Jurnal Minfo Polgan (JMP)
Volume 15, Nomor 2, Mei-Agustus 2026
DOI : https://doi.org/10.33395/jmp.v15i2.16148
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Implementation of Symmetric Key Cryptography Algorithm Using Vigenere Cipher Method for Data Security

[1]Nadia Widari Nasution, [2] Okki Kurnia, [3]Devid Trinaldo Simatupang, [4]Syahelma Fithri
[1*]Bisnis Digital, Institut Teknologi Batam, Batam, Indonesia
[2,3]Kewirausahaan, Institut Teknologi dan Bisnis Indobaru Nasional, Batam, Indonesia
[4]Sistem Informasi, Institut Teknologi Batam, Batam, Indonesia
**Korespondensi*: widari@iteba.ac.id

Submit : 27 April 2026 | **Diterima** : 24 Mei 2026 | **Terbit** : 30 Mei 2026

ABSTRACT

Confidentiality when sending text messages is a crucial aspect in today's information technology era. Data is a crucial asset that must be protected because it plays a strategic role in maintaining the continuity of an information system. Therefore, data security is a crucial aspect in information management. One way to maintain data security is through the application of cryptographic techniques. To secure data using cryptography, encryption and decryption are required. Encryption and decryption are two main processes in cryptography. Encryption is the process of scrambling original data into an unreadable secret code, while decryption is the reverse process, namely restoring the secret code to the original, understandable data. This research is limited to basic-level protection using the Python programming language.

Keywords*: Decryption, Encryption, Data Security, Cryptography, Vigenere Cipher*

ABSTRAK

Kerahasiaan saat mengirim pesan teks merupakan aspek yang sagat penting di era teknologi informasi saat ini. Data merupakan aset penting yang harus dilindungi karena memiliki peran strategis dalam menjaga keberlangsungan suatu sistem informasi. Oleh karena itu, keamanan data menjadi aspek yang sangat krusial dalam pengelolaan informasi. Salah satu upaya untuk menjaga keamanan data adalah melalui penerapan teknik kriptografi. Untuk mengamankan data menggunakan kriptografi, diperlukan enkripsi dan dekripsi. Enkripsi dan dekripsi adalah dua proses utama dalam ilmu kriptografi. Enkripsi adalah proses mengacak data asli menjadi kode rahasia yang tidak dapat dibaca, sedangkan dekripsi adalah proses kebalikannya, yaitu mengembalikan kode rahasia tersebut menjadi data asli yang dapat dipahami. Penelitian ini hanya terbatas pada perlindungan tingkat dasar menggunakan bahasa pemrograman Python.

Kata Kunci: Dekripsi, Enkripsi, Keamanan Data, Kriptografi, Vigenere Cipher

INTRODUCTION

Information security is a crucial issue in the digital world. Databases primarily utilize computer application technology and require server computers to store information for operations. It can be concluded that computer media is a crucial factor in data security. The biggest issue concerns not only data stored on computers, but also the security of data transmitted over computer networks and applications to computers, as well as the security of data stored in databases (Ridho et al., 2023).

One approach that has proven effective is the application of cryptography technology, the process of encrypting data so that only certain parties with the decryption key can access the information (Aditya & Romli, 2025). Cryptography is an alternative solution for data security or digital messages, which can encode information into another form. In general, cryptography consists of two main parts: encryption and decryption. In the process, the sender and recipient of information will agree on a key to carry out the encryption and decryption processes. In the encryption process, the sender converts a message in the form of information (plaintext) into a message in another, difficult-to-understand form (ciphertext) using the key, while the decryption process is the process of returning the difficult-to-understand message to understandable information using a key (Susila Bahri∗, 2023).

According to Bruce Scheiner in his book "Applied Cryptography", cryptography is a science and art to keep data of message safe. The principles are underlying cryptography as follows (Nasution et al., 2020):

1. Confidelity
2. Data Integrity
3. Authentication
4. Non-Repudiation

One type of cryptography is classical cryptography. This cryptography uses very simple encryption techniques, resulting in a relatively low level of security and is easily cracked by unauthorized parties. To address this issue, a encryption technique is needed that can increase message security, namely super encryption. This technique is a combination of substitution and transposition encryption techniques. In this study, the Vigenère Cipher, a substitution encryption technique, was combined with the Route Cipher, a transposition encryption technique. These two techniques were chosen because they not only increase message security but are also relatively easy to implement on a computer.

