PENGEMBANGAN ALGORITMA CAESAR CIPER UNTUK MENGAMANKAN DATA NASABAH APLIKASI TABUNGAN

Solichul Huda[1*], Ferdian Nur Fariza[2]
[1,2] Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Imam Bonjol No. 207, Pindrikan, Semarang 50131.
[*]Email: solichul.huda@dsn,dinus.ac.id

Abstrak

Data nasabah tabungan perlu diamankan supaya tidak dilihat oleh pengguna ilegal, salah satu caranya dengan melakukan enkripsi. Enkripsi pengamanan data teks dapat dilakukan menggunakan algoritma Caesar Ciper. Namun penggunaan algoritma tersebut terdapat beberapa kelemahan salah satunya dapat di bongkar menggunakan metode exhoutive key serach. Paper ini mengembangkan metode algoritma caesar cipher untuk menutupi kelemahan tersebut. Metode ini mengusulkan pengembangan kunci ke 2 pada subtitusi berganda dengan urutan huruf dalam plaintext. Dari ujicoba yang dilakukan, metode exhaostive key serach tidak dapat membuka enkripsi ini secara ilegal dan prosesnya juga sederhana. Pengembangan algoritma caesar yang diusulkan ini dapat mengamankan data teks lebih baik dibanding algoritma Ceasar Cipher kunci berganda.

Kata kunci: Caesar cipher, enkripsi, nasabah, Pengamanan, teks

1. PENDAHULUAN

Pengaman data teks itu sangat penting karena dapat mencegah akses tidak sah terhadap informasi rahasia. Dalam era digital saat ini, banyak data pribadi dan profesional disimpan dalam bentuk teks yang rentan terhadap pencurian atau peretasan. Dengan menerapkan sistem keamanan yang kuat, seperti enkripsi dan autentikasi, risiko kebocoran data dapat diminimalkan. Oleh karena itu, menjaga keamanan data teks menjadi tanggung jawab penting bagi setiap individu maupun organisasi (Wahyudi, 2024). Ada beberapa pengaman teks yang dapat digunakan untuk menjaga kerahasiaan data, salah satunya adalah Caesar Cipher (Hasanah, 2023). Metode ini bekerja dengan cara menggeser huruf-huruf dalam teks asli sejumlah langkah tertentu sehingga membentuk teks sandi. Meskipun tergolong sederhana, Caesar Cipher dapat menjadi dasar dalam memahami konsep enkripsi. Dengan penerapan yang tepat, metode ini dapat membantu melindungi pesan dari pihak yang tidak berhak membaca isinya

Namun Caesar Cipher memiliki beberapa kelemahan yang membuatnya kurang aman untuk digunakan pada sistem modern (Nasution2019). Salah satu kelemahannya adalah pola pergeseran huruf yang mudah ditebak jika seseorang mengetahui metode exhputive key serach. Penggunaan subtitusi bergandapun masih bisa diserang dengan brute force.

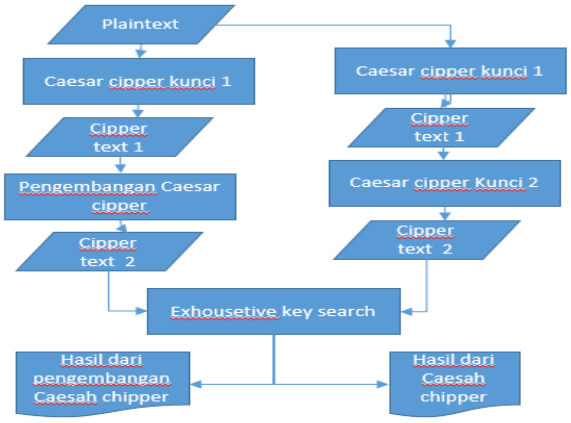
Caesar Cipher adalah salah satu metode enkripsi klasik yang digunakan untuk menyembunyikan pesan dengan cara menggeser huruf-huruf dalam teks asli (Pratama, 2025). Setiap huruf dalam plaintext diganti dengan huruf lain yang terletak beberapa posisi setelahnya dalam alfabet (Destari, 2025). Misalnya, jika pergeseran yang digunakan adalah 3, maka huruf A akan menjadi D, B menjadi E, dan seterusnya. Untuk mendekripsi pesan, penerima cukup menggeser huruf-huruf pada ciphertext ke arah sebaliknya dengan jumlah pergeseran yang sama. Enkripsi menggunakan cesar cipher kunci berganda sudah lebih baik, namun tetap bisa dibuka secar ilegal.

