ADIJAYA
Jurnal Multidisiplin
https://e-journal.naureendigition.com/index.php/mj
Vol. 01 No. 02, 2023, Hal. 354–362
E-ISSN : 2964-7606

Efektivitas Peningkatan Keamanan Login Pada Website Menggunakan Enkripsi Caesar Chipper

Fauziah Nur Faqih[1], Muhlis Tahir[2], Zarwanda Ashfarina[3], Robby Irsyad Faa'izzani[4], Salman Alfarisi[5], Faisal Erfani[6]

Fauziah.nf98@gmail.com muhlis.tahir@trunojoyo.ac.id
robbyirsad106@gmail.com 190631100105@student.trunojoyo.ac.id
putratunggal165954@gmail.com faisalerfaniist@gmail.com

Fakultas Ilmu Pendidikan, Universitas Trunojoyo Madura, Indonesia

Abstrak Algoritma Caesar Cipher merupakan salah satu algoritma kriptografi klasik yang digunakan untuk mengamankan pesan dengan cara menggeser setiap huruf pada pesan sebanyak n kali. Meskipun tergolong sederhana, algoritma ini masih sering digunakan dalam berbagai sistem pengamanan, termasuk dalam sistem login website. Tujuan dari penelitian ini ialah untuk mengetahui efektivitas dari penggunaan algoritma Caesar Cipher pada penerapan login website Algoritma Caesar Cipher memiliki kelebihan dalam hal keamanan, efisiensi, dan kemudahan penerapan. Penelitian ini menggunakan metode kualitatif dengan Teknik pengumpulan data studi literature review yang dapat dicari pada artikel ilmiah. Berdasarkan hasil menunjukkan bahwa algoritma Caesar Cipher masih relevan dan efektif digunakan dalam menjaga keamanan sistem login website di era digital saat ini. algoritma ini juga memiliki kelemahan dalam hal rentang kunci yang terbatas dan keterbatasan dalam penggunaannya untuk mengenkripsi data yang lebih kompleks. Dalam era digital saat ini, keamanan sistem login website sangat penting untuk melindungi data pribadi dan informasi sensitif pengguna. Dengan menggunakan algoritma Caesar Cipher sebagai teknik pengamanan, sistem login website dapat terhindar dari akses ilegal, pencurian, dan pemalsuan data. Implementasi algoritma ini dapat membantu dalam meminimalisir risiko keamanan dan menjaga privasi pengguna.

Kata Kunci: Kriptografi, Chiper Text, Login Website

Abstract *The Caesar Cipher algorithm is one of the classic cryptographic algorithms used to secure messages by shifting each letter in the message n times. Even though it is relatively simple, this algorithm is still often used in various security systems, including in website login systems. The purpose of this study is to determine the effectiveness of using the Caesar Cipher algorithm for implementing website logins. The Caesar Cipher algorithm has advantages in terms of security, efficiency, and ease of application. This study uses a qualitative method with data collection techniques for literature review studies that can be found in scientific articles. Based on the results, it shows that the Caesar Cipher algorithm is still relevant and effectively used in maintaining website login system security in today's digital era. This algorithm also has weaknesses in terms of limited key ranges and limitations in its use to encrypt more complex data. In today's digital era, website login system security is very important to protect users' personal data and sensitive information. By using the Caesar Cipher algorithm as a security technique, the website login system can avoid illegal access, theft, and data forgery. Implementation of this algorithm can help minimize security risks and maintain user privacy.*

Keywords: *Cryptography, Cipher Text, Website Login*

Pendahuluan

Peningkatan teknologi informasi dan internet telah membuat banyak orang bergantung pada internet untuk melakukan kegiatan sehari-hari, termasuk penggunaan website untuk berkomunikasi, berbelanja, atau bahkan melakukan transaksi keuangan. Namun, keamanan informasi pengguna menjadi isu penting dalam penggunaan website ini. Salah satu cara untuk meningkatkan keamanan login pada website adalah dengan menggunakan enkripsi Caesar Cipher. Enkripsi Caesar Cipher adalah salah satu metode enkripsi sederhana yang dapat membantu melindungi informasi login dari serangan hacker atau pencurian identitas (Setyawati, 2019).

