt is made by [56], as discussed in section 4.1 of this paper. However, the modification is not optimal.

In general, the simplicity and flexibility of the Polybius encryption have laid the foundation for better ciphertext generation and security performance. Furthermore, a perceived increase in security is one of the many benefits attained in the modification and improvements of the Polybius cipher.

6. RECOMMENDATIONS

The primary limitation of this literature review is the lack of prior research studies on resolving the drawback extent on frequency analysis attack. This prompted the authors to only include and review existing solutions on the concerns in relation to matrix size and secret keys, as well as hybridization, and process integrations of the Polybius square.

While current works relating to the Polybius square have established better cryptography, more improvements can still be made since security against attacks using frequency analysis is not optimal. Future works may focus on: (1) increasing its complexity through randomization such as the use of dynamic matrix controls, chaotic systems or random numbers, (2) introducing a new process for encryption and decryption, (3) hybridization with other cryptographic techniques, and (4) integrating the traditional Polybius cipher and its improved versions along with modified modern cryptographic algorithms such as AES, DES, Blowfish, and the likes. Further, future researches may focus on the modifications that will resolve issues regarding frequency analyses.

REFERENCES

[1] A. Rayarapu, A. Saxena, N. V. Krishna, and D. Mundhra, "Securing Files Using AES Algorithm," *Int. J. Comput. Sci. Inf. Technol.*, vol. 4, no. 3, pp. 433–435, 2013.

[2] S. B. Das, S. K. Mishra, and A. K. Sahu, "A New Modified Version of Standard RSA Cryptography Algorithm," *Smart Comput. Paradig. New Progresses Challenges. Adv. Intell. Syst. Comput.*, vol. 767, pp. 281–287, 2020. https://doi.org/10.1007/978-981-13-9680-9_24

[3] Y. Tian, Q. Li, J. Hu, and H. Lin, "Secure limitation analysis of public-key cryptography for smart card settings," *World Wide Web*, vol. 23, pp. 1423–1440, 2020.

[4] T. E. Jisha and T. Monoth, "Recent Research Advances in Black and White Visual Cryptography Schemes," *Soft Comput. Probl. Solving. Adv. Intell. Syst. Comput.*, vol. 1048, pp. 479–492, 2020. https://doi.org/10.1007/978-981-15-0035-0_38

[5] M. D. Singanjude and R. Dalvi, "Secure and Efficient Application of Manet Using RSA Using Vedic Method Combine With Visual Cryptography and Identity Based Cryptography Technique," in *3rd International Conference on Innovative Computing and Communication (ICICC)*, 2020, pp. 1–5.

[6] H. Mirvaziri and R. Hosseini, "A Novel Method for Key Establishment Based on Symmetric Cryptography in Hierarchical Wireless Sensor Networks," *Wirel. Pers. Commun.*, 2020. https://doi.org/10.1007/s11277-020-07155-y

[7] M. Abdulla and M. E. Rana, "Vulnerabilities in public key cryptography," *Int. J. Psychosoc. Rehabil.*, vol. 24, no. 5, pp. 3881–3886, 2020.

[8] H. Tao, M. Z. A. Bhuiyan, A. N. Abdalla, M. M. Hassan, J. M. Zain, and T. Hayajneh, "Secured Data Collection with Hardware-Based Ciphers for IoT-Based Healthcare," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 410–420, 2019. https://doi.org/10.1109/JIOT.2018.2854714

[9] H. Shin, H. K. Lee, H. Y. Cha, S. W. Heo, and H. Kim, "IoT Security Issues and Light Weight Block Cipher," in *1st International Conference on Artificial Intelligence in Information and Communication*, 2019, pp. 381–384.

[10] O. Reyad, "Cryptography and Data Security: An Introduction," 2018.

[11] K. Al Harthy, F. Al Shuhaimi, and K. K. J. Al Ismaily, "The upcoming Blockchain adoption in Higher-education: Requirements and process," in *4th MEC International Conference on Big Data and Smart City, ICBDSC 2019*, 2019, pp. 1–5.

