

## Modified Vigenere cryptosystem: An integrated data encryption module for learning management system

Jason P. Sermeno\*, Kenrick Agustin S. Secugal, Nelly E. Mistio

College of Computer Studies, University of Antique, Antique, Philippines

### ABSTRACT

Security is a practice of defending our computers, servers, networks, mobile devices, electronic systems, and digital information against accidental and malicious attacks in the field of Information Technology. One way to protect such valuable information is to use cryptography. Cryptography or encryption algorithm is the process of transforming sensitive data into confounding data in such a way that the person or the machine with a key can decode the hidden information. In this article, a hybrid approach of the Vigenere cryptosystem was used in encrypting and decrypting the data. This approach will be integrated with the learning management system using matrix manipulation and the Base94 encoding scheme. The experimental result of the study shows a significant high avalanche effect compared to the original Vigenere cryptosystem.

**Keywords:** Vigenere cryptosystem, Encryption algorithm, Table manipulation, Symmetric-key algorithm, Security cryptography.

### 1. INTRODUCTION

Many institutions today are taking advantage of learning management systems (LMS) solutions such as TalentLMS, Skyprep, Google Classroom, Canvass, Blackboard Learn, and Moodle, especially during a pandemic. These eLearning course platforms contain sensitive information, user data, and other content that must be secured. Thus, these LMS have security features that can help keep our data safe and sound. Among these features is data encryption which ensures that the data are secured when transmitted between applications

One popular encryption scheme is the Vigenere cryptosystem developed by Blaise De Vigenere in 1593. It is a polyalphabetic cipher that uses tabula recta and a custom key to manage the encryption and decryption of the message. So far, it has been the best-known poly-alphabetic substitution cipher which is more potent than Caesar cipher and much harder to decode (Aakash et al., 2017). With this scheme, the security of the system depends on the security of the keys used. One issue with the keys is the key exchange problem. In some situations, direct key exchange is possible, however, much commercial data exchange now takes place between parties that have never previously communicated with one another, and there is no opportunity to exchange keys in advance (Thorsteinson and Ganesh, 2003). The tabula recta also pose another problem because if ever the encryption key had been known, the hidden data could easily be deciphered using the fixed Vigenere table.

This study proposes a new approach to enhancing the Vigenere cryptosystem (Sermeno et al., 2020). It uses the matrix manipulation principle for simultaneous manipulation of the Vigenere table and involves a series of iterative substitution transformations using 2 keys for encrypting and decrypting the message as depicted in Fig. 1. The approach also implements the Base94 encoding scheme that alters the message to a different form so that it would offer a higher means of securing the

### OPEN ACCESS

**Received:** February 1, 2021


**Revised:** March 29, 2021

**Accepted:** April 9, 2021

#### Corresponding Author:

Jason P. Sermeno

[jason.sermeno@antiquespride.edu.ph](mailto:jason.sermeno@antiquespride.edu.ph)

 **Copyright:** The Author(s). This is an open access article distributed under the terms of the [Creative Commons Attribution License \(CC BY 4.0\)](https://creativecommons.org/licenses/by/4.0/), which permits unrestricted distribution provided the original author and source are cited.

#### Publisher:

[Chaoyang University of Technology](https://www.chaoyang.edu.ph/)

ISSN: 1727-2394 (Print)

ISSN: 1727-7841 (Online)

information. The modified Vigenere cryptosystem was integrated as a data encryption module in a database management system used by the learning management system. To determine the performance of the algorithm, the modified Vigenere cryptosystem will be compared to the original Vigenere encryption algorithm using the avalanche effect.

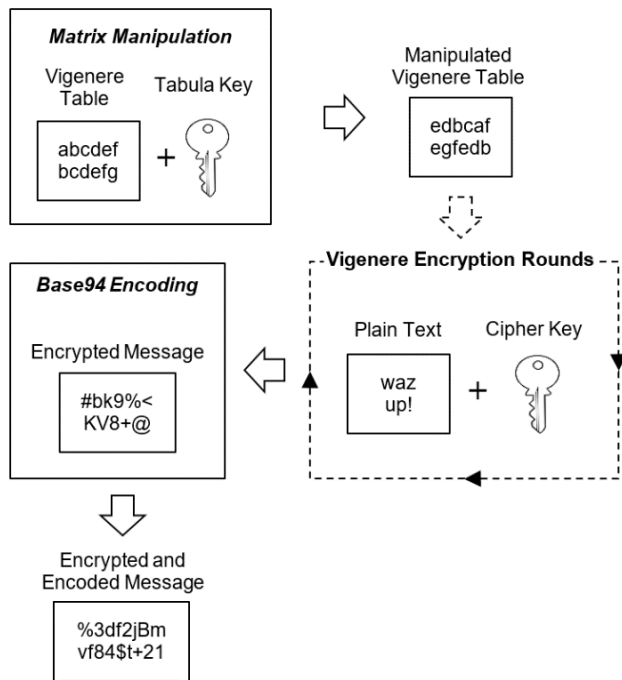


Fig. 1. Conceptual approach of the modified Vigenere algorithm

## 2. RELATED WORKS

The Vigenere cryptosystem is a popular polyalphabetic substitution cryptographic cipher. It is considered classical today because it is not used now but it had great importance in its history. This algorithm usually operates on letters and is implemented with a simple mechanical device or by hand. They were considered reliable at the moment it was developed but have little importance now due to the technological advancements.