The Vigenère Cipher technique performs encryption using the Vigenère table. The advantage of the Vigenère Cipher over previous classical methods is that its substitution for ciphertext is polyalphabetic, meaning the same character can have different substitution characters. However, this technique has a weakness: the number of characters in the plaintext will result in the same number of key characters, because the distance between the two numbers of words is a multiple of the number of keys used.

In the fields of cryptography and computing, the American Standard Code for Information Interchange (ASCII) is a basic character encoding standard widely used to support digital data communication processes. This standard was developed from the telegraph code and was first conceptualized on October 6, 1960, at the inaugural meeting of the American Standards Association (ASA) (Yuslita Dewi et al., 2025).

The objective of this research is to design data security in cipher message encryption and to protect and maintain data confidentiality using the Vigenère Cipher algorithms. In this research, the Vigenère Cipher algorithms will be implemented using the Python programming language. The Vigenere cipher is capable of providing security for text messages sent through various messaging platforms, so that users do not need to worry about their confidential messages being leaked (Rachmadsyah et al., 2020). This research is expected to make a tangible contribution to improving the security of school information systems while strengthening the integrity of student academic data (Jefry G G Saragih, 2025).

In addition, several studies in Indonesia have also compared the performance of the Vigenère algorithm with modern cryptographic algorithms such as RSA, showing differences in the level of security and efficiency in the context of digital data processing (Anzari et al., 2025).

METHODS

At this stage, the researcher designed a research framework including several stages as shown in Figure 2 below (Bima Putra et al., 2023).

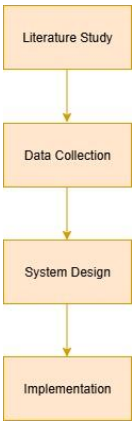

Figure 1. Research Framework

A. Literature Study

This study examines the methodology of a literature review, specifically a literature review to obtain references on cryptography and the Vigenère Cipher methods.

B. Data Collection
The researcher collected data through previous research on cryptography, specifically the RSA algorithm, and journals related to the research topic.

C. System Design
At this stage, the Vigenère Cipher cryptography system was designed by implementing the Python programming language.

D. Implementation
In this stage, the program is implemented using the method of executing the previously created program and encrypting the message.

Vigenere Cipher Algorithm

The Vigenere cipher algorithm was introduced in 1586 for the first time by the French cryptologist Blaise De Vigenere (Faris et al., 2023). The Vigenère Cipher is a polyalphabetic substitution cipher that is performed by adding each plaintext character index to the key character index based on the Vigenère Square or Vigenère Tableau. Figure 1 illustrates the Vigenère Square.

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

Figure 2. Vigere Cipher

The Vigenère table contains the alphabet written in 26 rows, each row shifted one order to the left from the previous row, forming the 26 possible Caesar ciphers. Each letter is encoded using a different row, corresponding to a repeated keyword. This cipher is widely known for its easy-to-understand and easy-to-execute operation, and for beginners, it is difficult to crack. The Vigenère Cipher technique can be implemented in two ways: using numbers and using letters (Amalia Zebua, 2022).

1. Number
   This technique is almost the same as the sliding technique or substitution technique by replacing letters with numbers.
2. Alphabetic
   Another method for encrypting the Vigenère Cipher is to use the tabula recta (also called the Vigenère square). Here's how to encrypt the Vigenère Cipher using letters, using the Vigenère Cipher table.

The encryption steps based on the Vigenère Cipher are:

1. Use the Vigenère Cipher table.

2. The table contains the alphabet written 26 times in different rows, with each letter shifted to the left relative to the previous letter, corresponding to the 26 possible Caesar Ciphers.
3. For each different letter in the encryption process, the coder uses a different alphabet from one of the rows.
4. The alphabet used for each letter is matched to the recurring keyword.

The steps for describing the Vigenère Cipher are:

1. Connect the first letter of the ciphertext to the first letter of the keyword on the line.
2. Drag to the right until you find the ciphertext.
3. Drag up to get a new letter from the table, which becomes the first letter of the plaintext, and so on.

