Indonesian Journal of Electrical Engineering and Computer Science
Vol. 24, No. 1, October 2021, pp. 548~553
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v24.i1.pp548-553

Linear equation for text cryptography using letters' coordinates

Thamir A. Jarjis, Yahya Q. I. Al-Fadhili
Department of Computer Science, College of Education for Pure Science, University of Mosul, Mosul, Iraq

Article Info

Article history:

Received Dec 16, 2020
Revised Aug 10, 2021
Accepted Aug 23, 2021

Keywords:

Cipher text
Frequency analysis
Linear-decryption
Linear-encryption
Secret key

ABSTRACT

The linear encryption such as Caesar, mono-alphabetic are used to solve the encryption problem in different fields. This module usually encrypts any letter to exact and one corresponding letter. With advanced technologies in computers, these algorithms seem not to be high level secure. This paper proposed a secure encryption algorithm using modified linear encryption by considering the letters' positions of the plaintext body. Two advantages the proposed algorithm has against traditional ones. First, the cryptography procedures are simple and secure. Secondly, it has higher security because of the non- ingrained nature of poly-alphabetic for substitution. Consequently, the plaintext body is considered as a 2-D matrix, such that, each letter has two coordinates, the i^{th} and j^{th}. These procedures depend on substituting the coordinates of the letter into a linear equation to provide a different substitution letter. The performance of these procedures showed better and robust results by applying the frequency analysis test for this proposed algorithm evaluating.

Corresponding Author:

Thamir A. Jarjis
Department of Computer Science, College of Education for Pure Science
University of Mosul
Al-Majmoa Al-Thaqafeya, Mosul, Iraq
Email: thamir@uomosul.edu.iq

1. INTRODUCTION

Cryptography is a term for the secret writing which is derived from a Greek word. Nowadays it refers to the science and art of messages transfer to secure them from attacks. It's a technique for messages encryption and decryption [1]. Therefore, cryptography is needed to encrypt the message at the sender side and decrypt it at the receiver side [2]. Figure 1 simplifies the techniques of cryptography are symmetric and asymmetric key cryptography [3]. Symmetric key cryptography is a shared key between sender and receiver. The sender uses the key and the encryption algorithm to encrypt the message. Whereas the same key and the decryption algorithm are used by the receiver to decrypt the same message. While a public key is used by the sender using asymmetric key cryptography [4], [5]. But a private secret key is assigned to the receiver only [6]. The public key of the receiver is used by the sender to encrypt the message, whilst the own receiver's private key is used to decrypt the message by the receiver [7]-[9].

The substitution and transposition cipher in traditional cipher algorithms are used in symmetric key cryptography [1], [10]. In substitution cipher, a symbol is replaced by another symbol with such ease. It has two types; the monoalphabetic substitution cipher and polyalphabetic substitution cipher. The monoalphabetic cipher, in which a letter is always replaced by exact same letter in the ciphertext. Caesar cipher is the well-known example of monoalphabetic substitution cipher which is always replaces a by d [11]. Whereas in polyalphabetic cipher a single letter is replaced by a different letter in the ciphertext each time the ciphering is took place by considering the position of the letter in the plaintext. Vigenere cipher is the well-known example of polyalphabetic substitution cipher which is changes a plaintext letter into many letters in the ciphertext [12]-[14].

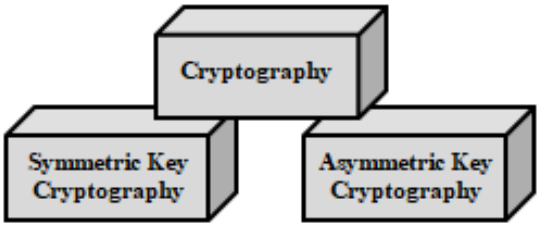

Figure 1. Types of cryptography [3]

In transposition cipher, the letters in the plaintext keep their plaintext form but swapped their positions to get the ciphertext. The plaintext is composed into two dimensional table and by using the predefined key the columns are exchanged accordingly [15], [16]. From the above preview, cryptography uses mathematical operations to encrypt and decrypt sensitive data and information for either to be stored or to be transmitted across networks securely. Therefore, these data/information are unreadable but the authorized recipient [17], [18]. Unlike cryptography, cryptanalysis is the science that studies the encrypted text then analyses and breaks it to gain the plaintext illegally. People who specialist with such science named as cryptanalysts but they much more called attackers. Cryptology consists of both cryptography and cryptanalysis [19]-[23]. The proposed algorithm overcomes the problem of encrypting the same letter from the plaintext into the same corresponding letter in the cipher text. This problem found in the traditional cryptography algorithms.