Nowadays, the Vigenere encryption algorithm had been used as one of the mechanisms for encrypting information in their applications for some studies. One particular research is the SMS (Short Message Service) encryption using the combination of the Vigenere and Caesar cipher encryption scheme for Android phones (Fahrianto et al., 2014). The research was just an improvement of a previous study wherein the number of characters was just increased to 94 to give the application a higher number of possible combinations. A similar study had also been conducted using the Least Significant Bit Steganography combined with the Vigenere Cipher for Android platforms (Danuputuri et al., 2015). Their approach uses arithmetic

coding and a hash function (SHA 256). The hybrid algorithm was able to enhance the security of the confidential data delivery process, reduce the file size, and detect the authenticity of the files being sent. In addition to this, it was able to encrypt different forms of image file (\*.gif, \*.jpeg, \*.png, \*.bmp) as well as document type files (\*.doc, \*.xls, \*.pdf, \*.txt). Another similar study focuses on digital image encryption using just the Vigenere itself (Gerhana et al., 2016). In their research, the image file along with its key is encrypted using a Red-Green-Blue (RGB) matrix as the Vigenere table. The same principle is being applied for the encryption scheme, only that the table is based on a 255 grayscale of red, green, and blue.

Aside from having the Vigenere algorithm as one of the mechanisms for a certain application being developed, there are also studies that involve the enhancement of the Vigenere cryptosystem by merging it with other existing encryption schemes making it more reliable and difficult to crack. One such enhancement involves a hybrid cryptographic method or a combination of the Hill and Vigenere cryptosystem over plain text (Touil et al., 2020). In this method, it takes advantage of using Hill and Vigenere encryption to group and regroup streaming and block ciphers on plain text. With the approach, the hybrid method was strong enough to withstand a bridge or statistical attacks due to the abstraction mode used in their method. Another similar study is the fusion of the chaos function on the Vigenere cipher (Triandi et al., 2018). With this approach, the chaos function was used to support the Vigenere cipher iteratively to generate and improve the quality of the key streams. This method increases the quality of the data security because the initial value of the secret key is so sensitive when replaced with a certain value, it produces a very different keystream making it difficult to decipher. A group of researchers conducted a similar study that extends the Vigenere table by including the characteristics, digits, special and rare symbols and combining it with Caesar cipher to generate a key according to its participant's decision (Hossain and Islam, 2018). It reduces the sizes of the cipher-text and keys where the symbols are arranged in the priority based on the increasing order of the number of rows and columns to increase its security over brute force attack.

To summarize the literature, Table 1 describes the summary of the related works in this study.

At the present time, cryptography relies greatly on the theory of mathematics and computer science. By using computational resistance in the designs of such algorithms, it only means that it is impossible to crack it in any current known way (Trappe and Washington, 2006). This indicates that faster computing technology and theoretical advancement entail constant modifications to these techniques. However, theoretically secure schemes had been proven to be impossible to crack if used correctly. This means that even with unlimited computing power these schemes still stand but they are very difficult to implement.

**Table 1.** Summary of related works

| Related works  | Description  | Limitations   |
|--|--|---|
| Encrypted SMS application on Android with the combination of Caesar cipher and Vigenere algorithm (Fahrianto et al., 2014) | an enhancement of a recent study by Abdur Rahman by combining Caesar and Vigenere cipher over a plain text   | <ul style="list-style-type: none"> <li>• relies on a fixed Vigenere square</li> <li>• limited symbols</li> <li>• uses a single key decode</li> </ul>  |
| Data security using LSB steganography and Vigenere cipher in an android environment (Danuputuri et al., 2015)              | uses Vigenere and Steganography LSB to encrypt and compress data image and other file type data  | <ul style="list-style-type: none"> <li>• decoding takes a little longer than the encoding process</li> <li>• uses a single key to decode</li> </ul>   |
| Design of digital image application using Vigenere cipher algorithm (Gerhana et al., 2016)                                 | focuses on encrypting digital image using Vigenere cipher with RGB   | <ul style="list-style-type: none"> <li>• fixed Vigenere square on RGB</li> <li>• encrypted image doesn't show disrupting pixel positions</li> <li>• uses a single key decode</li> </ul>                         |
| Improve security algorithm cryptography Vigenere cipher using chaos functions (Triandi et al., 2018)                       | it uses chaos function iteratively to obtain a key stream through Vigenere cipher that requires a constant $r$ and an initial $k_0$ value to encrypt and decrypt a message | <ul style="list-style-type: none"> <li>• relies on fixed Vigenere square for plain and cipher text</li> </ul>   |
| An extension of Vigenere technique to enhance the security of communication (Hossain and Islam, 2018)                      | a Vigenere table is modified to include numbers and rare characters along with the alphabets and uses Vigenere and Caesar cipher to encrypt and decrypt messages           | <ul style="list-style-type: none"> <li>• relies on a fixed Vigenere square for plain text</li> <li>• uses a single key decode</li> </ul>  |
| Text encryption: Hybrid cryptographic method using Vigenere and hill ciphers (Touil et al., 2020)                          | uses Hill cipher to encrypt 4 blocks of an indexed plain text and applies the Vigenere cipher to perform substitution over the first ciphered text                         | <ul style="list-style-type: none"> <li>• relies on a fixed index letters during the Hill cipher transformation</li> <li>• relies on a fixed 4x4 matrix for a key</li> <li>• uses a single key decode</li> </ul> |

