Indonesian Journal of Electrical Engineering and Computer Science
Vol. 23, No. 1, July 2021, pp. 431~437
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v23.i1.pp431-437

An improved vigener algorithm based on circular-left-shift key and MSB binary for data security

Aso Ahmed Majeed[1], Banaz Anwer Qader[2]
[1]Department of Parasitology, College of Veterinary Medicine, University of Kirkuk, Iraq
[2]Computer Department, College of Computer Science and Information Technology, University of Kirkuk, Iraq

Article Info

Article history:

Received Mar 3, 2021
Revised Apr 1, 2021
Accepted Jun 15, 2021

Keywords:

Asymmetric key cryptography
Cryptography
Substitution cipher
Symmetric key cryptography
Vigenere cipher

ABSTRACT

Cryptography is a significant study area at present since it can be vital to protect exceedingly sensitive and secret information from illegal fraud during network transmission. One of the basic cryptographic algorithms is the Vigenere cipher, which is a very easy encryption method to be used as an alternative to Caesar cipher for encrypting the text of the message. In this paper, we enhance the Vigenere algorithm and propose a new method by shifting the key in each message to prevent repeating the messages. Also, it converts the messages into binary form rather than an alphabet. Furthermore, it adds a few bits of random padding to each block of outputs to send a series of bits. The proposed algorithm is named "circular-left-shift key-based Vigener algorithm using most significant bit (MSB) binary (CLS-V-MSB)". Finally, this technique slightly raises the size of the ciphertext, but substantially increases the cipher's protection, achieves the security objectives (authentication, confidentiality, integrity, freshness, and non-repudiation), and avoids Kasiski and Friedman.

Corresponding Author:

Aso Ahmed Majeed
Department of Parasitology
University of Kirkuk, Kirkuk, Iraq
Email: asoalsalihi@gmail.com

1. INTRODUCTION

In the last centuries, after using the Vigenere cipher for nearly 300 years; attacks against the Vigenere cipher were discovered in the 19th century. The Vigenere cipher performance is similar to Caesar cipher in substituting each letter by a certain value. Whereas, the difference is the shift of each alphabet letter in Vigenere cipher according to a key consists of several alphabets in a way that then it is being progressed to cryptography. But in Caesar, the encryption has done through a key consists of one number [1], [2]. Usually, two parties need to exchange messages, but they need to dodge the understanding of the third party to these messages if those fall into his/her hands. The study of techniques of safe interactive communication between two parties is done by cryptography [3]-[5].

Along with the accelerated advancement of information technologies, the volume of data files that are exchanged over the Internet continues to grow. Thus, the safe transfer of secret knowledge across public networks has become a common topic and interest in academic research fields [6]. The idea of cryptography is divided into two basic components of substitution and transposition. In a substitution cipher, the plaintext letters are substituted by other letters to create the ciphertext, while transposition cipher involves scrambling the plaintext letters such that they occupy a different position [4], [7].

Cryptographic protocols are divided into two types which are: symmetric-key cryptography and asymmetric-key cryptography. In the first kind, the sender and receiver use a single key for both the encryption and

decryption process [8]-[10]. Whereas in the other kind which is known as asymmetric-key cryptography; there are two keys. The first key is named a public key and used for the encryption process. The second key is named a private key and used for the decryption process as well as using for signature [5], [11]. This paper uses both ideas of cryptography principle (substitution and transposition) and uses the symmetric key protocol which is suited for data security due to its lightweight.

The details of this article will be clarified in the following sections. In section 2, we summarize from the previous literature works several different algorithms that are recently written. The objectives of cryptography and an entire description of the proposed algorithm are demonstrated respectively in section 3. The security aspects and the attacks' analysis of the proposed algorithm is being discussed in section 4. Finally, section 5 includes detailed conclusions of this paper.

