ISBN 978-981-14-1684-2
Proceedings of 2019 the 9th International Workshop on Computer Science and Engineering
(WCSE 2019 SUMMER)
Hong Kong , 15-17 June , 2019 , pp . 789-794
doi: 10.18178/wcse.2019.06.117

Performance Analysis of the Modified Vigenere Algorithm to Secure Data

Daniel A. Neri [1+], Ariel M. Sison [2+] and Ruji P. Medina [3+]

[1] Technological Institute of the Philippines, Philippines
[2] Emilio Aguinaldo College, Philippines
[3] Technological Institute of the Philippines, Philippines

Abstract. The Vigenere algorithm is simple but considered unbreakable. However, the repeating key is its weakness and is still widely developed by researchers to increase the key length of the algorithm. This study aims to test and evaluate the security performance of the modified Vigenere cipher algorithm to address its vulnerability. The results show that the modified algorithm effectively overcomes Kasiski attack. Moreover, the frequency analysis test shows that the frequency of occurrence of alphabetic letters *I* and *O* obtained 9.0 curve value whereas *M* and *V* have 6.7 curve value. This frequency analysis result indicates that the enhanced Vigenere algorithm has reduced the effect of cryptanalysis. The modified algorithm has also passed the randomness ciphertext test when the frequency (monobit) test was performed. The result shows that the *p-value* computed is 0.841 which is higher than 0.01; hence, the generated ciphertext is considered random.

Keywords: key generation, security evaluation, Vigenere algorithm

1. Introduction

Data confidentiality is viewed as a central issue in the field of information protection. There is an increasing desire to use the public infrastructure like the Internet to store, send, or receive private information for availability and sharing of public and private digital data [1]. One way of guaranteeing the protection of information is through the application of cryptography [2]. Vigenere is a stream cipher and one of the classic cryptographic algorithms that is still widely developed by researchers [3][4].

The Vigenere cipher is no longer taken as a secure cipher and is not popularly used due to the increase of cryptanalytic skills [4]. However, the Vigenere cipher has been used in different fields of Information Technology such as microprocessor software security [5], image security [6], and communication [7]. This encryption stream cipher is considered as one of the most powerful tools to secure transmission over SMS technology [7], military and diplomatic circumstances [8], and Virtual Private Network (VPN) [4] where it is used in concealing information communication over secure and insecure lines.

The jumbling of characters, unlike the traditional Vigenere cipher in each row, makes the ciphertext difficult to crack [3]. Thus, the key length of the algorithm needs to be enlarged to increase its security [4]. Nevertheless, the method of attack on its weakness such as repeating nature of its key is called Kasiski. The Kasiski test estimates and finds the distance between the repeated groups of cipher-text letters. Several studies used different techniques such as key generation [9], extended approach tableau[10], random methods [11][12], and combined algorithms [13][14] to overcome its weakness. However, the authors suggested providing validation of the proposed techniques by performing security evaluation [11] and performance analysis [15]. Hence, the researchers modified the Vigenere cipher in their previous study

+ Corresponding author. Tel.: (+63)926-729-3972
E-mail address: danielneri24@gmail.com; ariel.sison@eac.edu.ph; ruji.medina@tip.edu.ph

through the implementation of key generation technique and tested its runtime performance [16]. Similarly, the researchers recommended evaluating the vulnerability of security attacks of the modified Vigenere cipher.

Thus, this study aims to test and evaluate the security performance of the modified Vigenere cipher using frequency test, frequency analysis, and Kasiski attack.

2. Proposed Algorithm

To improve the security of the classical method, the authors introduced new technique in the key generation process.

2.1. Proposed Key Generation Process in Vigenere Algorithm

Fig. 1 shows the flowchart of the proposed key generation to modify the Vigenere algorithm and its sample computation given in TABLE 1.