**Table 2.** Decoding the tabula key

| Tabula key | Binary representation   | Extra bits padded                  |
|------------|-------------------------|------------------------------------|
| B2 ... F3  | 1011 0010 ... 1111 0011 | 1011 0010 ... 1111 0011 <u>011</u> |
| 3A ... 2A  | 0011 1010 ... 0010 1010 | 0011 1010 ... 0010 1010 <u>010</u> |
| 7F ... B1  | 0111 1111 ... 1011 0001 | 0111 1111 ... 1011 0001 <u>001</u> |

### 3. THE MODIFIED VIGENERE CRYPTOSYSTEM

#### 3.1 Generating and Decoding the Tabula Key

There are four main steps in the encryption and decryption process of the modified Vigenere cryptosystem: 1. generation and decoding of tabula key; 2. manipulation of the Vigenere square; 3. iterative Vigenere encryption procedure; 4a. message-and-key fusion (during encryption); and 4b. message parsing (during decryption).

A tabula key is a 23-digit hexadecimal number that is randomly generated by the system. Its primary purpose is to provide a pair of swap patterns on the collective rows and columns of the Vigenere table based on the bit patterns of the tabula key in its binary form. Since this study uses a 95-

by-95 square matrix, three more bits will be appended at the end of the binary string. The way the extra bits are added will be the replica of the last binary digit in the existing set of bits, instead of adding series of zeroes at the end. Table 2 depicts some examples of how a portion of the tabula key is decoded.

The swap patterns are determined by reading the bits from left-to-right and right-to-left respectively where each bit of the tabula key corresponds to the position of the row or column to be swapped.

#### 3.2 The Manipulation Scheme of the Vigenere Square

In order to improve the complexity of the proposed algorithm, while improving the performance on confidentiality, 95 characters are taken into account that

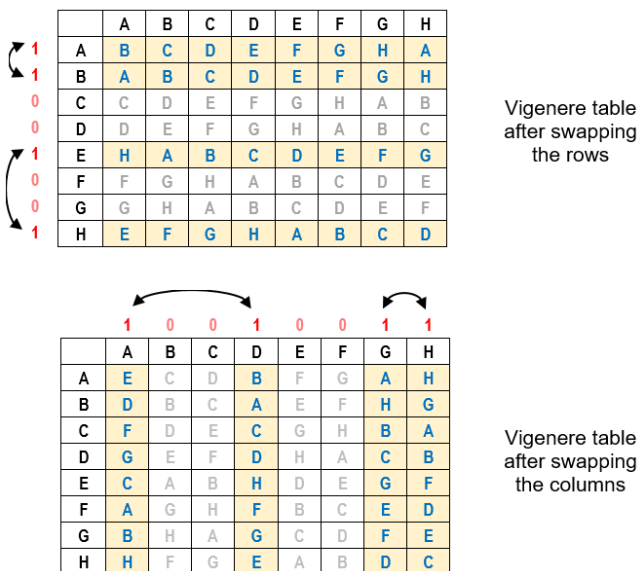
**Table 3.** The character set of the Vigenere square

| Character Description | Symbols   | ASCII code range |
|-----------------------|---|------------------|
| white space           |   | 32               |
| special characters    | ! ” # \$ % & ' ( * ) + , - . /                      | 33-47            |
| special characters    | : ; < = > ? @                                       | 58-64            |
| special characters    | [ \ ] ^ _ `   | 91-96            |
| special characters    | {   } ~   | 123-126          |
| numeric characters    | 0 1 2 3 4 5 6 7 8 9                                 | 48-57            |
| uppercase characters  | 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 | 65-90            |
| lowercase characters  | 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 | 97-122           |

includes special characters, numeric characters, upper- and lowercase alphabets whose ASCII character codes ranging from 32 to 126 as shown in Table 3. Thus, it will be difficult for the cryptanalysis to break the algorithm because 95 characters are taken instead of 26.

The idea behind this scheme is that before an encryption or decryption process takes place, the existing Vigenere square is being shuffled using the binary form of the tabula key. Reading the binary form from left to right, we swap the corresponding pair of rows where the occurrences of the pair of nonzero bits are positioned. Reading the binary form from right to left would allow us to swap the corresponding pair of columns in the table. Fig. 2 shows the manipulation process of the Vigenere table.

For example, if the tabula key is C9, its binary form is 11001001. From left to right, the 1st and 2nd rows are swapped, and then the 5th and 8th rows are swapped. From right to left, the 1st and 4th columns are swapped and the 7th and 8th columns are swapped too. If a certain row or column doesn't have a pair, that operation is skipped and proceeds with the next operation.



**Fig. 2.** Vigenere table manipulation process

The result of this operation should give us a good and nice scrambled Vigenere table that doesn't exhibit the order of the cycle in its original state. An attacker who knows the cipher key but doesn't have a clue about the tabula key would definitely have difficulty in cracking the code.