[12] P. Kuppuswamy, R. Banu, and N. Rekha, "Preventing and securing data from cyber crime using new authentication method based on block cipher scheme," in *2nd International Conference on Anti-Cyber Crimes, ICACC 2017*, 2017, pp. 113–117.

[13] R. Beck, M. Avital, M. Rossi, and J. B. Thatcher, "Blockchain Technology in Business and Information Systems Research," *Bus. Inf. Syst. Eng.*, vol. 59, no. 6, pp. 381–384, 2017.

[14] S. Cho, Y. Jeong, and C. Oh, "An efficient cryptography for healthcare data in the cloud environment," *J. Converg. Inf. Technol.*, vol. 8, no. 3, pp. 63–69, 2018.

[15] S. N. Kumar, "Review on Network Security and Cryptography," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 8, no. 6, p. 21, 2018.

[16] W. Stallings, *Cryptography and Network Security Principles and Practices*. Prentice Hall, 2015.

[17] D. Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. Scribner, 1996.

[18] P. W. L. McLaren, "Investigations into Decrypting Live Secure Traffic in Virtual Environments," 2019. https://doi.org/10.1016/j.diin.2019.03.010

[19] M. S. Hossain Biswas *et al.*, "A systematic study on classical cryptographic cypher in order to design a smallest cipher," *Int. J. Sci. Res. Publ.*, vol. 9, no. 12, pp. 507–11, 2019.

[20] M. Maxrizal and B. D. Aniska Prayanti, "Application of Rectangular Matrices: Affine Cipher Using Asymmetric Keys," *CAUCHY –Jurnal Mat. Murni dan Apl.*, vol. 5, no. 4, pp. 181–185, 2019.

[21] T. M. Aung and N. N. Hla, "A Complex Polyalphabetic Cipher Technique Myanmar Polyalphabetic Cipher," in *2019 International Conference on Computer Communication and Informatics, ICCCI 2019*, 2019, pp. 1–9.

[22] O. Laia, E. M. Zamzami, Sutarman, F. G. N. Larosa, and A. Gea, "Application of Linear Congruent Generator in Affine Cipher Algorithm to Produce

Dynamic Encryption," *J. Phys. Conf. Ser.*, vol. 1361, no. 1, pp. 1–6, 2019. https://doi.org/10.1088/1742-6596/1361/1/012001

[23] J. C. Das and D. De, "Atbash cipher design for secure nanocommunication using QCA," *Nanomater. Energy*, vol. 6, no. 1, pp. 36–47, 2017.

[24] H. Nurdiyanto, R. Rahim, A. S. Ahmar, M. Syahril, M. Dahria, and H. Ahmad, "Secure a Transaction Activity with Base64 Algorithm and Word Auto Key Encryption Algorithm," *J. Phys. Conf. Ser.*, vol. 1028, pp. 1–11, 2018.

[25] A. Abd and S. Al-Janabi, "Classification and Identification of Classical Cipher Type Using Artificial Neural Networks," *J. Eng. Appl. Sci.*, vol. 14, no. 11, pp. 3549–3556, 2019. https://doi.org/10.36478/jeasci.2019.3549.3556

[26] F. Anwar, E. H. Rachmawanto, C. A. Sari, and de Rosal Ignatius Moses Setiadi, "StegoCrypt Scheme using LSB-AES Base64," in *International Conference on Information and Communications Technology, ICOIACT 2019*, 2019, pp. 85–90.

[27] A. R. Pathak, S. Deshpande, and M. Panchal, "A Secure Framework for File Encryption Using Base64 Encoding," in *Computing and Network Sustainability*, vol. 75, Springer Singapore, 2019, pp. 359–366.

[28] R. Rahim, S. Sumarno, M. T. Multazam, S. Thamrin, and S. H. Sumantri, "Combination Base64 and GOST algorithm for security process," *J. Phys. Conf. Ser.*, vol. 1402, 2019. https://doi.org/10.1088/1742-6596/1402/6/066054

[29] A. Singh and S. Sharma, "Enhancing Data Security in Cloud Using Split Algorithm, Caesar Cipher, and Vigenere Cipher, Homomorphism Encryption Scheme," in *Emerging Trends in Expert Applications and Security*, 2019, vol. 841, pp. 157–166.

