Improving Security Using Refined 16 X 16 Playfair Cipher for Enhanced Advanced Encryption Standard (AES)

Ibukun Eweoya,

Olawande Daramola,

Nicholas Omoregbe

Covenant University, Ota, Nigeria
Email: ibukun.eweoya@covenantuniversity.edu.ng
olawande.daramola@covenantuniversity.edu.ng
nomoregbe@covenantuniversity.edu.ng

Abstract: The conventional playfair cipher has lost its potency due to the sophistication of modern systems that can break it by brute force. This work proposes an improved playfair encryption and decryption that will be hard to break by brute force procedure. It uses a 16 X 16 arrays of ASCII characters ensuring relevance in all computing fields instead of the conventional 26 upper case alphabets substitution. An implementation of the cryptographic concept was realized using PHP programming language and embedded in the Advanced Encryption Standard (AES) algorithm. We argue from the perspective of cryptanalysis that our proposed approach is stronger and will be more difficult to break.

Keywords*:* Playfair, cryptanalysis, encryption, decryption, security, ASCII.

1. Introduction

Millions of monetary transactions take place per second online. Also, daily business activities nowadays depend on software and the dire need for strong cryptographic algorithms or concepts cannot be overemphasized. The 21st century fraudsters or hackers are sophisticated in their malicious or criminal activities and therefore software security must be far ahead of them.

The conventional playfair is close to extinction because of the modern day computers with parallelism, pipelining and multiprocessing properties that can break the old playfair in seconds by brute force and frequency analysis thereby rendering it insecure (Tunga1& Mukherjee, 2012). The conventional playfair could not cater for special characters thus limiting the possible combination for keys formation, but the use of ASCII array manipulation as done in our approach is more encompassing.

In this paper, we have tried to overcome the above shortcomings of the conventional playfair by increasing the possible combinations from 2^{26} to 2^{256}. The special

characters that are represented in the plaintext are subsequently encrypted and decrypted just as normal characters; the use of extended character set based on ASCII and the introduction of a password concept into our proposed approach make the use of brute force and frequency analysis approach to break our proposed 16 x 16 playfair difficult. Hence, the proposed model is a modified encryption that is an extension of the basic playfair algorithm. Special rows and columns shifting were introduced into the ASCII representations, and also the use of password. The approach also takes care of instances where characters are repeated.

It is noteworthy that while old ciphers like Ceasar cipher, Hill cipher and Vigenere cipher cannot be disassociated from the playfair in some of their concepts (Tunga1& Mukherjee, 2012), (Stallings,2000). Popular block ciphers such as the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) took after the playfair, but have been significantly modified to achieve better security. The substitution and transposition as used in playfair still find their relevance in all of these encryption algorithms. However, in our approach, we have incorporated modified playfair into the Advanced Encryption Standard (AES) to increase its confusion and diffusion after the procedures of substituting bytes (Sub-Bytes), shifting rows (Shiftrows), mixing columns (Mixcolumns) and key manipulations (addroundkey) by mathematical concepts of non-linearity properties thereby strengthening the AES. We used counter mode of operation on the AES. The speed is very fast and it can be integrated into embedded systems.

The rest of the paper is as follows. Section 2 gives a background and related work, Section 3 explains the refined playfair. In Section 4, we discuss the implementation of the refined playfair, while Section 5 provides details of the cryptanalysis of the refined playfairThe paper is concluded in Section 6 with a brief note.

2. Literature Review and Related Work

Our society depends on cryptography for a secure information communication, monetary and online transactions (Huang et al., 2013). However many threats emerge constantly that must be avoided, or curbed, without loss of assets. Security challenges exist in several forms, which generally include brute force attack, mathematical attack, and timing attacks. Attackers use various methods to discover the encryption key, plaintext to ciphertext conversion, cipher identification. According to Tunga1& Mukherjee (2012) and Schneier (1996), frequency analysis have been used to break key encryption initiatives such as

Vigenere ciphers. Also, Stallings (2000) confirmed an attempt was made on DES and Blowfish by pattern recognition. Neural Networks have uncovered some stream ciphers and enhanced RC6. This scenario underscores the importance of cryptography.

Cryptography is the process of encryption and decryption of data, using mathematical algorithms, concepts and principles. Cryptography can be categorized into symmetric and asymmetric cryptography. Asymmetric cryptography, which is called public key encryption, entails using a public key to encrypt plaintext, such that the plaintext can only be decrypted with the corresponding private key. Symmetric cryptography is called secret key encryption, and it entails using the same key for both encryption and decryption. Symmetric cryptography plays a major role in Secure Socket Layer encryption, which is used by many Web applications.

