International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 6, December 2019, pp. 5400~5411
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i6.pp5400-5411

Modifying playfair cipher algorithm using KAJ spiral method to fit any language regardless of the number of characters

Ibrahim Abde Al-jalil Sholi[1], Mohamad A. Mohamed[2]
[1]Department of Management Information System, AL-Istiqlal University, Palestine
[2]Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Terengganu, Malaysia

Article Info

Article history:

Received Dec 26, 2018
Revised Apr 25, 2019
Accepted Jun 10, 2019

Keywords:

Characters in the language
Index of coincidece
KAJ spiral algorithm
Playfair cipher algorithm
Polyalphabetic

ABSTRACT

In this paper we proposed KAJ Spiral method for supporting PlayFair cipher algorithm to use languages other than English and utilize block with more than two characters at once. Original method does not support block of characters and other languages. The method uses a spiral shape with two axes (X, Y) and the letters are spread on the axis within circles depending on the language. We use Friedman method analysis (index of coincidence) as a tool to test and prove the efficiency of KAJ Spiral method, and we found that it is at least equally secure to the original PlayFair cipher. The aims of this is making cryptography just like mathematics a universal language such that people with different languages can use this algorithm for secure communication, and at the same time make the algorithm stronger and easy to use, with the ability to fit any language.

Corresponding Author:

Ibrahim Abde Al-jalil Sholi,
Department of Management Information System,
Al-Istiqlal University,
Cross Hisham Palace, Jericho, PO Box 10, Palestine.
Email: Ibrahim.sholi@gmail.com

1. INTRODUCTION

Information is considered as the most valuable source in the organization, and this valuable source should be protected as any other sources such as money, trade secret and military assets. People have become reliant on growing technology to access information, doing business, and performing social activity, which distinguish the knowledge society [1, 2]. There are many techniques and methods used to protect the information from any unauthorized access such as firewalls, access control, biometrics, antivirus, antispyware, and encryption. Cryptography is used to enforce network security and its the design of certain techniques for ensuring the secrecy and authenticity of information [3]. The strongest and the most valuable technique used from the beginning of humanity and still developed and used until these days is cryptography with its all types such as symmetric (classic and modern), asymmetric, and hybrid. Data authentication helps in privacy preservation and is based on encryption systems [4]. When researchers develop a new algorithm and rank it as strong or weak it will be subject to study and analysis, may be this algorithm will be used or be subject for improvement. If the algorithm is approved to be used the crackers will try to break the code using different methods like coincidence and Kasiski Analysis (duplicated form) methods [5]. These common methods are used against classic codes in addition to brute force attack. It could also be the case that the algorithm is hard to apply and perform due to the large amount of complicated requirements needed. But if the algorithm is to be accepted by the public, it should comply with the international standards, such as those standards that are suggested by Claude Shannon in 1949 [6]. In that the process should be as simple as possible. The set of keys and cryptographic algorithms must be free of complexity. Therefore, we proposed these easy modifications to make this algorithm useable in different languages to overcome language differences, and at the same time be secure equally or even stronger than the original one.

Language and communication between people around the world are various and complicated due to the large number of languages and different races. People need a universal language which can help them communicate easily and use tools simply. Recent research in cryptography provided some novel ways to enhance the security of the Playfair cipher [7].

Encryption can be defined as changing the original message into other form [8]. Cryptography can be used and developed using different methods and algorithms but some algorithms need modification to fit any languages, because the original format of algorithm such as PlayFair was developed, used, and designed for English language, and as we know English language has only 26 alphabets and the original PlayFair has a 5 x 5 table that can support only 26 alphabets with two letters J and I share the same cell.

But this is still not useful when it comes to the other languages and adding new characters, symbols, and numbers. So we need to develop something which can accept any number of characters or signs for example Italian language has only 21 letters, Arabic 28, Russian 33 letters [9-11]. Different keyboards, devices, and so on. Therefore, in this study we aim to design and develop modification than can fit any languages, any number of characters, symbols, keys, etc., and which can process blocks of more than two characters at once. This modification should be easy to use and simple as possible, avoid complexity, be fast and easy in execution and implementation, be free of complexity, avoid errors, and be strong and hard to break.

We reviewed several studies indicating many aspects of the subject of the study:

Safwat Hamad, in this modification, the author used a grid of 8X8 codon matrix using interweaving on DNA – encode data; this bioinformatics encryption technique depends on the same rules of PlayFair method. The purpose is to enhance and improve the encoding by using classic PlayFair, so they can encrypt any type of data and at the same time benefit from the concepts of biological informatics. Also the modification optimizes the security of encryption and video steganography [12].