- Frequency analysis test for evaluating the proposed algorithm

The redundancy of each letter, each letter's coordinates and the polyalphabetic in this algorithm has been analyzed. This analysis was implemented using the Frequency letter's presentation analysis test. Figure 2 illustrates the frequency analysis which is the approach that attempt to reveal the message. This reveal depends on the frequency of letters in a ciphertext [24]. The letters in English language appear in different frequencies [25]. The appearance of the most common letter in English language "e" is about 12%. The second common letter is "t" is about 9% [21], [26]. This frequency analysis test is used to evaluate the outcomes of the proposed algorithm.

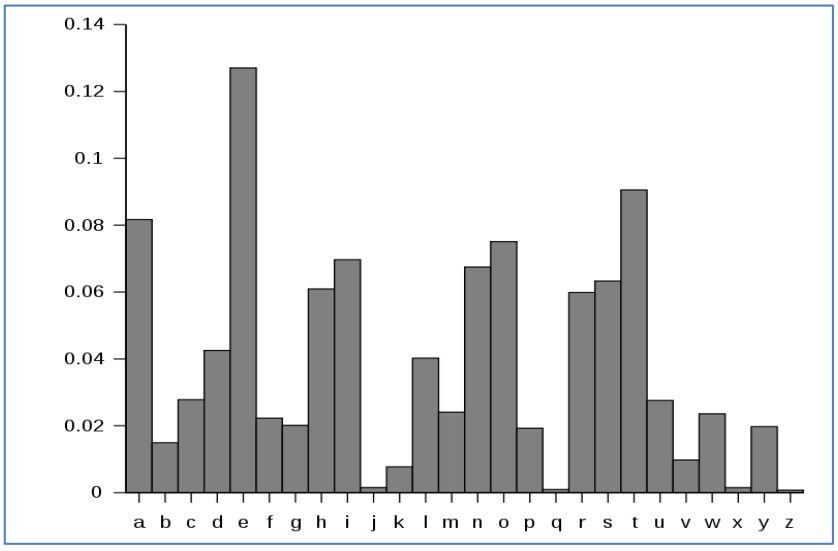

Figure 2. Frequency of English letters [24]

2. METHODOLOGY

In this paper a new encryption and decryption algorithm based on symmetric key is designed and implemented. This algorithm reads the plaintext, then considers the positions of each letter in the plaintext body as an element of 2-D matrix. Later, it obtains the encryption and decryption key according to the coordinates of each letter's i^{th} and j^{th} in the 2-D matrix. These coordinates represent the letter's locality; in

which line (row/i^{th}) the letter is and in which index (column/j^{th}) it is within this line. These coordinates are fulfilling the Kerckhoffs' principle for key secrecy [27]. Finally, the ciphertext is sent. The aim of using these coordinates as the key in the ciphertext is for overcoming the problem of replacing the letter in the plaintext by the exact same letter in the ciphertext. Also, to overcome the problem of distributing the traditional encryption/decryption key and to make this algorithm unbreakable.

The main two advantages of this algorithm which are represented in the simplicity of computation and security level. Consequently, the experimental results have been demonstrated that it is difficult to discover the used key. Figure 3 explains the cryptosystem of the algorithm has been divided into two modules [28], [29], which are; i) data encryption module and ii) data decryption module.