Block ciphers and stream ciphers are the two types of symmetric algorithms that are used for encryption. The block ciphers are excellent in performance on many hardware and software environments while the stream ciphers are used in secure communication for high throughput (Ravindra et al., 2011). The playfair cipher is symmetric and a block cipher.

In BBC (2012), to achieve a secure transmission of message from a suggested modified playfair, random number generator method was used, specifically Linear Feedback Shift Register. Also, an extended playfair cipher algorithm by Ashish et al. (2012) extended the former encryption from diagram to integrated three coplanar letters with C language implementation and confirmed the fundamentals in playfair encryption relevant in recent ciphers and a strong tool of success in World War I and II by the Americans and the British. Some of the recent efforts at modifying the playfair cipher have been reported in the literature. These include: 5 X 5 playfair cipher by Shang and Lu (2012), 7 X 4 playfair cipher by Amoroso (1994) , 16 X 16 modified playfair by Stallings and Lawrie (2008) , universal playfair cipher using MXN matrix by Alam et al. (2011) and An NXM Version of 5 X 5 Playfair Cipher for any Natural Language (Urdu as Special Case) by Salam et al. (2011). The drawback of the use of 5 X 5 matrix, and 7X4 matrix for extending the playfair cipher is that only relatively few characters are catered for. The 16 X 16 modified playfair by Stallings and Lawrie (2008) catered for a wider range of characters since it based on ASCII. It is also harder to break. Our proposed approach uses ASCII based 16 X 16 matrix, but in addition introduces use of password. The concept is then integrated with AES

in order to realize an impregnable software security platform.

2.1 Playfair Cipher

Playfair is the best known multiple-letter cipher (Ravindra et al., 2011). It is based on a 5 X 5 matrix of letters constructed based on a keyword that is chosen by a user. Here is an example in Table 1 as solved by Lord Peter Wimsey (Stallings, 2000).

Table 1: Example of Playfair Cipher

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

In the above example, the word MONARCHY is the key supplied by the user. The key is entered into the first section of the 5 X 5 array and then the alphabets are then entered but with no repetition. Since the letter A is in the key, it is not entered instead B is entered. In the instance of letter C, the key also contains C so, it is not entered, and the subsequent letters are then entered as long as they are not in the keyword.

Encryption in playfair is done based on substitution. Plaintext letters that fall on the same row matrix are each replaced by the right, with the first element of the row circularly following the last. The plaintext letters that fall on the same column are replaced by the one directly below them or the one at the beginning of the column in case of a letter in the last row. In a case where both conditions are not satisfied, the diagonal of letters are used to replace the plaintext.

1. The Refined Playfair Using 16 X 16 Matrix

Since the basic playfair cipher uses 26 characters of the alphabet (upper case only), our approach uses an extended set of characters comprising the 256 characters of the ASCII set. This is a further extension to modifications such as the use of Linear Feedback Shift Register by BBC (2012) , and use of a 7 X 4 matrix by Amoroso(1994). This is to enable selection from a larger combination of characters and to realize a stronger encryption. The proposed approach has the advantage that playfair cipher can be any character recognizable by the computer and can be used for encryption including special characters. This makes it possible to apply playfair in many more business domains.

A key is selected by the user and then entered. This key is then

converted to its ASCII values and then saved in the 16 X 16 array which is then populated by using a counter-controlled loop while making sure there is no repetition of the key. Figure 1 explains refined playfair.

107	101	121	0	1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76
77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92
93	94	95	96	97	98	99	100	102	103	104	105	106	108	109	110
111	112	113	114	115	116	117	118	119	120	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

Figure 1: Modified Playfair Cipher Using *key* as a Password

The figure above shows a 16 X 16 array with the word *key* represented in ASCII values as (107, 101, 121) and the result of the populated array with the remaining ASCII values. When it gets to 106, 107 is not repeated, it continues from 108 and the same is done for the other 2 numbers. The algorithm also ensures no duplication of any character of the key.

4. Implementation of the Refined 16x16 Playfair

Encryption in playfair is done based on substitution but in our approach diffusion and permutations have been introduced for enhanced security. Diffusion is simply a non-linear substitution step as achieved by Galoids Function (2^8) and s-boxes in AES; permutation is column mixing with uncertain factors or concepts, as achieved by columns multiplication with fixed polynomials in AES. Playfair encrypts the contents of the array two elements at a time. The "null" character is used to complete words with odd number of characters.