Seth A, Biswas SS., in this paper, the classical PlayFair Cipher is modified to 10 * 9 matrix. The approach proposed combines the Playfair algorithm encryption and the optimized chaotic genetic algorithm. The string encrypted once with the Playfair cipher is again subjected to encryption using the Genetic Algorithm with a Pseudo-random number generated by 1-D chaotic map [13].

Deepthi, in this paper, the author makes a comparison between many modifications on Playfair cipher and shows the weaknesses in these modifications on the original Playfair and found that no one discussed the effects of breaking the cipher text, and no one proved the power of his modification [14].

Sonal Namdev, Vimal Gupta (2016), in this paper, author proposes and discusses a modification on Playfair cipher based on merging with DNA and amino acid implementation. He proved that the weak algorithm can become more powerful in encryption by adding confusion and diffusion on the process, a new biological metric with classic Playfair improves encryption process [15].

Zakariyau et al., a new modification on classical Playfair with 17X17 matrix was proposed which allows using a long key with more than 64 character (long keyword) [16]. If we analyze the previous studies we find a lot of problems such as weaknesses and complexity, using data steganography in encrypting video will affect the quality of video like distortion [17], and modification process goes through many complicated steps. Moreover the security of these modifications has not been proved, and used in English language only. Maybe we don't need this amount of characters in case of languages with 21 letters. Modification is not tested in a proper method, and block size is still the same. But in our method (KAJ) we proved it is powerful using Index of Coincidence method, accepting any amount of characters, used in any language, and support any block size.

In this study we proposed a modification for the first time that can help people with different languages and using more symbols to be able to encrypt and decrypt messages without needing to alter tables. It is only one design that can be used universally. The importance of the study also lies in the possibility of generating useful ideas on the developing and enhancing cryptography and making it universal from the point of view of researchers to improve the art of cryptography and make new prospects, to help people with other languages use the PlayFair algorithm without a need to make new rectangles, squares, or confused, and the possibility to make the algorithm stronger.

2. PLAYFAIR CIPHER ALGORITHM

Playfair Cipher Algorithm is one of the famous algorithms in history of block cipher. It was invented by the English scientist Sir Charles Wheatstone 1854 [18]. And it's an example of polygraphed substitution that is based on replacing a group of characters in a message with a different group of letters or characters. Block cipher has no limits on the number of characters in the whole message, but it works on a block of two characters at once when encrypting and decrypting. The following example explains how it works and its rules.

2.1. Practical example

Encrypt the following text using Playfair Cipher Algorithm? (Example 2.1). Initially Sholi agreed with Mohamed a key word is “LIKE”. The plain text is: University of Unisza at TR. First: Create a table of 5x5, and apply 26 letters in 25 squares such that these two letters (J&I) incorporate into one identical square. Second: Keyword should be applied from left-to-right, and then the empty squares are filled in with the rest of the alphabets by making sure no letters are duplicated, as shown in Table 1. Third: If both letters are the same (or only one letter is left), add an "X" after the first letter, encrypt the new pair and continue.

Table 1. Original Playfair design with key example

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

2.2. Encryption rules

a. If both letters appear on the same row, replace them with the letters to their immediate right, respectively (if a letter in the original pair was on the end of the row go back to the start of the row and use the first letter to replace with the end letter).
b. If both letters appear on the same column of your table, replace them with the letters immediately below, respectively (if a letter in the original pair was on the bottom side of the column go back to the start of the column and use the first letter to replace with the end letter).
c. If the letters are not on the same row or column, imagine creating square or rectangle with the tow letters on the opposite side [19].

University of Unisza at TR UniversityofUniszaatTR UniversityofUniszaXatXtr

We use Table 1 to apply encryption rules on the plain text to get the cipher text by using Table 2.

Table 2. Making blocks, show method, and generate result

Plain text	Method	Encrypted
UN	3	SP
IV	3	LW
ER	3	IT
SI	3	RK
TY	2	YE
OF	2	TO
UN	3	SP
IS	3	KR
ZA	2	AG
XA	3	ZK
TX	3	SY
TR	1	US

when we applied encryption rules on the plain text using Table 1 we got the following result from Table 2. C: SPLWITRKYETOSPKRAGZKSYUS

2.3. Decryption rules

a. If the letters appear on the same row of your table, replace them with the letters to their immediate left, respectively (if the letter is at the start of row go to the end of the row).
b. If the letters appear on the same column of your table, replace them with the letters immediately above, respectively (if the letter at the start of column starts again from the end of the column (same).
c. If the letters are not on the same row or column, replace them with the letters on the same row, respectively but at the other pair of corners of the rectangle defined by the original pair. Note: The order is important – the first letter of the encrypted pair is the one that lies on the same row as the first letter of the plaintext pair [19].

