Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th June 2025. Vol. 4. No. 3; e-ISSN: 2808-4519

Application of Modified Vigenere Cipher Cryptography Technique in Text Data Encryption in Web Based Applications

Romanus Damanik[1]*, Hardiman Ruhut M. Simamora [2], Bersama Sinuraya[3], A M H Pardede[4]

[1,2]*Universitas Katolik Santo Thomas Medan*
[3]*Universitas Mandiri Bina Prestasi*
[4]*STMIK Kaputama*
rdfikom@gmail.com[1*], hardimansimamora@gmail.com[2], bersamaraya@gmail.com[3], akimmhp@Live.com[4]

Abstract

The development of information technology in today's digital era has brought rapid progress, especially in terms of data security which is a major concern in various sectors. In securing data or information, the application of cryptographic techniques is becoming increasingly important. The vigenere cipher algorithm is one of the classic cryptographic methods widely used for text encryption. However, the standard form of encryption algorithm has weaknesses, especially in terms of its vulnerability to frequency analysis attacks that can be used to break the encryption pattern if the key used is repeated.
This research aims to design and implement a modified Vigenere cipher on a web-based application to improve encryption security. The designed web-based application is a password manager that is used as a test to show what the application of the vigenere cipher modification looks like in an application. The password manager application designed has the features of registering, logging in, storing, managing, and securing various passwords and login information for websites, applications, or online services. sensitive data in this application such as login information is encrypted before being stored in the database and decrypted when displayed to the user.This implementation is expected to show the application of the Vigenere Cipher modification in securing data in web-based applications.

Keywords: *Information Technology, Data Security, Cryptography, Vigenere Cipher, Encryption, Web-based Application*

1. Introduction

With the rapid advancement of technology, digitalization has spread to various sectors of life such as education, government, banking, and other sectors. This digital transformation has brought many benefits, including increased operational efficiency, faster access to information, and better services. However, behind all this progress, the threat of cyber attacks continues to increase significantly. These attacks target critical data across various systems, from individuals and small businesses to large organizations [1].

According to data from the National Cyber and Cryptography Agency (BSSN), there were 403 million traffic anomalies or cyber attacks targeting Indonesia throughout 2023. This figure highlights the high risks faced by organizations and individuals in protecting their sensitive data. Cyberattacks can cause significant losses, as personal data, financial information, and trade secrets are often the primary targets. In such situations, data protection is a critical aspect for maintaining the confidentiality and integrity of information [2].

One effective way to secure data is through cryptography. Cryptography is the study of data security techniques, making information difficult to access or manipulate by unauthorized parties. One of the most widely used classical cryptographic methods is the Vigenère cipher, a substitution technique that encrypts text using a specific key. Although the Vigenère cipher is effective for encrypting text, the standard form of this encryption algorithm has weaknesses, such as its vulnerability to frequency analysis attacks, which can be used to break the encryption pattern because the key used is repeated.

Therefore, modifications to the Vigenère cipher are important to strengthen this encryption algorithm, making it more difficult for unauthorized parties to break. Modifications can be made by introducing dynamic keys and adding a shift stage to the Vigenère cipher encryption results over a specified number of steps. With these modifications, the encryption pattern becomes more complex, making it safer when applied to data security in application systems. This innovation is expected to address the weaknesses of the classical Vigenere Cipher and enhance its reliability in safeguarding data confidentiality [3].

Data security in text-based applications is a critical aspect, as applications often handle highly important and sensitive information. During data storage through application systems, without strong encryption, information can easily be intercepted or manipulated by unauthorized parties. By implementing the Vigenere Cipher innovation with additional shifting mechanisms and dynamic keys, the encryption process becomes stronger and more difficult to break. This is expected to provide greater protection for data sent and received through the application system, especially when sensitive information is involved.

As a test of the modified Vigenere Cipher implementation, a web-based password manager application was developed. This web-based application is designed to allow users to store accounts, various passwords, and login information for various websites, applications, or online services. In this web application, users' sensitive information will be encrypted using the modified Vigenere Cipher, and the encrypted results will be stored in a database. This web application was created to demonstrate how important data is secured by encrypting it before it is stored in the database.

This research aims to explore how modifications to the Vigenere Cipher can be applied to encrypt text data in web-based applications.

2. Research Method

There are several stages involved in this research. These include dataset gathering, data preparation, model creation, model conversion, and Android app creation.

2.1. Vigenere Cipher

The Vigenère cipher algorithm is part of polyalphabetic cryptography, first discovered in 1586 by French diplomat Blaise de Vigenère (1523-1596). The Vigenère cipher is the simplest type of polyalphabetic cipher. It employs a polyalphabetic substitution method and falls under the category of symmetric keys, where the key used for encryption is the same as the key used for decryption. The primary purpose of the Vigenère cipher is to hide the connection between plaintext and ciphertext by using a keyword [4], [5].