Penelitian pengamanan data teks menggunakan Caesar Cipher sudah pernah dilakukan oleh beberapa peneliti sebelumnya dengan berbagai pengembangan dan kombinasi metode. Diantaranya, penelitian oleh Pratama (2025), Wahyudi, (2024). Aranski (2023), Pratiwi (2022), Nasution, (2024), dan Pratiwi (2022). Mereka mengimplementasi algoritma Caesar Cipher dan mengembangkannya untuk melindungi data teks.

Penelitian Pratama dkk., dalam Pratama (2025) mengembangkan pengamanan data dengan mengombinasikan algoritma Vigenere dan algoritma Caesar untuk mengamankan data teks. Penggabungan dua algoritma tersebut dapat mengamankan data teks menjadi lebih kuat, namun proses enkripsinya memerlukan waktu yang lebih panjang. Penelitian ini mengusulkan pengembangan algoritma caesar cipher dengan kunci ganda dimana kunci ke dua tergantung dengan urutan huruf dalam plaintext. Pertama plaintext di subtitusi dengan kunci 1, lalu cipertext yang terbentuk di enkripsi kembali dengan kunci 2 yang berupa urutan posisi huruf dari plaint text. Metode yang diusulkan ini membuat enkripsi menjadi lebih kuat dari serangan user ilegal dan ringan prosesnya.

2. METODOLOGI

Penelitian ini mengembangkan algoritma caesar ciper dengan mengubah kunci kedua dengan angka posisi dalam huruf abjad. Pertama ditentukan plaintext yang akan diamankan. Kemudian plaintext tersebut dienkripsi menggunakan caesar ciper kunci standard. Cipher text yang terbentuk, di enkripsi kembali menggunakan posisi huruf ciphertext dalam urutan abjad. Enkripsi yang kedua menghasilkan cipher text. Gambar 1 menunjukkan tahapan dalam penelitian ini.



Gambar 1. Metodologi Penelitian

2.1. Penentuan Data

Penelitian ini diambil dari data sebuah Bank Perkreditan Rakyat (BPR) yang berfokus pada pengolahan dan pengamanan data nasabah. Data BPR terdiri dari identitas nasabah, transaksi keuangan, dan riwayat pinjaman. Namun dalam penelitian ini hanya menggunakan data nasabah tabungan sebagai objek penelitian. Penggunaan data dari BPR ini bertujuan untuk menguji efektivitas metode pengamanan teks dalam menjaga kerahasiaan informasi sensitif. Selain itu, penelitian ini juga menganalisis bagaimana penerapan pengembangan metode caesar cipher dalam sistem perbankan skala kecil. Dengan demikian, hasil penelitian diharapkan dapat memberikan kontribusi nyata dalam peningkatan keamanan data pada lembaga keuangan lokal yang diperoleh BPR berupa data nasabah tabungan. Date tabungan tersebut tendiri dari data text dan numerik. Dalam studi ini data yang dipilih untuk diamankan adalah data yang berupa karakter. Dengan demikian data yang berupa angka misalnya nomor rumah tidak dimasukkan untuk dienkripsi.

2.2. Penentuan Plaintext

Bentuk data nasabah tabungan pada sebuah BPR umumnya terdiri dari kombinasi huruf dan angka. Data tersebut meliputi nomor rekening, nama nasabah, alamat, serta kode identifikasi unik yang digunakan dalam sistem. Kombinasi huruf dan angka ini membantu memastikan bahwa setiap data nasabah bersifat unik dan mudah diidentifikasi. Selain itu, format data tersebut memudahkan proses pengolahan dan penyimpanan dalam basis data digital. Dalam penelitian ini, hanya data teks yang dipilih sebagai objek uji untuk proses enkripsi.