In order to determine the number of possible pair-swapping combinations that could be done in a square table, we use the formula:

$$\sum_{2 \leq k \leq n \text{ even}} \frac{n!}{(k!(n-k)!)} \tag{1}$$

where n is the total number of characters in the set and k is the total number of even numbers from 2 to n.

For example, an 8-by-8 matrix will give you 127 possible combinations because

$$\sum_{2 \leq k \leq n \text{ even}} \frac{n!}{(k!(n-k)!)} = \frac{8!}{(2!(8-2)!)} = 127$$

As used in this study, a character set of 95 is a large matrix that would yield a huge number of possibilities. That is,

$$\sum_{2 \leq k \leq n \text{ even}} \frac{n!}{(k!(n-k)!)} = \frac{95!}{(47!(95-47)!)} = 1.9807 \times 10^{28}$$

would provide us 1.9807x10<sup>28</sup> number of possible pair-swapping activities. This is a very large number in which it is difficult for the cryptanalysis to decode the matrix settings of a table.

### 3.3 The Algorithm Design

The Vigenere encryption algorithm is a very well-known multi-code encryption, in fact, it is a simplified form of auto-key cryptography, it is based on keywords, but it is not defined as using keywords like single-code keywords addition to the replacement in the form. This is the alternative of a multi-table encryption password that can be encrypted with different passwords on the same information in separate letters.

In this study, the encryption and decryption scheme will be in an iterative pattern encrypting or decrypting both the message and the cipher key using the newly scrambled Vigenere square. Fig. 3 shows the conceptual approach of the encryption and decryption process of the proposed algorithm design.

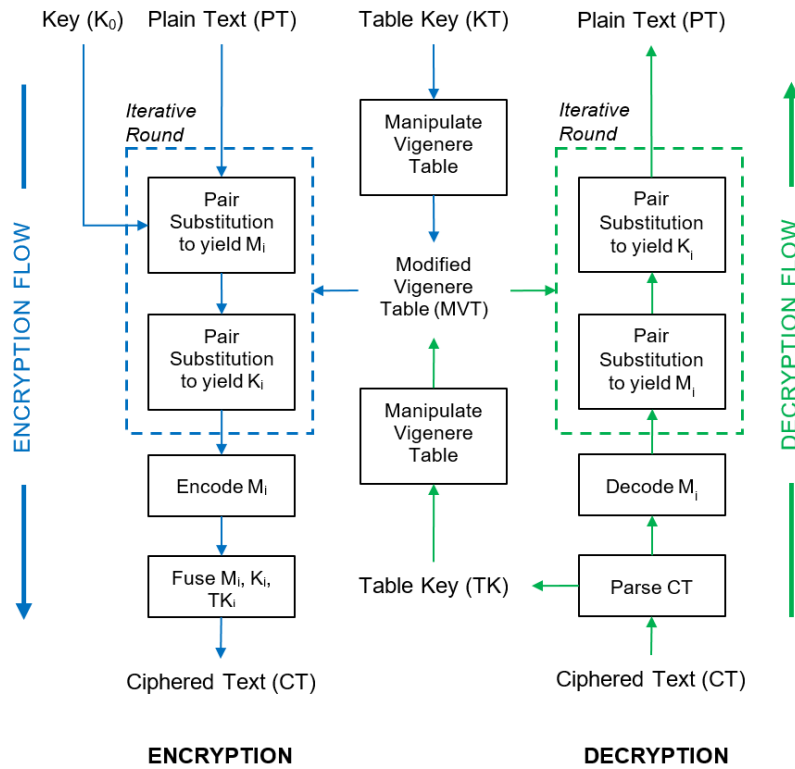


Fig. 3. Conceptual approach of the modified Vigenere cryptosystem

Fig. 4 illustrates the flow of the encryption process of the modified Vigenere cryptosystem. The encryption process starts with a random generation of the tabula key. The contents of the Vigenere table are then scrambled using the tabula key before acquiring input from the user for the plain text and the cipher key as well. Reading the characters from the file requires the size of the cipher key to be equal to the size of the plain text through a replication process. From here, each character of the message will be encrypted using this formula:  $EM_i = (PT_i + K_i) \bmod 95$ , where  $EM_i$  is the  $i^{\text{th}}$  character of the encrypted message,  $PT_i$  is the  $i^{\text{th}}$  character of the plain text and  $K_i$  is the  $i^{\text{th}}$  character of the cipher key.

The encryption process here is a loop operation that performs a substitution transformation on all characters of the plain message. Next, the plain text and the cipher key are interchanged using the following formulas:  $m = EM_i$ ;

$EM_i = K_{i-1}$ ; and  $K_i = EM_i$ , where  $m$  is a temporary storage for the encrypted message  $EM$  ( $m$  will be used to restore our encrypted message  $EM$  on the later part),  $K_{i-1}$  is the previous ciphered key on  $i^{\text{th}}-1$  encryption round and  $K_i$  is the current cipher key in the active iteration encryption round. The next process encrypts all the characters from the cipher key using the formula:  $K_i = (EM_i + K_i) \bmod 95$ . After two consecutive substitution transformations are done, the ciphered message is reverted back to its original content through the formula:  $EM_i = m$ . The whole procedure from reading the characters from files are repeated for 10 rounds. Once the 10th round is reached, the ciphered message is encoded using the Base94 encoder, and is fused with the ciphered key and the tabula key using the formula:  $CT = EM \& K \& HK$ . The outcome of this encryption process is one encrypted file.

