East African Scholars Journal of Engineering and Computer Sciences
Abbreviated Key Title: East African Scholars J Eng Comput Sci
ISSN: 2617-4480 (Print) & ISSN: 2663-0346 (Online)
Published By East African Scholars Publisher, Kenya
Volume-6 | Issue-7 | Dec-2023 | DOI: 10.36349/easjecs.2023.v06i07.002

OPEN ACCESS

Original Research Article

Implementation of the Vigenère Cipher Algorithm's for Securing Member Data

T. Husain[1]*
[1]Department of Information Systems, STMIK Widuri, Jakarta, Indonesia

Article History
Received: 04.10.2023
Accepted: 18.12.2023
Published: 27.12.2023

Journal homepage:
https://www.easpublisher.com

Quick Response Code

Abstract: Many companies and organizations are grabing reborn of technological advances to make it proner to in registered of user's in context daily activities in their business. But behind that, the data we store becomes much more vulnerable to being stolen. Data theft cannot be avoided, but we can increase data security to prevent our data from being misused. Therefore, an algorithm is needed that can disguise the data so that it cannot be read by parties who do not have the right to access the data. The Vigenère cipher algorithm's is a cryptographic technique that can help us to disguise data so that the data is not misused. The key used in this cryptographic method can be a series of characters or words so that people who do not know the key will find it difficult to guess what the actual data contains. Therefore, an application requires extra security so that the data we store there cannot be stolen and misused by irresponsible parties.

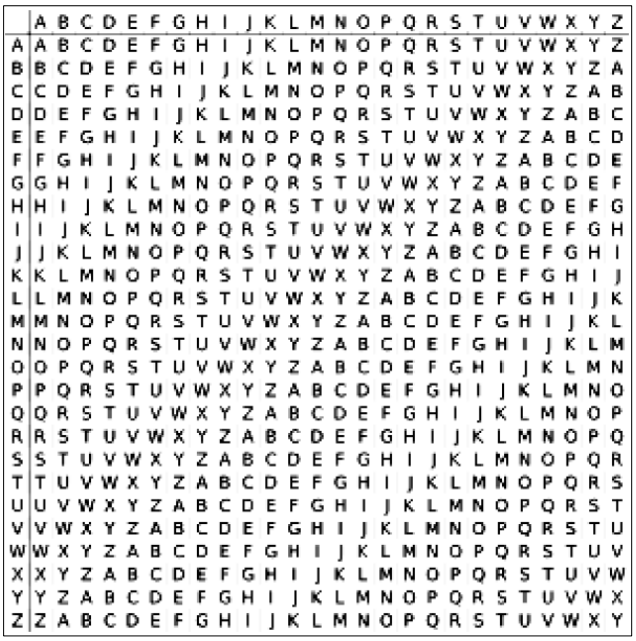
Keywords: Cryptographic, Data Security, Vigenère Cipher.

1. INTRODUCTION

Many companies and organizations are grabbing reborn of technological advances to make it prone to registered users in the context of daily activities in their business. However, the data security of its users must be allowed to prevent data theft. In this digital era [1]. In initial 2020, specifically in May, 91 million data user's and further than seven million Tokopedia merchant data were stolen and it was reported that they were sold on the dark web, such as Tokopedia data for sale containing user full name, e-mail, password, gender, location, address, cellphone number. However, there are several ways to secure data, contains using a technique to disguise data called 'cryptography' [2]. Cryptography initiaty of the Greek words 'kryptos' and 'graphein'. Kryptos means hidden or confidential, while graphein intends writing. So in general cryptography can be interpreted as a process of writing messages in a secret or hidden manner. Cryptography makes the "original text" (plaintext) scrambled using a secret key so that it becomes "scrambled text that is difficult to read" (ciphertext) so that people who do not have the secret key cannot read it [3].