Enkripsi Caesar Cipher adalah salah satu teknik enkripsi klasik yang sangat sederhana, di mana setiap karakter pada pesan diubah dengan karakter lain yang terletak pada jarak tetap pada alfabet. Metode ini dianggap sangat sederhana namun cukup efektif untuk mengamankan informasi login pada website. Dalam enkripsi Caesar Cipher, pesan yang dienkripsi dapat dengan mudah di-dekripsi dengan mengetahui jarak pergeseran dan alfabet yang digunakan. Oleh karena itu, meskipun metode ini sederhana, penggunaannya dalam meningkatkan keamanan login pada website tetap efektif dan banyak digunakan. Salah satu keuntungan utama menggunakan enkripsi Caesar Cipher untuk meningkatkan keamanan login pada website adalah kemudahan penerapan. Enkripsi Caesar Cipher dapat dengan mudah diterapkan pada website yang ada dengan biaya yang relatif murah. Selain itu, metode ini tidak memerlukan perangkat keras tambahan atau pengetahuan teknis yang mendalam untuk memahami atau menerapkannya. Oleh karena itu, enkripsi Caesar Cipher menjadi salah satu pilihan yang populer untuk meningkatkan keamanan login pada website.

Walaupun metode enkripsi Caesar Cipher cukup efektif, beberapa kelemahan tetap ada. Salah satu kelemahan utama dari metode ini adalah rentan terhadap serangan Brute Force, di mana serangan tersebut dapat memecahkan sandi dengan mencoba setiap kemungkinan pergeseran hingga sandi berhasil dipecahkan. Serangan Brute Force dilakukan dengan mencoba setiap kemungkinan pergeseran pada setiap karakter dalam sandi hingga sandi berhasil dipecahkan. Dalam kasus metode enkripsi Caesar Cipher, Brute Force dapat dilakukan dengan mencoba setiap kemungkinan pergeseran pada setiap karakter dalam pesan hingga pesan asli berhasil ditemukan. Oleh karena itu, perlu dilakukan beberapa modifikasi pada metode ini agar lebih sulit untuk dipecahkan dengan serangan Brute Force (Setiawan dan Fatimah, 2016). Meskipun begitu, enkripsi Caesar Cipher tetap menjadi salah satu cara yang efektif untuk

meningkatkan keamanan login pada website dengan biaya yang terjangkau dan kemudahan dalam penerapan.

Algoritma Caesar Cipher dapat digunakan dalam pengamanan login website dengan cara mengenkripsi password yang dimasukkan oleh pengguna sebelum dikirim ke server (Widodo, 2017). Dalam hal ini, password yang dimasukkan akan diubah menjadi teks acak yang hanya dapat dibaca oleh sistem yang memiliki kunci enkripsi yang tepat. Ketika pengguna melakukan login, password yang dimasukkan akan dienkripsi dan kemudian dibandingkan dengan password yang tersimpan di server yang juga telah dienkripsi menggunakan algoritma yang sama (Lombu et al, 2018). Jika kedua password yang telah dienkripsi cocok, maka pengguna diizinkan untuk mengakses akun mereka. Pada proses login website, pengguna biasanya diminta untuk memasukkan username dan password sebagai langkah verifikasi identitas. Namun, masalah keamanan dapat timbul ketika data yang dikirimkan antara pengguna dan server dapat disadap oleh pihak yang tidak bertanggung jawab. Untuk mengatasi hal ini, algoritma Caesar Cipher dapat digunakan sebagai metode pengamanan untuk melindungi password yang dimasukkan oleh pengguna.

Hal ini sesuai dengan penelitian yang berjudul "Improving Caesar Cipher Security by Random Key Generation" oleh Muhammad Saqib Niaz, Syed Ali Abbas Bukhari, dan Muhammad Asim membahas tentang penggunaan metode enkripsi Caesar Cipher dengan kunci acak dalam meningkatkan keamanan pada sistem keamanan login. Hasil penelitian ini menunjukkan bahwa penggunaan kunci acak pada enkripsi Caesar Cipher dapat mengurangi kemungkinan serangan Brute Force dan meningkatkan keamanan sistem (Wijaya, 2018). Metode yang digunakan dalam penelitian ini adalah eksperimen dengan membandingkan dua skenario enkripsi Caesar Cipher, yaitu dengan menggunakan kunci tetap dan dengan menggunakan kunci acak. Hasil dari eksperimen menunjukkan bahwa penggunaan kunci acak pada enkripsi Caesar Cipher dapat mengurangi kemungkinan serangan Brute Force dengan signifikan. Hal ini terbukti dari hasil uji coba di mana enkripsi Caesar Cipher dengan kunci acak menghasilkan nilai rata-rata waktu yang lebih tinggi dibandingkan dengan enkripsi Caesar Cipher dengan kunci tetap (Sudrajat Dan Windarto, 2018).