We use Table 1 to apply decryption rules on cipher text to get the plain text from Table 3.

Table 3. Making blocks, show method, and generate result

Encrypted	Method	Plain text
SP	3	UN
LW	3	IV
IT	3	ER
RK	3	SI
YE	2	TY
TO	2	OF
SP	3	UN
KR	3	IS
AG	2	ZA
ZK	3	XA
SY	3	TX
US	1	TR

when we applied the decryption rules on the cipher text using Table 1, we got the following result from Table 3. C: SPLWITRKYETOSPKRAGZKSYUS; P: University of Unisza at TR

3. KAJ SPIRAL ALGORITHM

KAJ Spiral algorithm is a method we proposed to make the PlayFair algorithm easy to use by people with languages more than 26 letters alphabet or if they need to add any symbols or characters without a need to design new tables. In addition, people with languages written from right-to-left, up-to-down, down-to-up, and left-to-right are also welcome. Characters in the language vary because we live in a universe with thousands even millions of accents, languages, and symbols. However, in our research we will focus on some languages other than English (which is considered the language of the inventor of Playfair algorithm), we will choose some languages such as Italian (21 letters), and Arabic (28 letters). By this, we can perform our analysis and prove the workability of our method. The method uses spiral shape with two axes (X, Y) and the letters are spread on that axis within circles depending on the language used. For example, English start from left-to-right, but in Arabic it starts from right-to-left and so on. Moreover, English starts at the left side of the x axis and the Arabic starts at the right side of the x axis. As in the PlayFair the key should be placed first and then the rest of letters of alphabets are continuously spread on axis within circles until none is left (we can add any numbers, letters or symbols by extending the circle and thus add more circles). Each circle has 4 letters of alphabets, and if the last circle is not fully used, it does not matter because the rule 3 will be also modified. The following images show how the letters of alphabets was distributed on the axis for languages (English-Figure 1, Arabic-Figure 2, and Italian-Figure 3).

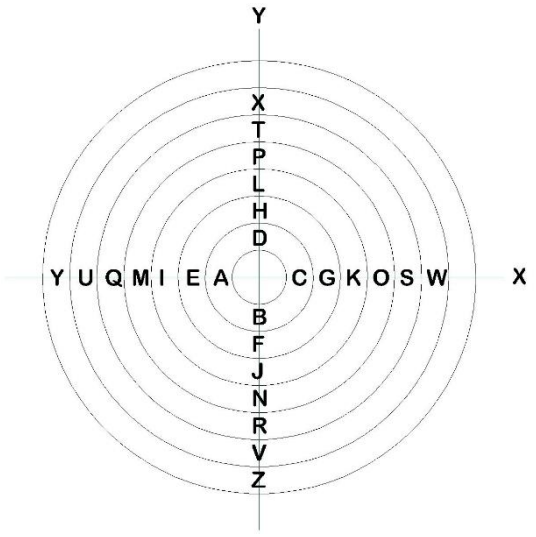

Figure 1. English language - letters of alphabets

Figure 1 shows the letters fit the seven circles. We didn't add or delete circles. The empty positions do not matter and we don't need to add anything. Figure 2 shows the letters fit the seven circles. We didn't add or delete circles, there are no empty positions. Figure 3 shows the letters fit to the five circles, only one letter is in circle sixth and we deleted circle seven. These examples show the flexibility of the new modification which fits Shannon rules of simplicity in algorithm design.