2. RELATED WORK

Aized *et al*. [12] have enhanced the Vigenere cipher by using a table consists of 8 shifting alphabet letters in order including the symbol '&' to create 8 lines of alphabet letters. This led to an increase the module 27 rather than 26. According to their algorithm, the index of plaintext would have been matching the index of the table. For example, the first letter would be encrypted according to the first line in the proposed table, and so on. To save the encryption message, it must never be redundant, but this point was missed in this algorithm. Researchers Khairun and Partha [6] have suggested an expanded version of the Vigenere Cipher utilizing the 95 × 95 Vigenere table, which furnished facilities for encrypting the lower-case letters (a-z), numbers (0-9), and 33 special characters involving the space that is utilized in keyboard and English Language. Their algorithm is somewhat equivalent to the singular algorithm because it benefited from modulo 95 instead of using modulo 26. The critical issue in cryptography is to prevent sending the same message twice, and the algorithm did not cover this issue. Surya *et al*. [13] added the Vigenere Goldbach codes to the Vigenere algorithm. Moreover, they changed the result of the Vigenere cipher to Goldbach codes then converted the result into ASCII code characters. The authors sent a special character and an alphabet character in the final code. This algorithm sends the same message again, this leads to exploring the algorithm through computing the repeated character. Fairouz and Falah [14] utilized a combination of the Vigenere with Stream cipher to create a ciphertext from a Plaintext through two keys which are: Vigenere traditional key and binary key. Firstly, the Vigenere algorithm was applied to the plaintext. After that, the plaintext was converted to its ASCII then XOR it with the binary key. Lastly, they appended the first alphabet ousted from the Vigenere with the first outed character from the stream cipher, and so on. The freshness is an issue in this algorithm because when sending a message twice, the same cipher will be sent.

The Vigenere encryption is close to Caesar encryption. Where it involves a key through it and the shifting will do for each letter. However, the distinction between them is that the size of shifting varies with each letter. Before continuing, it would be beneficial to display the encoding table that is called the tabula rectum as seen in Figure 1 [14], [15]. This method is not resistant to Kasiski and Friedman attacks.

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

Figure 1. Vigenere table [15]

Only the alphabets (A-Z) are encoded by the Vigenere cipher. Before encryption, all the lower-case alphabets and upper-case alphabets in a plaintext message must be converted to only the uppercase alphabets.

Algebraically, the Vigenere cipher can be perceived. By function E_k, the encryption feature generates the ciphertext. It is defined as $C_i = E_k(M_i) = M_i + K_i$ (mod 26) [16], [17]. Thus, C_i is the ith number of the ciphertext. M is the plaintext, M_i is the ith number in M. K is the key, K_i is the ith number in K Mod 26. If the letters A–Z are taken to be the numbers 0–25. Besides, a D_k decryption feature recovers the plaintext from the ciphertext. It is defined as $M_i = D_k(C_i) = (C_i - K_i)$ (mod 26) [18], [19].

In each cryptography, the security service is an essential part. The proposed algorithm CLS-V-MSB has also been evaluated to ensure an acceptable level of protection. In this algorithm, the security is obtained per certain basic security conditions are given below:

- Authentication; Authentication is the end receiver that checks the identity of the sender. The device or user may confirm their identity to another person who is unaware of their identity [20], [21].
- Confidentiality; The most widely debated objective is secrecy. Confidentiality is applied to prevent the third party from obtaining the information when two-person exchange this information [21], [22].
- Integrity; Integrity guarantees the message that has been received is of the same shape. It ensures that the received message is not altered or modified [21], [23].
- Freshness; Freshness guarantees modernity of all data and shared communications avoiding the re-sending of old information. Moreover, to prevent old messages from being re-transmitted by an attacker, a timestamp can be added to the packet to ensure the freshness of the data [8], [21].
- Non-Repudiation; Non-repudiation is a way of ensuring the exchange of messages by digital signature or encryption between parties. It aims to guard against the denial of authentication [8], [12].

The proposed algorithm CLS-V-MSB uses both ideas of cryptography principle (substitution and transposition) and uses the symmetric key protocol which protects the message from repeating. This leads to achieving authentication, confidentiality, integrity, freshness, and non-repudiation. And it avoids Kasiski and Friedman attacks.