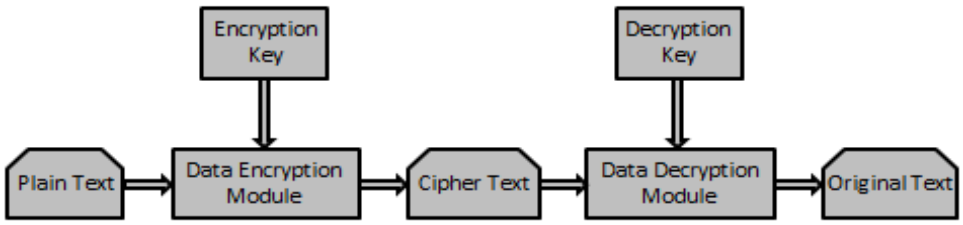

Figure 3. Cryptosystem of the proposed algorithm [28]

2.1. Data encryption module

In this module any data or plaintext to be sent to the receiver is encrypted prior to be transferred using the coordinates' letter by considering the plaintext as a 2-D matrix. Each letter will have its' i^{th} and j^{th} positions in this matrix. Finally, the ciphertext will be generated and sent to the destination. The main steps of the encryption algorithm are as follows:

Step 1: Read the plaintext.
Step 2: Transfer plaintext to 2-dimensional matrix.
Step 3: Obtain the key for each letter from its coordinates into the matrix according to the encryption linear equation: $C = a * P + b$
where P: is the plaintext, C: is the ciphertext, a: is the i^{th} coordinate, b: is the j^{th} coordinate
Step 4: Use the keys above to encrypt the whole plaintext to obtain the ciphertext.
Step 5: Send the ciphertext to the intended receiver.

In the previous third step which involves the obtaining of encryption key, there are two coefficients of the letter's coordinates (a and b) which make the encryption key changes after every letter being encrypted, as shown in Figure 4(a).

2.2. Data decryption module

When the encrypted data (Ciphertext) reaches the receiver, it cannot be read. In order to be read, the decryption key should be grabbed from the letters' positions within the ciphertext. Then the ciphertext is decrypted and converted to its original form using the decryption key using the letters' coordinates, i^{th} and j^{th}. At the receiver side the following steps should be done in order to get the original plaintext.

Step 1: Read the ciphertext.
Step 2: Transfer ciphertext to 2-D matrix.
Step 3: Obtain the decryption key from each letter's coordinates into the matrix according to the decryption linear equation: $P = (C - b)/a$
where: a, b are the coefficients of the linear equation.
Step 4: Decrypt the ciphertext using the decryption key.
Step 5: Obtain the original text.

The decryption part needs to find the mod inverse of the encrypted letter as shown in Figure 4(b). Figures 4 shows the pseudo codes for both encryption and decryption algorithms.

```
Open file to read the (Plaintext)
Reset row-counter
While not eof() do
   Increment row-counter
   Read line()
   Transfer the line into the matrix P[row-counter, line(:)]
   Save the length of the line into vector N
End while
For i = 1 to row-counter do
   For j = 1 to N(i) do
      Grab letter P(i,j)
      P(i,j) = get ascii(P(i,j)) – 97
      Calculate C(i,j) = (i * P(i,j) + j) mod 26
      C(i,j) = C(i,j) + 97
   End for
End for
Put matrix C into output file
```

(a)

```
Open file to read the (Ciphertext)
Reset row-counter
While not eof() do
   Increment row-counter
   Read line()
   Transfer the line into the matrix C[row-counter, line(:)]
   Save the length of the line into vector N
End while
For i = 1 to row-counter do
   For j = 1 to N(i) do
      Grab letter C(i,j)
      C(i,j) = get ascii(C(i,j)) – 97
      Find the mod inverse of x by:
      [g , x , d] = GCD(2*i+1,26)
      x = x mod 26
      Calculate P(i,j) = (x * (C(i,j) – j)) mod 26
      P(i,j) = P(i,j) + 97
   End for
End for
Put matrix P into output file
```

(b)

Figure 4. These figures are; (a) Pseudo code for the encryption algorithm and (b) Pseudo code for the decryption algorithm

3. RESULTS AND DISCUSSIONS

The proposed algorithm is tested on a set of plaintexts of different lengths. The results showed different representations for each letter sufficiently. Each letter was encrypted to a different letters in the ciphertext according to its' coordinates in the plaintext. Figure 5 showing the sample of the applied plaintext, the obtained ciphertext and the decryption text after running the algorithm using MATLAB.