Semua data yang digunakan dalam penelitian ini dipilih hanya yang berupa huruf saja. Pemilihan data huruf dilakukan untuk mempermudah proses enkripsi menggunakan algoritma Caesar Cipher. Dengan hanya menggunakan huruf, proses pergeseran karakter menjadi lebih sederhana dan konsisten. Selain itu, pemilihan data berupa huruf juga menghindari kesalahan dalam pengolahan simbol atau angka yang mungkin tidak termasuk dalam alfabet. Seandainya terdapat angka atau simbol dalam data nasabah, maka hanya teks yang di enkripsi

2.3. Algoritma Caesar Cipher

Caesar Cipher adalah algoritma kriptografi klasik yang digunakan untuk melakukan enkripsi (penyandian) teks dengan cara menggeser posisi huruf dalam alfabet sejauh nilai kunci tertentu. Caesar Cipher bekerja dengan mengubah setiap huruf dalam plaintext menjadi huruf lain berdasarkan jumlah pergeseran (key) yang telah ditentukan (Hidayat, Ridho, dan Zulfahmi Indra, 2024). Jika key = 3, maka A menjadi D, B menjadi E, C menjadi F, dan seterusnya. Setelah huruf Z, pergeseran akan kembali ke A (sistem melingkar atau *modular*).

Proses Caesar Cipher dapat dinyatakan dalam bentuk persamaan matematika modular sebagai berikut:

$$C=(P+K)\bmod 26 \quad (1)$$

$$P=(C-K)\bmod 26 \quad (2)$$

Dimana C adalah ciphertext, K adalah kunci, P adalah plaintext. Sedangkan modulo 26 menunjukkan bahwa perhitungan dilakukan dengan 26 huruf alfabet (A–Z).

2.4. Penentuan Kunci 1

Penentuan kunci pada algoritma Caesar Cipher sangat penting karena kunci inilah yang menentukan seberapa jauh pergeseran huruf dalam proses enkripsi dan dekripsi . Berikut penjelasannya:

1. Kunci (key) dalam Caesar Cipher berupa bilangan bulat (integer) yang menunjukkan jumlah pergeseran huruf dalam alfabet.
2. Misalnya, jika kunci = 3, maka huruf **A** akan digeser menjadi D**,** B menjadi E**,** dan seterusnya.
3. Nilai kunci biasanya dipilih dari 1 sampai 25**,** karena jika kunci = 0 atau 26 maka hasilnya sama dengan teks asli (tidak terjadi pergeseran).
4. Pemilihan kunci dapat dilakukan secara manual (ditentukan pengguna) atau otomatis (dihasilkan oleh sistem) sesuai kebutuhan keamanan.
5. Dalam dekripsi, prosesnya dibalik: huruf pada ciphertext digeser ke arah kiri sejauh nilai kunci yang sama untuk mendapatkan plaintext semula.

Contohnya terdapat Plaintext: SEMARANG menggunakan Kunci: 2 Ciphertext: UGOCTCPI

2.5. Pengembangan Kunci 2 dalam Algoritma Caesar Cipher

Algoritma Caesar cipher menggunakan kunci untuk jumlah pergeseran data yang yang dienkripsi. Untuk penguncian ganda, algoritma ini akan mengenkripsi sebanyak dua kali. Pertama menggeser sebanyak kunci ke 1 , lalu digeser lagi sebanyak kunci yang ke dua. Namun baik penguncian tunggal maupun penguncian berganda tetap bisa dibongkar menggunakan exhautive key serach. Penelitian ini melakukan pengembangan pada penguncian berganda, dimana kami akan menganti ke 2 secara dinamis.

Kunci ke 2 yang diusulkan oleh penelitian ini diambil dari urutan huruf didalam plaintext. Dengan demikian kunci akan berubah sesuai dengan urutan posisi setiap huruf di dalam plaintext, mulai dari kunci = 1, kunci = 2, sampai kunci = panjang plaintext. Modul Caesar Cipher yang dikembangkan ini dapat dinyatakan dalam bentuk persamaan matematika modular sebagai berikut:

$$C=(C1+K2) \bmod 26 \quad (3)$$
$$P=(C2-K2) \bmod 26 \quad (4)$$

Dimana C1 = cipher text hasil dengan kunci 1, C2 ciphertext hasil enkripsi kunci ke 2, K2= posisi huruf dalam urutan di plaintext (1–maksimal plaintext) dan mod 26 menunjukkan bahwa perhitungan dilakukan dengan 26 huruf alfabet (A–Z).