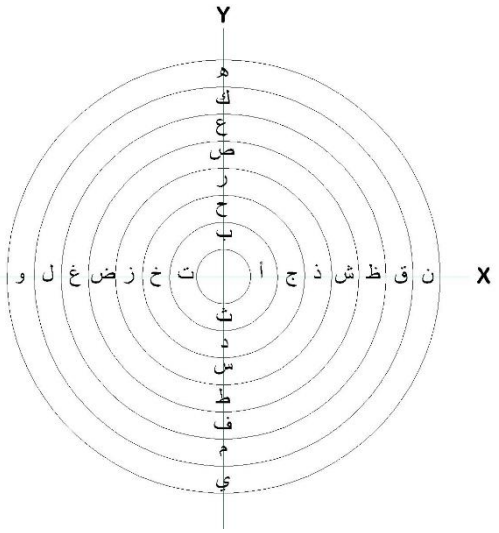

Figure 2. Arabic language - letters of alphabet

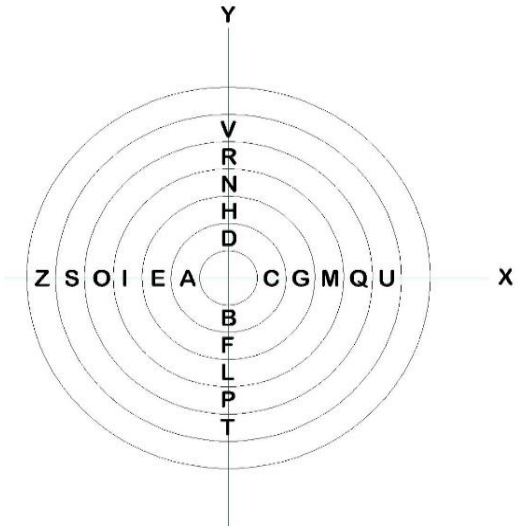

Figure 3. Italian language - letter of alphabet

3.1. The rules for KAJ method

a. There is no need to create tables, and the letters I & J do not need to share same position.
b. The keyword should be placed left-to-right first on X-axis for languages written left-to-right, and then the empty positions on both axes are filled in with the rest of letters of the alphabet and making sure no letters are duplicated.
c. The keyword should be placed right–to- left first on X Axis for languages written right–to- left, and then the empty positions on both axes are filled in with the rest letters of the alphabet with making sure no letters are duplicated.
d. If both letters are the same (or only one letter is left), add an "X" after the first letter. Encrypt the new pair and continue. But with languages with no x letters, we recommend using vowel from that language so the receiver can easily figure that.
e. If the language is written left-to-right, start spreading character on X Axes left side and then go down to Y Axes and continue spreading letters on Axes within circles. But if the language is written right-to-left, start spreading character on X Axes right side and then go up to Y Axes and continue spreading letters on Axes within circles.

3.2. Encryption rules

a. If both letters appear on the same row (X-axes), replace them with the letters to their immediate right, respectively (if a letter in the original pair was on the end of the row (X-axes), go back to the start of the row (X-axes), and use the first letter to replace with the end letter).
b. If both letters appear on the same column (Y-axes) of your table, replace them with the letters immediately below, respectively (if a letter in the original pair was on the bottom side of the column (Y-axes) go back to the start of the column(Y-axes) and use the first letter to replace with the end letter).
c. If the letters are not on the same row or column, go directly to the letter on the same circle on the other Axes (left-to-right for languages use left –to- right and right–to- left for languages use right–to- left).

3.3. Decryption rules

a. If both letters appear on the same row (X-axes), replace them with the letters to their immediate left, respectively (if a letter in the original pair was on the start of the row(X-axes), go back to the end of the row (X-axes), and use the last letter to replace with the first letter).

b. If both letters appear on the same column (Y-axes), replace them with the letters immediately up, respectively (if a letter in the original pair was on the start side of the column(Y-axes) go back to the end of the column (Y-axes) and use the end letter to replace with the first letter).
c. If the letters are not on the same row or column, go directly to the letter on the same circle on the other axes (right–to- left (returns) for languages use left –to- right and left –to- right for languages use right–to-left). Note: for languages with an up-down writing we could start from y- axes and apply the same rules.

3.4. Applied examples

The following three examples for 3 different languages prove the ability and validity (valid to use) of our method to handle and fit any language without designing new tables.

3.4.1. Example in English language

The following example in English language is used to make it more understandable and easy to analyze. We just use the same data we used in the original method in example 2.1. Encrypt the following text using PlayFair cipher by applying that on KAJ method. Initially, Sholi agreed with Mohamed a key word is "LIKE", and the plain text is "University of Unisza at TR". We applied KAJ encryption rules on the plaintext using Figure 4 and Table 4 to generate ciphertext.

University of Unisza at TR = UniversityofUniszaatTR = UniversityofUniszaXatXtr

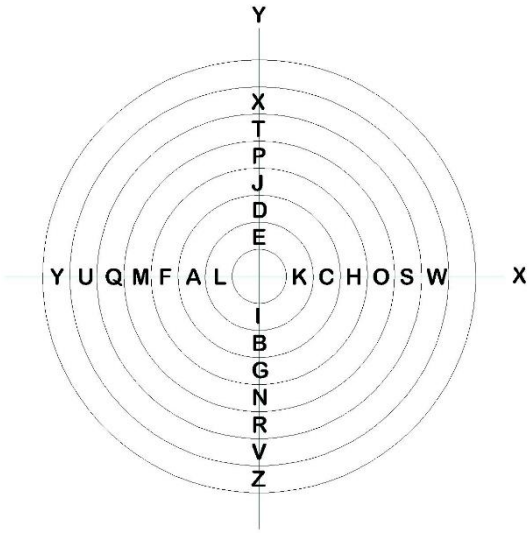

Figure 4. English language – letters of alphabet with Keyword example using KAJ Method encryption

Table 4. Making blocks, show method, and generate result

Plain text	Method	Encrypted
UN	3	VO
IV	2	BZ
ER	2	IV
SI	3	TK
TY	3	QZ
OF	1	SA
UN	3	VO
IS	3	KT
ZA	3	YB
XA	3	UB
TX	2	PT
TR	2	PV

The encrypted text is "VOBZIVTKQZSAVOKTYBUBPTPV"
Then we applied KAJ decryption rules on the ciphertext using Figure 4 and Table 5 to generate the plaintext.