3. THE PROPOSED ALGORITHM

The proposed algorithm CLS-V-MSB enhances the Vigenere algorithm by adding parameters to the encryption and decryption equations of the traditional Vigenere algorithm (substitution). It converts the results to binary system form (transposition). Also, it concatenates a shared symmetric key with each binary output of encryption. Moreover, the proposed method sends the alphabet location rather than the alphabet itself as shows in Algorithm 1 and 2. Besides, it consists of 26 letters and a space corresponded with their indexes as shown in Table 1.

Table 1. CLS-V-MSB table

Alphabet	Index	Alphabet	Index	Alphabet	Index	Alphabet	Index	Alphabet	Index
A	0	G	6	M	12	S	18	Y	24
B	1	H	7	N	13	T	19	Z	25
C	2	I	8	O	14	U	20	Ø	26
D	3	J	9	P	15	V	21	-	-
E	4	K	10	Q	16	W	22	-	-
F	5	L	11	R	17	X	23	-	-

Algorithm 1. CLS-V-MSB for encryption

1. Seize for each character 5 bits, because we have 27 locations for each one called a block.
2. Select p, p = plaintext.
3. Select K, l. K=key and l is the length of the key.
4. Define j=0 To 2l(p)-1, where j is an integer shared key starts from zero, l(p)= length of plain text. Besides, it is incremented automatically for the next message.
5. $C_{ini} = (K_i^l + P_i)\ mod\ 27$, where C_{ini} is the initial output of ciphertext, K_i^l the K is key and the l is the length of the key, and I the index. Finally, we use the space also; so that we have mod 27.
6. Use the index of each character to the binary bit.
7. $C_{fin} = C_{ini} \parallel$ j, where C_{fin} is the final ciphertext, || is concatenation where padded j (one bit) according to the most significant bit (MSB) for each block in the C_{fin}.
8. Increment j.
9. KCLS, where CLS is meant Circular Left Shift for next encrypts massage.
10. Wait 10 seconds.

Algorithm 2. CLS-V-MSB for decryption

1. Seize for each character 5 bits, because we have 27 locations for each one called a block.
2. Select *p*, *p* = plaintext.
3. Select *K*, *l*. *K*=key and *l* is the length of the key.

4. Define $j=0\ To\ 2^{l(p)}-1$.
5. *begin*
6. Find the $j_{receiver\ message}$ value, through the number of the received message.
7. Isolates the $j_{receiver}$ *message* (one bit) according to the most significant bit (MSB) for each block in the C_{fin}.
8. *If* $j == j_{receiver\ message}$ *then begin*
9. Change the binary bit to get the index of each character.
10. $P_i = (K_i^l - PC_{ini_i})\ mod\ 27$.
11. Save time received message.
12. Increment *j*.
13. K_{CLS}, where *CLS* is meant Circular Left Shift for next decrypt message.
14. Wait 10 seconds.
15. *end*
16. Else discard the message.
17. Wait 10 seconds
18. *end*

Example: Plaintext= HELLO, the key= WSN, the encryption that is done according to algorithm 1 will be as the following:

1. *p*=HELLO.
2. *K*=WSN, *l*=3.
3. *J*=0, $2^{l(p)}-1$ = 15.
4. $C_{ini} = (K_i^l + P_i)\ mod\ 27$
   H=V, 10101
   E=M, 01100
   L=Y, 11000
   L=Z, 11001
   O=W, 10110
5. 010101001100011000011001010110
6. *J*=1.
7. *K*= NWS.

The decryption of the ciphertext according to Algorithm 2 will be as the following:

1. *p*=HELLO.
2. *K*=WSN, l=3.
3. *J*=0, 2l(p)-1 = 15.
4. 010101001100011000011001010110
5. 00000=0 of receiver message.
6. 0 of receiver message=j.
7. 10101=V
   01100=M
   11000=Y
   11001=Z
   10110=W
8. $P_i = (K_i^l - PC_{ini_i})\ mod\ 27$
   V=H
   M=E
   Y=L
   Z=L
   W=O
9. *J*=1.
10. *K*= NWS.

The proposed algorithm CLS-V-MSB makes sure that each message has never been repeated until the shared key *j* reaches $2^{l(p)}$-1. When it reaches this value, the key must be changed and start from the beginning. Generally, the bit series which includes random bits and converted character bit; makes the language's characteristic ambiguous.