2.6. Penentuan Cipper text

Cara mengambil cipher text dari Caesar Cipher dilakukan melalui proses enkripsi dengan menggeser setiap huruf pada teks asli sejauh jumlah kunci yang telah ditentukan. Pertama, huruf-huruf pada plain text diubah menjadi bentuk angka sesuai urutan alfabet. Setelah itu, setiap angka digeser ke kanan sebanyak nilai kunci, dan hasilnya dikonversi kembali menjadi huruf. Misalnya, jika kunci yang digunakan adalah 3, maka huruf A akan berubah menjadi D, B menjadi E, dan seterusnya. Proses ini menghasilkan teks baru yang sudah terenkripsi, yang disebut cipher text**.** Dengan demikian, cipher text adalah hasil akhir dari penerapan Caesar Cipher pada teks asli menggunakan kunci tertentu.

3. HASIL DAN PEMBAHASAN

3.1. Hasil Simulasi

Penelitian ini mengambil dari nasabah tabungan BPR sebanyak 200 orang. Pengambilan datanya menggunakan distribusi posion. Data diambil secara acak dari 1500 data nasabah tabungan yang ada. Rincian data terdiri dari nomor rekening, nama lengkap, alamat lengkap, nama ibu, tanggal lahir, jenis kelamin dan jumlah saldo. Dalam simulasi ini, data yang dienkripsi adalah nama lengkap nasabah. Dalam uji coba, kami mengenkripsi dengan Algoritma Caesah Cipher dan algoritma Pengembangan yang diusulkan.

Tabel 1. Level perlunya keamanan per field

No.	Field	Level	Keterangan
1	No. Rekening	Sedang	Nomor rekening tabungan
2	Nama	Rendah	Nama lengkap nasabah
3	Alamat	Rendah	Alamat lengkap
4	Tanggal lahir	Rendah	Tanggal lahir
5	Jenis kelamin	Rendah	Jenis kelamin
6	Nama Ibu	Sedang	Nama ibu kandung nasabah
7	Saldo	Tinggi	Saldo akhir nasabah
8	Ahli waris	Rendah	Nama ahli waris dari nasabah

Tabel 2. Perbandingan Algoritma Caesar dengan Pengembangan Diusulkan

NO	Plaintext	Key	Caesar Cipher	Modifikasi Caesar Cipher
1	ANDI PRATAMA WIJAYA	11	LYOT ACLELXL HTULJL	MARX GJTNVIX VIKCBE
2	SITI NUR AISYAH	11	DTET YFC LTDJLS	EVHX EMK VEPWZH
3	BUDI SANTOSO PUTRA	11	MFOT DLYEZDZ AFECL	NHRX JSGNJOL OUUTD
4	RINA MAHARANI DEWI	11	CTYL XLSLCLYT OPHT	DVBP DSAUMWKG DFYL
5	AHMAD FAUZAN HAKIM	11	LSXLO QLFKLY SLVTX	MUAPT XTOUWK GALKP
6	DIAN KARTIKA SARI	11	OTLY VLCETVL DLCT	PVOC BSKNDGX RASK
7	JOKO TRI HARYANTO	11	UZVZ ECT SLCJLYEZ	VBYD KJB CWOWZNUQ

8	MAYA LESTARI UTAMI	11	XLJL WPDELCT FELXT	YNMP CWLNVNF TTBOL
9	RIZKY ADITYA PRATAMA	11	CTKVJ LOTEJL ACLELXL	DVNZO SWCOUX ORBVDQF
10	PUTRI AYU MAHARANI	11	AFECT LJF XLSLCLYT	BHHGY SRO IXFZRBPL
11	HENDRA GUNAWAN SAPUTRA	11	SPYOCL RFYLHLY DLAFECL	TRBSHR ZOIWTYM TCSYYXH
12	LAILA NUR RAHMA	11	WLTWL YFC CLSXL	XNWAQ FNL NXFLA
13	BAYU SETIAWAN PRATOMO	11	MLJF DPETLHLY ACLEZXZ	NNMJ JWMCVSXL PSCWSRU
14	INTAN CAHYA PERMATA	11	TYELY NLSJL APCXLEL	UAHPD UTBTW NDRNCWE
15	ARIF HIDAYATULLAH RAMADHAN	11	LCTQ STOLJLEFWWLS CLXLOSLY	MEWU YAWUTWQSKLBJ VFSHLQKY
16	NANDA FEBRI KUSUMA	11	YLYOL QPMCT VFDFXL	ZNBSQ XXVME ITSVOD
17	FARHAN YUSUF ALAMSYAH	11	QLCSLY JFDFQ LWLXDJLS	RNFWQE RONQC ZLBOVCFN
18	MEGA PUSPITA SARI	11	XPRL AFDATEL DLCT	YRUP GMLJDPX RASK
19	DIMAS ARYA NUGRAHA	11	OTXLD LCJL YFRCLSL	PVAPI SKSV KSFRBJD
20	NURUL FITRIA ZAHRA	11	YFCFW QTECTL KLSCL	ZHFJB XBNMEX YAITD
21	KEVIN JONATHAN PRASETYO	11	VPGTY UZYLESLY ACLDPEJZ	WRJXD BHHVPEYM QTDWJZFW
22	CLARA MELATI ANGGRAINI	11	NWLCL XPWLET LYRRCLTYT	OYOGQ EXFVPF ZNHIUENTP
23	SAMUEL ADRIAN HARTONO	11	DLXFPW LOCTLY SLCEZYZ	ENAJUC TXMEXL HBTWSSU