Cryptography uses techniques, such as algorithms in the process of encrypting and describing data to secure information on a platform or website. There are many symmetric key algorithms including AES (advanced encryption standard, IDEA, DES and 3DES, Blowfish, Twofish, MARS, and others with various methods when encrypting and decrypting data. At this encryption stage, the aim is to obscure plain text with functions such as transposition and substitution [4]. Vigenère cipher is one of the encoding methods in cryptography. The Vigenère cipher utilizes an array of differ Caesar ciphers built upon the letters of the keyword. In contrast to the Caesar cipher which only has one value, the Vigenère cipher uses a key in the form of a series of letters. This lock consents every letter in the plaintext to be encrypted with a different key [5]. A scientist in France located in the 16th century, the well-known Blaise de Vigenere discovered of Algorithm. In 1586, this algorithm could not be resolved up to 1917. By exploiting the iterative nature of the key Friedman and Kasiski can solve it [6,7,8].

***Corresponding Author:** T. Husain
Department of Information Systems, STMIK Widuri, Jakarta, Indonesia



	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

Fig. 1: Vigenère Square Table

The Vigenère Cipher is a polyalphabetic replacement, a by matrix 26 - 26 shifts in the Caesar Cipher. It consists of a set of monoalphabetic substitution rules of the Caesar cipher with shifts from 0 to 25 [9]-[10]. The technique was named after its inventor. It contains an aggregate of monoalphabetic to switch Caesar cipher instruction by transformation of 0 until 25 numeral. The technique was stated appellation after that contrivers.

Several studies that have implemented the Vigenère cipher technique include: [11], in the context of application blended learning of learning and teaching computer science's principles is "CS50 Introduction to Computer Science" in Ukrainian higher education institutions according to Professor David J. Malan from Harvard University, with results explaining the importance of this course was interpreted in Ukrainian acquainted in top-rated Ukrainian higher educational facilities those with blending format [12], in conference proceedings investigate the homophonic encryption on the instance of the illustrious ciphers i.e., Z340 and Z408, then analyze the problem for any more use of the yields of the article in probation to correct and renew and the main shorttage of this class of encryption. On this part, an encryption system identical to the Z408 has been generated, and a study of the complexity of automation in applying this encryption technique [13], in conference proceedings probes the main of the asymmetric password system with those constructs, and then presents the concept and common algorithm from asymmetric Two-Dimensional code encryption algorithm, and eventually capsulizes the scheming of two-dimensional code those with a relevant algorithm of the security application system. Following the encryption, the two-dimensional of security the code will be signed into practical application and be significantly escalated [14], is studied a new encryption strategy for converting data secure and safe by applying a new key generation resolve with the classic Vigenère cipher technique encrypting with Vigenère table 26x26. Researchers modified the classic Vigenère table to 95x95, which added more pattern letters, numbers, mathematical symbols, and punctuation in a criterion QWERTY keyboard composition. The gathered yields ensure that the proposed high performance compared to other algorithms in this study. The main aim of this study is to create password reading highly complex and to increase data security. Because of the importance of implementing this method, this research intends to design a user's information system including security using Vigenère cipher cryptography with *polyalphabetic cryptosystems*.

2. METHODOLOGY

This study is applied research, aiming to solve the problem when people think of a project; their minds tend to jump immediately to scheduling and measuring [15]. The research method uses a qualitative approach with cryptography is the 'Vigenère Cipher'. The mathematical model of encryption in the Vigenère cipher algorithm is as follows:

$Ci = (Pi + ki)\ mod\ 26$ … (1)

And the description model is:

$Pi = (Ci + ki)\ mod$ … (2)

Where:

Pi = i^{th} plaintext

Ci = i^{th} ciphertext

Ki = i^{th} key [16,17,18]

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

Fig. 2: Encoding of the letters in The Caesar Cipher

Before being entered into the formula, the letters are first converted into a value, namely "A" is zero, "B" is 1, "C" is 2, until "Z" is 25. Subsequent to the calculation process is identical to the Caesar Cipher, where each letter in the plaintext is shifted as far as the value of the key in the corresponding position [19]- [20]. Shifts of these letters can be made in a 26x26 table which sighted in (Fig. 1).