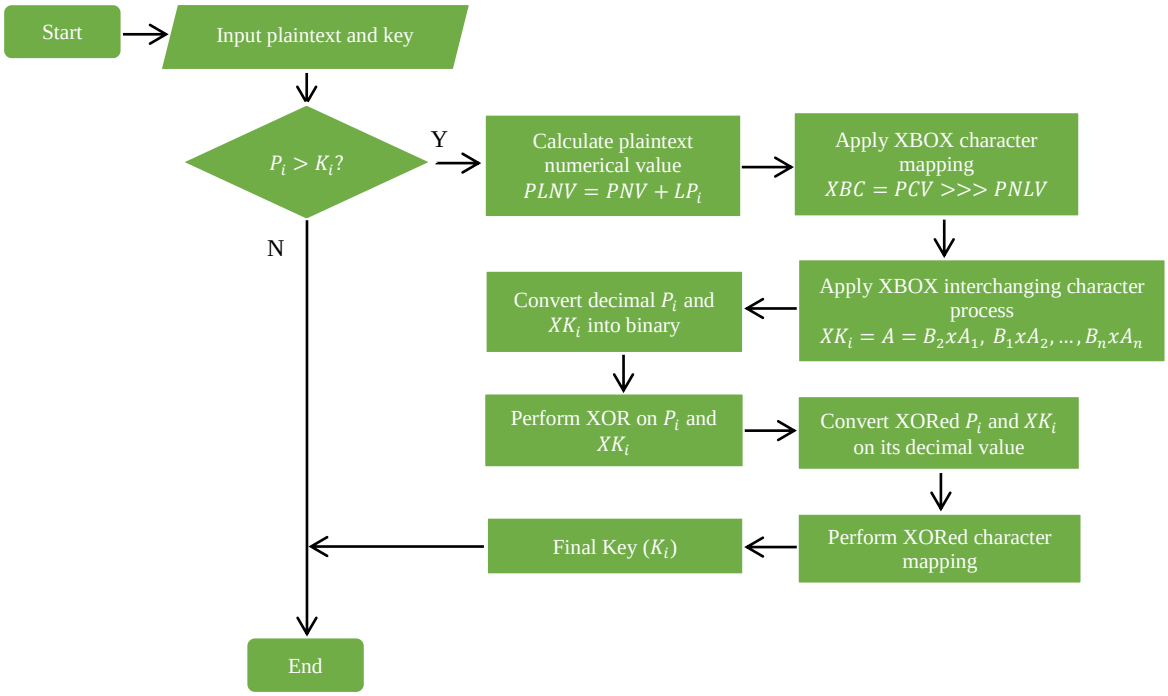

Fig. 1: Flowchart of the proposed key generation of Vigenere algorithm.

It starts with inputting plaintext and key. The key generation process is only applied when the key length is lesser than the plaintext. The plaintext numerical value is calculated by adding each plaintext character value to the plaintext length. The plaintext corresponds to character value (A-Z) and its plaintext number value (1-26). The result of each plaintext numerical value is applied to XBOX character mapping (see TABLE 2). The plaintext character value shift to its plaintext numerical value which is the result of XBOX character. After applying XBOX character mapping, the XBOX key generator produces the initial key of the Vigenere algorithm. The plaintext and XBOX initial key character are converted into decimal value using their equivalent values in the ASCII Table. These decimal values are then converted to binary values and XOR-ed to get their decimal value. To restore the key character of the decimal value of XOR-ed plaintext and XBOX initial key, the XOR-ed character mapping is applied (see Fig. 2). The keys are used in the encryption and decryption process of the Vigenere algorithm.

Table 1: Sample Key Generation of Vigenere Algorithm

PC	PN	LP_i	PLN	XB	R	A	B	XK_i	P_{idec}	XK_{idec}	P_{ibin}	XK_{ibin}	$XORedK_{idec}$	Char
H	8	5	13	O	C	B_2	A_2	G	72	71	0100	0100 0111	15	K
E	5	5	10	L	G	B_1	A_1	C	69	67	0100	0100 0011	6	T
L	12	5	17	G	G	B_4	A_4	L	76	76	0100	0100 1100	0	Z
L	12	5	17	G	L	B_3	A_3	G	76	71	0100	0100 0111	11	O
O	15	5	20	C	O	B_5	A_5	O	79	79	0100	0100 1111	0	Z

where:
PCV = plaintext character value
PNV=plaintext number value
LP_i = plaintext length
PLNV=plaintext numerical value
XBC= XBOX character
RC=reverse character of XBC
XK_i=initial key
P_{idec}=plaintext decimal value (ASCII)
XK_{idec}=initial key decimal value (ASCII)
P_{ibin}= plaintext binary value
XK_{ibin}= XBOX initial key binary value
$XORedK_{ibin}$= XORed binary value
$XORedK_{idec}$= XORed decimal value

Table 2: Xbox Character Mapping

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

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
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A
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
M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N
52	53	54	55	56	57	58	59	60	61	62	63	64	91	92	93	94	95	96	97	98	99	100	101	102	103
B	A	D	C	F	E	H	G	J	I	L	K	M	O	N	Q	P	S	R	N	Q	R	P	O	S	Z
104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127		
Y	X	W	V	U	T	G	F	E	D	C	B	A	M	L	K	J	I	H	U	T	W	V	Y		

Fig 2: XORed character mapping.

