UIJRT ISSN: 2582-6832

United International Journal for Research & Technology

Volume 04, Issue 07, 2023 | Open Access | ISSN: 2582-6832

Improving the Extended 10x10 Polybius Square Key Matrix for Playfair, Bifid, and Polybius Cipher

Gian Miguel M. Manliclic[1], Kiel Andrei R. Lamac[2], Richard C. Regala[3], Mark Christopher R. Blanco[4], and Raymund M. Dioses[5]

[1,2]Student, College of Engineering - Pamantasan ng Lungsod ng Maynila

[3,4,5]Professor, College of Engineering - Pamantasan ng Lungsod ng Maynila

Abstract**—** The Polybius Square is a cryptographic algorithm modified and enhanced over time to fit modern standards. A modification that is the focus of this study is the extension of the 5x5 Square Key Matrix into a 10x10 Square Key Matrix. This enhancement, however, has a glaring weakness, where using short keys would not give sufficient entropy to the extended key matrix, and the issue has not been thoroughly explored in most studies. This research proposes using the Linear Feedback Shift Register (LFSR) to solve this problem as a pseudo-random number generator using short keys to produce a more complicated key to create better entropy. The results show that the average avalanche effect of ciphers using the LFSR-enhanced 10x10 key matrix compared to ciphers that use an unmodified 10x10 key matrix is significantly improved, with some use-cases where an unmodified key matrix would yield an avalanche effect of 0% would jump to 50% using the LFSR-enhanced key matrix.

Keywords**—** Cryptography, Polybius Square, Key Matrix, Linear Feedback Shift Register

I. INTRODUCTION

Cryptography has been one of the oldest and most powerful techniques for providing information security, from classical to modern ciphers. Classical ciphers have been utilized throughout the ages and have been a reliable means of protecting critical data from unauthorized third parties. However, most of these ciphers have been unsecured and need improvements to keep pace with the modern age of encryption [1].

The Polybius Square Key Matrix is one of the first encryption techniques recorded and is considered one of the most widely used encryption method used in ciphers. The key matrix was first used in the titular cipher, the Polybius Cipher, and has since been modified and built upon by other ciphers still being used today [2]. Other classical ciphers, such as the Playfair Cipher [3], and even modern ciphers, such as AES [4], use the Polybius Square Key Matrix as a basis in their respective algorithms.

The extension of the Polybius Square Key Matrix from its original 5x5 matrix into a 10x10 matrix has helped modernize the algorithm, tremendously expanding the number of characters that can be used for encryption and decryption from only the 26 letters of the alphabet to 100 characters, typically in ASCII [5].

The lengthening of available characters and the enlargement of the matrix has made the Polybius Square Key Matrix more expansive. However, using the extended 10x10 polybius square matrix shows little to no avalanche effect when using shorter keys. While extending the Polybius Square Key Matrix into a 10x10 matrix increased the range of characters, a test of the avalanche effect of the extended matrix by flipping one bit of the key shows that slight changes in shorter keys result in little to no difference to the outputted ciphertext [6].

The Linear Feedback Shift Register, or LFSR, is a shift register, a circuit that holds and shifts multiple bits of data that creates a long pseudo-random string of bits from an initial seed. Its simplicity makes it easily implementable in lightweight hardware [7]. This study proposes securing the Extended 10x10 Polybius Square Key Matrix using the Linear Feedback Shift Register as a pseudo-random number generator for key-stretching functionalities, creating a more secure and easily implementable key matrix.

II. PROCEDURE FOR PAPER SUBMISSION

A. Polybius Square

The Polybius Square divides the letters of the alphabet in a 5x5 square and lists each letter in each cell horizontally, identified by its row and column. A key can also be implemented to increase security by arranging the letters of the square following the letters in the key and appending the rest of the alphabet after the key. In the original Polybius Cipher, the plaintext letters are encrypted as coordinates on the Polybius Square [8][9].