Template provides authors with most of the formatting specifications needed for preparing electronic versions of their papers. All standard paper components have been specified for three reasons: (1) ease of use when formatting individual papers, (2) automatic compliance to electronic requirements that facilitate the concurrent or later production of electronic products, and (3) conformity of style throughout a conference proceedings. Margins, line spacing, and type styles are built-in; examples of the type styles are provided throughout this document and are identified in italic type, within parentheses, following the example. Some components, such as multi-leveled equations, graphics, and tables are not prescribed, although the various table text styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

3. RESULT AND ANALYSIS

The design of member data application system with security below in Fig. 3:

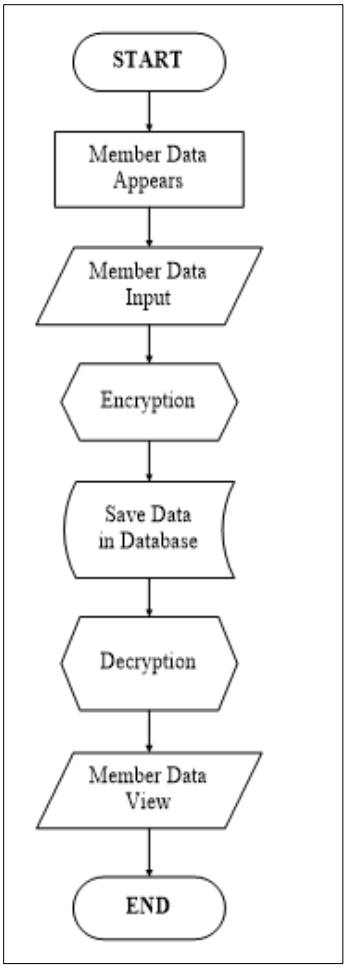


Fig. 3: Application Flowchart

In the application that will be created, the data displayed is original data. Data that has been encrypted is only available in the database. In Fig. 4 is the initial display of the member list page:

MEMBER LIST

Add Member

Name	Position	Phone Number	Address	
Abdu	Chairman	081367545565	Plaju	Deleted
Ahmat	Vice Chairman	081312345678	Kramat	Deleted
Hanya	Secretary	08121298765	West DKIJkt	Deleted
Hana	Treasurer	08125439876	West DKIJkt	Deleted
Husain	Member	081213130112	West DKIJkt	Deleted

Fig. 4: Member List

Meanwhile in Fig. 5 is the contents of the database, it sighted that the names have been encrypted so that they become random letters. Next, we will try adding data to verify whether the process is executing well.

In Fig. 6, we add a new member with the name 'Abdulah'. 'ABDULAH' name has been entered into the member list table (in Fig. 7).

+ Option

Name	Position	Phone Number	Address
degx	Chairman	081367545565	Plaju
elqex	Vice Chairman	081312345678	Kramat
lercl	Secretary	08121298765	West DKIJkt
kdqqd	Treasurer	08125439876	West DKIJkt
mzxfns	Member	081213130112	West DKIJkt

Fig. 5: Database View

MEMBER LIST

Name : Abdulah

Position : Member

Phone Number : 0813676746555

Address : Plaju

Submit

Fig. 6: List of Member (Edit)

MEMBER LIST

Add Member

Name	Position	Phone Number	Address	
Abdu	Chairman	081367545565	Plaju	Deleted
Ahmat	Vice Chairman	081312345678	Kramat	Deleted
Hanya	Secretary	08121298765	West DKIJkt	Deleted
Hana	Treasurer	08125439876	West DKIJkt	Deleted
Husain	Member	081213130112	West DKIJkt	Deleted
Abdulah	Member	0813676746555	Plaju	Deleted

Fig. 7: Member List (Edit)

+ Option

Name	Position	Phone Number	Address
degx	Vice Chairman	081312345678	Kramat
elqex	Secretary	08121298765	West DKIJkt
lercl	Treasurer	08125439876	West DKIJkt
kdqqd	Member	081213130112	West DKIJkt
mzxfns	Member	0813676746555	Plaju
eomltpz	Member	0813676746555	Plaju

Fig. 8: Database View (Edit)

In Fig. 8, the data has also been added on database, but Abdulah's name has been encrypted as 'eomltpz'. Next, we will check whether 'Abdulah', if encrypted with the keyword "ENKRIPSI", will match what is stated in the database. First of all, we change the letters from "ABDULAH" and also the letters from "ENKRIPSI" into numbers.