4. RESULTS AND DISCUSSION

The proposed method CLS-V-MSB makes the encryption process strong by encrypting the same message more than once and give different results. This advantage is gotten by using both (substitution, transposition) and symmetric shared keys. As shown in Table 2, the message was repeated in [6], [12], [13], [24] for the plaintext “GOOD MORNING" with a key "SURYA”. But in the proposed algorithm the message will not be repeated till the symmetric key *j* reach $2^{l(p)}$-1.

Table 2. Comparison between the proposed algorithm CLS-V-MSB and other algorithms

Algorithms	Round 1	Round 1	Round 1
Vigenere	YIFBMGLEGNY	YIFBMGLEGNY	YIFBMGLEGNY
[12]	XE&URTVTJF&T	XE&URTVTJF&T	XE&URTVTJF&T
[13]	ÚŒ–¢: G	ÚŒ–¢: G	ÚŒ–¢: G
[6]	Yifb eiilIfa	Yifb eiilIfa	Yifb eiilIfa
[24]	4FC8TDIBDU5	4FC8TDIBDU5	4FC8TDIBDU5
CLS-V-MSB	GBWDØMBZNINU	UWODØØWRNIAO	OOODNUORNWVG

The ciphertext converts each character or symbol to a block of five binary bits values according to their index in Table 1 to be (0011000001101100001111010011000000111001011010100001101101 00) for (GBWDØMBZNINU), (1010010110011100001111010110101011010001011010100000000011 10) for (UWODØØWRNIAO), and (0111001110011100001101101101000111010001011011011010101001 10) for (OOODNUORNWVG). Furthermore, the final step is padding the shared key *j* which, in this example, starts from five and consequently increased by one after each message according to Algorithm 1; leading to the results: (**1**00110**0**0000**1**1011**0**0000**1**1**0**11010**0**0110**0**0000**1**0110**0**10**0**1101**0**0100**0**01101**0**10100) when the shared key is *j*=5, (**1**10100**1**10110**0**01110**0**0001**1**0**1**1010**0**11010**0**10110**0**1000**1**0**0**1101**0**0100**0**0000**0**01110) when *j*=6, and (**1**01110**1**01110**1**01110**0**0001**1**0**0**1101**0**10100**0**01110**0**1000**1**0**0**1101**0**1011**0**10101**0**00110) when *j*=7. The message is different from one round to another as shown in Figure 2.

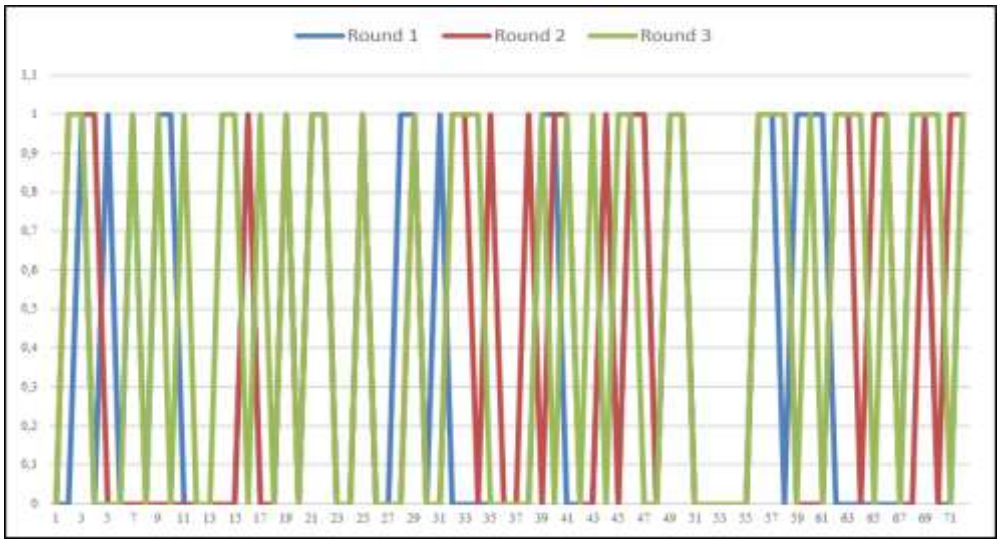

Figure 2. Comparison between encrypted messages

Another comparison in Table 3 shows that the proposed method CLS-V-MSB is better than [6], [12], [13], [24], [25] in terms of security goals as the following:

- Authentication: The authentication is absent in the Vigenere algorithm and [3], [6], [7], [13] because there is nothing that proves the encrypted message is coming from an authorized party. For example, when Alice sends a message to Bob and Eve gains this message. The next time when Eve sends the same message to Bob without altering it, the last party will receive the message thinking it's come from a legitimate party, and he will exchange messages with Eve. Finally, the intruder Eve can get the algorithm after swapping some messages. But, in the proposed algorithm CLS-V-MSB when the message is appended with a shared key which is j; the legitimated last party will check the shared key j. If the key j is not equivalent, it will know that the message comes from Eve or a malicious party.
- Confidentiality: all algorithms achieve this goal; because they send ambiguous messages.
- Integrity: all algorithms achieve this goal; because they send encrypted messages, and the receiver follows the same steps for decrypting the message.
- Freshness: The freshness is absent in the Vigenere algorithm and [6], [12], [13], [24] because they are repeating the sent message as shown in Table 2. For example, when Alice twice sends the same message to Bob; this will be incompatible with the freshness goal. On the other hand, in the proposed algorithm; the same message will be sent with different outputs as shown in Table 2. Moreover, there is a shared key j padded to the result and added to the original different output messages for the same message.

– Non-repudiation: The Vigenere algorithm and [3], [6], [7], [13] are incompatible with this goal because they cannot be authenticated. Conversely, in the proposed algorithm CLS-V-MSB, the receiver checks the shared key. If it's not equivalent, he discards the message as mentioned in Algorithm 2, to result in that the message has come from a legitimate party.

Table 3. Comparison between the proposed algorithm CLS-V-MSB and other algorithms in security terms

Algorithms	Authentication	Confidentiality	Integrity	Freshness	Non-Repudiation
Vigenere	No	Yes	Yes	No	No
[12]	No	Yes	Yes	No	No
[13]	No	Yes	Yes	No	No
[6]	No	Yes	Yes	No	No
[24]	No	Yes	Yes	No	No
CLS-V-MSB	Yes	Yes	Yes	Yes	Yes

The trouble with Eve is that she doesn't have any information about the key's length, therefore, she's either guessing or searching for clues in the message. Several ways are provided to obtain hints about knowing the length of the key. Kasiski and Friedman work with alphabets only. Their examinations were the first trial at that, and here is the idea: some letter combinations or words may be duplicated in the message such as (TH, RR, CH, etc.). The key in the proposed algorithm CLS-V-MSB shifted with each message to result in it a unique message which never repeated as shown in Table 2. Furthermore, the CLS-V-MSB algorithm sends a series of binary bits rather than letters that causes its resistance to Kasiski and Friedman attacks.

5. CONCLUSION

Though the Vigenere cipher is not safe for encrypting unpadded messages, it with other substitution ciphers can be made as stable as other block ciphers by inserting random padding bits to each block to distribute the language characteristics. This padding technique would be perfectly safe as the calculation of discrete logarithm is tedious, and it is hard to separate added shared key bits from converted ciphertext bits. This shared key padding may also be applied to improve a block cipher's protection or build only a pad to encode each message until use another key. Moreover, the key will be shifted after each message. The output of the encrypted message will be inserted and coded in the message to allow the key to be transferred securely. The message is not repeated till the shared key reaches (2l (p)-1), and the final sends a message that includes a series of binary bits rather than alphabet characters. The analysis of the proposed algorithm CLS-V-MSB proves that it achieves the security goals (authentication, Confidentiality, Integrity, freshness, and non-repudiation), and it much secure against Kasiski and Friedman attacks.