The encryption and decryption processes using the Vigenère Cipher can be summarized as follows:

$$C_i = E_k(P_i) = (P_i + K_i) \bmod 26$$
$$P_i = D_k(C_i) = (C_i - K_i) \bmod 25$$

Vigenère Cipher Encryption and Decryption Flow

The encryption process flow occurs when a plaintext or original text is inputted with a key, then the encryption process is carried out or the process of converting a text into a code or cipher form, then it will produce a cipher text (ciphertext). Then the decryption process occurs when the ciphertext or coded text is inputted using the same key, then the decryption process is carried out, namely the process of converting the cipher or code into the original text form, then it will produce the original text, then it will produce the original text (plaintext) (Karima et al., 2024).

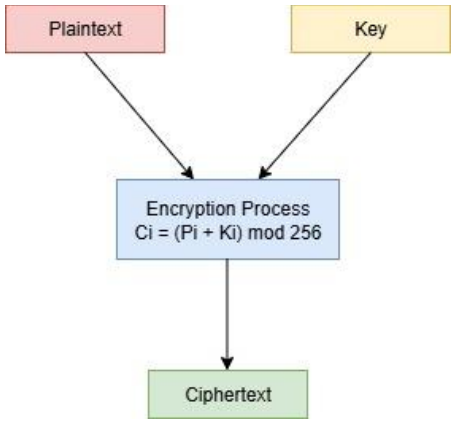

Figure 3. Vigenere Cipher Encryption Process Flow

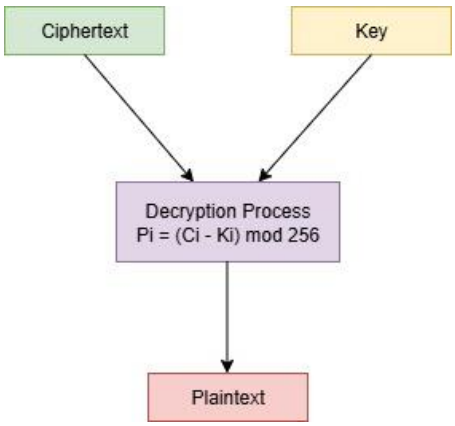

Figure 4. Vigenere Cipher Decryption Process Flow

The encryption and decryption algorithms in the Vigenère Cipher have several characteristics, namely:

1. It only accommodates 26 letters of the alphabet in lowercase, while other punctuation marks are not legible.
2. Input only accepts results in lower case, if there are capital letters they must be converted first to upper case.
3. The length of the received key must be the same as the length of the plaintext (P_i), so it requires a very large amount of memory, which results in a long process(Fitra Syawal et al., 2016).

RESULT AND DISCUSSION

Encryption and Decryption Process of Vigenere Cipher Algorithm on Text Messages

Encryption and decryption process of the Vigenère cipher:
Encryption: Ci = (Pi + Ki) mod 26 (1)
Decryption: Di = (Ci – Ki) mod 26 (2)

Description:
Ci = Ciphertext from C_0 to Cn
Pi = Plaintext from P_0 to Pn
Ki = Key from K_0 to Kn

	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
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
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
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
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
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
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

Figure 5. Encryption Process with Tabula Recta

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Figure 6. Encryption Process with Equations

Encryption: Ci = (Pi+Ki) mod 26

Plaintext :	I	N	F	I	N	I	T	Y
Key :	K	R	I	P	T	O	K	R

Manual calculation of the Vigenere Cipher method to find the ciphertext generated from the plaintext “INFINITY” and the key “KRIPTOKR” can be done using equation (1). So, the encryption process that can be obtained is as follows:

Encryption Process:
C_1 = (I + K) mod 26 = (8 + 10) mod 26 = 18 mod 26 = 18 → S
C_2 = (N + R) mod 26 = (13 + 17) mod 26 = 30 mod 26 = 4 → E
C_3 = (F + I) mod 26 = (5 + 8) mod 26 = 13 mod 26 = 13 → N
C_4 = (I + P) mod 26 = (8 + 15) mod 26 = 23 mod 26 = 23 → X
C_5 = (N + T) mod 26 = (13 + 19) mod 26 = 32 mod 26 = 6 → G
C_6 = (I + O) mod 26 = (8 + 14) mod 26 = 22 mod 26 = 22 → W
C_7 = (T + K) mod 26 = (19 + 10) mod 26 = 29 mod 26 = 3 → D
C_8 = (Y + R) mod 26 = (24 + 17) mod 26 = 41 mod 26 = 15 → P