B. Polybius Square Based Ciphers

The Playfair Cipher is one of the classical ciphers that use the Polybius Square [3]. The Playfair Cipher was initially created by Sir Charles Whetstone but was advocated by Lord Playfair to be used by the British government, hence the name "Playfair". It uses the Polybius Square to divide the letters of the alphabet into rows and columns, similar to the original Polybius Cipher but uses a different set of encryption rules; of note is the division of the plaintext into digraphs, with letters without a pair or pairs with the same letter paired with an "X". These pairs are then encrypted using the Polybius Square with different rules depending on the position of the pair of letters in the square [10][11]. Cryptographer Felix Destalle has also created ciphers that make use of Polybius Squares. Most relevantly, the Bifid Cipher, which combines Polybius Square and Transposition [10][12], and two ciphers that are similar to the Playfair Cipher but are cryptographically more complex and secure, named the Two-Square Cipher, which uses two Polybius Squares with a separate key for each square, and the Four-Square Cipher which use four Polybius Squares, two plaintext squares, and two ciphertext squares with a separate key for each square as well [13].

C. Polybius Square Extensions

The original 5x5 Polybius Square can only accommodate 25 letters from its 5x5 square. Often the letters "J" and "I" are combined in one cell to fit all of the English Alphabet within the square [2]. At the same time, a Russian version of the Polybius Cipher called the Nihilist Cipher extends the Polybius Square into a 6x6 square to use the 35-Letter Cyrillic Alphabet [9]. Different matrix sizes have been developed to modernize the Polybius Square to account for new characters such as numbers, special characters, and uppercase and lowercase letters. An enhancement to the original Polybius Cipher consists of adding new encryption functions and extending the Polybius Square into an 8x8 square matrix, expanding the character pool to 64 characters [8]. The extension of the matrix size of the Four-Square Cipher into a 10x10 square matrix expanded the range of the matrix to encompass all printable ASCII characters plus five special characters [14]. An application of the extended 6x6 and 10x10 square matrix into AES notes that these changes slightly increased security but also increased execution time [4]. The extended Playfair Cipher into a 10x10 square matrix has been tested with the avalanche effect based on minimal changes to the plaintext and the keyword, concluding that "One of the probable weaknesses of the expanded 10x10 cipher is the avalanche effect of the minimal changes of keywords on the ciphertext" and that "keywords should be changes extensively to create different ciphertext" [6]. There is an improved Bifid Cipher with a 10x10 square matrix in conjunction with a CBC mode of encryption using a 100-character, or 800-bit, key [12]. Analysis of different matrix sizes used in Playfair Ciphers, specifically analyzing 9x9, 10x10, and 11x11 square matrices, note that the size of the plaintext itself does not have a significant effect on the output; however, "increasing the key size, proportionally increased the number of characters changed in the encrypted output" [5].

D. Key Stretching

Key Stretching is a cryptographic technique used to make weak keys into more substantial and more secured keys (Kelsey, 1998) [15]. This is achieved by a key derivation function (KDF) which is a cryptographic algorithm that uses pseudo-random functions to generate secret keys from an initial value, such as passwords (Camenisch, 2011) [16]. Key stretching improves security from brute-force attacks and password cracking, especially where key length is limited, making it an industry standard for low-entropy keys [17].

E. Linear Feedback Shift Register

LFSR is a shift register wherein the input bits are a linear function of its previous state, which means its outputs are deterministic based on the initial value called the seed. It uses a feedback function of exclusive-ors (XORs) or inverse-XORs of bits in the shift register, called taps, to shift and output the bits. These taps dictate the length of the output and, with a well-chosen feedback function, can output a long sequence of seemingly random bits before all possible states of the register are reached and the output cycles [18]. Because of its simple structure and ease of implementation, it is used as a pseudo-random number generator for less resource-intensive hardware and software [7][19]. A combination of LFSR with the Vigenere Cipher and one-time pad shows results as a lightweight encryption scheme reduces computational complexity but retains security [20]. LFSR is also used extensively by lightweight stream ciphers designed for low hardware complexity, but are now considered unsecured [7]. LFSR has been used to improve the Vigenere Cipher by using LFSR to create a key longer than the plaintext and using the new key for encryption in the Vigenere Cipher, concluding that the improved algorithm provides better security than conventional Vigenere Cipher and LFSR-based stream ciphers while having almost the same speed/cost ratio however the range of characters only encompassed 26 letters [21].