A	B	D	U	L	A	H
0	1	2	20	11	0	7

E	N	K	R	I	P	S	I
4	13	10	17	8	15	18	8

Because "ABDULAH" only has 7 letters in it, we only use 7 letters from the word "Enkripsi", namely "ENKRIPS". Then we enter these numbers into the Vigenère cipher cryptography formula below:

$C1 = (P1 + k1)\ mod\ 26$ ... (3)
$= (0 + 4)\ mod\ 26$
$= 4 \rightarrow$ E

$C2 = (P2 + k2)\ mod\ 26$ ... (4)
$= (1 + 13)\ mod\ 26$
$= 14 \rightarrow$ O

$C3 = (P3 + k3)\ mod\ 26$ ... (5)
$= (2 + 10)\ mod\ 26$
$= 12 \rightarrow$ M

$C4 = (P4 + k4)\ mod\ 26$ ... (6)
$= (20 + 17)\ mod\ 26$
$= 11 \rightarrow$ L

$C5 = (P5 + k5)\ mod\ 26$ ... (7)
$= (11 + 8)\ mod\ 26$
$= 19 \rightarrow$ T

$C6 = (P6 + k6)\ mod\ 26$ ... (8)
$= (0 + 15)\ mod\ 26$
$= 15 \rightarrow$ P

$C7 = (P7 + k7)\ mod\ 26$ ... (9)
$= (7 + 18)\ mod\ 26$
$= 25 \rightarrow$ Z

Therefore, the encryption result of the word "ABDULAH" with the keyword "ENKRIPSI" is "EOMLTPZ". From the calculation results above, the encryption results that we calculated manually are the same as in the database. In other words, the program has been successful.

4. CONCLUSION

Data security is important, especially when it includes personal data. Many parties want to take someone's personal data to use for their own or group interests. Therefore cryptography can help us to maintain the confidentiality of our data. Cryptography can change the original message into random letters making it difficult to understand. Even though it is not 100% safe, at least cryptography can help reduce the risk of data theft.

Conflicts of Interest: The authors declare no conflicts of interest

Funding: The authors received no direct funding for this research

REFERENCES

1. IES > NCES, "Safeguarding Your Technology: Practical Guideliness for Electronic Education Information Security," in *Chapter 3: Security Policy Development and Implementation*. Washington, DC: National Center for Education Statistics, December 1998, ch. 3, p. 141. [Online]. https://nces.ed.gov/pubs98/safetech/chapter3.asp
2. Fanny Potkin. (2020) Reuters. [Online]. https://www.reuters.com/article/idUSKBN22E0P9/ [Accessed October. 2023]
3. James Clerk Maxwell, *A Treatise on Electricity and Magnetism*, 3rd Ed. Britania Raya: Cambridge University Press, 2011, vol. 3. Doi: doi:10.1017/CBO9780511709333
4. Timothy J. Shimeall and Jonathan M. Spring, "Chapter 8 - Resistance Strategies: Symmetric Encryption," in *Introduction to Information Security: A Strategic-Based Approach*, 1st Ed.: Elsevier Inc, 2014, pp. 155-183. doi:10.1016/C2011-0-00135-7