3.2. Evaluasi dan Pembahasan

Dalam penelitian ini untuk menunjukkan keunggulan pengembangan Algoritma Caesar Chiper yang diusulkan oleh penelitian, dilakukan evaluasi dengan 2 skenario, (1) mengenkripsi menggunakan algoritma Caesar Cipher, (2) mengenkripsi menggunaaan algoritma Caesar Cipher yang dikembangkan dalam penelitian ini, (3) membandingkan hasil enkripsi yang dihasilkan kedua metode. Metode evaluasi ini seperti yang dilakukan oleh Wahyudi dalam (Wahyudi, 2024). Untuk mencapai pengamanan yang sepadan dengan waktu yang diperlukan, penelitian ini menentukan level keamanan data nasabah tabungan BPR. Tabel 2 menunjukkan level keamanan dari data nasabah tabungan BPR.

Pertama, mengenkripsi data menggunakan Algoritma Caesar Cipher. Lalu dengan data yang sama, dilakukan enkripsi menggunakan algoritma Caesar Cipher yang dikembangkan dalam penelitian ini. Contoh hasil enkripsi kedua metode tersebut ditunjukkan dalam Tabel 2.

Langkah terakhir, penelitian ini melakukan perbandingan chipertext yang dihasilkan kedua Algoritma tersebut. Berdasarkan level keamanan masing-masing field, maka untuk yang keamanan rendah penggunaan Algoritma Caesar Cipher yang diusulkan oleh penelitian ini tetap lebih menguntungkan. Pengembangan Algoritma Caesar Cipher ini sudah lebih baik dibanding algoritma Caesar berganda dengan menggunakan kunci berganda namun dengan kunci ganda berupa pergeseran berdasarkan nomor urut huruf. Pengembangan dengan menambah pergeseran nomor urut huruf sebetulnya bagus, namun penggunaan nomor urut plaintext dalam daftar huruf alfabet tetap bisa ditebak.

Tabel 3. Subtitusi menggunakan pengembangan Algoritma Caesar yang diusulkan

No.	Plaintext	Caesar Key 3	Pengembangan	Keterangan
1	J	M	N	geser 1 karena posisi plaintext ke 1
2	O	R	T	geser 2 karena posisi plaintext ke 2
3	K	N	Q	geser 3 karena posisi plaintext ke 3
4	O	R	V	geser 4 karena posisi plaintext ke 4
5	P	S	X	geser 5 karena posisi plaintext ke 5
6	R	U	A	geser 6 karena posisi plaintext ke 6
7	A	D	K	geser 7 karena posisi plaintext ke 7
8	M	P	X	geser 8 karena posisi plaintext ke 8
9	U	X	G	geser 9 karena posisi plaintext ke 9
10	D	G	Q	geser 10 karena posisi plaintext ke 10
11	A	D	O	geser 11 karena posisi plaintext ke 11

Penelitian ini pengembangan Algoritma Caesar Cipher ditambah dengan posisi huruf di dalam rangkaian huruf dalam plainteks. Kriptanalis akan kesulitan menganalisis karena harus mengetahui plaintextnya terlebih dahulu. Dari uji coba yang dilakukan ciphertext yang terbentuk sulit untuk di buka secara ilegal.