III. PROPOSED METHOD

Polybius Square-based ciphers use different encryption methods, but all use the Polybius Square as the key matrix to base the encryption from. In the 10x10 extension of the square matrix, there are 100 characters within the square in ASCII encoding that uses 95 printable ASCII characters and 5 extended ASCII characters.

It uses a key to initialize the characters of the square matrix and is encoded into each cell of the square from the top left to the right row by row, ignoring the repeating characters from the key. Once all characters of the key have been encoded into the square, all other characters of the square matrix not within the key are appended in the remaining cells in the default order of characters in the 10x10 square [9].

	!	"	#	$	%	&	'	(	)
*	+	,	-	.	/	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	[
\	]	^	_	`	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	{	|	}	~	¡	¢	£	¤	¥

Figure 1: *Default Extended 10x10 Polybius Square Key Matrix*

LFSR creates a long, seemingly random sequence of bits by creating a linear feedback loop using XOR or XNOR on specific bits called taps from an initial seed.

The rightmost bits are outputted and popped from the shift register, and the output of the XORed taps is pushed into the leftmost bit, shifting all the bits to the right.

The register has a finite number of possible states, meaning it will eventually enter a repeating cycle; however, it can output a long sequence of bits before this can be reached by choosing the proper feedback function of XOR taps [22].

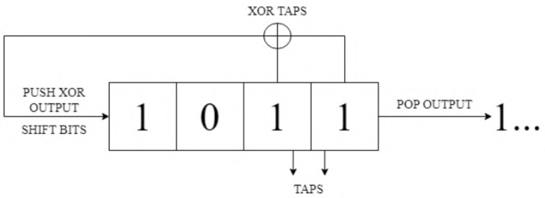

Figure 2: *LFSR Model*

In order to achieve the advanced security of a long key and the convenience of a short key, the study proposes to use LFSR as a key derivative function to apply key stretching to an 8-character user-typed key. This will be done by using the typed key as the initial seed for LFSR and using it as a pseudorandom number generator, will output a longer and more complex key that will be used by Polybius Square based ciphers as the new key in its extended 10x10 square key matrix for encryption.

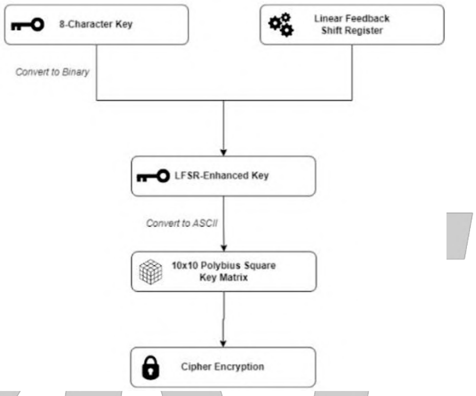

Figure 3: *General Model of Proposed Method*

For this research, the system for the base 10x10 Polybius Square Key Matrix, LFSR-enhanced 10x10 Polybius Square Key Matrix, and the ciphers and performance metrics used to evaluate the key matrices were written in Python using VSCode with NumPy and PIP as dependencies. A 10x10 2D array is encoded with the 95 printable characters of ASCII and 5 special characters from the extended ASCII. A keyword provided by the user is then used to add entropy to the square. The LFSR Model is imported from pylfsr under PIP, wherein the model is set to 128-bit, and the taps are set to output the maximum length of bits in an 8-character keyword [23]. Utilizing the same keyword as a seed for the LFSR model, the binary output is converted into a set of ASCII characters, and the unique characters are encoded into a new 10x10 2D array. This process is repeated until all 95 unique ASCII have been encoded into the array, and the 5 special extended ASCII characters are added afterward. The ciphers to be focused on in the study will be the Polybius Cipher, Bifid Cipher, and Playfair Cipher. The mechanics of these ciphers will be based on the various literatures revolving around each cipher [9][10].

