Indonesian Journal of Electrical Engineering and Computer Science
Vol. 18, No. 2, May 2020, pp. 1028~1034
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v18.i2.pp1028-1034

New symmetric key cipher capable of digraph to single letter conversion utilizing binary system

Najdavan Abduljawad Kako[1], Haval Tariq Sadeeq[2], Araz Rajab Abrahim[3]
[1]Technical Institute of Administration, Duhok Polytechnic University, Iraq
[2]Duhok Technical Institute, Duhok Polytechnic University, Iraq
[3]Technical College of Administration, Duhok Polytechnic University, Iraq

Article Info

Article history:

Received Aug 6, 2019
Revised Nov 7, 2019
Accepted Nov 21, 2019

Keywords:

ASCII code
Cryptography
Digraph
Playfair cipher
Symmetric cipher
XNOR

ABSTRACT

In this paper, a new Playfair cipher built on bits level symmetric key cryptographic was proposed for the purpose of converting pairs of letters (digraphs) into single letters. The proposed algorithm is capable to overcome many of the shortcoming and vulnerabilities that exist in the current classical version of Playfair algorithm. The Playfair cipher is exceedingly complex than a classical substitution cipher, but still simple to hack using automated tactics. It is famous as a digraph cipher because two letters are exchanged by other two letters. This destroys any solo letter occurrence statistics, but the digraph statistics still unaffected (frequencies of two letters). Unluckily letter pairs have a flatter distribution than the one letter frequencies, so this intricacy matters for solving the code using pen and paper procedures. The suggested encryption process is conducted as follows; letters are first arranged in a spiral manner in Polybius square, afterwards, each pair will be replaced utilizing before-after technique if we are arranging pairs horizontally and down-up technique (vertically). The former process produces pairs of Plaintext that will be converted to binary bit stream then will be divided over blocks with stable sizes. Bits of these blocks are taken from pairs then fit them into square matrix of suitable order to put the concept of row-wise and revers row-wise matrix. Bits of this matrix are split into 2x2 square matrixes. The sub-matrixes are formed 8 bits. Here the XNOR operation is taken into consideration for bitwise operation to generate the keys for decryption and produce the cipher-text.

Corresponding Author:

Najdavan Abduljawad Kako,
Technical Institute of Administration,
Duhok Polytecgnic University, Iraq.
Email: najdavan.kako@dpu.edu.krd

1. INTRODUCTION

Data and information security are ancient sciences for communicating significant messages between sender and receiver. After appearing internet in all over the world and developing communication, heavily sharing of information in many features of our life, from our expert career, to social assemblies, to our family life. Cryptography plays a vital role in transmitting and protecting data from eavesdroppers. Encryption is the technique and science of keeping data from unwanted individuals by changing it into a non-detectable form by its cryptanalysis when saving and transferring data [1, 2].

Internet security algorithms stayed complex into some extent, therefore, research on making it light and robust through coming up with different cryptography algorithms is ongoing [3-15]. Apparently, each algorithm has its advantages as well as its limitations. The classical Playfair cipher is an example of one of those algorithms that has the same mentioned feature which is concentrated on the use of 5 by 5 matrix of letters are constructed by using a keyword [16, 17]. The reason behind choosing this cipher because thus remarkably complicate to breakdown as the frequency analysis applied for plain substitution codes does not

deal with it. The frequency analysis of digraph is conceivable, but extremely harder [18]. With a possible 600 digraph instead of the 26 possible one letters, in order to be effective, a large cipher-text is needed. The matrix is built on padding the letters of key from left to right and top to bottom, so the rest of the matrix are stuffing in the remaining alphabetic order [19-21]. In this paper a new symmetric key cryptographic method based on converting digraph in one that has been proposed. Second section of this paper contains the algorithms for enciphering, deciphering and key generation. Third section proves the proposed technique with a suitable example. Conclusion is drawn in the fourth section.

2. LITERATURE REVIEW

M. Paul and J. Mandal proposed that a symmetric cipher termed spiral matrix based a bit orientation technique (SMBBOT) has based bit level symmetric key technique (2013). SMBBOT theorize the input plain text as binary bit stream. Those bits are taken from Most Significant Bit to Least Significant Bit and chopped into a managed sized blocks. SMBBOT compared with existing and technically accepted TDES and AES. The algorithm has been shown a straightforward and simple for understanding. The key variation enhances the security features and it is viable to ensure high security for message communication [17].