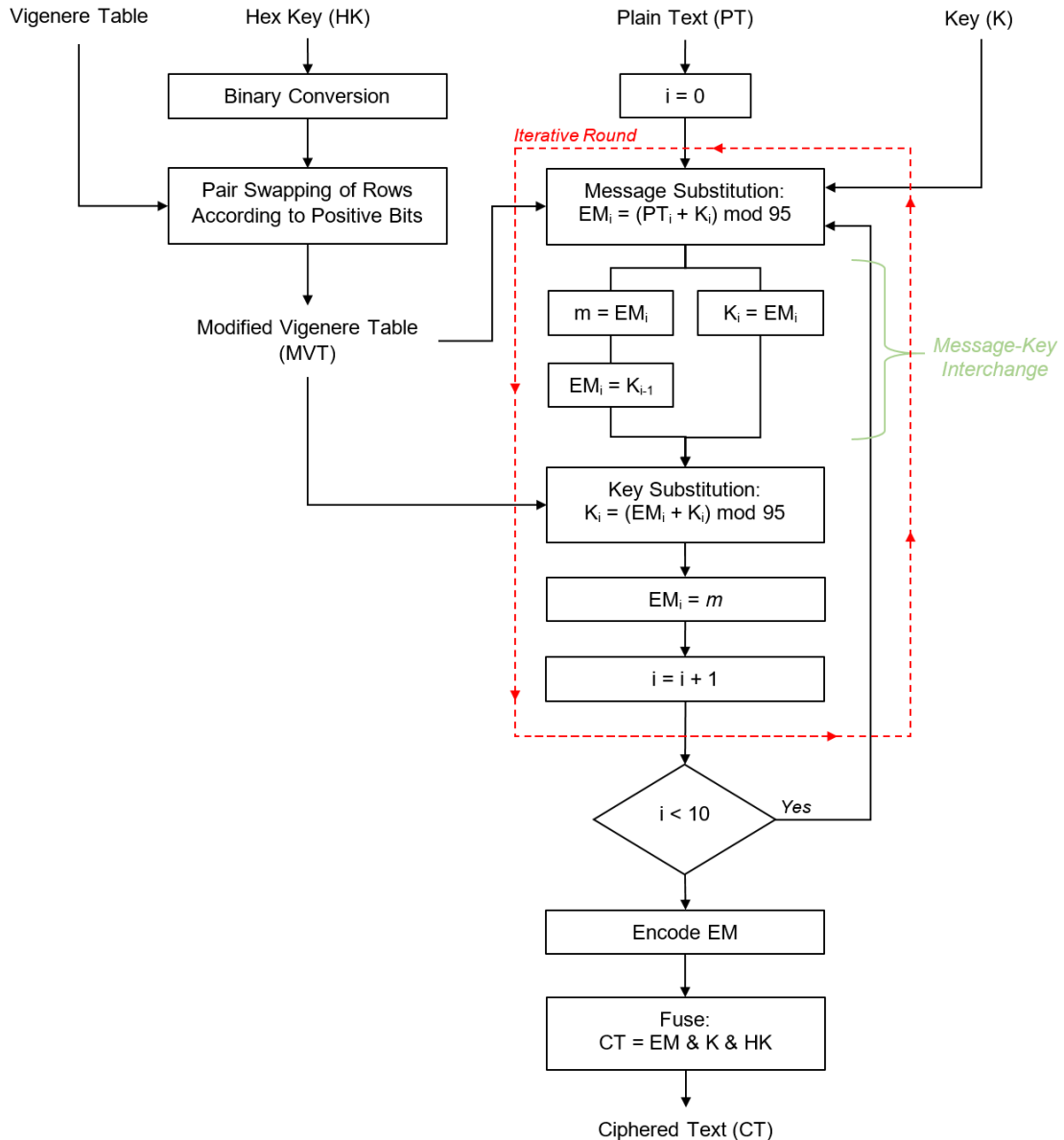


Fig. 4. Flowchart of the encryption process

In the decryption process, as shown in Fig. 5, the procedure is the reverse of the encryption method. It starts with the extraction of the ciphered message and keys of the encrypted file. The ciphered text is then decoded using the Base94 decoder.

The contents of the Vigenere table are then arranged according to its tabula key. During the 10 rounds of the decryption process, the ciphered key is first decrypted using the formula:  $K_i = (EM_i + K_i) \text{ mod } 95$ . After decrypting the key, the ciphered key and message are again interchanged through the following formulas:  $m = K_i$ ;  $EM_i = K_i$ ; and  $K_i = EM_{i-1}$ . The next process after this step is to decrypt the ciphered message using  $EM_i = (EM_i + K_i) \text{ mod } 95$ . After the

substitution process, the deciphered key is then reverted back to its original value. On the 10th iteration decryption round, the message including the key are revealed in its original form.