IV. RESULTS AND DISCUSSION

The enhancements of the proposed algorithm will be determined by the measure of the avalanche effect test that will evaluate its efficacy compared to the existing algorithm. The original extended 10x10 Polybius Square Key Matrix will act as the baseline. Three ciphers will be used by both the proposed and the baseline algorithms for encryption, and each performance metric will be applied to each cipher. The ciphers to be used are Playfair Cipher, Bifid Cipher, and the Polybius Cipher. The testing of the avalanche effect based on the minimal changes in the keyword is implemented to quantify the strength of a cryptographic algorithm. The avalanche effect is a cryptographic property in which a slight change in input, such as the change of one bit, would significantly change the output [24]. The avalanche effect test would be conducted by encrypting one plaintext using ten keywords for each cipher. The plaintext would then be encrypted by the same keywords with one changed letter to each keyword. The ciphertext of the original keyword and the ciphertext of the changed keyword would be XORed together, calculating the percentage of the difference between the two ciphertexts to represent the avalanche effect. The percentage average of these ten results would then be calculated to evaluate the overall average avalanche effect of the cipher.

The LFSR-enhanced key matrix shows significant improvement in the average avalanche effect of each cipher used compared to the base key matrix. While some keywords show minimal improvements, some keywords in the base matrix show a 0% avalanche effect, meaning there is no difference in the ciphertext between the two different keywords, which the LFSR-enhanced key matrix dramatically improves. The results show that the avalanche effect of other Polybius Square-based ciphers can also show a 0% avalanche effect in some instances and could be mitigated by the LFSR enhancement.

Table 1: *Average Avalanche Effect Base 10x10 Key Matrix*

Keywords	Avalanche Effect %		
	Polybius Cipher	**Bifid Cipher**	**Playfair Cipher**
seecrets | Seecrets	5.3779%	14.7826%	38.7812%
password | passworD	8.1395%	16.7139%	25.2033%
code1234 | cOde1234	4.9419%	24.9292%	14.0921%
flare555 | glare555	1.3937%	2.3188%	1.9830%
a1234567 | a1234560	0.00%	0.00%	0.00%
queueing | queUeing	3.7791%	25.4958%	14.4044%
kiel8231 | Kiel8231	3.1977%	11.6147%	11.3821%
gian7230 | gian7231	0.00%	0.2833%	0.00%
tre$bien | tre#bien	0.00%	0.00%	1.6260%
stressed | ttressed	1.3081%	7.8261%	4.8159%
Average Avalanche %	**2.8138%**	**10.3964%**	**11.2288%**

Table 2: *Average Avalanche Effect LFSR 10x10 Key Matrix*

Keywords	Avalanche Effect %		
	Polybius Cipher	**Bifid Cipher**	**Playfair Cipher**
seecrets | Seecrets	22.8198%	46.4191%	39.9433%
password | passworD	21.9477%	53.5411%	43.6314%
code1234 | cOde1234	24.5640%	54.5213%	45.2575%
flare555 | glare555	17.5872%	47.3684%	51.6575%

a1234567 | a1234560	21.3663%	45.7995%	47.6965%
queueing | queUeing	23.5465%	46.0705%	54.2005%
kiel8231 | Kiel8231	21.8023%	50.00%	54.2005%
gian7230 | gian7231	21.2209%	50.8523%	54.4444%
tre$bien | tre#bien	20.6395%	51.1111%	53.3666%
stressed | ttressed	21.8023%	49.8645%	45.7995%
Average Avalanche %	**21.7297%**	**49.5548%**	**49.0198%**

V. CONCLUSION AND RECOMMENDATIONS

This study concludes that the employment of the Linear Feedback Shift Register to the extended 10x10 Polybius Square Key Matrix as a key stretching function for short keys to simulate a longer key improves the avalanche effect of the key matrix when used by ciphers, most especially in some instances where the avalanche effect of the base 10x10 key matrix would result in 0%. For future works, the researchers recommend that the LFSR be examined further to use a model with higher bits to increase the probability of entropy and that the LFSR-enhanced 10x10 Polybius Square Key Matrix be applied to other Polybius Square-based ciphers that were not more thoroughly covered in the study such as the Two-Square cipher and Four-Square cipher.

REFERENCES

[1] Katz, J., & Lindell, Y. (2020). *Introduction to modern cryptography*. CRC press.

[2] Arroyo, J. C., Dumdumaya, C., & Delima, A. (2020a). Polybius square in Cryptography: A brief review of literature. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(3), 3798–3808.

[3] Kong, X. (2022). *Polybius Square Ciphers* [Bachelor's Dissertation, Linnaeus University]. Digitala Vetenskapliga Arkivet.