3D - Playfair Cipher and additional Bitwise Operation proposed by V. Verma and D. Kaur (2013). In this algorithm cipher, the tri-graphs of plaintext are addressed as a single unit that transformed it to corresponding cipher text tri-graphs. Linear Feedback Shift Register is used for producing random keys based XOR or XNOR operations. 3D-Playfair Cipher and additional Bitwise Operation together are exhibited a high confusion and diffusion rate rapidly that enhance the cipher text security and can be simply implemented with coming of new computer [22] This algorithm is improving classical Playfair but is still converting pairs to pairs not to single.

The use of ASCII characters for symmetric key algorithm proposed [23] by Ayushi (2010). Anyone can understand the text clearly as knowingly the language text if it doesn't apply enciphered method to the message in any approach. Thus, it must hide message from anyone, those we want, even they are observed for enciphered data to ensure that we must use encryption scheme. This algorithm has been intended in a quite easy mode but of course not forgoing the security issues. A single key is used for both encipher and decipher i.e. it is fallen under private key cryptographic algorithm. But as public key cipher is more secured then private key cipher the algorithm is need be to develop and implement a public key in an easy mode [22].

In this research both S. Shakti Srivastava and N. Gupta (2011), introduce an extended Playfair cipher "8*8 Playfair cipher" which are the digraphs in the plaintext handled as a one unit and changed into consequent cipher digraph texts. Proposed 8*8 Playfair cipher and linear-feedback shift register (LFSR) are combined to create the traditional Playfair cipher at match with developed ciphers that existed like Advanced Encryption Standard (AES) and Data Encryption Standard (DES). Strong encryption does not ensure strong integrity, weak encryption certainly ensure weak integrity. The protocol and administration engaged in carrying out the encryption are equally crucial The paper deals with the proposed cipher's security parts and found it to be highly secure against attacks even when the randomization is extended to higher levels based on the entire linear-feedback shift register (LFSR) design. It is therefore not feasible to connect plaintext to cipher-text. Furthermore, from the analysis made, this cipher is potentially a strong one [24].

In (2015) S. Singh and R. Singh proposed "Developing 3D-Playfair Cipher Algorithm Using Structure Rotation". That approach invented to develop the shape rotation idea on key matrix of 3D-Playfair cipher using key randomly to reach the objectives. Due to its simplex and preferable performance, random sequences are generated by Linear Feedback Shift Register (LFSR). This Playfair cipher gives high ratio of confusion and diffusion. But it can still be possible to hack if there is adequate text by well-known plaintext raid technique due to the construction of key matrix is static however contribution of the form of rotation decreases this disadvantage up to a passable locate by concealment the real key matrix from the attackers. 3D-Playfair Cipher with the form of rotation will advance the security using key matrix dynamically. Using Linear Feedback Shift Register (LFSR) to create numbers randomly serves to preserve the difficulty of this practice [3, 25].

3. THE PROPOSED SCHEME

Before delving into explaining the proposed scheme, three important processes should be explained that represent the whole ciphering process. The first phase is the encryption phase which is the process of enciphering data followed by decryption. The second phase is the process of taking enciphered data and converting it back to the original text. The third one is the process of key generation. The above-mentioned three processes are described in detail in the following sub-sections.

3.1. Encryption Algorithm

This type of algorithm takes source data plaintext as input and generates encrypted data cipher-text as output.

a) *First step*: Dividing plaintext into two-letter segments. Repeated letters in the same segment are usually separated by an X sign. If the number of letters in the text is not even, it was padded with a sign X.
b) *Second step*: Taking pairs of letters and look at their positions in the grid (Matrix). If they used as horizontal technique, we would take the letters before each pair. Otherwise, the vertical takes the letters down of each the pairs.
c) *Third step*: The second step output is regarded as a stream with a restricted binary number (ASCII to Binary) bits which are arranged in row-wise and revers row-wise in 4x4 matrix.
d) *Fourth step*: This matrix divided into 4 sub-matrix which is named A, B, C, and D sequentially.
e) *Fifth step*: This binary sequence splits into controllable -sized blocks with lengths of 4 bits according to the sequence of A, D and B, C.
f) *Sixth step*: A, D bite's stream will XNOR with B, C ones to give key2 and finally to give cipher-text which is a single letter converted from binary.