In this study, ASCII 256 was used. Therefore, the modulo formula is replaced by 256, where Ci is the ciphertext from C_0 to Cn, Pi is the plaintext from P_0 to Pn, and Ki is the key from K_0 to Kn. Therefore, the encryption and decryption formulas used are as follows:

Encryption: Ci = (Pi + Ki) mod 256 (3)
Decryption: Di = (Ci – Ki) mod 256 (4)

For example, in the case study, it is known that “INFINITY” is a plaintext and “KRIPTO” is a key, then based on the formula above, the encryption process is as follows:

$C_1 = (P_1 + K_1) \bmod 256$
= (I + K) mod 256
= (73 + 75) mod 256
= 148 mod 256
= 148 (ö)

$C_2 = (P_2 + K_2) \bmod 256$
= (N + R) mod 256
= (78 + 82) mod 256
= 160 mod 256
= 160 (á)

$C_3 = (P_3 + K_3) \bmod 256$
= (F + I) mod 256
= (70 + 73) mod 256
= 143 mod 256
= 143 (Å)

$C_4 = (P_4 + K_4) \bmod 256$
= (I + P) mod 256
= (73 + 80) mod 256
= 153 (Ö)

$C_5 = (P_5 + K_5) \bmod 256$
= (N + T) mod 256
= (78 + 84) mod 256
= 162 (ó)

$C_6 = (P_6 + K_6) \bmod 256$
= (I + O) mod 256
= (73 + 79) mod 256
= 152 (ÿ)

$C_7 = (P_7 + K_7) \bmod 256$
= (T + K) mod 256
= (84 + 75) mod 256
= 159 (ƒ)

$C_8 = (P_8 + K_8) \bmod 256$
= (Y + R) mod 256
= (89 + 82) mod 256
= 171 ($^1/_2$)

So, the ciphertext obtained is: ö á Å Ö ó ÿ ƒ $^1/_2$

Plaintext	I	N	F	I	N	I	T	Y
Key	K	R	I	P	T	O	K	R
Ciphertext	ö	á	Å	Ö	ó	ÿ	ƒ	$^1/_2$

To convert ciphertext into the original message (plaintext), the same key, "KRIPTOKR," is used. The decryption process is as follows:

Decryption Process in Vigenere Cipher

$D_1 = (C_1 - K_1) \bmod 256$
= (148 – K) mod 256
= (148 – 75) mod 256
= (73) mod 256
= 73 (I)

$D_2 = (C_2 – K_2) \bmod 256$
= (160 – R) mod 256
= (160 – 82) mod 256
= (78) mod 256
= 78 (N)

$D_3 = (C_3 – K_3) \bmod 256$
= (143 – I) mod 256
= (143 – 73) mod 256
= (70) mod 256
= 70 (F)

$D_4 = (C_4 – K_4) \bmod 256$
= (153 – P) mod 256
= (153 – 80) mod 256
= (73) mod 256
= 73 (I)

$D_5 = (C_5 – K_5) \bmod 256$
= (162 – T) mod 256
= (162 – 84) mod 256
= (78) mod 256
= 78 (N)

$D_6 = (C_6 – K_6) \bmod 256$
= (152 – O) mod 256
= (152 – 79) mod 256
= (73) mod 256
= 73 (I)

$D_7 = (C_7 – K_7) \bmod 256$
= (159 – K) mod 256
= (159 – 75) mod 256
= (84) mod 256
= 84 (T)

$D_8 = (C_8 – K_8) \bmod 256$
= (171 – R) mod 256
= (171 – 82) mod 256
= (89) mod 256
= 89 (Y)

So, the plaintext obtained is: INFINITY

Ciphertext	ö	á	Å	Ö	ó	ÿ	ƒ	½
Key	K	R	I	P	T	O	K	R
Plaintext	I	N	F	I	N	I	T	Y

Here, the implementation of Vigenere Cipher using Python Programming Language:

https://colab.research.google.com/drive/1-Sd-Y6Dyc8lE6ZroYLs13KXPMYT7SRf3?usp=sharing

CONCLUSION

The implementation of the Vigenere Cipher as a symmetric key cryptography algorithm reveals that while it is an effective foundational tool for securing data, its classical form has significant limitations in modern environments. The Vigenere Cipher successfully maintains data confidentiality by ensuring only authorized parties with the correct key can access the original information. It is particularly effective for encrypting sensitive social assistance and personal data in localized management systems. The primary weakness of the standard Vigenere Cipher is its vulnerability to frequency analysis and brute force attacks due to the repetitive nature of its key. If the key is short or reused, attackers can identify patterns to decrypt messages.