[4] Permatasari, S., Aminudin, A., & Arifianto, S. (2020). Modification Encryption and Decryption of AES with Polybius Cipher in Data Security. *JRST (Jurnal Riset Sains Dan Teknologi)*, *4*(1), 41–46.

[5] Khan, S. A. (2015). Design and analysis of Playfair ciphers with different matrix sizes. *International Journal of Computing and Network Technology*, *3*(3), 117–122.

[6] Ferrer, J. C., Guzman, F. E., Gardon, K. L., Rosales, R. J., Dell Michael Badua, D. A., & Marcelo, D. R. (2018). Extended 10 x 10 playfair cipher. *2018 IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology,Communication and Control, Environment and Management (HNICEM)*.

[7] Deb, S., Bhuyan, B., & Gupta, N. C. (2018). Design and analysis of LFSR-based stream cipher. *Proceedings of the International Conference on Computing and Communication Systems*, 631–639.

[8] Arroyo, J. C., Reyes, A., & Delima, A. (2020b). A novel ASCII code-based polybius square alphabet sequencer as enhanced cryptographic cipher for Cyber Security Protection (APSAlpS-3CS). *International Journal of Advanced Computer Science and Applications*, *11*(7).

[9] Salomon, D. (2011). *Data Privacy and Security: Encryption and Information hiding*. Springer.

[10] Lanaki. (1996). *Lesson 17: Headline Puzzles, Play fair, Foursquare Fractionation And Delastelle Systems*. Classical Cryptography Course.

[11] Christensen, C. (2006). *MAT/CSC 483 - Polygraphic Ciphers*. Northern Kentucky University.

[12] Goyal, D., Hemrajani, N., & Paliwal, K. (2019). GPH algorithm: Improved CBC improved bifid cipher symmetric key algorithm. *International Journal of Communication and Computer Technologies*, *1*(2).

[13] Bowers, W. M. (1959). *Digraphic substitution: The playfair cipher, the four square cipher*. American Cryptogram Association.

[14] Aishwarya, J., Palanisamy, V., & Kanagaram, K. (2014). An extended version of four-square cipher using 10 x 10 matrixes. *International Journal of Computer Applications*, *97*(21), 9–13.

[15] Kelsey, J., Schneier, B., Hall, C., & Wagner, D. (1998). Secure applications of low-entropy keys. *Lecture Notes in Computer Science*, *1396*, 121–134.

[16] Camenisch, J., Fischer-Hübner Simone, Rannenberg, K., Di Vimercati, S. D. C., Foresti, S., Paraboschi, S., Pelosi, G., & Samarati, P. (2011). Data Privacy. In *Privacy and identity management for life* (pp. 185–186). essay, Springer-Verlag Berlin Heidelberg.

[17] Povšič, J., & Brodnik, A. (2021). Zero-knowledge authentication. *Proceedings of the 2021 7th Student Computer Science Research Conference (StuCoSReC)*, 7–10.

[18] Bhowmik, A., & Karforma, S. (2021). Linear feedback shift register and integer theory: A state-of-art approach in security issues over e-commerce. *Electronic Commerce Research*, *22*(4), 1–21.

[19] Kumar, B. A., Kumar, R. A., & Krishna, P. B. M. (2018). Implementation of Novel Approach LFSR Architecture for Power Optimized Applications. *IOSR Journal of Engineering*, *8*(8), 44–48.

[20] Wu, G., Wang, K., Zhang, J., & He, J. (2018). A lightweight and efficient encryption scheme based on LFSR. *International Journal of Embedded Systems*, *10*(3), 225.

[21] Razzaq, A., & Mahmood, Y. (2012). Strong Key Mechanism Generated by LFSR based Vigenère Cipher. *The 13th International Arab Conference on Information Technology ACIT'2012*, 544–548.

[22] Fischer, P. (2018). Maximum Length Linear Feedback Shift Registers. Universität Heidelberg.

[23] Alfke, P. (1996). Efficient Shift Registers, LFSR Counters, and Long Pseudo-Random Sequence Generators. Xilinx Publication XAPP052.

[24] Alankar, B., & Haris, M. (2017). A Survey Paper on Different Modification of Playfair Cipher. *International Journal of Advanced Research in Computer Science*, 8, 490-492.