3.2. Decryption Algorithm

This algorithm takes encrypted data cipher-text as input and generates source data plaintext as output.

a) *First step*: The cipher-text (encrypted data) is regarded as a binary bit sequence.
b) Second step: This binary string will XNOR with key2 after processing the session key2 data to offer 16-bit block.
c) *Third step*: Square matrix of order number 4 is generated for each block of length 4 (A, B, C and D). Using all these 2x2 sub-matrixes a single square matrix of suitable order is generated.
d) *Forth step*: The block in length 16 is generated after taking the bits from the Polybius square matrix then following the row-wise and reverse row-wise Matrix. The digraph is constructed then converting it from binary to ASCII.
e) *Fifth step*: Taking pairs of letters and look at their positions in the grid. If they used as horizontal, we would take the letters before each pair. Otherwise, the vertical takes the letters up each one of the pairs.
f) *Sixth step*: The plaintext is formed after reversing the first step from encryption algorithm

3.3. Keys Generation

In this section we have two types of key, key for Playfair cipher and a key when converting digraph into single and those keys are private because is known only by the client and server.

3.3.1 Playfair key

The 'key' that is used for a Playfair cipher is generally a word (without numbers and symbols), this is used to generate randomly a 'key square. The matrix is constructed by padding with the letters of the key (without duplicates) in spiral matrix along clock-wise direction starting from right to the center in spiral form as shown in Figure 1, and then padding in the remainder of the matrix with the remaining letters in English alphabetic. The letters I and J act as a single letter. Plaintext is encrypted in to two letters at the same time, in two ways: is used as horizontal (before - after) and used vertical (down - up) as this. To do that: to encrypt the message horizontally, for each letter in plaintext we take the letter that lies before the chosen letter in spiral matrix and for decryption we take the letter that lies after. Likewise, in vertical method we use (down - up) instead of (before - after). Concept of Row-Wise and reverse Row-Wise as shown in Figure 2.

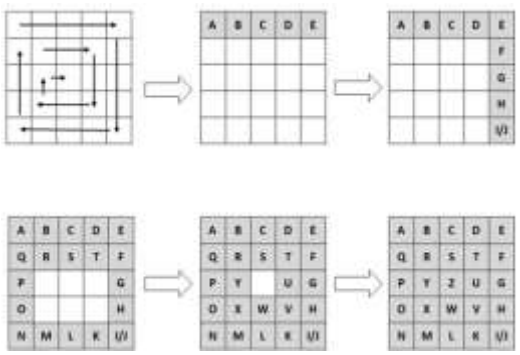

Figure 1. Concept of Spiral Matrix

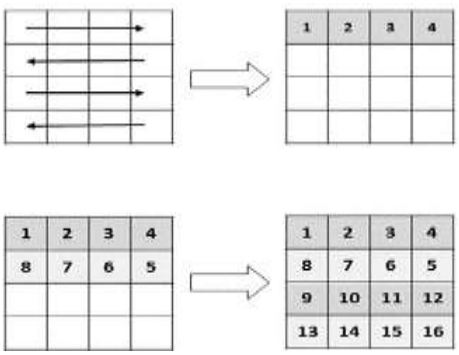

Figure 2. Concept of Row-Wise and reverse Row-Wise

3.3.2 Digraph - Single key

The sender and receiver both contribute to starting this key, and the resulting secret is not ever known to outside parties. The secret key is shaped during a process known as a key exchange algorithm. This process will be achieved using key exchange algorithm which result will be by the sender and receiver in a manner of using same key independently and employing them with certain secret data. The symmetrical encipher key formed by this process is session-based and constitutes the real encipher for the information sent between sender and receiver. Once this is built, the rest of the information must be enciphered with this shared secret. This is done to ensure much more security to algorithm. This technique divides the input binary bit stream interactively into 2 portions, one of this portion is generating key of 8 bits for each session.