REFERENCES

[1] G. Wu, K. Wang, J. Zhang and J. He, "A lightweight and efficient encryption scheme based on LFSR," *International Journal of Embedded Systems*, vol. 10, no. 3, pp. 225-232, 2018, doi: 10.1504/IJES.2018.091785.
[2] S. R.-Salzedo, "The vigenere cipher," in *Cryptography*, Springer, Cham, 2018, pp. 41-54, doi: 10.1007/978-3-319-94818-8_5.
[3] A. E. Omolara and A. Jantan, "Modified honey encryption scheme for encoding natural language message," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 3, pp. 1871-1878, 2019, doi: 10.11591/ijece.v9i3.pp1871-1878.
[4] S. Budi, A. B. Purba, and J. Mulyana, "Secure document files using a combination of substitution methods and vigenere cipher in Bahasa Pengamanan file dokumen menggunakan kombinasi metode subtitusi dan vigenere cipher," *ILKOM Jurnal Ilmiah*, vol. 11, no. 3, pp. 222-230, 2019, doi: 10.33096/ilkom.v11i3.477.222-230.
[5] N. A. Kako, H. T. Sadeeq, and A. R. Abrahim, "New symmetric key cipher capable of digraph to single letter conversion utilizing binary system," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 18, no. 2, pp. 1028-1034, 2020, doi: 10.11591/ijeecs.v18.i2.pp1028-1034.
[6] K. Nahar and P. Chakraborty, "A Modified Version of Vigenere Cipher using 95×95 Table," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 9, no. 5, pp. 1144-1148, 2020, doi: 10.35940/ijeat.E9941.069520.
[7] T. M. Aung, H. H. Naing, and N. N. Hla, "A complex transformation of monoalphabetic cipher to polyalphabetic cipher:(Vigenère-Affine cipher)," *International Journal of Machine Learning and Computing*, vol. 9, no. 3, pp. 296-303, 2019, doi: 10.18178/ijmlc.2019.9.3.801.
[8] A. Majeed, "Cluster forming based on spatial information using HMAC in WSN," *Tikrit Journal of Pure Science*, vol. 22, no. 6, pp. 131-139, 2017.
[9] M. T. Islam and M. S. Hossain, "Hybridization of vigenere technique with the collaboration of RSA for secure communication," *Australian J. of Eng. and Innovative Tech.*, vol. 1, no. 6, pp. 6-13, 2019, doi: 10.34104/ajeit.019.06013.