In general, every time the sender sends a message over a communication channel, the contents of the Vigenere table are freshly disarranged. It is important that the receiver receives the unaltered tabula key to unlock the right pattern of the table to be used in the decryption process. Both the tabula key and the ciphered keys are shared across the communication channel that are embedded within the encrypted file.



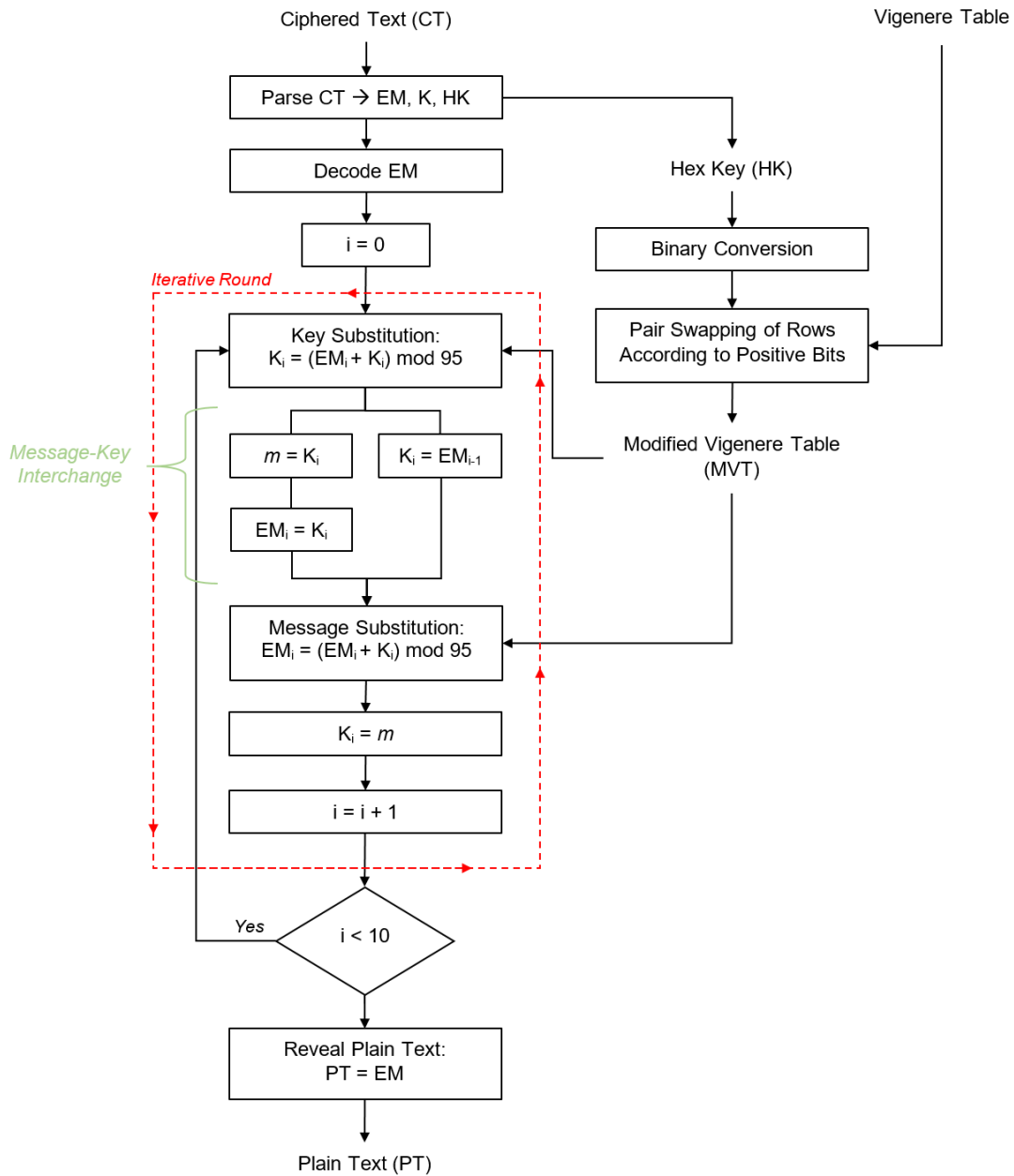


Fig. 5. Flowchart of the decryption process

### 3.4 Data Encryption Module for the Learning Management System

The learning management system uses the internet to distribute data and information. However, the internet as a backbone of any learning management system is prone to hardware and software attacks. Moreover, the LMS relies on its database management system to store and retrieve

vital information and knowledge about the learners and institutes or organizations.

In order to ensure the security of the data and information stored in a database management system, the proponents have developed a data encryption module using the modified Vigenere cryptosystem, as depicted in Fig. 6, as a plug-in method that works independently of the application.