Table 5. Making blocks, show method, and generate result

Encrypted	Method	Plain text
VO	3	UN
BZ	2	IV
IV	2	ER
TK	3	SI
QZ	3	TY
SA	1	OF
VO	3	UN
KT	3	IS
YB	3	ZA
UB	3	XA
PT	2	TX
PV	2	TR

The decrypted text is “University of Unisza at TR”

3.4.2. Example in Arabic language

Initially Sholi agreed with Mohamed a key word is LIKE= نحب

The plain text is University of Unisza at TR=جامعة يونيزا في تر

We apply the encryption rules of the KAJ spiral method on plaintext using Figure 5 and Table 6 to generate ciphertext.

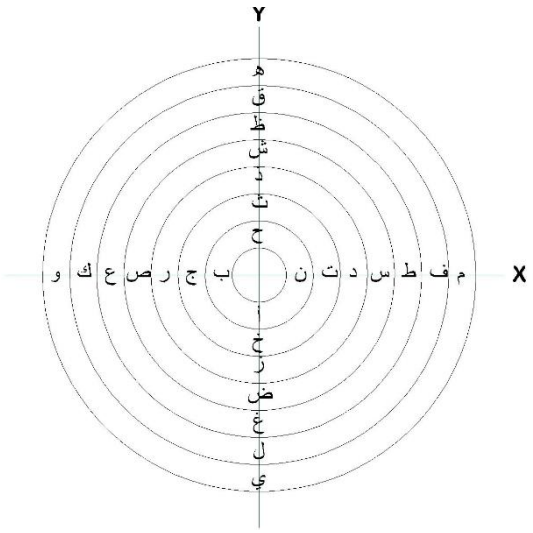

Figure 5. Arabic language – letters of alphabet with Keyword example using KAJ Method

جامعة يونيزا في تر

جامعةيونيزافيتر

Table 6. Making blocks, show method, and generate result

Plain text	Method	Encrypted
حا	3	خز
مع	1	فك
هء	2	قه
وز	1	مب
بز	2	هض
اف	3	نق
بت	3	مث
را	3	زز

جامعة يونيزا في تر-p= خنفكقهمبهضنقمثزن=c

Then we apply the decryption rules of KAJ spiral method on ciphertext using Figure 5 to generate plaintext inverse the procees). خنفكقهمبهضنقمثزن= جامعة يونيزا في تر

3.4.3. Example in the Italian language.

Initially, Sholi agreed with Mohamed a keyword is LIKE=*piace*.

The message is University of Unisza at TR = *Università di Unisza presso TR.*

Università di Unisza presso TR. UniversitàdiUniszapressoTR. UniversitàdiUniszapresAsoTR.

Note that because there are no (X, Y) letters in Italian language we separated the duplicates letters (vowel A, and for y, we just use the letter a).

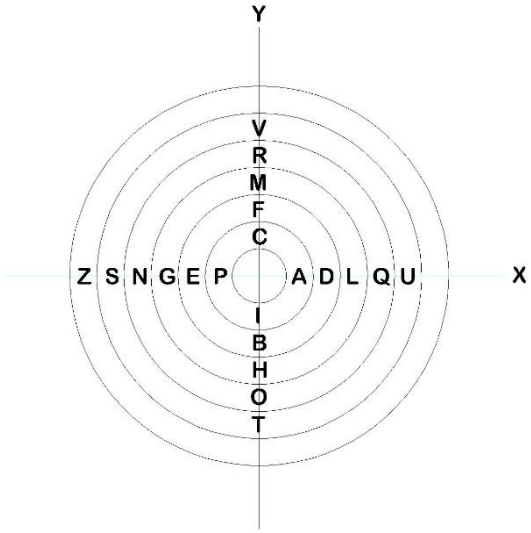

Figure 6. Italian language - letter alphabet with Keyword example using KAJ Method

We apply the encryption rules of KAJ spiral method on plaintext using Figure 6 and Table 7 to generate ciphertext.