[30] I. Gunawan, Sumarno, H. S. Tambunan, E. Irawan, H. Qurniawan, and D. Hartama, "Combination of Caesar Cipher Algorithm and Rivest Shamir Adleman Algorithm for Securing Document Files and Text Messages," *J. Phys. Conf. Ser.*, vol. 1255, 2019.

[31] D. Gautam, C. Agrawal, P. Sharma, M. Mehta, and P. Saini, "An Enhanced Cipher Technique Using Vigenere and Modified Caesar Cipher," in *2nd International Conference on Trends in Electronics and Informatics, ICOEI 2018*, 2018.

[32] J. Liu *et al.*, "The Reincarnation of Grille Cipher: A Generative Approach," *Cryptogr. Secur.*, pp. 1–27, 2018.

[33] P. E. Coggins and T. Glatzer, "An Algorithm for a Matrix-Based Enigma Encoder from a Variation of the Hill Cipher as an Application of 2 × 2 Matrices," *Primus*, vol. 30, no. 1, 2020. https://doi.org/10.1080/10511970.2018.1493010

[34] M. Shumay and G. Srivastava, "PixSel: Images as book cipher keys an efficient implementation using partial homophonic substitution ciphers," *Int. J. Electron. Telecommun.*, vol. 64, no. 2, pp. 151–158, 2018.

[35] G. Zhong, "Cryptanalysis of Homophonic Substitution Cipher Using Hidden Markov Models," 2016.

[36] R. Deepthi, "A Survey Paper on Playfair Cipher and its Variants," *Int. Res. J. Eng. Technol.*, vol. 4, no. 4, pp. 2607–2610, 2017.

[37] M. Syahrizal, M. Murdani, S. D. Nasution, M. Mesran, R. Rahim, and A. P. U. Siahaan, "Modified Playfair Cipher Using Random Key Linear Congruent Method," in *International Seminar: Research, Technology and Culture*, 2017.

[38] R. Rahim and A. Ikhwan, "Cryptography Technique with Modular Multiplication Block Cipher and Playfair Cipher," *Int. J. Sci. Res. Sci. Technol.*, vol. 2, no. 6, pp. 71–78, 2016.

[39] M. Maity, "A Modified Version of Polybius Cipher Using Magic Square and Western Music Notes," *Int. J. Technol. Res. Eng.*, vol. 1, no. 10, pp. 1117–1119, 2014.

[40] A. Banerjee, M. Hasan, and H. Kafle, "Secure Cryptosystem Using Randomized Rail Fence Cipher for Mobile Devices," in *Intelligent Computing - Proceedings of the Computing Conference*, 2019, pp. 737–750.

[41] A. P. U. Siahaan, "Rail Fence Cryptography in Securing Information," *Int. J. Sci. Eng. Res.*, vol. 7, no. 7, pp. 535–538, 2016.

[42] J. F. Dooley, *History of Cryptography and Cryptanalysis*. 2018. https://doi.org/10.1007/978-3-319-90443-6

[43] D. Salomon, *Coding for Data and Computer Communication*. Springer, 2005.

[44] P. Kumar and S. B. Rana, "Development of modified AES algorithm for data security," *Optik (Stuttg).*, vol. 127, no. 4, pp. 2341–2345, 2016.

[45] Z. Rahman, A. D. Corraya, M. A. Sumi, and A. N. Bahar, "A Novel Structure of Advance Encryption Standardwith 3-Dimensional Dynamic S-box and KeyGeneration Matrix," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 2, pp. 314–320, 2017.

[46] I. B. Venkateswarlu and J. Kakarla, "Password security by encryption using an extended ADFGVX cipher," *Int. J. Inf. Comput. Secur.*, vol. 11, no. 4–5, pp. 510–523, 2019. https://doi.org/10.1504/IJICS.2019.101938

[47] R. Mahendran and K. Mani, "Generation of Key Matrix for Hill Cipher Encryption Using Classical Cipher," *2nd World Congr. Comput. Commun. Technol. WCCCT 2017*, pp. 51–54, 2017.