4. IMPLEMENTATION

4.1. Encryption

To illustrate the algorithm, let us consider a plaintext “HIDE THE GOLD IN THE TREE STUMP”. To encode this message. The message would become “HI DE TH EG OL DI NT HE TR EX ES TU MP". Next, you take your letter pairs and look at their positions in the grid designed by key “PLAYFAIR EXAMPLE” would become “PLAYFIREXM”. If we are using > horizontal, the result will be as follows:

Table 1. Encryption

PT	CT1	Text to Binary	Splits over blocks				$AD \oplus BC$	K2	CT2
			A	*B*	*C*	*D*			
HI	QR	0101 0001 0101 0010	0110	0100	0101	0100	11011110	E	Þ
DE	TX	0101 0100 0101 1000	0100	0110	0100	0101	11011110	d	Þ
TH	RU	0101 0010 0101 0101	0101	0100	0110	0110	11011110	F	Þ
EG	ET	0100 0101 0101 0100	0110	0010	0100	0110	10111101	$	½
OL	PN	0101 0000 0100 1110	0100	0100	0101	0011	11111001	E	ù
DI	QX	0101 0001 0101 1000	0110	0100	0100	0101	11011110	D	Þ
NT	UK	0101 0101 0100 1011	0110	0110	0111	0001	11111001	g	ù
HE	TR	0101 0100 0101 0010	0100	0110	0101	0100	11011110	e	Þ
TR	SU	0101 0011 0101 0101	0111	0100	0110	0110	11001111	F	Ï
EX	MT	0100 1101 0101 0100	0110	0011	0100	0110	10101101	4	
ES	ZT	0101 1010 0101 0100	0101	0101	0100	0110	11111101	T	ý
TU	VU	0101 0110 0101 0101	0110	0110	0110	0110	11111111	f	ÿ
MP	FB	0100 0110 0100 0010	0110	0010	0101	0000	10111010	%	º

PT: Plaintext, CT: Cipher-text and K: Key.

4.2. Decryption

For decryption process, exactly reverse steps of the encryption with using generated key2 “EdF$EDgeF4Tf%”. Figure 3 shows the flow diagram of algorithm. Flow diagram of decryption as shown in Figure 4. Encryption & decryption time for different sizes in 1 MS as shown in Figure 5.

Table 2. Decryption

CT 2	CT2 to bin	K2	K to bin (block *B* & *C*)	CT2 ⊕ K2 – (block *A* and *D*)	Rearranging Blocks				CT1	PT
					A	*B*	*C*	*D*		
Þ	11011110	E	01000101	01100100	0110	0100	0101	0100	QR	HI
Þ	11011110	d	01100100	01000101	0100	0110	0100	0101	TX	DE
Þ	11011110	F	01000110	01010110	0101	0100	0110	0110	RU	TH
½	10111101	$	00100100	01100110	0110	0010	0100	0110	ET	EG
ù	11111001	E	01000101	01000011	0100	0100	0101	0011	PN	OL
Þ	11011110	D	01000100	01100101	0110	0100	0100	0101	QX	DI
ù	11111001	g	01100111	01100001	0110	0110	0111	0001	UK	NT
Þ	11011110	e	01100101	01000100	0100	0110	0101	0100	TR	HE
Ï	11001111	F	01000110	01110110	0111	0100	0110	0110	SU	TR
	10101101	4	00110100	01100110	0110	0011	0100	0110	MT	EX
ý	11111101	T	01010100	01010110	0101	0101	0100	0110	ZT	ES
ÿ	11111111	f	01100110	01100100	0110	0110	0110	0110	VU	TU
º	10111010	%	00100101	01000101	0110	0010	0101	0000	FB	MP

