ILKOMEDIA
JURNAL ILMU KOMPUTER DAN MULTIMEDIA

Jurnal ILKOMEDIA | Vol. 1, No. 1, Juni 2024
DOI: https://doi.org/10.46510/ilkomedia.v1i1.10 | https://ilkomedia.akb.ac.id/
E-ISSN 3048-1236 | P-ISSN 3048-1678

Pendekripsian *Caesar Chiper* Dengan Menggunakan Teknik-Teknik Kriptanalisis

Uci Julya Ningsih*[1], Sophia Salsabila[2], Isniar Hutapea[3], Dewi Santika[4], Indra Gunawan[5]

[1,2,3,4]Program Studi Sistem Informasi, STIKOM Tunas Bangsa
Pematangsiantar, Indonesia
[5]Program Studi Teknik Informatika, STIKOM Tunas Bangsa
Pematangsiantar, Indonesia

ucijulianingsih@gmail.com[1], sophiasalsabila04@gmail.com[2], isniarhutapea833@gmail.com[3], dewisantika3103@gmail.com[4], indra@amiktunasbangsa.ac.id[5]

Abstract. Cryptology is the science of secret writing that has two parts. Cryptography is a secret writing technique and cryptanalytics is a cryptographic deciphering technique. This research aims to investigate the security and weaknesses of Caesar Cipher, a classic encryption method that has long been known in cryptography. Evaluating the effectiveness and efficiency in decrypting Caesar Cipher's encryption was done by applying various cryptanalysis techniques, including known plain attacks, frequency analysis, and Brute force Search. The security implications of this study highlight the importance of avoiding the use of weak encryption algorithms in modern information security. To be stronger and more resilient to crypto-analysis attacks, it is recommended to switch to encryption algorithms such as AES or RSA.

Keywords: *Cryptography, Cryptanalysis, Frequency Analysis, Brute force Search, Known Plain Attack.*

Abstrak. Kriptologi adalah ilmu penulisan rahasia yang memiliki dua bagian. Kriptografi merupakan teknik penulisan rahasia dan kriptanalisis merupakan teknik menguraikan kriptografi. Penelitian ini bertujuan menginvestigasi keamanan dan kelemahan dari *Caesar Cipher*, sebuah metode enkripsi klasik yang telah lama dikenal dalam kriptografi. Mengevaluasi efektivitas dan efisiensi dalam memecahkan enkripsi *Caesar Cipher* dilakukan dengan menerapkan berbagai teknik kriptanalisis, termasuk *known plain attack*, analisis frekuensi, dan *Brute force Search*. Hasil dari temuan ini menghasilkan bahwa bahwa *Caesar Cipher* rentan terhadap serangan kriptanalisis, seperti yang terungkap melalui analisis yang telah dilakukan. Implikasi keamanan dari hasil penelitian ini menyoroti pentingnya menghindari penggunaan algoritma enkripsi yang lemah dalam keamanan informasi modern. Untuk menjadi lebih kuat dan tangguh terhadap serangan kriptanalisis, direkomendasikan beralih menggunakan algoritma enkripsi seperti AES atau RSA.

Kata Kunci: *Kriptografi, Kriptanalisis, Analisis Frekuensi, Brute force Search, Caesar Chiper, Known Plain Attack.*

I. PENDAHULUAN

Kriptologi adalah ilmu penulisan rahasia. Ini memiliki dua bagian: kriptografi, yang merupakan teknik penulisan rahasia, dan kriptanalisis, yang merupakan teknik menguraikan kriptografi. Kriptologi telah menciptakan beberapa jenis sistem untuk menyembunyikan teks selama 2.500 tahun terakhir. Kriptografi telah digunakan di berbagai bidang dan aplikasi, termasuk komunikasi yang aman, forensik digital, identifikasi dan otentikasi, berbagi rahasia dan menyembunyikan data, pembayaran E, dan sertifikasi [1].