To determine the character shift, the Vigenère cipher uses a standard Vigenère table to encrypt the message. The table used is a standard 26-letter alphabetical table, starting from A to Z. The key in the Vigenère cipher is repeated as many times as the number of messages to be encrypted. The more diverse the alphabetical letters used as the key, the stronger the security of the Vigenère cipher algorithm. Here are the encryption and decryption formulas for the Vigenère cipher [7].
Encryption: Ci = Pi + ki mod 26…….... (1)
Decryption: Pi = Ci - ki mod 26……(2)

2.1.1. Encryption Vigenere Cipher

Encryption is the process of converting plaintext into ciphertext. To perform encryption using the Vigenere method, the easiest way is to use a Vigenere table. Here is an image of a Vigenere table:

	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: Table Vigenere

For example, if we encode or encrypt a text message using the Vigenère cipher, such as the text message “MAHASISWA,” and the key between the sender and recipient is “UNIKA,” since there are 9 letters, the cipher will be repeated as UNIKAUNIK. Adjust the key repeatedly according to the number of words in question. In the table, M corresponds to U at the letter ‘G’, then A corresponds to N at the letter ‘N’, and so on.
Original Text: MAHASISWA
Keyword: UNIKAUNIK
Vigenère Result: GNPKSCFEK
Thus, the Vigenère cipher encryption result using the Vigenère table is “GNPKSCFEK”.

2.1.2. Decryption Vigenere Cipher

In addition to the encryption process, there is also a decryption process in this technique that converts the resulting ciphertext into plaintext or original text so that the text data can be understood by users who use the system following the process of converting ciphertext into plaintext if we use the Vigenère table. To decrypt a message that has been encrypted using the Vigenère cipher method, we follow a process that is basically the reverse of encryption. First, we need the same Vigenère table used during encryption and the corresponding keyword.

Suppose the encrypted message is “GNPKSCFEK” and the keyword used is “UNIKA.” The first step is to repeat the keyword so that its length matches the length of the encrypted text, resulting in “UNIKAUNIK.” Next, for each letter in the encrypted text, we find the original letter by referring to the Vigenère table. For example, if the encrypted letter is ‘G’ and the letter in the keyword is ‘U’, we look for the

letter at position 'G' in the 'U' row of the Vigenère table. This process is repeated for each letter. By performing this search, we can decrypt the letters into 'M', 'A', 'H', 'A', 'S', 'I', 'S', 'W', and 'A', resulting in the original text "MAHASISWA". This process ensures that the encrypted text can be converted back to its original form using the same method and table to maintain consistency and accuracy of the decrypted data.

2.1.3. Modification of Vigenere Cipher Cryptography

The Vigenère cipher is one of the classic cryptographic methods that encrypts text by shifting each letter based on a key that is repeated throughout the text according to the alphabetical order. Although considered strong, the standard encryption technique of this method has several weaknesses and is vulnerable to certain attacks, one of which is frequency analysis. Frequency analysis is a cryptanalysis technique that can be used to break the Vigenère Cipher by exploiting patterns in the occurrence of letters in the ciphertext, thereby enabling unauthorized parties to predict the key used.

To address these weaknesses, innovations or modifications are required. In this study, modifications were made by applying a dynamic key, where the key repetition is taken from the original text (plaintext) to be encrypted. Additionally, two additional shifts of the standard Vigenère Cipher encryption result were added after the initial encryption process with the dynamic key was completed.

With these two additional shifting stages, the encryption pattern becomes more complex and harder to break, making this method more secure when used to protect data in application systems. With the innovations and modifications made to the standard encryption results, the encryption pattern becomes more complex and can be made more secure when applied in data protection within application systems. It also addresses the weaknesses of the Vigenère Cipher and enhances its reliability.

2.1.4. The Encryption and Decryption Process of the Modified Vigenere Cipher

The encryption and decryption processes of the modified Vigenere Cipher are similar to those of the standard method, which utilizes substitution tables and basic encryption equations. In this modification, there are two main modifications.

The first modification is the use of a dynamic key. In the standard Vigenere Cipher encryption, the key is adjusted to the length of the original text (plaintext). If the key length is shorter than the plaintext length, the key is repeated until it matches the plaintext length. However, in this modification, the key repetition is not taken from the initial key but from the letters in the plaintext itself. For example, if we have the plaintext "mahasiswa" with the initial key "unika," the key repetition to match the plaintext length would be "unikamaha."