Contoh terdapat plaintext "JOKO PRAMUDA" dienkripsi menggunakan pengembangan algoritma yang di usulkan oleh paper ini dengan key 3. Pertama data akan dienkrispi kunci pertama yaitu pergeseran 3, lalu pergeseran ke 2 sesuai dengan urutan huruf tersebut dalam plaintext. Rincian cara kerja mengenkripsi ditunjukkan dalam Tabel 3.

Dari plaintext tersebut terdapat 2 huruf yang sama yaitu pertama huruf O, namun ciphertextnya beda dimana 'O' pertama ciphertextnya 'T' dan ciphertext kedua 'V'. Huruf 'A' plaintext juga ada 2, namun berbeda ciphertextnya. 'A' pertama ciphertextnya 'K' sedangkan ke 2 ciphertextnya 'O'. Plaintext yang berurururutan di ururtan abjad dan urutan plaintext seperti 'O' dengan 'P' , juga ciphertext memiliki jarak yaitu 'V' dan 'X'.

4. KESIMPULAN

Penelitian ini mengembangkan algoritma Caesar Cipher untuk mengamankan data nasabah tabungan BPR. Pengembangan dilakukan dengan mengubah kunci ke 2 dengan menggunakan posisi huruf tersebut dalam plaintext. Model ini membuat ciphertext yang terbentuk menjadi berbeda pada huruf yang sama yang terdapat dalam plaintext. Pengembangan ini membuat akses ilegal menjadi lebih sulit dilakukan. Hasil uji coba menunjukkan enkripsi menggunakan algoritma Caesar yang dikembangkan dalam usulan ini tetap sederhana dipemrograman namun kuat dalam pengamanan data. Metode enkripsi yang diusulkan akan membuat data yang berupa teks lebih kuat dalam pengamanan data.

DAFTAR PUSTAKA

Aranski, A.,W., dan kawan kawan(2023) Kamanan Data Anggota Perpustakaan di Universitas XYZ *Jurnal Siteba*, 2, 1, PP. 34-41

Destari, R., A.,(2025) Implementasi Kriptografi dengan *Caesar Cipher* pada Fitur Pesan di WhatsApp untuk Keamanan, *Jurnal Teknik Mesin, Industri, Elektro dan Ilmu Komputer*, 3,4, pp. 169-176

Ferdiansyah, M., Muhammad, H., dan Indra, R., Z., (2024) Implementasi Metode Caesar Cipher Dalam Kriptografi Untuk Keamanan Data Pesan, *Jurnal Multidisiplin Indonesia*, 3, 2, pp. 1296-1302

Hasanah, A., dan kawan kawan (2023), Implementasi Algoritma *Caesar Cipher* untuk Pengamanan Pesan Menggunakan *Java NetBeans, Digital Transformation Technology*, 3,1, pp. 11-19

Hidayat, M., F., Ridho, M., dan Zulfahmi Indra, Z (2024), Metode Caesar Cipher Dalam Kriptografi Untuk Keamanan Data Pesan, *QISTINA: Jurnal Multidisiplin Indonesia* , 3,2, pp. 1296-1302.

Nasution, S., D., (2024), Modifikasi Algoritma Caesar Cipher Menggunakan Linear Congruent Method Untuk Mengamankan Data, Jurnal Informatika, 1,3, pp .95-101

Nasution, A., B., (2019), Implementasi Pengamanan Datta Dengan Menggunakan Algoritma Caesar Cipher dan Transposisi Cipher, Jurnal Teknologi Informasi, 3,1, pp. 1-6

Pratama, P., dan kawan-kawan (2025), Kriptografi Klasik dan Keamanan Dasar : Implementasi Kasir Restoran dengan Pendekatan Metode Caesar Cipher, *Jurnal Sistem Informasi* , 17,1, PP. 243-251.

Pratiwi R. dan kawan-kawan (2022), Perancangan Keamanan Data Pesan Dengan Menggunakan Metode Kriptografi Caesar Cipher, *Bulletin of Information Technology*, 3,4, pp. 267-373

Wahyudi, E., N., dan kawan kawan ((2024), Peningkatan Kemanan Data Melalui Teknik Super Enkripsi Menggunakan Algoritma Vigenere dan Caesar, *Jurnal Informatika Polinema*, 10, 3, pp. 315–321.