2.2. Security Evaluation

The security of the proposed key generation algorithm of Vigenere was evaluated in terms of frequency (monobit) test, frequency analysis, and Kasiski attack resistance.

2.2.1. Frequency (Monobit) Test

This test evaluated the closeness of the fraction of ones to 1/2 (i.e. the number of ones and zeroes in a sequence should be about the same). In this study, the length of the bit string is 89, and the sequence of bits was generated through binary conversion of the ciphertext. The following are the steps to attain the said test:

- Conversion to ± 1: The zeros and ones of the input sequence (e) are converted to values of -1 and +1 and are added together to produce $S_n = X_1 + X_2 + \cdots + X_n$, where $X_i = 2e_i - 1$.
- Compute the test statistic $s_{obs} = \frac{|S_n|}{\sqrt{n}}$. S_{obs} is the absolute value of the sum of the X_i (where $X_i = 2e - 1 = \pm 1$) in the sequence divided by the square root of the length of the sequence.
- Compute $P - value = erfc\left(\frac{S_{obs}}{\sqrt{2}}\right)$, where $erfc$ is the complementary error function.

As to the decision rule, the sequence is non-random if the calculated P-value is < 0.01, otherwise, the sequence is random[17].

2.2.2. Relative Frequency Analysis

The basic theme of Vigenere cipher is to disguise plaintext letter frequencies by defeating simple frequency analysis. This cipher encrypts plaintext message with different letters at different points. But the primary weakness of the Vigenere cipher is the repeating nature of its key. If a cryptanalyst correctly guesses the key's length, then the ciphertext can be treated as can be easily broken [18].

To compute the relative frequency of the message, the equation below is used.

$$\boldsymbol{RFreqL} = \left(\frac{\boldsymbol{CML}}{\boldsymbol{TNLM}}\right) * \mathbf{100}$$

where:

$\boldsymbol{RFreqL}$ = relative frequency of a letter, $\boldsymbol{CML}$ = counts of the letter message, $\boldsymbol{TNLM}$ = total number of the letter message

2.2.3. Kasiski Attack

The modified Vigenere algorithm was evaluated in terms of its resistance to Kasiski attack using Cryptocrack. Cryptocrack is a software that attempts to crack ciphertext using Kasiski pattern to provide match keys and plaintext as shown in Fig. 3. The counts of all match patterns are listed in TABLE 3.

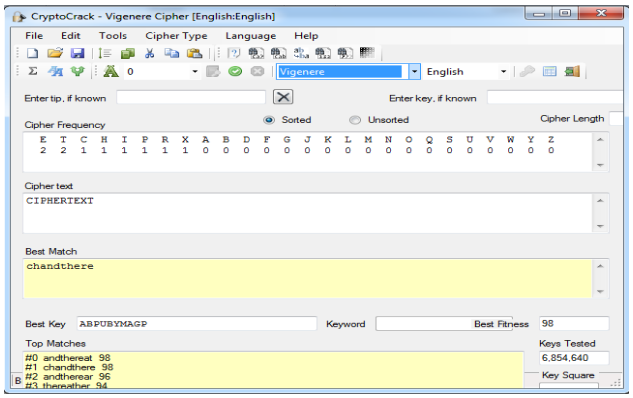

Fig. 3: Cryptocrack software.

Table 3. List of the Count of Match Pattern Attempts

Attempts	Plaintext and Key	Correct Match
Success	2 correct	Count 1
Fail	1 correct	Count 2
	0 correct	Count 3

3. Discussion of Results

3.1. Frequency (Monobit) Test

Fig. 4 shows the result of the frequency monobit test on the modified Vigenere algorithm (XBOX and XOR). The result indicates that the *p-value* computed is about 0.841 which is higher than 0.01; hence, the generated ciphertext by the modified algorithm is considered random.