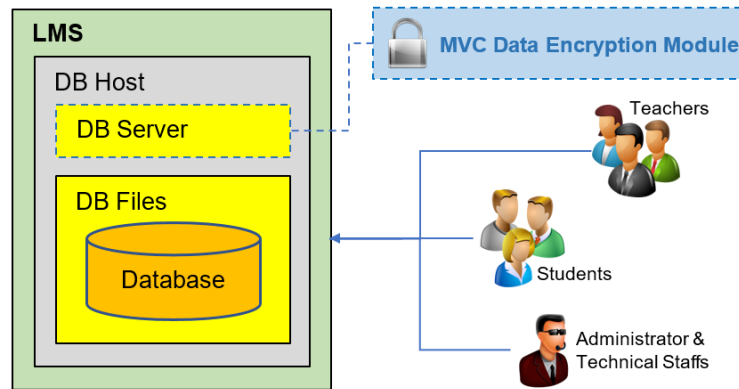


Fig. 6. Integrating the modified Vigenere cryptosystem as data encryption module

Encrypting all the data in the database of an LMS would be impractical because this would perceive as an “extra” security step that comes with added design complexity and potential performance degradation. To overcome this issue, a recommended encryption level is determined and applied only on specific and sensitive data that are defined in the policies and procedures formulated by the security group of the institution. In this case, administrators’, students’, and teachers’ accounts that contain their password use column-level encryption, while its corresponding records could be optionally encrypted in tablespace-level. A mandatory “transparent encryption” of the entire database will only be done when the data are at rest for conducting backup operations and system maintenance.

#### 4. RESULTS AND DISCUSSIONS

Every encryption technique has its own strengths and weaknesses. The analysis of these techniques based on several features is critically necessary. In this experiment, the proponent used the Avalanche effect to analyze the performance and security of the modified Vigenere algorithm against the original. The following formula is used in this experiment:

$$Avalanche\ Effect = \frac{No.\ of\ Chars\ Changed\ in\ Ciphered\ Text}{Total\ No.\ of\ Chars\ in\ Ciphered\ Text} \times 100 \quad (2)$$

In this section, the modified Vigenere cryptosystem has been compared with the original Vigenere cryptosystem using the Avalanche effect as a performance metric. Considering various case scenarios on the simulation, the input data for both versions of the encryption techniques were randomly altered on its plain text, cipher key, and the tabula key by changing the bit information from a single bit to eight bits in range.

The first simulation was conducted by changing the bit information in the plain text on a random location of the string. In Fig. 7, the result shows that the modified version has a higher Avalanche effect over the original version ranging from 17% to 19%, that is, 25 to 29 bits of information were altered out of 152 bits of the plain text.

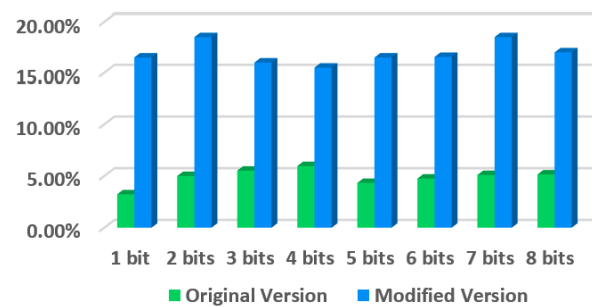


Fig. 7. Avalanche effect on the bit change on the plain text

The next simulation conducted was to determine the Avalanche effect with regards to their alterations on their cipher key on random locations. Fig. 8 depicts the result of changing the bit information of the cipher key. The results show that the Avalanche effect of altering the cipher key of the modified version is higher than that of the original version. As an observation, 34% to 44% of the bit information of the modified version’s cipher key is altered during the simulation.

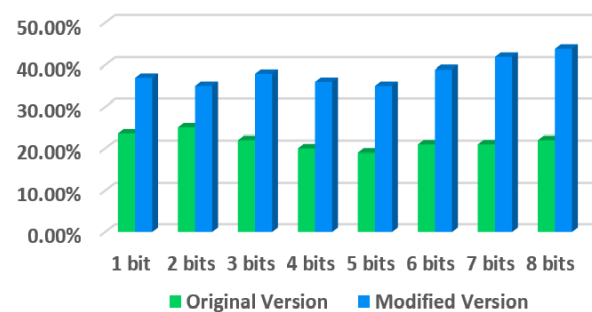


Fig. 8. Avalanche effect on the bit change on the cipher key

The final simulation was carried to determine the Avalanche effect if the tabula key is being altered. Since the original version doesn’t have this type of key, the modified version was tested instead. Fig. 9 shows the graphical result of the Avalanche effect when a tabula key is modified. It shows that by flipping the bits, more than 60% of the encrypted bit information will definitely change.



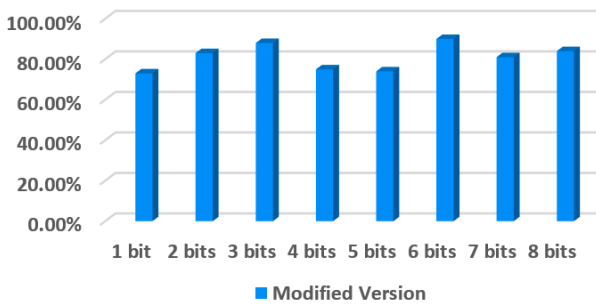


Fig. 9. Avalanche effect on the bit change on the cipher key

The graph depicted in Fig. 10 summarizes the overall result of the Avalanche effect of both versions of the Vigenere encryption techniques used in this study.

Based on the overall result, the modified Vigenere cryptosystem offered quality and higher security compared to the original Vigenere cryptosystem due to its high Avalanche effect on the three categories of the simulation.

