JURRIPEN: Jurnal Riset Rumpun Ilmu Pendidikan
Volume. 4 Nomor. 1 April 2025
e-ISSN: 2828-8483; p-ISSN: 2828-8432, Hal. 777-786
DOI: https://doi.org/10.55606/jurripen.v4i1.6154
Available online at: https://prin.or.id/index.php/JURRIPEN

Penerapan Teori Graph dan Aljabar Boolean dalam Kriptografi

I Putu Jefa Kurniadi [1*], Ni Luh Desy Muliani [2], Ni Kadek Ayu Lestari Dewi [3]
[1-3] Universitas Udayana, Indonesia
Email : jefakurniadi0521@gmail.com

Alamat: Jalan Raya Kampus Unud Jimbaran, Bukit Jimbaran, Kuta Selatan, Badung, Bali
Korespondensi penulis: jefakurniadi0521@gmail.com *

Abstract. *Advances in technology and computers are utilized in various fields of contemporary applications, especially in cryptography and data security in graph theory applications. By understanding the concepts of graph theory, researchers and developers can design cryptographic algorithms that are stronger, more efficient and resistant to attacks. One of the cryptographic applications that has been implemented is the XNOR algorithm. This algorithm has been applied to encryption and decryption as well as the use of stream ciphers. By using 64 bits, the XNOR algorithm can expand encryption and decryption capabilities and increase the security of encrypted data. In this research, an analysis was carried out regarding information encryption and decryption algorithms with the application and development of the XNOR gate logic circuit method in Boolean algebra and graph theory. This research uses the example of the word MATH, which can be changed into a code or password and vice versa to secure information that you want to keep secret. Apart from that, an analysis of the graph formation of each character in the word MATH was also carried out using Python which produced semi-Euler and Hamilton graphs*

Keywords: *Cryptography, Decryption, Encryption, Graph, XNOR*

Abstrak. Kemajuan teknologi dan komputer dimanfaatkan dalam berbagai bidang aplikasi kontemporer, khususnya dalam kriptografi dan keamanan data melalui penerapan teori graf. Dengan memahami konsep-konsep dalam teori graf, para peneliti dan pengembang dapat merancang algoritma kriptografi yang lebih kuat, efisien, dan tahan terhadap berbagai serangan. Salah satu algoritma kriptografi yang telah diterapkan adalah algoritma XNOR. Algoritma ini digunakan dalam proses enkripsi dan dekripsi, serta dalam penerapan stream cipher. Dengan memanfaatkan 64 bit, algoritma XNOR mampu meningkatkan kemampuan enkripsi dan dekripsi sekaligus memperkuat keamanan data yang dienkripsi. Pada penelitian ini dilakukan analisis terhadap algoritma enkripsi dan dekripsi informasi melalui penerapan dan pengembangan metode rangkaian logika gerbang XNOR dalam aljabar Boolean dan teori graf. Penelitian ini menggunakan contoh kata MATH, yang diubah menjadi kode atau sandi tertentu, kemudian dapat dikembalikan ke bentuk semula untuk menjaga kerahasiaan informasi. Selain itu, dilakukan pula analisis terhadap pembentukan graf dari masing-masing karakter dalam kata MATH menggunakan Python, yang menghasilkan graf semi-Euler dan Hamilton.

Kata kunci: Dekripsi, Enkripsi, Graf, Kriptografi, XNOR

1. LATAR BELAKANG

Teori *graph* merupakan cabang matematika yang mempelajari sifat-sifat *graph* (Khairani & Siambaton, 2023). Aplikasi teori *graph* menjadi penting dalam berbagai bidang aplikasi kontemporer karena kemajuan teknologi dan komputer. Banyak bidang yang memanfaatkan teori *graph*, terutama dalam kriptografi dan keamanan data**.** *Smart grid*, *blockchain*, dan steganografi merupakan contoh penerapan kriptografi dalam keamanan data. Teori *graph* menyumbangkan analisis pada struktur kunci publik (*public key*), optimasi jaringan kunci (*key network optimization*), analisis kompleksitas algoritma, serta pengembangan algoritma efisien

Received: Februari 15, 2025; Revised: Maret 23, 2025; Accepted: April 29, 2025; Published: April 30, 2025;

yang semuanya merupakan elemen penting dalam keamanan data. Dengan memahami konsep teori graph, para peneliti dan pengembang dapat merancang algoritma kriptografi yang lebih kuat, tahan terhadap serangan, dan efisien.