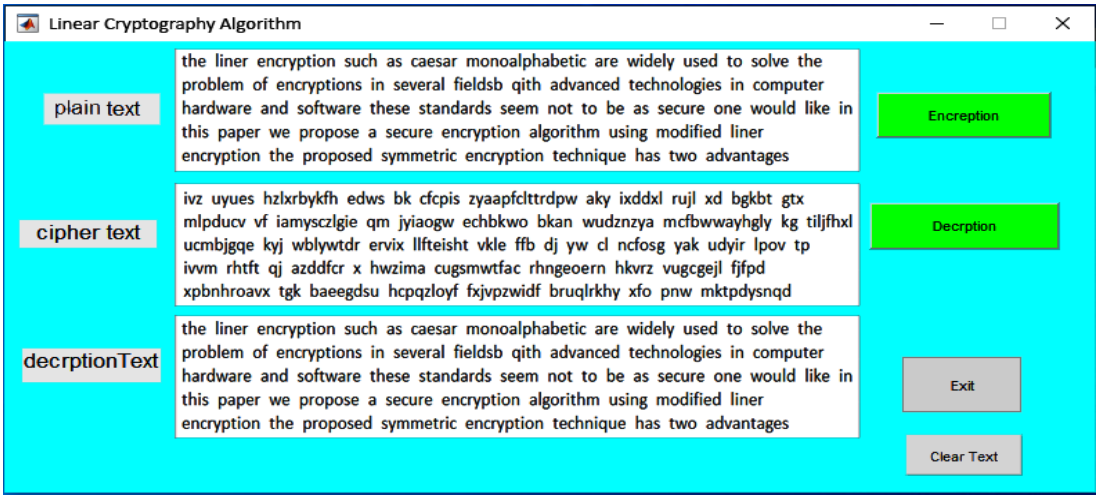

Figure 5. The applied plaintext, the obtained ciphertext and decryption text

The letter "o" in the word "monoalphabetic" in the plaintext have been encrypted in two different letters "y" and "a" in the ciphertext respectively. In addition, the word "the" has been mentioned in the first line twice and had been encrypted in different words "ivz" and "gtx" respectively.

Furthermore, frequency analysis test is applied to both the plaintext and the resulted ciphertext. The frequencies of the letters in the ciphertext are totally different from both the standard frequencies of English language letters and the plaintext as shown in Table 1. In Table 1, the percentage of each letter frequency in the plaintext and the ciphertext was calculated by dividing this frequency of each letter by the total number of letters in the text. This was done by a letter-count script. The obtained frequency of the letters in the ciphertext using the proposed algorithm is entirely different from the frequency of both the sample plaintext and the standard English language letters. This proves that the results of the proposed algorithm are difficult to be detected using frequency analysis techniques.

Table 1. Results of proposed algorithm evaluation using the frequency analysis test

English alphabet	Frequency of English letters	Sample of the plaintext	Ciphertext
a	8.17	6.99	4.55
b	1.49	0.91	3.34
c	2.78	4.55	5.77
d	4.25	4.25	3.34
e	12.7	13.98	3.34
f	2.23	1.21	4.55
g	2.02	1.21	3.64
h	6.09	3.95	2.43
i	6.97	6.99	4.25
j	0.15	0.00	3.03
k	0.77	0.30	1.82
l	4.03	3.64	2.73
m	2.41	2.43	3.34
n	6.75	7.59	3.64
o	7.51	7.90	2.73
p	1.93	4.25	4.25
q	0.10	0.30	3.64
r	5.99	6.99	3.95
s	6.33	7.29	3.34
t	9.06	7.29	4.25
u	2.76	2.43	3.95
v	0.98	1.21	0.67
w	2.36	2.12	5.16
x	0.15	0.00	5.16
y	1.97	2.21	1.51
z	0.07	0.00	5.77

4. CONCLUSION

The encryption and decryption algorithms using linear equation based on letter's coordinates in the plaintext body are robust, and their results are difficult to be revealed. Considering the key of the encryption and decryption processes from the letter's coordinates in the 2-D matrix which is represented from the plaintext body is for overcoming the problem of distributing the secret key and to make the algorithms more secure and unbreakable. The results of the implementation algorithms showed that the same letters in different positions in the plaintext are encrypted to different letters in ciphertext. This makes the algorithms overcome the problem of the classic algorithms which is always encrypt the letter to one exact corresponding letter.