Table 4. Encryption Process of the Proposed and Traditional Vigenere Algorithm for Relative Frequency Analysis Test

	PROPOSED VIGENERE ALGORITHM
Plaintext	ENCRYPTIONWORKSPROPERLYIMPLEMENTEDSTRONGCRYPTOSYSTEMSAREONEOFTHEFEWTHINGSTHATYOUCANRELYON
Key	OIGFIQNAQDIYPWLRVQTEMFZKFRVJWJIMKPOKKQTIUFCDVSLHUNOJLQVWSCKHHMBEJOSHIYZCWKTSMIHGEKIMMPQCC
Ciphertext	SVIWGFGIEQEMGGDGMEIIDQXSRGGNINVFOSGDBEGOWWASOGDFMGSVDQMAGPOVMFIIOSOAPGMIODASFGVAGKVDQAOQP
	TRADITIONAL VIGENERE ALGORITHM

Plaintext	ENCRYPTIONWORKSPROPERLYIMPLEMENTEDSTRONGCRYPTOSYSTEMSAREONEOFTHEFEWTHINGSTHATYOUCANRELYON
Key	CRYPTOCRACK
Ciphertext	GEAGRDVZOPGQIIHIFQGETVAZKEESOVNVOFJRGHBITRAZVFQNLHGDSCBGFLTHTVYEHOYKFXGUUKHCDAFSRTBTVLAYP

Fig. 4: Modified Vigenere algorithm frequency (Monobit) test.

3.2. Frequency Analysis

It can be gleaned from Fig. 5 and TABLE 4 the relative frequency analysis and encryption process of the traditional and modified Vigenere algorithm respectively. It shows the percentage distribution of letters of the existing and modified algorithm. It is noteworthy to mention that the frequency of occurrence of alphabetic letters I, O have curve values of 9.0 and (M, V) have their result curve values of 6.7. The result shows that the frequency distribution of letters in the modified algorithm is almost flat. Therefore, it is hard to crack.

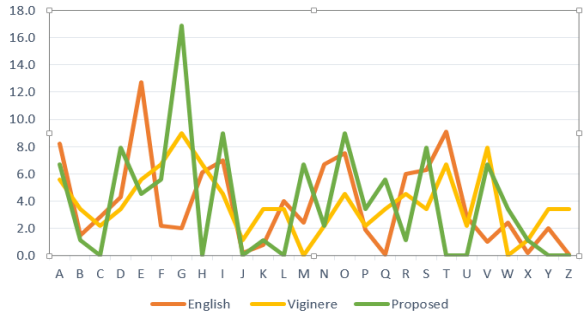

Fig. 5: Relative frequency analysis of the ciphertext in traditional and proposed Viginere algorithm.

3.3. Kasiski Attack

TABLE 5 gives the Kasiski attack resistance result using the modified and traditional Vigenere algorithm. The cryptographic software (Cryptocrack) used to recover the plaintext and key is through the implementation of Kasiski attack which attempts to match the ciphertext by using the patterns stored in the software database. We check whether it can be decrypted using the Cryptocrack. The results show that the traditional Vigenere algorithm was unsecured and cracking tool successfully match the plaintext and key. However, the modified Vigenere algorithm was secured, and the cracking tool failed to match the plaintext and key.

Table 5: Kasiski Attack on Traditional Viginere Algorithm Resistance Result

Attempts	Plaintext and Key	Correct Match Case	
		Vigenere Algorithm	Modified Vigenere Algorithm
Success	2 correct	1	0
Fail	1 correct	9	0
	0 correct	0	10

4. Conclusion and Future Work

In this paper, a key generation technique using XBOX and XOR bitwise operations were applied to modify Vigenere algorithm. The results show that it has enhanced the security against known attacks. The performance assessment also shows that the modified Vigenere algorithm has effectively overcome Kasiski attack and frequency analysis.

In the future, other techniques to evaluate the security of the modified Vigenere algorithm are considered. Moreover, implementation of the modified Vigenere algorithm into an application system is suggested to further evaluate its performance.