Selain itu, penelitian ini juga menunjukkan bahwa penggunaan kunci acak pada enkripsi Caesar Cipher dapat meningkatkan keamanan sistem secara keseluruhan. Hal ini dikarenakan dengan penggunaan kunci acak, maka setiap pesan yang dienkripsi akan menggunakan kunci yang berbeda-beda, sehingga mengurangi kemungkinan terjadinya serangan dengan teknik yang sama pada pesan yang berbeda. Dengan demikian, maka peneliti teratirk untuk menganalisis keefektifan penggunaan enkripsi Caesar Cipher dalam meningkatkan keamanan login pada website.

Metode

Penelitian ini akan menggunakan metode penelitian kualitatif, yang bertujuan untuk memahami fenomena sosial atau manusia secara mendalam, serta mengeksplorasi makna dan pengalaman yang terkait dengan topik penelitian. Teknik pengumpulan data yang digunakan adalah studi literatur, dengan cara mengumpulkan karya ilmiah seperti jurnal, artikel, buku, dan dokumen lainnya yang relevan dengan topik penelitian (Khairina, 2016). studi literatur adalah teknik penelitian yang dilakukan dengan mempelajari dan menganalisis berbagai sumber literatur atau dokumen yang relevan dengan topik penelitian yang ingin diangkat. Sumber literatur yang dimaksud dapat berupa buku, jurnal ilmiah, tesis, laporan penelitian, artikel, dan berbagai dokumen lainnya yang berkaitan dengan topik yang akan diteliti.

Dengan mengumpulkan 10 jurnal yang berkaitan dengan topik penelitian, peneliti akan menganalisis dan mengevaluasi hasil penelitian yang dilakukan oleh peneliti lain di masa lalu, serta memperoleh landasan teori dan konsep yang dibutuhkan dalam penelitian ini. Selain itu,

penelitian ini juga akan menggunakan teknik analisis data yang relevan dengan metode penelitian kualitatif, seperti content analysis atau thematic analysis, untuk menganalisis data yang diperoleh dari sumber literatur yang telah dikumpulkan.

Hasil dan Pembahasan

Dalam era digital saat ini, keamanan informasi menjadi hal yang sangat penting. Banyak organisasi dan perusahaan yang memerlukan sistem keamanan yang efektif untuk melindungi data mereka dari ancaman keamanan. Salah satu teknik yang dapat digunakan untuk mengamankan data adalah kriptografi, yaitu teknik pengamanan data yang menggunakan algoritma kunci untuk mengenkripsi data agar hanya dapat diakses oleh orang yang memiliki kunci yang tepat.

Salah satu algoritma kriptografi yang populer dan masih banyak digunakan hingga saat ini adalah algoritma Caesar Cipher. Algoritma ini sangat sederhana, namun cukup efektif dalam menjaga keamanan data. Berdasarkan hasil yang telah peneliti peroleh melalui studi literature review dapat dilihat pada tabel berikut ini:

Tabel 1. Hasil Studi Literature Review

Penulis	Judul	Hasil Penelitian
bri Aditya , Mohammad Rizky , Revano Arya Saputra , Fikri Abei	"Sistem Login Menggunakan Caesar Chipper Berbasis Web Login System Using Web-Based Caesar Chipper"	penerapan Algoritma Caesar chipper bisa dijadikan Teknik pengamanan system login dengan baik walaupun Algoritma ini tergolong sederhana namun tingkat keamanan nya cukup baik dalam melindungi para user atau pengguna agar lebih aman dari para penyadap dan peretas yang tidak bertanggung jawab maupun mejadi upaya dalam perlindungan data data yang di miliki (Aditya et al, 2023).
Fcahry Franata	"Implementasi Algoritma Base 64 dan Caesar Chipher dalam pengamanan web login siswa pada SMK-TR panca budi Medan"	Dengan diterapkannya metode ini, maka dapat mencegah serta meminimalisir kemungkinan terjadinyaakses ilegal,pencurian, dan pemalsuandata. SelProses dalam penerapan base64dan Caesar cipherini tidakterlalu rumit, akan tetapi dampak dalam pengamanan data cukup baik (Franata, 2021).
Vebby , Sya'banu Ahmad , Lucky Lhaura Van FC	"Penerapan Algoritma Caesar Cipher Dalam Metode Kriptografi Klasik Pada Panic Button (Studi Kasus Fasilkom Unilak)"	Algoritma Caesar Cipher dan dimodelkan dengan metode FAST. Dimana nantinya sistem login untuk user akan dienkripsi dengan metode kriptografi klasik. Hasil penelitian ini berupa sistem pengaduan berbasis web yang akan memudahkan mahasiswa dalam melaporkan pengaduan yang mana sistem ini bersifat anonym (Veby dan Van, 2023)
Radithya Pramuditha Yenadi, Fauziah, Deny Hidayatullah	"Implementasi Metode Caesar Cipher Dalam Penerapansistem E-Voting Berbasis Web Pada Pemilihan Abangnone Jakarta"	Hasil penelitianyang dilakukan terbukti berhasil baik dari segi penggunaan web untuk melakukan pemilihan dankeamanan yang digunakan berhasil melakukan enkripsi dan dekripsi data penggunanya (Yenadi et al, 2020)
Adnan Buyung Nasution	"Implementasi Pengamanan Data Dengan Menggunakan Algoritma Caesar Cipher Dan Transposisi Cipher"	Caesar Cipher dan Transposisi dapat mengamankan data dan mengembalikan data tanpa merubah bentuk dari aslinya (plainteks) (Nasution, 2019).

Transposisi Cipher untuk meningkatkan tingkat keamanan sistem. Selain itu, Caesar Cipher juga telah diterapkan dalam berbagai jenis aplikasi seperti pengaduan berbasis web dan sistem e-voting berbasis web. Penelitian menunjukkan bahwa metode ini cukup efektif dalam mengamankan data pengguna dan meningkatkan integritas sistem. Oleh karena itu, algoritma Caesar Cipher masih relevan dan efektif dalam menjaga keamanan sistem di era digital saat ini. Meskipun algoritma Caesar Cipher telah ada selama berabad-abad dan termasuk algoritma kriptografi yang relatif sederhana, tetapi masih banyak digunakan dalam menjaga keamanan sistem di era digital saat ini. Algoritma ini dianggap relevan karena keamanannya masih cukup baik dalam melindungi data dari para pengintai yang tidak bertanggung jawab. Meskipun algoritma ini sederhana, tetapi tetap efektif dalam menjaga keamanan data.

Algoritma Caesar Cipher dianggap efektif dalam menjaga keamanan sistem di era digital saat ini karena tingkat keamanannya yang cukup tinggi dan penerapannya yang mudah. Dalam penelitian-penelitian yang dilakukan, banyak hasil yang menunjukkan bahwa penggunaan algoritma ini dapat mencegah akses ilegal, pencurian, pemalsuan, serta melindungi data pengguna agar lebih aman dari para penyadap dan peretas yang tidak bertanggung jawab. Oleh karena itu, algoritma ini masih banyak digunakan dalam sistem keamanan, terutama pada sistem login dan web-based.

Dalam era digital saat ini, keamanan data merupakan hal yang sangat penting dan vital. Oleh karena itu, diperlukan teknologi dan metode kriptografi yang mumpuni untuk menjaga keamanan data yang ada (Gunadhi dan Nugraha, 2016). Meskipun banyak teknologi kriptografi baru yang berkembang, namun algoritma Caesar Cipher masih menjadi salah satu pilihan yang dipertimbangkan karena mudah diterapkan dan memiliki keamanan yang cukup baik. Algoritma ini mampu menjaga keamanan data dengan baik dan terbukti efektif dalam penerapannya pada berbagai sistem keamanan di era digital saat ini.

Salah satu kelebihan algoritma Caesar Cipher dalam pengamanan login website adalah kemudahan dalam implementasinya. Algoritma ini cukup sederhana dan mudah dipahami, sehingga dapat diimplementasikan dengan cepat pada sistem login website tanpa memerlukan sumber daya yang besar. Selain itu, Caesar Cipher juga cukup efektif dalam mengamankan data login karena tingkat keamanannya yang relatif tinggi dibandingkan dengan metode pengamanan login website yang lebih sederhana, seperti password yang lemah atau tanpa pengamanan sama sekali.