Table 7. Making blocks, show method, and generate result

Plain text	Method	Encrypted
UN	*1*	*ZG*
IV	*1*	*BR*
ER	*3*	*BQ*
SI	*3*	*TA*
TA	*3*	*UC*
DI	*3*	*FA*
UN	*1*	*ZG*
IS	*3*	*AT*
ZA	*1*	*SD*
PR	*3*	*IN*
ES	*1*	*PN*
AS	*1*	*DN*
OT	*2*	*TV*
RA	*3*	*NC*

The encrypted text for *Università di Unisza presso* is *ZGBRBQTAUCFAZGATSDINPNDNTVNC*. Then we apply the decryption rules of KAJ method on the ciphertext using Figure 6 to generate plaintext (inverse the process).The result (plain text) = *Università di Unisza presso TR.*

4. RESULTS AND ANALYSIS

If we compare the two methods (Playfair and KAJ) result (ex. 2.1 and 3.4.1) we find no big differences. Indeed, this has proved the validity (useable, strong, and work well) of new method, and as we said, it is subjected for modifying because this is only first imagination for the KAJ method.

Original PlayFair-P: University of Unisza at TR = C: SPLWITRKYETOSPKRAGZKSYUS

KAJ - Result: University of Unisza at TR = C:VOBZIVTKQZSAVOKTYBUBPTPV

The comparison in Table 8 shows the frequency of ciphertext letter as a result of both methods and we find no differences in both, and thus proved that they are equally secure. The differences are not significant, so this has proven the validity of KAJ Spiral Method. We will show the results using numbers and equation on the following discussion, with other two applied examples (Arabic and Italian). KAJ can help us in the future to make a step in making cryptography universal language without any sophisticated and difficulties for all.

Table 8. KAJ Spiral Design and Original Playfair cipher text for the English example

Original Playfair	KAJ method
SPLWITRKYETOSPKRAGZKSYUS	VOBZIVTKQZSAVOKTYBUBPTPV

4.1. The advantages of KAJ Spiral Method over original PlayFair and benefits

a. Fit any language regardless of the number of characters or symbols. We proved that by applying examples on English, Arabic, and Italian languages.
b. Serving the educational purpose (Knowledge is power). As we know, the classic cryptography was the basis and origin of the modern cryptography, KAJ Spiral method is completely new and has never been used before and it is subjected to development with more than only 2 axes, so we have more flexibility and these examples could be applied and popularized on the modern algorithms.
c. User acceptance and ease of use, people with different language don't have to learn English but they can use an easy method to perform cryptography, and they can discover what the coincidence index in their language, what duplication can make their languages weak, and what make their language strong.
d. Original PlayFair Cipher use only blocks with 2 characters at once but in KAJ Spiral method we can use three characters or more or less no matter the size of the block, the following example show to us how we can use the three characters at once (prove that we can use any block size). Table 9 shows the ability of KAJ Spiral Design on making blocks more than two and in this case it is three. Note that we use the same data as found in example 3.4.1 using English language) but we change the block size and we applied the plain text on.KAJ Spiral method using Figure 4 to generate cipher text with 3 blocks. UniversityofUniszaXatXtr

Table 9. Making blocks, show method, and generate result

Plain text	Method	Encrypted
UNI	3	VOK
VER	2	ZIV
SIT	3	TKA
YOF	1	USA
UNI	3	VOK
SZA	3	TYB
XAT	3	UBQ
XTR	2	TPV

e. The most important thing we have is a proof that the KAJ Spiral method is stronger than Original PlayFair Cipher by using methods for attacking the cipher text used by cryptanalyst. And that is Friedman method analysis (index of coincidence). Index Coincidence (IC), which was invented by American cryptanalyst WILLIAM FREDERICK FRIEDMAN (1891-1969), [20]. is an important tool in decrypting messages, and that depends on finding coincidence in encrypted text and that can find and guess two things?

- If the message is encrypted using a polyalphabetic substitution (multiple substitution) or not, use (1), [21, 22].
- And then figure out the key length used in encrypted message using the result of IC in (2), [21, 22].

The IC in English equals to 0.065, for messages with IC between 0.0385 and 0.065, the polyalphabetic substitution is used, and if the IC closer to the 0.065 then the message text is encrypted using mono alphabetic. The Equation (1) is used to determine if a polyalphabetic substitution is used or not.

$$IC = \frac{\sum_{i=1}^{c} ni(ni-1)}{n(n-1)} \quad (1)$$

Equation 1:Index of coincidence

And then we use the (2) to figure out (guess) the key length used in the encrypted message.

$$L = \frac{0.027n}{(n-1)I - 0.038n + 0.065} \quad (2)$$

Equation2:Numbor of characters of key

By applying Friedman method on both original PlayFair and KAJ Spiral method. Next, we need to find out if the polyalphabetic substitution is used or not based on data from Table 10. Original PlayFair:

$$IC = \frac{\sum_{i=1}^{c} ni(ni-1)}{n(n-1)} = \frac{26}{24(24-1)} = 0.047101449 \quad (3)$$

IC between 0.0385 and 0.065, the polyalphabetic substitution used. KAJ Spiral method:

$$IC = \frac{\sum_{i=1}^{c} ni(ni-1)}{n(n-1)} = \frac{32}{24(24-1)} = 0.057971014 \quad (4)$$

IC between 0.0385 and 0.065, the polyalphabetic substitution used.