[48] G. Lasry, I. Niebel, N. Kopal, and A. Wacker, "Deciphering ADFGVX messages from the Eastern Front of World War I," *Cryptologia*, vol. 41, no. 2, pp. 101–136, 2017.

[49] A. Borodzhieva, "MATLAB-based software tool for implementation of Bifid Ciphers," in *International Conference on Computer Systems and Technologies*, 2017, pp. 326–333.

[50] E. V. Haryannto, M. Zulfadly, Daifiria, M. B. Akbar, and I. Lazuly, "Implementation of Nihilist Cipher Algorithm in Securing Text Data with Md5 Verification," *J. Phys. Conf. Ser.*, vol. 1361, no. 012020, 2019.

[51] R. N. Sari, R. S. Hayati, Hardianto, A. H. Azhar, L. Sipahutar, and I. Lazuly, "Implementation of Trifid Cipher Algorithm in Securing Data," in *2019 7th International Conference on Cyber and IT Service Management, CITSM*, 2019.

[52] "Unbreakable' Codes Throughout History: The

Polybius Square and the Caesar Shift," 2011. [Online]. Available: https://freshmanmonroe.blogs.wm.edu/2011/07/17/"unbreakable"-codes-throughout-history-the-polybius-square-to-the-caesar-shift/.

[53] M. G. Vigliotti and H. Jones, "Cryptography for Busy People," in *The Executive Guide to Blockchain*, 2020, pp. 23–40. https://doi.org/10.1007/978-3-030-21107-3_3

[54] M. Lavanya, E. Nixson, R. Vidhya, R. V. Sai, and K. Chakrapani, "Efficient data security algorithm using combined aes and railfence technique," *Int. J. Pure Appl. Math.*, vol. 118, no. 20, pp. 3219–3227, 2018.

[55] G. Sharma, "Analysis and Implementation of DES Using FPGA," Thapar University, 2012.

[56] T. S. Kondo and L. J. Mselle, "An Extended Version of the Polybius Cipher," *Int. J. Comput. Appl.*, vol. 79, no. 13, pp. 30–33, 2013.

[57] S. B. Olaleye and S. Ojha, "Improved Advanced Encryption Using Four Square Cipher for User Anonymity and Untraceability in Mobile Cloud Computing," *Int. J. Innov. Sci. Eng. Technol.*, vol. 4, no. 2, pp. 113–121, 2017.

[58] B. N. Rao, D. Tejaswi, K. A. Varshini, K. P. Shankar, and B. Prasanth, "Design of modified AES algorithm for data security," *Int. J. Technol. Res. Eng.*, vol. 4, no. 8, pp. 1289–1292, 2017.

[59] P. Kumar and S. B. Rana, "Development of Modified Polybius Technique for Data Security," *Int. J. Innov. Eng. Technol.*, vol. 5, no. 2, pp. 227–229, 2015.

[60] E. W. Weisstein, "Magic Square," *From MathWorld--A Wolfram* Web Resource https://mathworld.wolfram.com/MagicSquare.html.

[61] C. Kumar, S. Dutta, and S. Chakraborty, "A Hybrid Polybius-Playfair Music Cipher A Hybrid Polybius-Playfair Music Cipher," *Int. J. Multimed. Ubiquitous Eng.*, vol. 10, no. 8, pp. 187–198, 2015.

[62] G. Manikandan, P. Rajendiran, R. Balakrishnan, and S. Thangaselvan, "A Modified Polybius Square Based Approach for Enhancing Data Security," *Int. J. Pure Appl. Math.*, vol. 119, no. 12, pp. 13317–13324, 2018.

[63] H. B. Macit, A. Koyun, and M. E. Yüksel, "Embedding Data Crypted With Extended Shifting Polybius Square Supporting Turkish Character Set," *BEU J. Sci.*, vol. 8, no. 1, pp. 234–242, 2019. https://doi.org/10.17798/bitlisfen.455126