We have implemented a software module that allows a user to choose a key, thereafter the program converts the key to their ASCII codes (see Figure 3). A one dimensional array stores the ASCII values of the key and later they are the first in a two dimensional array of 16 X 16. Filling up the 256 uniquely and key dependent generated array, no ASCII value of the key member is repeated. The elements to be encrypted are treated in pairs, when the pair is on

the same row, a left shift is done once and the last on the row falls back on the first. A pair on the same column entails a downward shift and the last on the column falls back on the first on the column. The pair on different row and different column is replaced by diagonal ASCII values for the encryption. The implemented playfair algorithm was embedded in AES.

The hardware configuration of the computer used to execute the algorithm is a factor in the processing speed. A Pentium processor N270 of 1 GB RAM and 1.60 GHz speed executed the refined 16 x 16 playfair in 236ms (microseconds) when the word 'daddy' is used as key (see the screenshot in figure 2)

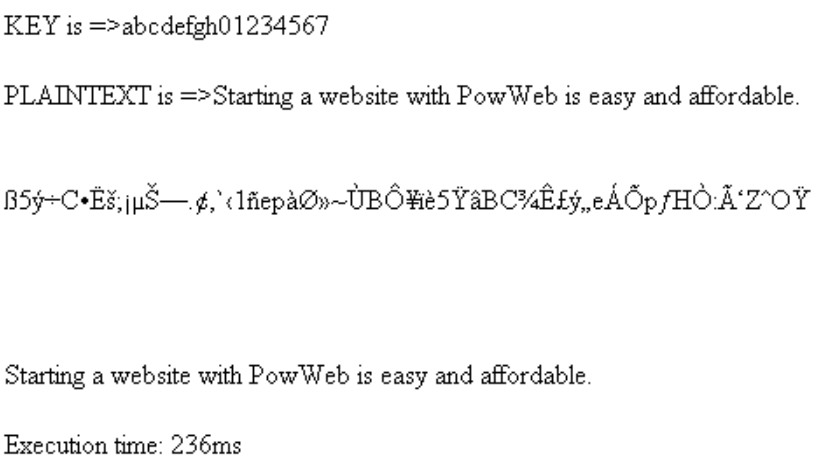

Figure 2: A screenshot of the output

The repetition of characters are neglected, hence *daddy* is treated as *day*, neglecting the middle ds. Figure 3 gives an expression of the above. 100, 97, 121 are ASCII codes for d, a and y respectively.

100	97	121	0	1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76
77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92
93	94	95	96	98	99	101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

Figure 3: Modified playfair using daddy as the key

5. Cryptanalysis of The Refined 16 X16 Playfair

In this section, we argue from the perspective of cryptanalysis that our proposed refined playfair cipher will be harder to break compared to the conventional playfair. In addition, we compare with other previous extensions to the playfair to show how our proposed approach overcomes their limitations.

Going by brute force attacks, the complexity to break the modified playfair cipher has increased from 2^{26} to 2^{256}, which affords a better security compared to the traditional playfair cipher. The use of password and string manipulation was involved which ensures a better diffusion and makes using frequency analysis to break the cipher unproductive. The written code takes any character and converts to ASCII values and the password used determines the positions of the characters, numbers, keywords and special characters causing positions to change, and still ensuring rows and columns right shift and downward shifts respectively.

The traditional playfair with 5 X 5 matrix takes I and J as one character but this is not the best, also when a message in pairs of letters end as an odd number instead of even, X is added at the end but neglected for decryption (Dhenakaran and Ilayaraja, 2012). The 5 X 5 matrix approach has the following limitations: i) 26 letters alone can be taken as keywords without duplicates, ii) Space between two words in the plaintext is not considered as one character; iii) It cannot use special characters and numbers; iv) It has uppercase alphabets only; v) Double letters in plaintext as a pair end up with an X separator whereas the letter X itself gets used as another recognized letter

in the matrix and therefore leads to complications. Our refined playfair has avoided the outlined limitations because empty spaces, special characters and numbers are recognizable as characters for the encryption and decryption processes with case sensitivity.

The use of the 7 X 4 matrix playfair Amoroso(1994) only introduced CRYPTO as its keyword, avoiding repetitions as a rule and the remaining two cells filled with special characters # and * . This is still very close to the conventional playfair except that:

i). When same letters fall in a pair it adds "*" so that the message TILLS become TIL*LS.

ii). If a word consists of odd number of letters, it will add symbol "#" to complete the pair. So BIT becomes BIT#. The symbol # is simply ignored when the ciphertext is decrypted.

It has the following limitations:

i) Only 26 characters can be taken as a keyword without any repetition

ii) The space between two words in the plaintext is not considered as one character

iii) It cannot use numbers and special characters except "*" and "#"

iv)It is not case sensitive. It ignores the symbols "*" and "#" at the time of decryption. Our approach overcomes these limitations.