After we used data from Table 10 and applied results on (1), we find that the polyalphabetic substitution was used in both methods. But the result of the KAJ Spiral method is closer to .065 than the original PlayFair and that will confuse the cryptanalyst at least.

Table 10. Used to find and generate data used to find results for both equation (1) and (2)

	Original PlayFair				KAJ Spiral		
i	ni	ni-1	ni(ni-1)	i	ni	ni-1	ni(ni-1)
A	1	0	0	A	1	0	0
B	0	-1	0	B	3	2	6
C	0	-1	0	C	0	-1	0
D	0	-1	0	D	0	-1	0
E	1	0	0	E	0	-1	0
F	0	-1	0	F	0	-1	0
G	1	0	0	G	0	-1	0
H	0	-1	0	H	0	-1	0
I	1	0	0	I	1	0	0
J	0	-1	0	J	0	-1	0
K	3	2	6	K	2	1	2
L	1	0	0	L	0	-1	0
M	0	-1	0	M	0	-1	0
N	0	-1	0	N	0	-1	0
O	1	0	0	O	2	1	2
P	2	1	2	P	2	1	2
Q	0	-1	0	Q	1	0	0
R	2	1	2	R	0	-1	0
S	4	3	12	S	1	0	0
T	2	1	2	T	3	2	6
U	1	0	0	U	1	0	0
V	0	-1	0	V	4	3	12
W	1	0	0	W	0	-1	0
X	0	-1	0	X	0	-1	0
Y	2	1	2	Y	1	0	0
Z	1	0	0	Z	2	1	2
	24		26		24		32

Now we will apply results of equation 1 on the equation 2 to determine the length of the key.

$$L = \frac{0.027n}{(n-1)IC - 0.038n + 0.065} \quad (5)$$

1- Original PlayFair:

$$L = \frac{0.027n}{(n-1)IC - 0.038n + 0.065} = \frac{0.027*24}{(24-1)0.047101449 - 0.038*24 + 0.065} =$$

$$L = \frac{0.648}{0.236333327} = 2.741890059 \quad (6)$$

2- KAJ Spiral PlayFair:

$$L = \frac{0.027n}{(n-1)IC-0.038n+0.065} = \frac{0.027*24}{(24-1)0.057971014-0.038*24+0.065}$$

$$L = \frac{0.648}{0.486333322} = 1.332419496 \quad (7)$$

Now if we take both results from both equations we can find the following:
Original PlayFair = 2.741890059 if we approximate it then will be 3.
KAJ Spiral Method = 1.332419496 if we approximate it then will be 1.
The approximate will be up in case number >.5 and down if number < .5, depends on cryptanalyst expectations.

In the case of an approximation of the estimate by the cryptanalyst, then he will use the 3 as a key length to find the plain text using Kasiski cipher decoder duplicates from as a method used to attack the cipher text, and then he will go up to 4, in case of 3 doesn't succeed, and that will be easy for him to figure the key and decrypt the message as we know the key used was 4 characters (like), but in KAJ spiral method the result is closer to one and that will make code cryptanalyst go for more three steps to find the key because the distance to reach 1-4 far than 3-4, and that's why I said KAJ spiral methods equal to and stronger than Original PlayFair. So if the key was 4 characters – keyword (like) then the original show it 3 but KAJ show it 1. So the results show that KAJ more confusable than Original and that an advantage shows the ability of new algorithm.

f. Also from the general benefits of using different language in encrypting messages, the attackers from other languages have obstacles, because they need to learn a new language and that will increase the time and cost on attackers [23, 24].

5. CONCLUSION

KAJ Spiral method helps enhancing, improving, and developing cryptology by adding new features that were never used before which in turns makes the process of encrypting information easier. Moreover, it also allows using the new designed with any language. A rare and perhaps unique method so far that allows people use encryption easily using their language, as well as the only way that allows for block encryption with any block size and can provide the stream cipher at the same time.