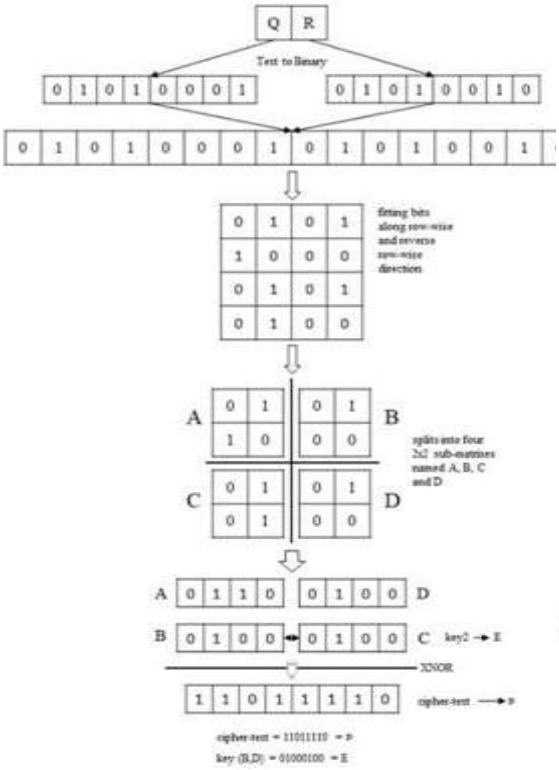

Figure 3. Flow diagram of encryption

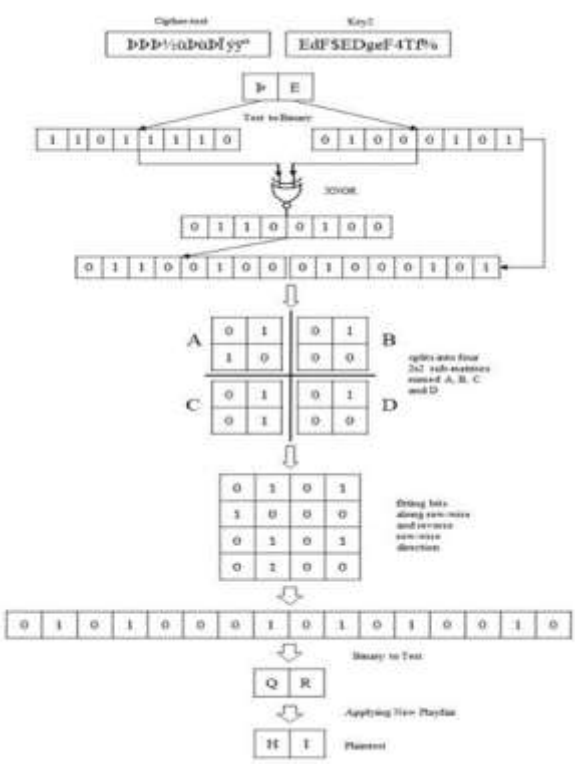

Figure 4. Flow diagram of decryption

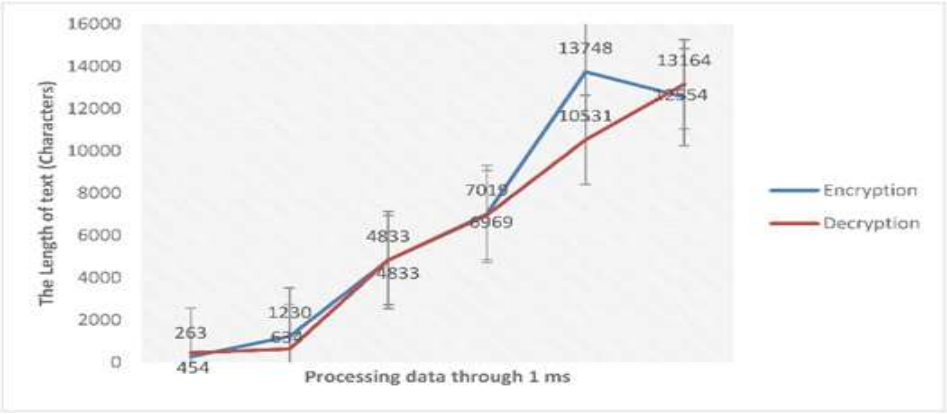

Figure 5. Encryption & decryption time for different sizes in 1 MS

5. CONCLUSION

The algorithm provides high confusion ratio and diffusion ratio, there are huge number of possibilities so it's very difficult to execute brute-force raid on it. Since the cipher using two methods horizontal and vertical and it is working on all characters that known by computer compiler so the possibility of occurrence of a character in algorithm is so less. Also, the second key (sequence of keys equals the length of the message) strengthens the algorithm because it is not known and is created during the encryption. But still it can be broken if the sufficient text is existed as it known as plaintext attack technique due the structure of cipher is well recognized by everyone but contribution of bitwise operation at cipher text decreases the weakness according to a passable limit by concealment the original cipher text from the interloper one.