Kriptografi telah menjadi salah satu bidang yang penting dalam dunia keamanan informasi. Seiring dengan kemajuan teknologi, perlindungan terhadap informasi sensitif menjadi semakin krusial. Konsep dari sistem kriptografi pada pengamanan autentikasi dokumen adalah menjamin keaslian, kerahasiaan, dan keamanan dari dokumen elektronik tersebut. Mengetahui bahwa sistem kriptografi dapat menjaga keamanan yang sangat ketat, karena tidak memungkinkan adanya kejadian penyadapan dan pengubahan data oleh pihak luar yang tidak sah. Digunakannya teknik sistem kriptografi untuk melakukan transfigurasi dan transisi terhadap data yang dihasilkan agar tidak dapat dipahami oleh pihak ketiga dengan cara dibuatnya penyandian enkripsi dan deskripsi, untuk menjamin keaslian, kerahasiaan dan keamanan dokumen elektronik [3]. Salah satu teknik kriptografi yang telah dikenal sejak zaman kuno adalah Enkripsi *Caesar Cipher.* Penelitian ini berfokus pada *Caesar Cipher*, sebuah metode kriptografi yang lebih sederhana. Meskipun *Caesar Cipher* lebih sederhana, penelitian ini menunjukkan bahwa metode ini masih memiliki relevansi dan penting untuk dipelajari, terutama dalam konteks kriptanalisis. Dengan memahami kelemahan dan potensi solusi untuk meningkatkan keamanan *Caesar Cipher*, penelitian ini dapat memberikan kontribusi penting dalam pengembangan sistem keamanan informasi yang lebih kokoh di masa depan.

Dalam kasus enkripsi, *Caesar Cipher* adalah salah satu metode kriptografi paling sederhana dan paling awal yang pertama kali digunakan oleh Kaisar Romawi Julius Caesar untuk mengirim pesan rahasia kepada para jenderal tentaranya. Enkripsi ini didasarkan pada pergeseran karakter dalam alfabet sebanyak kunci tertentu. Misalnya, dengan pergeseran 1, A akan digantikan oleh B, B akan digantikan oleh C, dan seterusnya [2]. Namun, seiring dengan perkembangan teknologi dan keterampilan kriptanalisis yang semakin canggih, keamanan *Caesar Cipher* telah menjadi rentan.

Teknik-teknik seperti *known plain attack*, analisis frekuensi dan *Brute force Search* dapat dengan relatif mudah membongkar enkripsi ini.

Pada jurnal ini, akan membahas tentang implementasi pemecahan enkripsi *Caesar Cipher* dengan menggunakan berbagai teknik kriptanalisis yang tersedia. Tujuan dari penelitian ini adalah untuk mengidentifikasi kelemahan dalam enkripsi *Caesar Cipher* serta mengevaluasi efektivitas dan efesiensi dari berbagai teknik kriptanalisis dalam memecahkan enkripsi tersebut. Analisis terhadap beberapa teknik kriptanalisis yang umum digunakan akan dilakukan, seperti *known plain attack*, analisis frekuensi dan *Brute force Search*.

Dengan memahami secara mendalam tentang cara kerja teknik-teknik kriptanalisis tujuan penelitian ini dapat memberikan wawasan yang berharga dalam mengembangkan sistem keamanan informasi yang lebih kokoh di masa depan. Melalui eksperimen dan analisis yang dilakukan dalam jurnal ini. Pemahaman yang lebih baik tentang kelemahan dan potensi solusi untuk meningkatkan keamanan sistem enkripsi akan didapatkan. Dengan demikian, upaya-upaya untuk melindungi informasi sensitif dari ancaman yang berkembang terus menerus dapat ditingkatkan secara signifikan.

II. METODE PENELITIAN

Metode yang digunakan dalam penelitian atau penyusunan jurnal ini adalah metode penelitian kualitatif yaitu dengan melakukan review buku dan karya ilmiah yang akan menjadi tuntunan/rujukan dalam penelitian terhadap teknik-teknik kriptanalisis dan cara teknik-teknik kriptanalisis tersebut mendekripsikan teknik enkripsi *Caesar Cipher.*

Untuk menyusun jurnal ini penulis menggunakan review dari berbagai sumber buku dan juga karya ilmiah. langkah-langkah yang dilakukan penulis dalam melakukan menyusun jurnal adalah sebagai berikut:

1) Mengidentifikasi masalah, yaitu penulis melakukan observasi dan mengulas kembali apa yang telah di ketahui mengenai *Caesar Cipher*, kriptografi dan kriptanalisis, kemudian penulis mengevaluasi apa kelemahan *Caesar Cipher* terhadap teknik-teknik pendekripsian kriptanalisis serta mengidentifikasi apakah teknik-teknik tersebut efesien dan efektif untuk digunakan.
2) Melakukan seleksi dan penyaringan buku dan karya ilmiah yang relevan, yaitu penulis mulai mencari buku atau pun karya ilmiah yang memuat tentang teknik-teknik kriptanalisis.
3) Memulai menganalisis data, yaitu setelah peneliti berhasil mengumpulkan informasi terkait kriptanalisis dan Caesar Cipher, peneliti memulai uji coba untuk mendekripsikan teks yang sebelumnya telah dikunci oleh enkripsi *Caesar Cipher* menggunakan teknik-teknik kriptanalisis.
4) Pelaporan hasil penelitian, setelah penulis melakukan uji coba dan sudah mendapatkan efektivitas dan efesiensi, hasil tersebut dituliskan di sebuah laporan yang mencakup latar belakang hingga kesimpulan.
5) Rekomendasi, penulis memberikan rekomendasi yang sesuai dengan apa yang didapatkan. Rekomendasi yang ditulis dapat menjadi bahan pertimbangan untuk penelitian kedepanya. Hal ini tertulis dengan jelas di bagian kesimpulan.

III. HASIL DAN PEMBAHASAN

A. Hasil

1) *Known-Plain Attack*

Efektivitas :

a) Keterbukaan: *Known-plaintext attack* dapat membantu dalam mengidentifikasi kunci enkripsi yang digunakan dalam enkripsi dan dekripsi. Dengan demikian, kriptanalisis dapat menggunakan *plaintext* yang diketahui untuk memprediksi *ciphertext* yang dihasilkan dan kemudian menggunakan *ciphertext* untuk memprediksi *plaintext* yang diketahui.
b) Keterintegrasi: *Known-plaintext attack* dapat digunakan dalam berbagai aplikasi, seperti enkripsi pesan teks, enkripsi gambar, dan enkripsi audio. Dengan demikian, kriptanalisis dapat menggunakan *plaintext* yang diketahui untuk memprediksi *ciphertext* yang dihasilkan dan kemudian menggunakan *ciphertext* untuk memprediksi *plaintext* yang diketahui.
c) Keteraplikasian: *Known-plaintext attack* dapat digunakan dalam berbagai teknologi, seperti algoritma enkripsi simetris dan asimetris. Dengan demikian, kriptanalisis dapat menggunakan *plaintext* yang diketahui untuk memprediksi *ciphertext* yang dihasilkan dan kemudian menggunakan *ciphertext* untuk memprediksi *plaintext* yang diketahui.

Efisiensi :

a) Ketercepatan: *Known-plaintext attack* dapat dilakukan dengan cepat dan efisien, sehingga dapat membantu dalam menghemat waktu dan sumber daya.

b) Keterbantu: *Known-plaintext attack* dapat membantu dalam mengembangkan strategi kriptanalisis yang efektif dan efisien, sehingga dapat membantu dalam menghemat biaya dan sumber daya.

c) Keterintegrasi: *Known-plaintext attack* dapat digunakan dalam berbagai aplikasi dan teknologi, sehingga dapat membantu dalam meningkatkan keterintegrasi dan keterbantu dalam pengembangan sistem keamanan.

2) Analisis Frekuensi

Efektivitas :

a) Sederhana: Analisis Frekuensi adalah teknik yang relatif sederhana dan mudah diterapkan, sehingga

dapat digunakan oleh para ahli kriptografi dengan tingkat keahlian yang berbeda.

b) Efektif: Analisis Frekuensi dapat membantu dalam mengidentifikasi pola-pola yang digunakan dalam enkripsi, seperti substitusi, transposisi, dan penggunaan kunci. Dengan demikian, analisis ini dapat membantu dalam mengembangkan strategi kriptanalisis yang efektif.

c) Keterbukaan: Analisis Frekuensi dapat digunakan untuk menguji efektivitas dan keamanan penggunaan berbagai algoritma enkripsi, termasuk algoritma yang menggunakan kunci simetri dan asimetri.

d) Keteraplikasian: Analisis Frekuensi dapat digunakan dalam berbagai aplikasi, seperti enkripsi pesan teks, enkripsi gambar, dan enkripsi audio.