Penelitian terdahulu yang menggunakan konsep kriptografi yaitu oleh Khairani (2023), menggunakan algoritma ElGamal dan XOR dengan tujuan pengamanan data pada teks. Algoritma ElGamal berfokus pada penyelesaian masalah terkait logaritma diskret, sedangkan Algoritma XOR merupakan algoritma sederhana yang penggunaannya berdasarkan prinsip logika. Selain itu, penelitian lainnya yang dilakukan Yoga Pratama (2023) menunjukkan bahwa pemanfaatan teknik kriptografi dengan algoritma *blowfish* pada sampel data teks dapat digunakan sebagai alternatif untuk pengamanan data, yang dilakukan dengan metode penjumlahan, pergeseran, XOR, dan *tables lookup* pada 32 bit. Penelitian terdahulu yang menggabungkan algoritma XOR dan 32 bit lainnya seperti yang dilakukan oleh Dr. M. Latlitha, S.Vasu pada tahun 2023, mengusulkan *Cipher* yang dapat dikonversi ke dalam *graph* untuk komunikasi rahasia dengan mengusulkan penyandian serta penguraian kode *Python* yang digunakan untuk mengubah teks biasa menjadi teks sandi, juga sebaliknya.

Berdasarkan penelitian terdahulu yang telah dipaparkan, terdapat peluang untuk mengembangkan algoritma kriptografi dengan metode baru. Pada penelitian ini, digunakan kombinasi baru yaitu algoritma XNOR dengan 64 bit. XNOR (*exclusive* NOR) merupakan salah satu rangkaian logika dalam Aljabar Boolean yang penggunaannya berdasarkan kombinasi antara rangkaian logika XOR (*exclusive* OR) dan NOT dengan *output* berbanding terbalik dengan XOR (Kurniawan, 2020). Algoritma XNOR telah diterapkan pada beberapa aplikasi kriptografi seperti enkripsi dan deskripsi serta penggunaan *stream cipher*. Dengan menggunakan 64 bit, algoritma XNOR dapat memperluas kemampuan enkripsi dan deskripsi serta meningkatkan keamanan data terenkripsi.

2. KAJIAN TEORITIS

Untuk memperjelas landasan dalam penelitian ini, terlebih dahulu disajikan beberapa teori yang berkaitan dengan topik yang dibahas. Adapun isi kajian ini disusun sebagai berikut:

Kriptografi

Kriptografi merupakan ilmu yang bertujuan untuk melindungi keaslian pesan agar tidak disalahgunakan sehingga hanya dapat diakses jika memiliki kunci akses (Ziliwu et al., 2022). Kriptografi dirancang untuk mencegah adanya intervensi oleh pihak yang tidak berwenang dengan memastikan pesan dapat dikenali dengan baik oleh pengirim dan penerima.

Enkripsi

Enkripsi disebut sebagai proses penyandian pesan atau mengubah informasi menjadi teks yang tidak dapat dibaca (Rivaldi et al., 2023).

Dekripsi

Dekripsi merupakan proses mengembalikan pesan terenkripsi menjadi informasi aslinya (Rivaldi et al., 2023).

Plaintext

Plaintext adalah informasi asli yang akan dikomunikasikan antara pengirim dan penerima (Bai'at et al., 2023).

Ciphertext

Ciphertext merupakan *output* dari proses enkripsi pesan atau data yang dibentuk menjadi sandi atau data acak yang tidak bermakna (Zulkarnain et al., 2023).

Array

Kumpulan data yang terstruktur terdiri dari elemen-elemen sejenis dan diberi nama tertentu disebut *array* (Sihombing, 2019). *Array* dapat diibaratkan sebagai sejumlah kotak yang menyimpan sejumlah elemen bertipe sama.

***Graph* Euler**

Graph Euler merupakan *graph* yang memenuhi sirkuit Euler yaitu sirkuit di *graph* G yang memuat semua sisi G.