The playfair that uses 6 X 6 matrix overcome some shortcomings of the 5 X 5 matrix as it is alphanumeric in keyword and plaintext. Letter I is completely separated from J and treated differently in both encryption and decryption. It takes 36 characters as keyword without replication but it is still not case sensitive and space in between words not considered a character. It does not accept special characters and the letter X substitution in odd pairs and identical pair persists.

The refined playfair reported in this work has many benefits, the characters used as keyword has no restrictions (uppercase, lowercase, numbers, alphabet, special characters.) The space between two words is actually a character, users can efficiently encrypt and decrypt alphanumeric characters and others. It is case sensitive, letters I and J are different entities, the "null" character completes uncompleted pairs. In comparison to other algorithms, plaintext discovery from ciphertext is difficult due to a large sample space. Furthermore we incorporated our refined playfair into the Advanced Encryption Standard in other to realize a highly secured encryption module.

6. Conclusion

This work has discussed playfair cipher as a powerful tool during World War II but nearing extinction, modern computers rendered it insecure for their strength to easily break it, though its rudiments have been used to birth other algorithms of relevance today. However, further

researches can make it secure and reliable for modern applications thereby revolutionizing speed and security in software. This work turns the traditional playfair of 26 characters substitution into 256 ASCII codes substitution, and introduces confusion, transposition and permutation into playfair encryption. In addition, the refined playfair was integrated with 128 bits AES in order to create an enhanced security module. It is envisioned that a hardware implementation that is based on our refined playfair plus AES security module would be a worthy investment for embedded systems security in form of FPGA,VDHL or ASIC.

References:

Alam A., Ullah S., Wahid I., Khalid S.,(2011) "Universal Playfair Cipher Using MXN Matrix", International Journal of Advanced Computer Science, Vol.1, No.3, Pp.113-117.

Amoroso, E. (1994), Fundamentals of Computer Security Technology, New York: Prentice Hall.

Ashish N., Farswan S.J, Thakkar V.M, Ghansala S. , (2012), Cryptography Playfair Cipher using Linear Feedback Shift Register, IOSR Journal of Engineering, May. 2012, Vol. 2(5) pp: 1212-1216, http://www.iosrjen.org/Papers/vol2_issue5/AX2512121216.pdf

Cody, P. (2007). AES Implementation in PHP. www.phpaes.com.

Dhenakaran, S., Ilayaraja, M. (2012), Extension of Playfair Cipher using 16 x 16 matrix, International Journal of Computer Applications, *(0975 – 888)*, Vol. 48, No. 7

Huang, X., Wang, C., Huang, W., Li J. (2013), The Nonlinear Filter Boolean Function of LILI-128 Stream Cipher Generator Is Successfully Broken Based on the Complexity of Nonlinear 0 1 Symbol Sequence, Circuits and Systems, Vol.4 No.2(2013), Article ID:29860,DOI:10.4236/cs.2013.42022, file.scirp.org/Html/5-7600234_29860.htm

Monoalphabetic cipher algorithms http://www.bbc.co.uk/dna/h2g2/alabaster/A583878

Ravindra, K., Kumar, S. , Vinay A., Aditya V.S., Komuraiah P. (2011),An Extension to Traditional Playfair Cryptographic Method, International Journal of Computer Applications (0975 – 8887),Vol.17 No.5,March 2011, available at: http://www.ijcaonline.org/volume17/number5/pxc3872814.pdf

Salam, M., Rashid, N., Khalid, S., Khan, M.R. (2011), A NXM Version of 5X5 Playfair Cipher

for any Natural Language (Urdu as Special Case), World Academy of Science, Engineering and Technology 73 2011.

Schneier, B., "Applied Cryptography," 2nd Edition, John Wiley and Sons, Hoboken, 1996.

Shang Y., Lu L. (2012), An Extended Algorithm Based on Playfair Cipher, National Conference on Information Technology and Computer Science (CITCS). www.atlantis-press.com/php/download_paper.php?id=2979

Stallings, W. (2000). Cryptography and Network Security: Principles and Practice, 2nd ed., Prentice Hall, Inc.

Stallings, W., Lawrie, B. (2008). Computer security: Principles and practice, Pearson Prentice Hall.

Tunga1, H., Mukherjee, S. (2012), A New Modified Playfair Algorithm Based On Frequency Analysis, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 1, January 2012 http://www.ijetae.com/files/Volume2Issue1/IJETAE_0112_50.pdf