After applying the dynamic key, the second modification is the addition of two extra shifts to the standard Vigenère Cipher encryption result after the initial encryption process. For example, with the plaintext "mahasiswa" and the dynamic key "unikamaha," the standard encryption result is "gnpksusda." By applying two additional shifts to this standard encryption result, the final ciphertext is obtained, which is "iprmuwufc."

After the encryption process is complete and the ciphertext is obtained, the next step is to convert the ciphertext back into plaintext using the modified Vigenere Cipher on the generated ciphertext, which is "iprmuwufc." This decryption process involves two main steps, similar to the encryption process: reversing the additional two-step shift and performing standard decryption with the dynamic key.

The first step is that, since the initial result of the Vigenere Cipher in the encryption process was shifted two steps forward, to decrypt we need to reverse that shift by shifting each ciphertext letter two steps backward in the alphabet. From this step, we obtain the intermediate result "gnpksusda," which is the ciphertext generated by the standard Vigenere Cipher encryption before the additional shift was applied.

The second step is standard Vigenere Cipher decryption using the dynamic key "unikamaha." This dynamic key is obtained by extending the initial key 'unika' to match the length of the plaintext "mahasiswa," which is the expected original result. In standard decryption, each ciphertext letter resulting from standard encryption is reduced by the corresponding letter position in the dynamic key, followed by mod 26 to keep the result within the A-Z alphabet. After performing these steps, the plaintext or original text "mahasiswa" is recovered.

3. Results and Discussion

At this stage, the system display or user interface of the designed web-based password manager application is implemented. The password application is implemented only as a test or general overview for the application of Vigenère cipher cryptography techniques in an application. The encryption and decryption modules that have been built are applied to this password manager application system. Data from the interface entered by the user is forwarded to the backend or API, where the data is encrypted using the modified Vigenère cipher module that has been built and stored in the database. The interface that will be applied to this application can be seen in the image below.

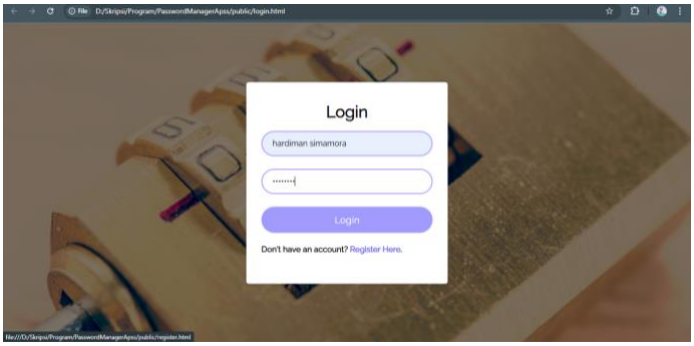

Fig. 2: User Interface Login Page

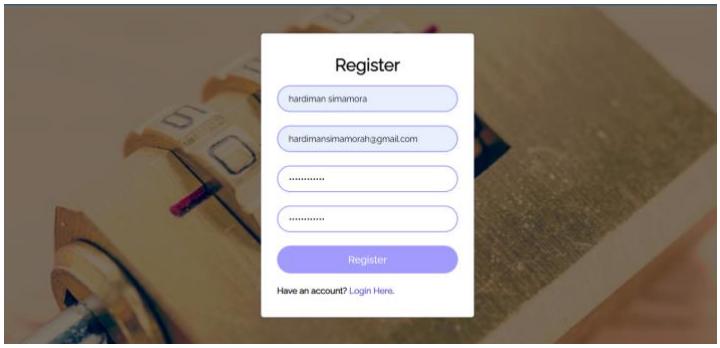

Fig. 3: User Interface Register Page

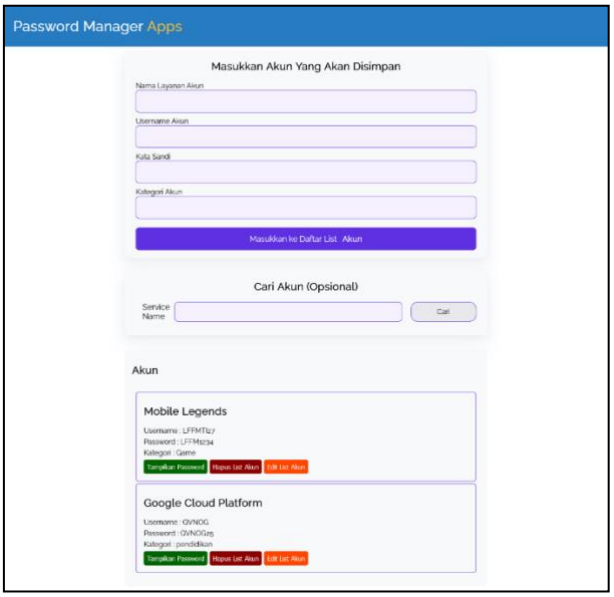

Fig. 4: User Interface Home Page

After that, testing was carried out to determine whether the features in the password manager application were working properly. The functionality of this application was tested using the black box testing method.