***Graph* Hamilton**

Siklus yang melalui semua titik tepat satu kali dalam sebuah *graph* merupakan definisi dari siklus Hamilton (Prasetyo et al., 2022). *Graph* yang memiliki siklus Hamilton dikenal sebagai *graph* Hamilton.

3. METODE PENELITIAN

Kriptografi adalah ilmu tentang penulisan rahasia dengan tujuan menyembunyikan makna dari sebuah informasi sehingga tidak ada pihak ketiga yang dapat memahami data asli saat transmisi dari sumber ke tujuan. Penelitian ini akan membahas sebuah algoritma enkripsi dan dekripsi informasi dengan penerapan dan pengembangan metode rangkaian logika gerbang XNOR dalam Aljabar Boolean serta teori *graph*. Berikut merupakan setiap tahapan yang akan dilakukan:

1. Algoritma Enkripsi

a. Konversikan setiap karakter dalam informasi yang akan dikirim menjadi kode ASCII.

b. Ambil nilai ASCII dari setiap karakter yang telah dikonversikan dan bentuk kode binernya.
c. Setelah diperoleh format biner dari setiap karakter dalam ASCII, operasikan setiap kode dengan kode biner yang bernilai 64 menggunakan rangkaian logika XNOR.
d. Bentuk matriks $\boldsymbol{A}$ dengan ukuran $k \times k$, dengan k merupakan banyak angka 1 dalam kode biner yang diperoleh dari hasil operasi XNOR sebelumnya.
e. Bentuk matriks simetri $\boldsymbol{A} = (a_{i,j})$, dengan $a_{i,j}$ merupakan elemen pada baris ke-i dan kolom ke-j dengan diagonal utamanya bernilai 0. Karena matriks ini simetri, maka $a_{i,j} = a_{j,i}$.
f. Hitung jumlah 0 yang berada di antara angka 1 ke-i dan ke-j dalam kode biner yang bersesuaian dengan elemen matriks yang ingin dicari $(a_{i,j})$, masukkan nilai elemen tersebut sebagai $a_{i,j} =$ jumlah $0 + 1$.
g. Proses f diulang hingga elemen matriks $a_{i,j}$ dengan $i = k - 1$ dan $j = k$.
h. Setelah mencapai elemen 1 terakhir dari kode biner, maka masukkan $a_{1,j} = a_{j,1} = 1$, dengan $j = k$.
i. Jika kode biner diakhiri dengan angka 1 dan diikuti oleh L jumlah bilangan 0, maka masukkan $a_{1,k} = a_{k,1} = L + 1$.
j. Masukkan angka 0 untuk elemen $a_{i,j} = a_{j,i}$ lainnya dengan $|j - i| \neq 1$.
k. Susun *array* yang berisikan elemen dari diagonal matriks yang berada tepat di atas diagonal utamanya serta elemen $a_{1,k}$.
l. *Array* tersebut dikirim ke penerima.

2. Algoritma Dekripsi

a. Penerima memperoleh *array* yang disusun dari matriks simetri $\boldsymbol{A}$.
b. Periksa jumlah elemen dalam *array* sebanyak k yang merupakan banyaknya angka 1 dalam kode biner yang akan dicari.
c. Setiap kode biner diawali oleh angka 1.
d. Periksa elemen *array* yang diperoleh. Elemen ke-i menyatakan jumlah angka 0 antara angka 1 ke-i dan angka 1 ke-$(i + 1)$ ditambahkan 1, dengan $i < k$. Dengan demikian, ketika melakukan dekripsi dari *array* menuju kode biner, maka jumlah angka 0 antara angka 1 ke-i dan ke-$i + 1$ merupakan nilai elemen *array* ke-i dikurangi 1.
e. Proses d diulang hingga elemen *array* ke-i, dengan $i = k - 1$.

f. Elemen *array* ke-k (elemen terakhir) menyatakan jumlah angka 0 yang mengikuti angka 1 terakhir ditambahkan 1. Dengan demikian, ketika melakukan dekripsi dari *array* menuju kode biner, maka jumlah angka 0 yang mengikuti angka 1 terakhir sebanyak nilai elemen *array* ke-k dikurangi 1.
g. Diperoleh kode biner XNOR dari *array* yang diterima.
h. Penerima melakukan operasi kode biner tersebut dengan kode biner yang bernilai 64 menggunakan algoritma terbalik rangkaian logika XNOR untuk memperoleh kode biner ASCII setiap karakter dalam informasi aslinya.
i. Konversikan setiap kode biner menjadi kode ASCII yang bersesuaian dengan setiap karakter dalam informasi aslinya.
j. Penerima memperoleh informasi asli dari pengirim.