Selain itu, algoritma Caesar Cipher juga dapat digunakan untuk melakukan enkripsi data dalam jumlah besar dengan cepat. Hal ini membuat algoritma ini ideal digunakan dalam sistem login website yang memiliki banyak pengguna. Dengan menggunakan Caesar Cipher, sistem login website dapat mengenkripsi data login secara otomatis dengan cepat dan mudah, sehingga dapat mengamankan data login pengguna dengan efektif. Dalam hal ini, Caesar Cipher dapat membantu melindungi informasi sensitif dan data pribadi dari para pengguna website dari ancaman yang tidak diinginkan seperti akses ilegal, pencurian data, atau peretasan sistem.

Algoritma Caesar Cipher memiliki beberapa kelemahan yang dapat dieksploitasi oleh penyerang. Beberapa kelemahan yang terdapat pada algoritma ini antara lain:

1. Rentang kunci yang terbatas

Kelemahan pertama dari algoritma Caesar Cipher adalah rentang kunci yang terbatas. Algoritma ini hanya memiliki 25 kemungkinan kunci, yaitu setiap pergeseran huruf dalam alfabet. Artinya, jika pesan yang dienkripsi menggunakan Caesar Cipher, maka hanya ada 25 kemungkinan kunci yang harus dicoba oleh penyerang untuk membuka pesan tersebut. Rentang kunci yang terbatas ini membuat mudah bagi penyerang untuk melakukan serangan brute force, yaitu mencoba semua kemungkinan kunci hingga menemukan kunci yang tepat. Dengan adanya

teknologi komputer saat ini, serangan brute force menjadi lebih mudah dilakukan karena komputer dapat melakukan percobaan kunci secara otomatis dalam waktu yang sangat singkat (Munawar dan Putri, 2020).

Sebagai contoh, jika pesan yang dienkripsi adalah sebuah kata yang hanya terdiri dari 4 huruf, maka hanya ada 25 x 25 x 25 x 25 = 390,625 kemungkinan kunci yang harus dicoba oleh penyerang. Meskipun angka ini mungkin terlihat kecil, namun jika pesan yang dienkripsi lebih panjang dan kompleks, maka jumlah kemungkinan kunci yang harus dicoba juga semakin besar. Hal ini membuat algoritma Caesar Cipher menjadi kurang efektif dalam mengamankan pesan.Pola huruf yang terlihat. Karena algoritma ini hanya melakukan pergeseran huruf dalam alfabet, maka pola huruf pada teks asli dan hasil enkripsi masih terlihat sama. Hal ini dapat memudahkan penyerang untuk melakukan analisis dan menebak kunci yang digunakan.

2. Rentang karakter yang terbatas

Algoritma Caesar Cipher hanya dapat mengenkripsi karakter-karakter tertentu dalam alfabet, seperti huruf, angka, dan beberapa tanda baca yang terbatas. Karakter-karakter lain seperti gambar, suara, atau video tidak dapat dienkripsi menggunakan algoritma ini. Hal ini membuat algoritma ini kurang fleksibel dalam mengenkripsi data yang lebih kompleks, terutama pada era digital saat ini di mana data yang digunakan semakin beragam dan kompleks.

Selain itu, meskipun algoritma Caesar Cipher dapat mengenkripsi karakter-karakter tertentu, namun proses enkripsi yang dilakukan masih dapat ditebak oleh penyerang yang ahli di bidang kriptografi. Sebagai contoh, jika penyerang mengetahui bahwa pesan yang dienkripsi menggunakan algoritma Caesar Cipher, maka penyerang dapat dengan mudah melakukan serangan brute force dengan mencoba semua kemungkinan kunci enkripsi yang tersedia, yaitu sebanyak 25 kemungkinan pergeseran huruf dalam alfabet. Oleh karena itu, algoritma Caesar Cipher kurang aman jika digunakan untuk mengamankan data-data rahasia yang sangat penting dan bersifat kritikal, seperti data kesehatan, keuangan, atau data militer.

3. Rentang serangan yang luas

Selain serangan brute force, algoritma Caesar Cipher juga rentan terhadap serangan lain seperti analisis frekuensi dan serangan kombinasi. Serangan analisis frekuensi dilakukan dengan menganalisis frekuensi kemunculan huruf pada teks terenkripsi untuk menebak kunci yang digunakan. Sedangkan serangan kombinasi dilakukan dengan mengombinasikan beberapa algoritma enkripsi untuk meningkatkan kekuatan serangan.