The modified Playfair cipher with providing bitwise operation improves the cipher text security rapidly and can simplify to apply on initiation of a new machine. Generation of random keys leads XNOR, the operation of XNOR in hardware and software is very simple, and it's costless and is so fast as compared to other approaches. It is the first real step that is recognized the converting the two letters in algorithm to a single

letter. It can be concluded, that the repetition of the same letter in cipher-text respectively or randomly not always referred to the same letter in original text as compared with classical symmetric cipher which replace by the same letter.

The major advantages of this work is to treat the weakness of traditional Playfair cipher which are that a digraph in the cipher-text YZ and its reverse ZY will match plaintexts such us LM and ML (and also cipher-text LM and ML will match to plaintext YZ and ZY, i.e. the change is opposite). That can be breached readily with the help of frequency analysis, where the alphabets of the plaintext are well-known. In addition, the messages that already end with an 'X', and have an odd number of characters, for example, "REX" becomes "RE XX" this case has been resolved with adding letter "Q".

All of the above weaknesses were addressed in the second part of the algorithm where two letters of plain text are converted into one character to avoid frequency analysis and as we are dealing with the binary system the results of this work may result in a letter or number or symbol and these are all difficult to trace or hack. This work was created to deal with English characters only, since each character is consisting of eight bits. The algorithm platform accepts only eight bits. Therefore, it is difficult to apply them to other language characters such as Arabic because some of their letters contain more than eight bits.

REFERENCES

[1] D. E. Robling Denning, *Cryptography and data security*. Addison-Wesley Longman Publishing Co., Inc., 1982.

[2] R. M. Redlich and M. A. Nemzow, "Data security system and method." Google Patents, 05-Sep-2006.

[3] W. Stallings, *Cryptography and Network Security: Principles and Practice, International Edition: Principles and Practice*. 2014.

[4] D. A. Zebari, H. Haron, S. R. M. Zeebaree, and D. Qader Zeebaree, "Multi-Level of DNA Encryption Technique Based on DNA Arithmetic and Biological Operations," *ICOASE 2018 - Int. Conf. Adv. Sci. Eng.*, pp. 312–317, 2018, doi: 10.1109/ICOASE.2018.8548824.

[5] A. M. A. Brifcani and W. M. A. Brifcani, "Stego-Based-Crypto Technique for High Security Applications," *Int. J. Comput. Theory Eng.*, vol. 2, no. 6, pp. 835–841, 2010, doi: 10.7763/ijcte.2010.v2.249.

[6] A. M. Abdulazeez and A. S. Tahir, "Design and Implementation of Advanced Encryption Standard Security Algorithm using FPGA," *Int. J. Comput. Technol.*, vol. 4, no. 9, pp. 1988–1993, 2013.

[7] P. Utomo, N. W. Nasution, Arisman, and R. W. Sembiring, "A theoretical and experimental comparison of one time pad cryptography using key and plaintext insertion and transposition (KPIT) and key coloumnar transposition (KCT) method," *Adv. Sci. Technol. Eng. Syst.*, vol. 2, no. 5, pp. 31–34, 2017, doi: 10.25046/aj020506.

[8] C. Paper and A. N. St, "Symmetric Key Cryptography Using Random Key Symmetric key cryptography using Random key generator," no. November, 2015.

[9] A. M. Abdulazeez and F. S. Khamo, "A Proposed Data Security Algorithm Based on Cipher Feedback Mode and its Simulink Implementation," vol. 4, no. 9, pp. 1598–1606, 2013.

[10] R. K. Meenakshi and A. Arivazhagan, "RTL modelling for the cipher block chaining mode (CBC) for data security," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 8, no. 3, pp. 709–711, 2017, doi: 10.11591/ijeecs.v8.i3.pp709-711.