4. HASIL DAN PEMBAHASAN

Operasi logika yang digunakan dalam metode enkripsi yang diusulkan adalah operasi XNOR. XNOR dinotasikan sebagai: $(A \oplus B)' = \overline{A \oplus B}$

Tabel Operasi XNOR:

A	B	$XNOR$
0	0	1
0	1	0
1	0	0
1	1	1

Misalkan informasi yang ingin disampaikan yaitu **MATH**. Konversikan setiap karakter menjadi kode ASCII lalu dibuat kode binernya. Selanjutnya, lakukan operasi XNOR untuk kode setiap karakter dengan kode biner bernilai 64 sehingga diperoleh:

$XNOR\ 64\ bit\ (1000000)$

Karakter	Kode ASCII	Kode Biner	Hasil $XNOR$
M	77	1001101	1110010
A	65	1000001	1111110
T	84	1010100	1101011
H	72	1001000	1110111

Setelah itu, bentuk matriks dengan ukuran $k \times k$, dengan k merupakan banyak angka 1 dalam kode biner yang diperoleh dari hasil operasi XNOR sebelumnya. Isi setiap elemen

matriks sesuai algoritma yang telah dibuat. Selanjutnya, susun *array* yang berisikan elemen dari diagonal matriks yang berada tepat di atas diagonal utamanya serta elemen $a_{1,k}$. Pesan berupa *array* ini kemudian dikirimkan kepada penerima.

$$\boldsymbol{M} = \begin{bmatrix} 0 & 1 & 0 & 2 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 3 \\ 2 & 0 & 3 & 0 \end{bmatrix} = [1 \quad 1 \quad 3 \quad 2]$$

$$\boldsymbol{A} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 2 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 2 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} = [1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 2]$$

$$\boldsymbol{T} = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 2 & 0 & 0 \\ 0 & 2 & 0 & 2 & 0 \\ 0 & 0 & 2 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} = [1 \quad 2 \quad 2 \quad 1 \quad 1]$$

$$\boldsymbol{H} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} = [1 \quad 1 \quad 2 \quad 1 \quad 1 \quad 1]$$

Penerima memperoleh *array* yang disusun dari matriks simetri untuk pesan **MATH**. Selanjutnya, penerima memeriksa jumlah elemen dalam *array* sebanyak k yang merupakan banyaknya angka 1 dalam kode biner yang akan dicari. Dengan menggunakan algoritma yang telah dibuat, penerima memperoleh kode biner XNOR untuk setiap karakter dari informasi yang ingin disampaikan pengirim kepada penerima.

$1132 = 1110010$

$111112 = 1111110$

$12211 = 1101011$

$112111 = 1110111$

Penerima melakukan operasi kode biner tersebut dengan kode biner yang bernilai 64 menggunakan algoritma terbalik rangkaian logika XNOR untuk memperoleh kode biner ASCII setiap karakter dan memperoleh informasi asli dari pengirim.

$1110010 = \boldsymbol{M}$

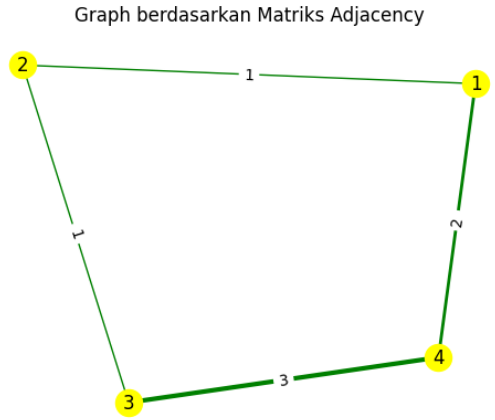
$1111110 = \boldsymbol{A}$

$1101011 = \boldsymbol{T}$

$1110111 = \boldsymbol{H}$

Selain mengembangkan algoritma enkripsi dan dekripsi pada kata **MATH**, dilakukan pula analisis apakah setiap karakter dapat membentuk *graph* tertentu. Melalui penggunaan kode *Python*, diperoleh *output* sebagai berikut:

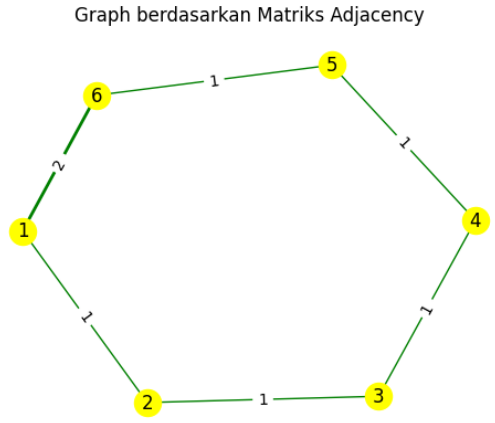
- Huruf **M**




```
Graph ini termasuk Semi-Euler
Graph ini termasuk Hamilton
```

Dari hasil tersebut, didapatkan bahwa matriks dari huruf **M** membentuk *graph* semi euler dan hamilton. Hal ini dibuktikan dengan adanya tepat dua simpul yang berderajat ganjil dan memiliki sirkuit yang setelah mengunjungi semua simpul kembali ke simpul awal.

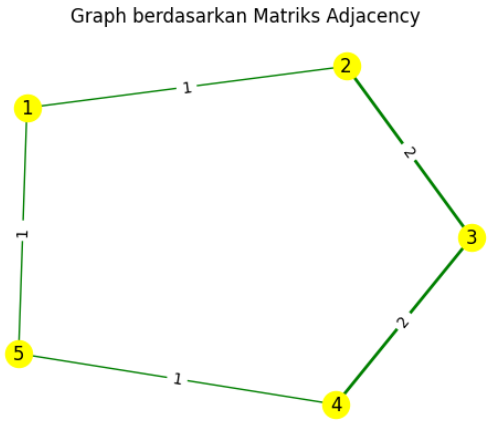
- Huruf **A**




```
Graph ini termasuk Semi-Euler
Graph ini termasuk Hamilton
```

Dari hasil tersebut, didapatkan bahwa matriks dari huruf **A** membentuk *graph* semi euler dan hamilton. Hal ini dibuktikan dengan adanya tepat dua simpul yang berderajat ganjil dan memiliki sirkuit yang setelah mengunjungi semua simpul kembali ke simpul awal.

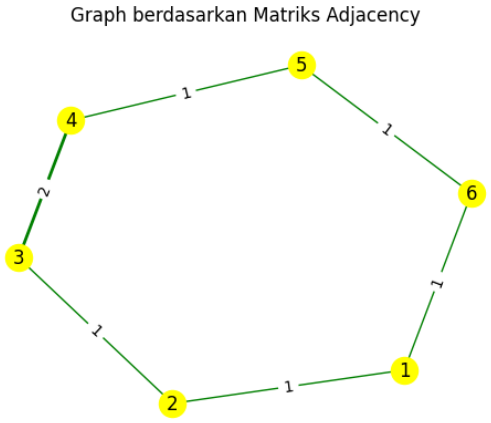
- Huruf **T**




```
Graph ini termasuk Semi-Euler
Graph ini termasuk Hamilton
```

Dari hasil tersebut, didapatkan bahwa matriks dari huruf **T** membentuk *graph* semi euler dan hamilton. Hal ini dibuktikan dengan adanya tepat dua simpul yang berderajat ganjil dan memiliki sirkuit yang setelah mengunjungi semua simpul kembali ke simpul awal.

- Huruf **H**




```
Graph ini termasuk Semi-Euler
Graph ini termasuk Hamilton
```

Dari hasil tersebut, didapatkan bahwa matriks dari huruf **H** membentuk *graph* semi euler dan hamilton. Hal ini dibuktikan dengan adanya tepat dua simpul yang berderajat ganjil dan memiliki sirkuit yang setelah mengunjungi semua simpul kembali ke simpul awal.