ACKNOWLEDGMENTS

Thanks for unlimited support by AL-Istiqlal University, Supervisor Dr. Mohamad A. Mohamed

REFERENCES

[1] Omolara A. E. and Jantan A., "Modified honey encryption scheme for encoding natural language message," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, pp. 1871-1878, 2019.
[2] Gupta A. and Reddy L. S., "An Efficient Cloud Scheduling Algorithm for the Conservation of Energy through Broadcasting," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, pp. 179-188, 2018.
[3] Vatsa S, et al., "Novel Cipher Technique Using Substitution Method," *International Journal of Information & Network Security (IJINS)*, vol. 1, pp. 313-320, 2012.
[4] Sodhi G. K., et al., "Preserving Authenticity and Integrity of Distributed Networks through Novel Message Authentication Code," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 12, pp. 1297-1304, 2018.
[5] Al-Hamami A. and Ani S., "Technology of information security and protection systems," *1ST Ed. AMMAN, Dar Wael*, pp. 89-116, 2007.
[6] Dulaney E., "CompTIA Security + Study Guide," 4th Ed. Indianapolis, Wiley Publishing Inc., pp. 311-379, 2009.
[7] Srivastava S. S., *et al.*, "Modified Version of Playfair Cipher by using 8x8 Matrix and Random Number Generation," *2011 IEEE 3rd International Conference on Computer Modeling and Simulation (ICCMS)*, pp. VI615-VI617, 2011.
[8] T NB., et al., "Implementation of High Security Cryptographic System with Improved Error Correction and Detection Rate using FPGA," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 6, pp. 602, 2016.
[9] Omniglot, "Italian alphabet," 2019. Available: https://learnamo.com/en/italian-alphabet/
[10] Abdo M., et al., "Arabic Alphabet and Numbers Sign Language Recognition," *(IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 6, pp. 209-214, 2015.

[11] Optilingo, "Learn the Russian alphabet," 2019. Available: https://www.optilingo.com/blog/russian/russian-alphabet/
[12] Hamad S., "A Novel Implementation of an Extended 8x8 Playfair Cipher Using Interweaving on DNA-encoded Data," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 4, pp. 93-100, 2014.
[13] Seth A. and Biswas S. S., "Chaotic Genetic Enhancements to the Modified PlayFair Algorithm," *International Journal of Computer Sciences and Engineering*, vol. 6, pp. 245-250, 2018.
[14] Deepthi R., "A Survey Paper on Playfair Cipher and its Variants," *International Research Journal of Engineering and Technology (IRJET)*, vol. 4, pp. 2607-2610, 2017.
[15] Namdev S. and Gupta V., "A Dna and Amino-Acids Based Implementation of Four-Square Cipher," *Int. Journal of Engineering Research and Applications*, vol. 6, pp. 90-96, 2016.
[16] Zakariyau Y., et al., "Securing Message Transactions through Modified Playfair Cipher Technique," *IJISET - International Journal of Innovative Science, Engineering & Technology*, vol. 2, pp. 760-770, 2015.
[17] Arraziqi D. and Haq E. S., "Optimization of Video Steganography with Additional Compression and Encryption," *TELKOMNIKA – Telecommunication, Computing, Electronic and control*, vol. 17, 2019.
[18] Khan S., "Design and Analysis of Playfair Ciphers with Different Matrix Sizes," *International Journal of Computing and Network Technology*, vol. 3, pp. 119-122, 2015.
[19] Basu S. and Ray U. K., "Modified Playfair Cipher using Rectangular Matrix," *International Journal of Computer Applications*, vol. 46, pp. 28-30, 2012.
[20] Gaddy D., "The Friedman-Legacy," 3rd Ed., Washington, National Security Agency, pp. 2-200, 2006.
[21] Rees D., "A beginner's guide to Polyalphabetic Ciphers Part 2 Friedman Decryption)," 2014. Available: https://www.youtube.com/watch?v=31NI8LD8jdg
[22] Rees D., "Polygraphic Part 1 - Playfair Ciphers Encryption/Decryption," 2014. Available: https://www.youtube.com/watch?v=52QCEiMqtJE
[23] Gaines G., "Cryptanalysis A Study of Ciphers and Their Solution," Dover, Dover Publications, pp. 9-88, 1989.
[24] Singh S., "The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography," New York, A division of random house Inc., pp. 20-30, 2000.

BIOGRAPHIES OF AUTHORS

Ibrahim Abde Al-jalil Sholi received his Master in Information Security in 2007 from Chicago and currently serves as a licturer at Alistiqlal University, and a full time PHD student in the Universiti Sultan Zainal Abidin, major Computer Security. His research interests include both theoretical and application issues in Cryptography and information security.

Mohamad Afendee Mohamed received his PhD in Mathematical Cryptography in 2011 and currently serves as an associate professor at Universiti Sultan Zainal Abidin. His research interests include both theoretical and application issues in the domain of data security, and mobile and wireless networking.