Efisiensi :

a) Ketercepatan: Analisis Frekuensi dapat dilakukan dengan cepat dan efisien, sehingga dapat membantu dalam menghemat waktu dan sumber daya.

b) Keterbantu: Analisis Frekuensi dapat membantu dalam mengembangkan strategi kriptanalisis yang efektif dan efisien, sehingga dapat membantu dalam menghemat biaya dan sumber daya.

c) Keterintegrasi: Analisis Frekuensi dapat digunakan dalam berbagai aplikasi dan teknologi, sehingga dapat membantu dalam meningkatkan keterintegrasi dan keterbantu dalam pengembangan sistem keamanan.

3) *Brute force Search*

Efektivitas :

a) Sederhana dan mudah: *Brute force Search* adalah metode yang paling sederhana dan mudah dalam melakukan kriptanalisis. Teknik ini mencoba semua kemungkinan yang ada untuk memecahkan *plaintext*, sehingga sangat efektif dalam menemukan jawaban yang tepat.

b) Pasti menemukan jawabannya: *Brute force Search* pasti akan menemukan jawaban yang tepat jika dimungkinkan, karena mencoba semua kemungkinan yang ada.

c) Tidak bergantung pada pengetahuan: *Brute force Search* tidak bergantung pada pengetahuan tentang algoritma atau kunci yang digunakan, sehingga efektif dalam menemukan jawaban yang tepat tanpa memerlukan pengetahuan tentang sistem kriptografi yang digunakan.

Efisiensi :

a) Tidak efisien: *Brute force Search* tidak efisien karena memerlukan kompleksitas waktu yang besar. Teknik ini mencoba semua kemungkinan yang ada, sehingga memerlukan waktu yang lama untuk menemukan jawaban yang tepat.

b) Lambat: *Brute force Search* sangat lambat, terutama jika panjang *plaintext* atau kunci yang digunakan sangat besar. Hal ini karena teknik ini harus mencoba semua kemungkinan yang ada, sehingga memerlukan waktu yang lama.

c) Tidak kreatif: *Brute force Search* tidak kreatif karena hanya mencoba semua kemungkinan yang ada tanpa menggunakan pengetahuan tentang algoritma atau kunci yang digunakan. Hal ini membuat teknik ini tidak efektif dalam menemukan jawaban yang tepat jika sistem kriptografi yang digunakan sangat kompleks.

B. Pembahasan

1) *Known-Plain Attack*

Known-Plain Attack adalah teknik pencarian kunci enkripsi berdasarkan pengetahuan mengenai pasangan *Plain text-Cipher text*. *Known-Plain Attack* dapat mencari kunci enkripsi pada teknik enkripsi yang masih tergolong rentan, misalnya teknik *Caesar Chiper*. *Caesar Chiper* adalah jenis enkripsi yang menggunakan cara *shift transformation,* dengan rumus umum:

$$C = P + b; \text{ jika } P + b < n P + b - n; \text{ jika } P + b \geq n$$

Dimana :

C = Chiper text
P = Plain text
b = parameter
n = besar pembendaharaan karakter

Sehingga rumus untuk dekripsi dapat diketahui sebagai :

$$P = C - b; \text{ jika } C \geq b C - b + n; \text{ jika } C < b$$

Sebagai contoh:

Tabel 1. Contoh

P/C	Text
P	STIKOM TUNAS BANGSA
C	XYNPTR YZSFX GFSLXF

Jika suatu pasangan *Plain text-Cipher text* diketahui seperti di dalam Tabel 1, maka berdasarkan posisinya, misal

'S' dengan 'X' (S=18, X=23) sehingga dapat diketahui dengan segera parameter *b*=(23-18) mod 26 = 5.