5. KESIMPULAN DAN SARAN

Penelitian ini melakukan analisis terkait algoritma enkripsi dan dekripsi informasi dengan penerapan dan pengembangan metode rangkaian logika gerbang XNOR dalam Aljabar Boolean serta teori graph. Dengan menggunakan contoh kata **MATH**, kita dapat mengubah

informasi tersebut dari teks biasa menjadi kode atau sandi, juga sebaliknya dari kode atau sandi menjadi teks biasa untuk mengamankan informasi yang ingin dirahasiakan. Selain itu, dilakukan juga analisis pembentukan *graph* setiap karakter dengan kode *Python*. Berdasarkan kode yang dibuat, diperoleh bahwa setiap karakter dalam kata **MATH** menghasilkan *graph* semi-Euler dan Hamilton, di mana terdapat tepat dua simpul yang berderajat ganjil dan memiliki sirkuit yang setelah mengunjungi semua simpul kembali ke simpul awal.

DAFTAR REFERENSI

Bai'at, A. A., Fahlevvi, M. R., & Ariandi, W. (2023). Metode Algoritma RC4 (Rivest Code 4) Untuk Pengamanan Database Transaksi Pada Glory Digital Sablon. *Explore*, *13*(1), 20–31. https://doi.org/10.35200/ex.v13i1.33

Khairani, & Siambaton, M. Z. (2023). Pengamanan Data Teks Menggunakan Algoritma Kriptografi Elgamal dan XOR dari Serangan Hacker. *Sudo Jurnal Teknik Informatika*, *2*(4), 176–187. https://doi.org/10.56211/sudo.v2i4.401

Kurniawan, A. (2020). *SIMULASI PENGISIAN AIR KETEL MENGGUNAKAN RANGKAIAN IC GERBANG LOGIKA DASAR SESUAI DI KAPAL MV. TANTO SETIA*. POLITEKNIK ILMU PELAYARAN.

Prasetyo, Y. D., Armond, A. M., & Ediningrum, W. (2022). PENERAPAN MODEL MATEMATIKA ALGORITMA ANT COLONY OPTIMIZATION DALAM PENENTUAN RUTE BUS TRANS BANYUMAS. *JURNAL MATHEMATIC PAEDAGOGIC*, *7*(1), 12–23. https://doi.org/10.36294/jmp.v7i1.2701

Pratama, Y., & Sutabri, T. (2023). Analisis Kriptografi Algoritma Blowfish pada Keamanan Data menggunakan Dart. *Jurnal Informatika Terpadu*, *9*(2), 126–135.

Rivaldi, M., Harahap, I. Z., Isdianto, H., & Putri, R. A. (2023). Implementasi Algoritma Kriptografi Vigenere Cipher Pada Pengamanan Pesan Text Berbasis Web. *Positif: Jurnal Sistem Dan Teknologi Informasi*.

Sagayaraj, C. C., Gp, A., Amudha, P., Charles Sagayaraj, A., Sheela, Acs., & Professor, A. (2018). An Application of Graph Theory in Cryptography. *International Journal of Pure and Applied Mathematics*, *119*(13), 375–383.

Siambaton, M. Z. (2023). Pengamanan Data Teks Menggunakan Algoritma Kriptografi Elgamal dan XOR dari Serangan Hacker. *Sudo Jurnal Teknik Informatika*, *2*(4), 176–187.

Sihombing, J. (2019). Penerapan stack dan queue pada array dan linked list dalam java. *INFOKOM (Informatika & Komputer)*, *7*(2), 15–24.

Ziliwu, K. B., Maslan, A., & Kremer, H. (2022). Implementasi Caesar Cipher pada Algoritma Kriptografi Klasik dalam Penyandian Pesan. *Computer and Science Industrial Engineering (COMASIE)*, *7*(2), 117–126.

Zulkarnain, A. N., Tahir, M., Wahyuningsih, U., Andreani, A. D. P., Firdausi, A., Wijayaningrum, A. I., & Nasihuddin, M. (2023). Analisis Proses Enkripsi Algoritma Kriptografi Modern Advanced Encryption Standard (AES). *Jurnal Adijaya Multidisplin*, *1*(02), 380–387.