Kesimpulan

Berdasarkan pembahasan di atas, dapat disimpulkan bahwa algoritma Caesar Cipher memiliki hasil yang sangat efektif untuk digunakan sebagai pssword login website. kelebihan dan kelemahan dalam penggunaannya untuk menjaga keamanan sistem login pada website. Kelebihan utamanya adalah mudah diimplementasikan dan cukup efektif dalam menjaga keamanan data, terutama jika digunakan bersamaan dengan teknik pengamanan lainnya. Namun, kelemahannya termasuk rentang kunci yang terbatas dan rentan terhadap serangan brute force.

Daftar Referensi

Aditya, F., Rizky, M., Saputra, R. A., & Abei, F. (2023). Sistem Login Menggunakan Caesar Chipper Berbasis Web. *Prosiding Sains dan Teknologi*, *2*(1), 267-271.

Aditya, F., Rizky, M., Saputra, R. A., & Abei, F. (2023). Sistem Login Menggunakan Caesar Chipper Berbasis Web. Prosiding Sains dan Teknologi, 2(1), 267-271.

Franata, F. (2021). Implementasi Algoritma Base64 dan Caesar Cipher Dalam Pengamanan Web Login Siswa Pada SMK-TR Panca Budi 1 Medan. *Kumpulan Karya Ilmiah Mahasiswa Fakultas sains dan Tekhnologi*, *1*(1), 175-175.

Gunadhi, E., & Nugraha, A. P. (2016). Penerapan Kriptografi Base64 Untuk Keamanan URL (Uniform Resource Locator) Website Dari Serangan SQL Injection. Jurnal Algoritma, 13(2), 391-398.

Khairina, D. M. (2016). Analisis Keamanan Sistem Login. Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer, 6(2), 64-67.

Lombu, D., Tarihoran, S. D., & Gulo, I. (2018). Kombinasi Mode Cipher Block Chaining Dengan Algoritma Triangle Chain Cipher Pada Penyandian Login Website. J-SAKTI (Jurnal Sains Komputer dan Informatika), 2(1), 1-11.

Munawar, Z., & Putri, N. I. (2020). Keamanan Jaringan Komputer Pada Era Big Data. J-SIKA| Jurnal Sistem Informasi Karya Anak Bangsa, 2(01), 14-20.

Nasution, A. B. (2019). Implementasi Pengamanan Data Dengan Menggunakan Algoritma Caesar Cipher Dan Transposisi Cipher. *(JurTI) Jurnal Teknologi Informasi*, *3*(1), 1-6.

Setiawan, A., & Fatimah, T. (2021). Implementasi Algoritma Kriptografi RC4 Untuk Keamanan Database Aplikasi Penggajian Karyawan Berbasis Web Pada PT. Trans Intra Asia. SKANIKA, 4(1), 66-71.

Setyawati, E., Widjayanti, C. E., Siraiz, R. R., & Wijoyo, H. (2021). Pengujian keamanan komputer kriptografi pada surat elektronik berbasis website dengan enkripsi metode MD5. Jurnal Manajamen Informatika Jayakarta, 1(1), 56-67.

Sudrajat, A., & Windarto, W. (2018). APLIKASI KEAMANAN DATABASE MENGGUNAKAN ALGORITMA KRIPTOGRAFI TRIANGLE CHAIN CIPHER BERBASIS DESKTOP. SKANIKA, 1(2), 597-603.

Vebby, V., & Van FC, L. L. (2023). PENERAPAN ALGORITMA CAESAR CIPHER DALAM METODE KRIPTOGRAFI KLASIK PADA PANIC BUTTON. *ZONAsi: Jurnal Sistem Informasi*, *5*(1), 126-136.

Widodo, A. (2017). Implementasi Monitoring Jaringan Komputer Menggunakan Dude. Jurnal Teknologi Informasi, 11(1).

Wijaya, H. (2020). Implementasi Kriptografi AES-128 Untuk Mengamankan URL (Uniform Resource Locator) dari SQL Injection. Akademika Jurnal, 17(1), 8-13.

Yenadi, R. P., Fauziah, F., & Hidayatullah, D. (2020). Implementasi Metode Caesar Cipher dalam Penerapan Sistem E-Voting Berbasis Web pada Pemilihan Abang None Jakarta. *STRING (Satuan Tulisan Riset dan Inovasi Teknologi)*, *4*(3), 235-246.