Caesar Chiper sendiri menggunakan huruf A-Z (dengan kode 0-25) sebagai pembendaharaan karakter untuk enkripsi, maka jika digunakan parameter b=5 akan menghasilkan rumus enkripsi:

C = P + 5; jika P < 21P - 21; jika P ≥ 21

Jadi untuk enkripsi (0=A) ditukar dengan (5=F), (1=B) ditukar dengan (6=G) dan begitu juga seterusnya. Sehingga rumus dekripsi dapat diketahui sebagai:

P = C - 5; jika C ≥ 5C + 21; jika C < 5

Known-plaintext attack terhadap enkripsi *Caesar Cipher* adalah jenis serangan yang dapat diprediksi, di mana jika pasangan (atau beberapa pasangan) teks biasa-teks sandi diketahui, maka kunci dapat ditentukan dengan pasti. Kesulitan *known-plaintext attack* yang diketahui tergantung pada kompleksitas rumus enkripsi yang digunakan. Semakin rumit rumusnya, semakin sulit untuk melakukan serangan teks terbuka yang diketahui.

Rumus linear dianggap sederhana dan mudah diserang oleh *Known-plaintext attack*, sementara semakin kompleks dan non-linear rumusnya serta semakin banyak parameter yang digunakan, semakin sulit untuk menghitung kunci berdasarkan rumus tersebut.

2) Analisa Statistik

Semua algoritma enkripsi yang memanfaatkan transformasi pergeseran rentan terhadap analisis statistik, seperti pada pengamatan frekuensi. Contohnya, enkripsi *Caesar Cipher* sangat rentan terhadap analisis frekuensi, karena menggunakan rumus enkripsi sebagai berikut:

C = P + b (Mod n)

Jika nilai n diketahui dan pasangan C dan P dapat ditebak secara tepat, maka parameter b dapat dihitung. Pasangan nilai yang direkomendasikan untuk dicoba adalah yang sesuai dengan statistik frekuensi penggunaan.

Sebagai Misalnya, dalam Bahasa Indonesia, huruf 'A' memiliki frekuensi penggunaan tertinggi, sementara dalam Tabel 1, huruf 'F' dan 'X' adalah yang paling umum digunakan. Oleh karena itu, kemungkinan besar huruf 'F' atau 'X' adalah hasil enkripsi dari 'A'. Dengan demikian, jika kita menggunakan 'F' atau 'X' sebagai nilai C dan 'A' sebagai P, kemungkinan besar rumus enkripsi akan menghasilkan parameter b yang benar.

Maka akan diuji dua kemungkinan yang dapat menghasilkan Plain text yang masuk akal:

Tabel 2. Pengujian

Pasangan	Kode acak	Kode asli	Nilai *b*	Hasil dekripsi
F-A	5	0	b=5	STIKOM TUNAS BANGSA
X-A	23	0	b=23	ABQSWU BCVIA JIVOAI

Dari analisis frekuensi, ditemukan bahwa hanya ketika b=5 hasil dekripsi adalah "STIKOM TUNAS BANGSA", yang merupakan teks yang masuk akal. Oleh karena itu, kita dapat memastikan bahwa b=5.

Analisis frekuensi di atas dilakukan dengan asumsi bahwa teks asli berbahasa Indonesia, di mana huruf "A" memiliki frekuensi penggunaan yang paling tinggi. Namun, teks asli tidak selalu akan mencerminkan statistik empiris dengan sempurna. Meskipun demikian, secara umum, semakin panjang teks yang digunakan untuk analisis, semakin mirip statistik penggunaannya dengan data empiris. Hal ini berarti semakin besar kemungkinan keberhasilan analisis frekuensi. Pada contoh di atas, frekuensi penggunaan huruf "A" cukup mendekati data empiris, sehingga analisis frekuensi berhasil.

Pada *shift transformation*, karena rumusnya sederhana dengan hanya satu parameter, setiap percobaan cukup dilakukan dengan satu persamaan. Strategi pencarian yang efektif adalah menggunakan pasangan yang memiliki frekuensi penggunaan yang tinggi, yaitu mengaitkan huruf yang sering muncul dalam teks terenkripsi dengan huruf yang frekuensinya besar menurut data empiris. Namun, jika rumus transformasinya lebih kompleks dengan lebih dari satu parameter, setiap percobaan akan memerlukan lebih dari satu persamaan, di mana jumlah persamaan yang dibutuhkan setidaknya sama dengan jumlah parameter yang harus dicari.

3) *Brute force Search*

Salah satu karakteristik dari sistem enkripsi yang efektif adalah bahwa dekripsi tanpa kunci hanya bisa dipecahkan melalui *Brute force Search*, di mana semua kemungkinan kunci harus diuji. Jumlah kemungkinan kunci tersebut sebaiknya besar sehingga memakan waktu yang sangat lama untuk mencoba semuanya. Jika jumlah kunci yang harus diuji terlalu sedikit, maka sistem enkripsi dapat rentan terhadap serangan *brute force*.