[10] A. Subandi, R. Meiyanti, C. L. M. Sandy, and R. W. Sembiring, "Three-pass protocol implementation in vigenere cipher classic cryptography algorithm with keystream generator modification," *Advances in Science, Technology and Engineering Systems Journal*, vol. 2, no. 5, pp. 1-5, 2017, doi: 10.25046/aj020501.
[11] B. B. Ahamed and M. Krishnamoorthy, "SMS Encryption and Decryption Using Modified Vigenere Cipher Algorithm," *J. Oper. Res. Soc. China*, pp. 1-14, 2020, doi: 10.1007/s40305-020-00320-x.
[12] A. A. Soofi, I. Riaz, and U. Rasheed, "An Enhanced Vigenere Cipher for Data Security," *International Journal of Scientific & Technology Research*, vol. 5, no. 3, pp. 141-145, 2016.
[13] S. D. Nasution, G. L. Ginting, M. Syahrizal, and R. Rahim, "Data Security Using Vigenere Cipher and Goldbach Codes Algorithm," *Int. J. Eng. Res. Technol*, vol. 6, no. 1, pp. 360-363, 2017.
[14] N. H. Htet and Z. M. Aye, "Innovation Security of Beaufort Cipher by Stream Cipher Using Myanmar-Vigenere Table and Unicode Table," in *Proceedings of the 10th International Workshop on Computer Science and Engineering (WCSE 2020)*, 2020, pp. 52-56, doi: 10.18178/wcse.2020.02.009.
[15] T. M. Aung and N. N. Hla, "A Complex Polyalphabetic Cipher Technique Myanmar Polyalphabetic Cipher," *2019 International Conference on Computer Communication and Informatics (ICCCI)*, 2019, pp. 1-9, doi: 10.1109/ICCCI.2019.8821797.
[16] P. A. M. Hara and H. Manurung, and D. Filina, "Vigenere Cipher and Hill Cipher Algorithm in Data Security Applications in Document Files in Bahasa Algoritma Vigenere Cipher Dan Hill Cipher Dalam Aplikasi Keamanan Data Pada File Dokumen," *Jurnal Teknik Informatika Kaputama*, vol. 1, no. 1, pp. 26-33, 2017, doi: 10.31227/osf.io/7h36y.
[17] N. Ahmad, "Design of a Web-Based Goods Inventory Data Security System at Nanda Stores Using the Vigenere Cipher Cryptography Method in Bahasa Perancangan Sistem Keamanan Data Inventory Barang Di Toko Nanda Berbasis Web Menggunakan Metode Kriptografi Vigenere Cipher," *Jurnal Teknologi Informasi MURA*, vol. 11, no. 1, pp. 29-36, 2019, doi: 10.32767/JTI.V11I1.451.
[18] Z. Shabrizqi, "Application of the Vigenere Cipher and Vernam Cipher Algorithms in Security of Text Files in Penerapan Algoritma Vegenere Cipher Dan Vernam Cipher Dalam Penggamanan File Text," *JURIKOM (Jurnal Riset Komputer)*, vol. 6, no. 3, pp. 326-332, 2019.
[19] H. H. Sami and A. S. Mahmood, "Encoding Syriac Letters in Partition Theory Using Extended Vigenere Cipher," *Eastern-European Journal of Enterprise Technologies*, vol. 1, no. 2, pp. 37-46, 2020, doi: 10.15587/1729-4061.2020.196831.
[20] R. Damara Ardy, O. R. Indriani, C. A. Sari, D. R. I. M. Setiadi, and E. H. Rachmawanto, "Digital image signature using triple protection cryptosystem (RSA, Vigenere, and MD5)," *2017 International Conference on Smart Cities, Automation & Intelligent Computing Systems (ICON-SONICS)*, 2017, pp. 87-92, doi: 10.1109/ICON-SONICS.2017.8267827.
[21] A. A. Agarkar, M. Karyakarte and H. Agrawal, "Post Quantum Security Solution for Data Aggregation in Wireless Sensor Networks," *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, 2020, pp. 1-8, doi: 10.1109/WCNC45663.2020.9120843.
[22] I. Saputra, N. A. Hasibuan, Mesran, and R. Rahim, "Vigenere cipher algorithm with grayscale image key generator for secure text file," *International Journal of Engineering Research & Technology*, vol. 6, no. 1, pp. 266-269, 2017.
[23] W. Itani, A. Kayssi, and A. Chehab. "Wireless Body Sensor Networks: Security, Privacy, and Energy Efficiency in the Era of Cloud Computing," in *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications*, Management Association, Information Resources, Pennsylvania, USA: IGI Global, 2019, pp. 731-763, doi: 10.4018/978-1-5225-8897-9.ch035.
[24] A. Saraswat, C. Khatri, Sudhakar, P. Thakral, and P. Biswas, "An Extended Hybridization of Vigenere and Caesar Cipher Techniques for Secure Communication," in *Procedia Computer Science*, vol. 92, pp. 355-360, 2016, doi: 10.1016/j.procs.2016.07.390.
[25] F. M. S. Ali and F. H. Sarhan, "Enhancing security of vigenere cipher by stream cipher," *International Journal of Computer Applications*, vol. 100, no. 1, pp. 1-4, 2014.

BIOGRAPHIES OF AUTHORS

Aso Ahmed Majeed is currently an instructor at the University of Kirkuk Kirkuk, Iraq. He received a B.Sc. in software engineering from Technical College, Kirkuk, Iraq in 2004 and M.Sc. in Computer Engineering from Cankaya University, Ankara, Turkey in 2015. He published his research in the following areas: data security, security in wireless sensors network, and AI.

Banaz Anwer Qader is currently an instructor at the University of Kirkuk, Kirkuk, Iraq. She received a B.SC. in Computer Science from College of Science, Kirkuk, Iraq in 2006 and M.Sc. in Computer Science from University of Anbar, Anbar, Iraq in 2014. She published her researches in the following areas: data mining, deep learning, AI, data distribution.