Table 1: Functionality Test Results

Test Description	Input	Expected Results	Result
Using the Login feature	Enter a valid username and password	Users can log in by entering a valid username and password.	successful
Using the registration feature	Enter your username, email address, password, and confirm your password.	Users can register by entering their username, email address, password, and password confirmation.	successful
Using the Add Data feature	Enter the account service name, account username, password, and account category.	Users can add login information (account service name, account username, password, account category) from accounts used on various websites.	successful

ing the account data search feature	Enter some letters based on the name of the account service you are looking for.	Users can search for login information from accounts that have been entered by users.	successful
Using the show password feature	Data entered by users when adding account login information	The original data/plaintext entered by the user is displayed on the main page when clicking the "show password" button. Data entered by the user when adding account login information.	successful
Using the Delete Data feature	Data entered by users when adding account login information	Users can delete stored account login information by clicking the delete account list button.	successful
Using the Data edit feature	Enter new data, namely account service name, account username, password, account category	Users can edit stored account login information by clicking the edit account list button.	successful

Then there is Encryption and Decryption Testing. This test is conducted to ensure that the encryption and decryption modules implemented in the password manager application are functioning properly or in accordance with the designed criteria. The test is conducted by taking data from the registration results that have been carried out with encryption keys generated by the system through manual calculations by applying modifications to the Vigenère cipher.

Table 2: Comparison of manual and system calculation results

Perhitungan	Plaintext	Dynamic key	Encryption	decryption
System	andrewdamanik23	CZGCGQVXANDREW	EOLVMOAZOPSBQ3	andrewdamanik3
Manual	andrewdamanik23	CZGCGQVXANDREW	EOLVMOAZOPSBQ3	andrewdamanik3

From the comparison of the results in the table above, it can be seen that the manual calculation and the system results are the same, so it can be concluded that the encryption and decryption module using the modified Vigenère cipher applied to the password manager application system is successful and works well.

4. Conclusion

The standard Vigenère cipher is still vulnerable to frequency analysis attacks, because the repeated use of the same key allows crackers or attackers to see patterns in the decryption results.

By modifying the standard Vigenère cipher—specifically, by implementing a dynamic key and adding a stage to shift the standard encryption output—one of the weaknesses of the Vigenère cipher against frequency analysis, which attackers could exploit, can be reduced. The results of this modification show that eliminating the repetitive nature of the standard Vigenère cipher key makes it more dynamic, as the key is derived from the plaintext letters. Attackers must identify patterns and determine the two-step shift applied to decrypt the original message.

References

[1] Putra, N. B., Andika, B. C., Purba, A. D., & Ridwan, M. (2023). Implementasi Sandi Vigenere Cipher dalam Mengenkripsikan Pesan. JOCITIS-Journal Science Infomatica and Robotics, 1(1), 42-50.

[2] Fajri, G. R., Sembiring, E. H., & Hasan, M. A. (2020). Keamanan data pada pengarsipan surat menggunakan metode kriptografi klasik vigenere cipher dan shift cipher. ZONAsi: Jurnal Sistem Informasi, 2(1), 61-72.

[3] Ziaurrahman, M., Utami, E., & Wibowo, F. W. (2019). Modifikasi Kriptografi Klasik Vigenere Cipher Menggunakan One Time Pad Dengan Enkripsi Berlanjut. Informasi Interaktif, 4(2), 63-68.

[4] Bale, A., Ghorpade, N., K, B., Hashim, M., H., C., & R, H. (2023). Modifikasi Cipher Vigenère untuk Mengatasi Serangan Kasiski dan Friedman. Konferensi Internasional Pertama tentang Sirkuit, Daya, dan Sistem Cerdas (CCPIS) 2023 , 1-5. https://doi.org/10.1109/CCPIS59145.2023.10291990.

[5] Hardita, V. C., & Sholeha, E. W. (2021). Penerapan Kombinasi Metode Vigenere Cipher, Caesar Cipher Dan Simbol Baca Dalam Mengamankan Pesan. Jurnal Saintekom: Sains, Teknologi, Komputer dan Manajemen, 11(1), 34-43..

[6] D. Niyigena, C. Habineza, and T. S. Ustun, "Computer-based smart energy management system for rural health centers," 2016, doi: 10.1109/IRSEC.2015.7455005.

[7] Pardede, A. M. H., Manurung, H., & Filina, D. (2017). Algoritma Vigenere cipher dan Hill cipher dalam aplikasi keamanan data pada file dokumen. *JTIK (Jurnal Teknik Informatika Kaputama)*, *1*(1), 26-33.