[11] Y. Kiran Kumar and R. Mahammad Shafi, "An efficient and secure data storage in cloud computing using modified RSA public key cryptosystem," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 1, pp. 530–537, 2020, doi: 10.11591/ijece.v10i1.pp530-537.

[12] H. Ali-Pacha, N. Hadj-Said, A. Ali-Pacha, M. A. Mohamed, and M. Mamat, "Cryptographic adaptation of the middle square generator," *Int. J. Electr. Comput. Eng.*, vol. 9, no. 6, pp. 5615–5627, 2019, doi: 10.11591/ijece.v9i6.pp5615-5627.

[13] D. V. and K. Anup, "A Modified Feistel Cipher Involving Modular Arithmetic Addition and Modular Arithmetic Inverse of a Key Matrix," *Int. J. Adv. Comput. Sci. Appl.*, vol. 3, no. 7, pp. 35–39, 2012, doi: 10.14569/ijacsa.2012.030705.

[14] S. R. M. Zeebaree, "DES encryption and decryption algorithm implementation based on FPGA," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 18, no. 2, pp. 774–781, 2020, doi: 10.11591/ijeecs.v18.i2.pp774-781.

[15] S. R. M. Zeebaree, A. B. Sallow, B. K. Hussan, and S. M. Ali, "Design and Simulation of High-Speed Parallel/Sequential Simplified des Code Breaking Based on FPGA," *2019 Int. Conf. Adv. Sci. Eng. ICOASE 2019*, pp. 76–81, 2019, doi: 10.1109/ICOASE.2019.8723792.

[16] V. Subhashini, N. Geethanjali, P. Vidyasagar, and P. Amrutha, "A Novel Approach on Encryption and Decryption of 5X5 Playfair Cipher Algorithm," no. 1, pp. 102–105, 2017.

[17] P. Murali and G. Senthilkumar, "Modified version of playfair cipher using linear feedback shift register," *Proc. - 2009 Int. Conf. Inf. Manag. Eng. ICIME 2009*, pp. 488–490, 2009, doi: 10.1109/ICIME.2009.86.
[18] S. Krishnaswamy and H. K. Pillai, "On the number of linear feedback shift registers with a special structure," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1783–1790, 2012, doi: 10.1109/TIT.2011.2174332.
[19] B. A. Forouzan, *Cryptography & network security*. McGraw-Hill, Inc., 2007.
[20] N. A. Kako, "Classical Cryptography for Kurdish Language," in *4th International Engineering Conference on Developments in Civil & Computer Engineering Applications (IEC2018)*, 2018, vol. 2018, pp. 20–28, doi: 10.23918/iec2018.02.
[21] W. Abduallah and S. Mohammed Zeebaree, "New Data hiding method based on DNA and Vigenere Autokey," *Acad. J. Nawroz Univ.*, vol. 6, no. 3, pp. 83–88, 2017, doi: 10.25007/ajnu.v6n3a83.
[22] V. Verma, D. Kaur, R. K. Singh, and A. Kaur, "3D - Playfair cipher with additional bitwise operation," *2013 Int. Conf. Control. Comput. Commun. Mater. ICCCCM 2013*, no. Iccccm, 2013, doi: 10.1109/ICCCCM.2013.6648913.
[23] A. Ayushi, "Symmetric key cryptographic algorithm," *Int. J. Comput. Appl.*, vol. 1, no. 15, pp. 1–2, 2010.
[24] S. S. Srivastava and N. Gupta, "Security aspects of the extended playfair cipher," *Proc. - 2011 Int. Conf. Commun. Syst. Netw. Technol. CSNT 2011*, pp. 144–147, 2011, doi: 10.1109/CSNT.2011.37.
[25] S. Singh, R. K. Singh, A. Kaur, and D. Kaur, "Developing 3D-Playfair Cipher algorithm using structure rotation," *Conf. Proceeding - 2015 Int. Conf. Adv. Comput. Eng. Appl. ICACEA 2015*, pp. 1004–1008, 2015, doi: 10.1109/ICACEA.2015.7164853.