ACKNOWLEDGEMENTS

The authors acknowledge the support from University of Mosul, College of Education for Pure Science, and they gratefully appreciate.

REFERENCES

[1] B. A. Forouzan, *Data Communications and Networking*, USA: McGraw-Hill Higher Education, 2006.
[2] W. S. Kareem, R. Z. Yousif, and S. M. J. Abdalwahid, "An approach for enhancing data confidentiality in Hadoop," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 20, no. 3, pp. 1547-1555, 2020, doi: 10.11591/ijeecs.v20.i3.pp1547-1555.
[3] M. Sharma, Cryptography, Slide Share, 2016. [Online]. Available: https://www.slideshare.net/MileeSharma/cryptography-67584248
[4] N. N. Kulkarni and S. A. Jain, "Checking integrity of data and recovery in the cloud environment," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 13, no. 2, pp. 626-633, 2019, doi: 10.11591/ijeecs.v13.i2.pp626-633.
[5] B. Muruganantham, P. Shamili, S. Ganesh Kumar, and A. Murugan, "Quantum cryptography for secured communication networks," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 1, pp. 407-414, 2020, doi: 10.11591/ijece.v10i1.pp407-414.
[6] S. Rajesh, V. Paul, V. Menon, and M. Khosravi, "A Secure and Efficient Lightweight Symmetric Encryption Scheme for Transfer of Text Files between Embedded IoT Devices," *Symmetry*, vol. 11, no. 2, 2019, doi: 10.3390/sym11020293.
[7] A. A. Alam, B. S. Khalid, and C. M. Salam, "A Modified Version of Playfair Cipher Using 7×4 Matrix," *Int. Journal of Computer Theory and Engineering*, vol. 5, no. 4, pp. 626-628, 2013, doi: 10.7763/IJCTE.2013.V5.762.
[8] A. J. Paul, V. Paul, and P. Mythili, "A fast and secure encryption algorithm for message communication," *2007 IET-UK International Conference on Information and Communication Technology in Electrical Sciences (ICTES 2007)*, 2007, pp. 629-634, doi: 10.1049/ic:20070688.
[9] S. Abed, L. Waleed, G. Aldamkhi, and K. Hadi, "Enhancement in data security and integrity using minhash," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 3, pp. 1739-1750, 2021, doi: 10.11591/ijeecs.v21.i3.pp1739-1750.