Ukuran kunci enkripsi, yang diukur dalam jumlah bit, menentukan jumlah kemungkinan kunci yang perlu diuji dalam serangan *brute force*. Untuk kunci sebesar n bit, jumlah kemungkinan kunci adalah 2n, dan secara rata-rata, kunci akan ditemukan setelah mencoba 2n-1 kemungkinan (setengah dari semua kemungkinan). Oleh karena itu, keamanan enkripsi dapat terancam oleh serangan *brute force* jika jumlah kemungkinan kunci yang dapat diuji mencapai 2n dalam waktu

yang relatif singkat. Namun, selain bergantung pada jumlah kemungkinan kunci yang perlu diuji, waktu yang diperlukan juga bergantung pada kecepatan perangkat keras yang digunakan.

Caesar Cipher dapat dipecahkan tidak hanya melalui analisis frekuensi atau *known-plaintext attack*, tetapi juga melalui *Brute force Search* karena semua kemungkinan kunci (dari b=1 hingga b=25) dapat dicoba dalam waktu yang relatif singkat. Tabel 1 menunjukkan hasil dari *Brute force Search* pada teks acak *Caesar cipher*. Dari seluruh kemungkinan kunci, hanya b=5 yang menghasilkan teks yang masuk akal. Karena jumlah kemungkinan kunci tergolong kecil, *Brute force Search* dapat dilakukan tanpa menggunakan komputer. Namun, jika jumlah kunci yang perlu diuji sangat besar, komputer dapat digunakan untuk membantu dalam analisis.

IV. KESIMPULAN

Penelitian ini merupakan upaya untuk menyelidiki keamanan dan kelemahan dari *Caesar Cipher*, salah satu bentuk enkripsi klasik yang masih banyak dipelajari dalam konteks kriptografi. Dengan menerapkan berbagai teknik kriptanalisis yang tersedia, mengidentifikasi sejumlah kerentanan dalam *Caesar Cipher* dan mengevaluasi efektivitas berbagai pendekatan untuk memecahkan enkripsi tersebut telah berhasil dilakukan.

Pertama, hasil analisis menegaskan bahwa *Caesar Cipher* tidak lagi menjadi pilihan yang aman untuk digunakan dalam komunikasi yang membutuhkan tingkat keamanan yang serius. Kelemahan mendasar terhadap serangan *brute force* dan analisis frekuensi membuatnya rentan terhadap serangan bahkan oleh penyerang yang memiliki pengetahuan dasar tentang kriptografi. Kebutuhan akan keamanan informasi yang modern menuntut algoritma enkripsi yang lebih tangguh dan lebih mampu melawan serangan kriptanalisis.

Dengan menerapkan teknik-teknik kriptanalisis seperti *known-plaintext attack*, analisis frekuensi, dan *Brute force Search*, enkripsi *Caesar Cipher* dengan cepat mampu dipecahkan. Hasil analisis tersebut menunjukkan bahwa bahkan dengan sumber daya yang terbatas, penyerang dapat dengan mudah mengungkapkan pesan yang dienkripsi menggunakan Caesar Cipher. Oleh karena itu, penting bagi pengguna untuk memahami batasan keamanan dari algoritma ini dan mempertimbangkan opsi yang lebih aman.

Dalam konteks implikasi keamanan, penelitian ini menyoroti pentingnya mengadopsi praktik kriptografi yang kuat dan aman. Penggunaan algoritma enkripsi yang lemah seperti *Caesar Cipher* dapat mengakibatkan kerentanan serius terhadap serangan dan eksploitasi oleh pihak yang tidak bermaksud baik. Oleh karena itu, disarankan untuk menghindari penggunaan *Caesar Cipher* dalam aplikasi yang membutuhkan tingkat keamanan yang tinggi, dan sebaliknya, beralih ke algoritma modern seperti AES atau RSA yang telah terbukti lebih kuat dan lebih tahan terhadap serangan kriptanalisis.