### 5. CONCLUSIONS

In this paper, a modified version of the Vigenere cryptosystem has been designed and introduced using matrix manipulation of the Vigenere square and Base94 encoding scheme. The design also integrates a scheme that performs iterative rounds of substitution transformation of the message and the key. The modified Vigenere cryptosystem showed a high Avalanche effect as compared to the traditional Vigenere encryption algorithm. With this encryption method, it is obvious that the MVC has a property that offers additional protection and improves the quality of security of the database management system of the LMS that is flexible and requires less code management and modification because it works independently of the application.

This research opens up many possible avenues for future investigation. One particular area in this study could involve the combination of more efficient encryption algorithms such as the advance encryption standard (AES) or rivest-shamir-adleman (RSA) to increase the complexity and level of security. Another area for refinement that could be considered is an integration of a compression scheme to reduce the size of the encrypted data being generated. Other encoding schemes could be considered to suit different applications or operating system platforms. The matrix manipulation scheme doesn't end here, there are better ways to shuffle the contents of the Vigenere square with a better random value distribution.

### ACKNOWLEDGMENT

This paper has been supported and funded by the University of Antique.

### REFERENCES

- Aakash, Soni, J.K., Sharma, B. 2017. A.J. Cipher. 2017 2nd International Conference on Telecommunication and Networks (TEL-NET), Noida, 1–6, doi: 10.1109/TEL-NET.2017.8343547.
- Danuputuri, C., Mantoro, T., Hardjianto, M. 2015. Data security using LSB steganography and vigenere cipher in an adroid environment. 2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec), Jakarta, Indonesia, 22–27, doi: 10.1109/CyberSec.2015.14.
- Fahrianto, F., Masruroh, S.U., Ando, N.Z. 2014. Encrypted SMS application on android with combination of caesar cipher and vigenere algorithm. 2014 International Conference on Cyber and IT Service Management (CITSM), November 3–6, 2014, South Tangerang, Indonesia, 31–33, doi: 10.1109/CITSM.2014.7042170.

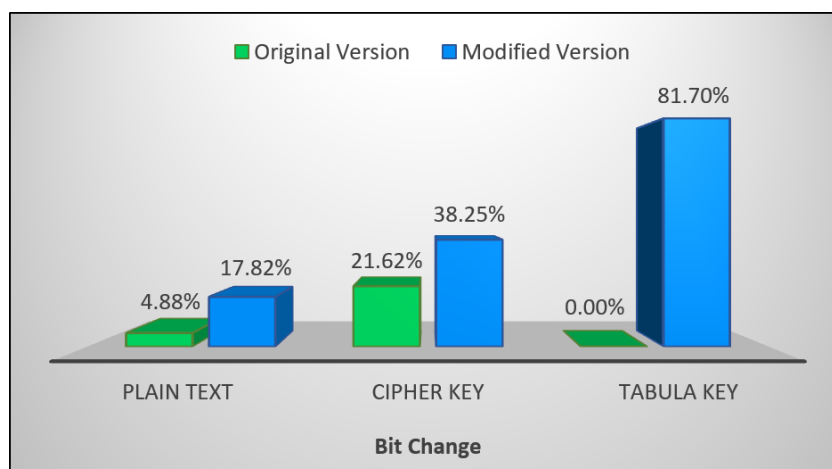


Fig. 10. Overall result of the Avalanche effect

- Gerhana, Y.A., Insanudin, E., Syarifudin, U., Zulmi, M.R. 2016. Design of digital image application using vigenere cipher algorithm. 2016 4th International Conference on Cyber and IT Service Management, Bandung, Indonesia, 1–5, doi: 10.1109/CITSM.2016.7577571.
- Hossain, M.S., Islam, M.T. 2018. An extension of vigenere technique to enhance the security of communication. 2018 International Conference on Innovations in Science, Engineering and Technology (ICISSET), Chittagong, Bangladesh, 79–85, doi: 10.1109/ICISSET.2018.8745638.
- Sermeno, J., Secugal, K.A., Mistio, N. 2020. Modified vigenere cryptosystem using matrix manipulation and base94 encoding scheme. 2020 International Conference on Innovative Technology Convergence (ICITC 2020). Journal of Innovative Technology Convergence, 2, ISSN No. 2704-4440.
- Thorsteinson, P., Ganesh, G.G., 2003. NET security and cryptography (First Edition). USA, Prentice Hall, ISBN: 013100851X.
- Touil, H., Akkad, N.E., Satori, K. 2020. Text encryption: Hybrid cryptographic method using vigenere and hill ciphers. 2020 International Conference on Intelligent Systems and Computer Vision (ISCV), Fez, Morocco, 1–6, doi: 1109/ISCV49265.2020.9204095.
- Trappe, W., Washington, L.C. 2006. Introduction to cryptographic with coding theory (2nd edition). Prentice Hall.
- Triandi, B., Ekadiansyah, E., Puspasari, R., Iwan, L.T., Rahmad, F. 2018. Improve security algorithm cryptography vigenere cipher using chaos functions. 2018 6th International Conference on Cyber and IT Service Management (CITSM), Parapat, Indonesia, 1–5, doi: 10.1109/CITSM.2018.8674376.