[10] H. V. Gamido, "Implementation of a bit permutation-based advanced encryption standard for securing text and image files," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 19, no. 3, pp. 1596-1601, 2020, doi: 10.11591/ijeecs.v19.i3.pp1596-1601.
[11] J. Pieprzyk, T. Hardjono, and J. Seberry, *Fundamentals of Computer Security*, New York, USA: Springer, 2003.
[12] A. M. Al and A. Olaniyan, "Vigenere Cipher: Trends, Review and Possible Modifications," *International Journal of Computer Applications*, vol. 135, no. 11, pp. 46-50, 2016, doi: 10.5120/ijca2016908549.
[13] Q. A. Kester, "A cryptosystem based on Vigenère cipher with varying key," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 1, no. 1, pp. 108-113, 2012.
[14] A. A. Bruen and M. A. Forcinito, *Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century*, New York, USA: John Wiley & Sons, 2011.
[15] S. Ahmad, K. M. R. Alam, H. Rahman, and S. Tamura, "A comparison between symmetric and asymmetric key encryption algorithm based decryption mixnets," *2015 International Conference on Networking Systems and Security (NSysS)*, 2015, pp. 1-5, doi: 10.1109/NSysS.2015.7043532.
[16] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, and Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms," *2017 Int. Conf. Eng. Tech.*, 2017, pp. 1-7, doi: 10.1109/ICEngTechnol.2017.8308215.
[17] S. William, *Cryptography and Network Security Principles And Practice*, London, UK: Pearson Education, 2017.
[18] H. Delfs and H. Knebl, *Introduction to Cryptography: Principles and Applications*, Germany: Springer, 2002.
[19] Z. Kasiran, S. Abdullah, and N. M. Nor, "An advance encryption standard cryptosystem in IoT transaction," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 17, no. 3, pp. 1548-1554, 2020, doi: 10.11591/ijeecs.v17.i3.pp1548-1554.
[20] P. K. Arya, M. S. Aswal, and V. Kumar, "Comparative Study of Asymmetric Key Cryptographic Algorithms," *International Journal of Computer Science & Communication Networks*, vol. 5, no. 1, pp. 17-21, 2015.
[21] S. E. Ghrare, H. A. Barghi, and N. R. Madi, "New Text Encryption Method Based on Hidden Encrypted Symmetric Key," *International Conference on Advanced Computer Information Technologies (ACIT)*, 2018, pp. 240-244.
[22] M. S. Mahmod, "SMS-Phishing on Android Smart Phone," *J. Edu. Sci.e*, vol 27, no. 3, pp. 120-135, 2018, doi: 10.33899/edusj.2018.159322.
[23] S. K. Ibrahim and W. M. H. Yousif, "Hiding Data In A Text Using Color Variance," *Journal of Education and Science*, vol. 26, no. 3, pp. 194-215, 2013, doi: 10.33899/edusj.2013.89907.
[24] A. Dhavare, R. M. Low, and M. Stamp, "Efficient cryptanalysis of homophonic substitution ciphers," *Cryptologia*, vol. 37, no. 3, pp. 250-281, 2013, doi: 10.1080/01611194.2013.797041.
[25] 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.
[26] I. A. Al-Kadi, "Origins of Cryptology: The Arab Contributions," *Cryptologia*, vol. 16, no. 2, pp. 97-126, 1992, doi: 10.1080/0161-119291866801.
[27] S. Mrdovic and B. Perunicic, "Kerckhoffs' principle for intrusion detection," *Networks 2008 - The 13th Int. Telecom. Net. Strategy and Planning Symposium*, 2008, pp. 1-8, doi: 10.1109/NETWKS.2008.6231360.
[28] R. F. Abdel-Kader, S. H. El-sherif, R. Y. Rizk, "Efficient two-stage cryptography scheme for secure distributed data storage in cloud computing," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 3, pp. 3295-3306, 2020, doi: 10.11591/ijece.v10i3.pp3295-3306.
[29] K. R. Raghunandan, A. Ganesh, S. Surendra, K. Bhavya, "Image Encryption Scheme in Public Key Cryptography Based on Cubic Pells Quadratic Case," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 20, no. 1, pp. 385-394, 2020, doi: 10.11591/ijeecs.v20.i1.pp385-394.

BIOGRAPHIES OF AUTHORS

Dr Thamir Abdulhafedh Jarjis: B.Sc. from Math./Comp. Department, College of Education, University of Mosul, Mosul-Iraq in 1988. M.Sc. from Comp. Department, College of MIPA, Gajamada University, Indonisiain 1997. Ph.D. degree from Electrical Engineering department, College of Engineering, Gajamada University, Indonisia in 2005. Fields of interest: security, algorithms and simulation.

Dr Yahya Qasim Ibrahim Al-Fadhili: B.Sc. from Math./Comp. Department, College of Education, University of Mosul, Mosul-Iraq in 1989. M.Sc. from Comp. department, College of Science, University of Mosul, Mosul-Iraq in 2002. Ph.D. degree from Comp. department, School of Science, Loughborough University, UK in 2018. Fields of interest: algorithms, parallel algorithms, simulation, image processing, 3D simulation and AI.