REFERENCES

Aditya, F., & Romli, M. A. (2025). *Implementasi Metode Kriptografi Advanced Encryption Standard 256 Bit Berbasis Web dan Mobile Pada Pengamanan Dokumen Notaris*. *6*(6), 707–714. https://doi.org/10.47065/tin.v6i6.8637

Amalia Zebua, S. (2022). Modifikasi Algoritma Vigenere Cipher dengan Pembangkit Kunci Random Number Generator Dalam Pengamanan Citra Digital. *Journal of Computing and Informatics Research*, *1*(3), 71–81. https://doi.org/10.47065/comforch.v1i3.345

Anzari, Y., Rachmawati, A., Damas Fatih, M., & Pariyadi. (2025). IMPLEMENTASI BRUTE FORCE ATTACK TERHADAP VIGENERE CIPHER: PENGARUH PANJANG KUNCI DAN PANJANG TEKS. *J-ENSITEC*, *12*(01), 10315–10322. https://doi.org/10.31949/j-ensitec.v12i01.16393

Bima Putra, N., Cirya Andika, B., Daniata Purba Bagas, A., Ridwan, M., Amik Riau, S., & Indah, J. (2023). Implementasi Sandi Vigenere Cipher Dalam Mengenkripsikan Pesan. *Jocotis*, *1*(1), 42–50.

Faris, F. A. E. F., Febi, F. Y., Iwan, I. I., & Pizaini, P. (2023). Kombinasi algoritma kriptografi vigenere cipher dengan metode zig-zag dalam pengamanan pesan teks. *Jurnal CoSciTech (Computer Science and Information Technology)*, *4*(1), 182–192. https://doi.org/10.37859/coscitech.v4i1.4787

Fitra Syawal, M., Chandra Fikriansyah, D., Agani, N., Kunci, K., & Chiper, V. (2016). Implementasi Teknik Steganografi Menggunakan Algoritma Vigenere Cipher Dan Metode LSB. *Jurnal TICOM*, *4*(3), 93707.

Jefry G G Saragih. (2025). Penerapan Kriptografi untuk Pengamanan Data Nilai Siswa dengan Algoritma Super Enkripsi. *ADA Journal of Information System Research*, *2*(2), 77–85. https://doi.org/10.64366/adajisr.v2i2.78

Karima, N. A., Aisyah, A. N., Silla, H. V., Handoko, L. B., & Sani, R. R. (2024). Kriptografi Teks Berbasis Algoritma Substitusi Vigenere Cipher 8 Bit. *Jurnal Masyarakat Informatika*, *15*(1), 1–13. https://doi.org/10.14710/jmasif.15.1.60836

Nasution, N. W., Efendi, S., & Sawaluddin. (2020). Analysis of RSA variants in securing message. *IOP Conference Series: Materials Science and Engineering*, *725*(1). https://doi.org/10.1088/1757-899X/725/1/012131

Rachmadsyah, A., Perdana, A., & Budiman, A. (2020). Kombinasi Algoritma Beaufort Cipher dan Vigenere Cipher untuk Pengamanan Pesan Teks Berbasis Mobile Application. *Jurnal Minfo Polgan*, *9*(2), 12–17.

Ridho, R., Bisri, C., & Harahap, A. M. (2023). Penerapan Kriptografi Enkripsi Dan Deskripsi Dalam Pendataan Pasien Klinik Mama Harfas Tembung Menggunakan Visual Basic. *Januari*, *2*(1), 30. https://doi.org/10.47233/jppie.v2i1.676

SUSILA BAHRI*, F. J. B. R. (2023). *IMPLEMENTASI ALGORITMA SUPER ENKRIPSI VIGENERE CIPHER DAN ROUTE CIPHER PADA PENYANDIAN PESAN TEKS*.

Yuslita Dewi, E., Aricho Sundawa, D., Hermansyah, B., Nur Azizah, A., & Nurul Huda, U. (2025). *CAESAR TIME ASCII CIPHER (CAESAR CIPHER VERSI WAKTU + ASCII)*.