5. References

[1] T. F. G. Quilala, A. M. Sison, and R. P. Medina, "Securing Electronic Medical Records Using Modified Blowfish Algorithm," vol. 6, no. 3, 2018.

[2] T. F. G. Quilala, A. M. Sison, and R. P. Medina, "Modified Blowfish Algorithm," vol. 12, no. 1, pp. 38–45, 2018.

[3] E. H. A. Mendrofa, E. Y. Purba, B. Y. Siahaan, and R. W. Sembiring, "Collaborative Encryption Algorithm Between Vigenere Cipher , Rotation of Matrix (ROM), and One Time Pad (OTP) Algoritma," *Adv. Sci. Technol. Eng. Syst. J.*, vol. 2, no. 5, pp. 13–21, 2017.

[4] S. K. Mandal and A. R. Deepti, "A Cryptosystem Based On Vigenere Cipher By Using Mulitlevel Encryption Scheme," vol. 7, no. 4, pp. 2096–2099, 2016.

[5] L. M. K. Massoud Sokouti, Babak Sokout, Saeid Pashazadeh, "FPGA implementation of improved version of the Vigenere cipher," *Indian J. Sci. Technol.*, vol. 3, no. 4, pp. 459–462, 2010.

[6] Y. A. Gerhana, E. Insanudin, U. Syarifudin, and M. R. Zulmi, "Design of digital image application using vigenere cipher algorithm," *Proc. 2016 4th Int. Conf. Cyber IT Serv. Manag. CITSM 2016*, pp. 1–5, 2016.

[7] F. Fahrianto, S. U. Masruroh, and N. Z. Ando, "Encrypted SMS Application on Android with Combination of Caesar Cipher and Vigenere Algorithm," vol. 3, pp. 31–33, 2014.

[8] A. M. Aliyu, "Vigenere Cipher : Trends , Review and Possible Modifications Vigenere Cipher : Trends , Review and Possible Modifications," no. February, 2016.

[9] A. Subandi, R. Meiyanti, C. Lika, M. Sandy, and R. W. Sembiring, "Three-Pass Protocol Implementation in Vigenere Cipher Classic Cryptography Algorithm with Keystream Generator Modification," *Adv. Sci. Technol. Eng. Syst. J.*, vol. 2, no. 5, pp. 1–5, 2017.

[10] K. I. Rahmani, N. Wadhwa, and V. Malhotra, "Alpha-QWERTY Cipher: An Extended Vigenere Cipher," *Adv. Comput. An Int. J.*, vol. 3, no. 3, pp. 107–118, 2012.

[11] R. S. Kartha and V. Paul, "An efficient algorithm for polyalphabetic substitution using random tables," vol. 5, no. 43, pp. 124–133, 2018.

[12] V. Subhashini and N. Geethanjali, "AN ENHANCED APPROACH ON VIGENERE CIPHER BY POLYALPHABETICS," no. 1, pp. 372–379, 2017.

[13] Q.-A. Kester, "a Hybrid Cryptosystem Based on Vigenère Cipher and Columnar Transposition Cipher," *Int. J. Adv. Technol. Eng. Res.*, vol. 3, no. 1, pp. 141–147, 2013.

[14] A. Razzaq, Y. Mahmood, F. Ahmed, and A. Hur, "Strong Key Machanism Generated by LFSR based Vigenère Cipher," *Int. Arab Conf. Inf. Technol.*, pp. 554–548, 2012.

[15] A. Al-Ahwal and S. Farid, "The Effect Of Varying Key Length On A Vigenère Cipher," *IOSR J. Comput. Eng.*, vol. 17, no. 2, pp. 2278–661, 2015.

[16] D. A. Neri, R. P. Medina, and A. M. Sison, "An XBOX-based Key Generation Technique for Vigenere Algorithm," *Int. Conf. Cryptogr. Secur. Privacy(ICCSP)*, pp. 66–70, 2019.

[17] J. P. Songcuan and A. M. Sison, "Jumbled PassSteps : A Hotspot Guessing Attack Resistant Graphical Password Authentication Scheme Based on the Modified PassMatrix Method," *Int. Conf. Cryptogr. Secur. Privacy(ICCSP)*, pp. 55–59, 2019.

[18] Y. K. Marwati, R., "Cryptanalysis on classical cipher based on Indonesian language," *IOP Conf. Ser. J. Phys.*, 2018.