5. Aakash, Jitendra Soni, and Bharti Sharma, "A. J. Cipher," in *2nd International Conference on Telecommunication and Networks (TEL-NET)*, Noida, India, 2017, pp. 1-6. doi:10.1109/TEL-NET.2017.8343547
6. Dony Ariyus, *Introduction to Cryptography, Theory, Analysis and Implementation*. Yogyakarta: Andi Publisher, 2008.
7. Mohammed Aliyu Al-Amin and Abdulrahman 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
8. M. Iqbal Bhat and Kaiser J. Giri, "Impact of Computational Power on Cryptography," in *Multimedia Security*, Kaiser J. Giri et al., Eds. Singapore: Springer, 2021, pp. 45-88. doi:10.1007/978-981-15-8711-5_4
9. Duncan Buell, "Simple Ciphers," in *Fundamentals of Cryptography: Undergraduate Topics in Computer Science*. Cham: Springer International Publishing, 2021, pp. 11-26. doi:10.1007/978-3-030-73492-3_2
10. Anurag Jagetiya and C. Rama Krishna, "Design and Analysis of Security Protocol for Communication," in *Evolution of Information Security Algorithms*, Dinesh Goyal et al., Eds. Beverly, MA: Scrivener Publishing LLC, 2020, ch. 2, pp. 29-78. doi:10.1002/9781119555759.ch2
11. Radmila Segol and Andrii Parkhomenko, "Massive Open Online Course “CS50 Introduction to Computer Science” by Harvard University Implementation Into Ukrainian Educational Process," *International Scientific Journal "Industry 4.0"*, vol. IV, no. 4, pp. 195-197, 2019.
12. Oleksandr Mamro, Andrii Lagun, and Bohdan Dupak, "Investigation of Homophonic Encryption on Zodiac Z408 and Z340 Ciphers," in *IEEE 12th International Conference on Electronics and Information Technologies (ELIT)*, 2021, pp. 109-112. doi:10.1109/ELIT53502.2021.9501114
13. Guofang Huang and Xiping Liu, "Application of Two-Dimensional Code Encryption Algorithm Under Asymmetric Cipher System," in *International Conference on Multi-modal Information Analytics (ICMMIA)*, Huhehaote, China, 2022, pp. 464-471. doi:10.1007/978-3-031-05484-6_58
14. Thamer Hassan Hameed and Haval Tariq Sadeeq, "Modified Vigenère Cipher Algorithm Based on New Key Generation Method," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 28, no. 2, pp. 954-961, November 2022. doi:10.11591/ijeecs.v28.i2.pp954-961
15. HBR Editors, "The Four Phases of Project Management: Planning, Build-up, Implementation, and Closeout," in *Pocket Mentor: Managing Projects*. USA: Harvard Business Publishing, 2016. [Online]. https://hbr.org/2016/11/the-four-phases-of-project-management
16. Hazim Noman Abed, Zainab Mohammed Ali, and Ahmed Luay Ahmed, "A Robust Encryption Technique Using Enhanced Vigenre Cipher," *International Journal of Nonlinear Analysis and Applications*, vol. 12, no. 2, pp. 447-454, 2021. doi:10.22075/IJNAA.2021.5071
17. Munura Maihankali and Esther Chinwe Eze, "Symmetric Cryptography for Confidential Communications: Implemented by Enhancing the Caesar Cipher," *International Journal of Computing and Engineering*, vol. 2, no. 1, pp. 1-13, 2021.
18. Udochukwu Iheanacho Erondu, Emmanuel Oluwatobi Asani, Michael Olaolu Arowolo, Amit Kumar Tyagi, and Nehemiah Adebayo, "An Encryption and Decryption Model for Data Security Using Vigenere With Advanced Encryption Standard," in *Using Multimedia Systems, Tools, and Technologies for Smart Healthcare Services*. New York: IGI Global, 2023, Ch. 9, pp. 141-159. doi:10.4018/978-1-6684-5741-2.ch009
19. Christof Paar, Jan Pelzl, and Tim Güneysu, *Understanding Cryptography: From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms*, 2nd Ed. Berlin, Heidelberg: Springer, 2024. doi:10.1007/978-3-662-69007-9_3
20. Rajkumar Banoth and Rekha Regar, "An Introduction to Classical and Modern Cryptography," in *Classical and Modern Cryptography for Beginners*. Cham: Springer Nature Switzerland, 2023, pp. 1-46. doi:10.1007/978-3-031-32959-3_1.

Cite This Article: T. Husain (2023). Implementation of the Vigenère Cipher Algorithm’s for Securing Member Data. *East African Scholars J Eng Comput Sci, 6*(7), 102-107.