DAFTAR PUSTAKA

[1] A. Al-Sabaawi, "Cryptanalysis of Vigenère cipher: *method implementation. In 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*," IEEE, pp. 1-4, Dec. 2020.

[2] A. Al-Sabaawi, "Cryptanalysis of Classic Ciphers: Methods Implementation Survey. In 2021 International Conference on Intelligent Technologies (CONIT)," IEEE, pp. 1-6, June. 2021.

[3] A. R Harahap and T. A. Salim, "Sistem kriptografi pada Pengamanan Autentikasi Dokumen Elektronik: Systematic Literature Review," KHAZANAH: Jurnal Pengembangan Kearsipan, vol. 16, no. 2, pp. 203-220, 2023.

[4] F. D. Ardiansyah, A. Damayanti, C. A. M. Putri, A. F. D. Rany, S. J. Biroso and M. Tahir, "Implementasi Kriptografi Caesar Chiper Pada Aplikasi Enkripsi dan Dekripsi," Jurnal ilmiah Sistem Informasi dan Ilmu Komputer, vol. 3, no. 1, pp. 105-112, 2023.

[5] F. N. Faqih, M. Tahir, Z. Ashfarina, R. I. Faa'izzani, S. Alfarisi and F. Erfani, "Efektivitas Peningkatan Keamanan Login Pada Website Menggunakan Enkripsi Caesar Chipper," Jurnal Adijaya Multidisplin, vol. 1, no. 2, pp. 354-362, 2023.

[6] M. Hidayat, M. Tahir, A. Sukriyadi and A. Sulton, "Penerapan Kriptografi Caesar Chiper dalam Pengamanan Data," Jurnal Ilmiah Multidisiplin, vol. 2, no. 03, pp. 35-41, 2023.

[7] Sentot Kromodimoeljo, "Teori Dan Aplikasi Kriptografi," SPK IT Consulting, 2019.

[8] A. Luthfi, B. S. Pramono, and D. R. Havatilla, "Implementation of *Caesar Cipher* and Transposition Cipher Cryptography on Telegram Bot," Prosiding Sains dan Teknologi, vol. 3 no. 1, pp. 35-40, 2023.

[9] A. S. Manjunatha, "Secure Data Transmission Using *Caesar Cipher* Encryption in Wireless Sensor Networks," Journal of Namibian Studies: History Politics Culture, vol. 34, pp. 1165-1178, 2023.

[10] M. I. Mihailescu and S. L. Nita, "Classic Cryptography. Cryptography and Cryptanalysis in MATLAB: Creating and Programming Advanced Algorithms," pp. 51-68, 2021.

[11] R. Sinaga, "Modifikasi Algoritma Caesar Chiper Dengan Menambahkan Key Untuk Peningkatan Keamanan," Computer Science Research and Its Development Journal, vol. 15, no. 2, pp. 156-166, 2023.

[12] A. Tripathi, J. Chakraborty, S. Anzum and S. B. Pal, "A new Modified method of Cryptography using Caesar Cipher," American Journal of Electronics & Communication, vol. 1, no. 4, pp. 13-15, 2021.

[13] D. Veera, R. Mangrulkar, C. Bhadane, K. Bhowmick and P. Chavan, "Modified *Caesar Cipher* and Card Deck Shuffle Rearrangement Algorithm for Image Encryption," Journal of Information and Telecommunication, pp. 1-21, 2023.

[14] R. Verma, A. Kumari, A. Anand and V. S. S. Yadavalli, "Revisiting shift cipher technique for amplified data security," Journal of Computational and Cognitive Engineering, vol. 3, no. 1, pp. 8-14, 2024.

[15] M. Hidayat, M. Tahir, A. Sukriyadi, A. Sulton, A. C. A. S., and F. S. A., "Penerapan Kriptografi Caesar Chiper dalam Pengamanan Data," Jurnal Ilmiah Multidisiplin, vol. 2, no. 03. [Online]. Available: https://doi.org/10.56127/jukim.v2i03.619.

[16] M. Hamni, M. K. Amri, S. Rezeky and A. B. Nasution, "Penerapan Keamanan Data dengan Menggunakan Metode Caesar Chiper Untuk Mengamankan Database MySQL," Jurnal Informatika Teknologi dan Sains, vol. 4, no. 4, pp. 472-477, Nov. 2022.