Jurnal Teknik Mesin, Industri, Elektro Dan Informatika (JTMEI)
Vol.2, No.2 Juni 2023
e-ISSN: 2963-7805; p-ISSN: 2963-8208, Hal 64-76

Perancangan Aplikasi Enkripsi Deskripsi Mengunakan Metode Caesar Chiper Berbasis Web

Mohammad Harun Alfirdaus[1], Muhlis Tahir[2], Nabilla Enno Dewanti[3], Riki Ardianto[4], Nela Nur Azurah[5], Nanang Firman Cahyono[6]
[1,2,3,4,5] Pendidikan Informatika, Fakultas Ilmu Pendidikan, Universitas Trunojoyo Madura
Alamat: Jl. Raya Telang, PO.Box. 2 Kamal, Bangkalan – Madura
Korespondensi penulis: harunalfirdaus@gmail.com

Abstract*. Cryptography is a solution or method of information security that is good for maintaining the confidentiality and security of information, and can improve information or information security in an era of very rapid development of information technology. The rapid development of this technology, many new implications and problems arise in the delivery and communication of information, this is because everyone has easy access to the media and this affects the security of information and messages on the media. Therefore, to protect messages, we can use Caesar encryption, which is relatively easy to implement in PHP. How to apply message security in this study by designing web-based applications using the PHP and HTML programming languages. Message protection uses the Caesar encryption algorithm by changing every character of the original message into ciphertext. Characters in plain text are replaced with keys that are determined based on the number of alphabetical orders of plain text. In this way, unauthorized parties cannot read these private messages and users can interact with private messages more freely.*

Keywords*: caesar cipher, encryption, security, message*

Abstrak. Kriptografi merupakan solusi atau metode keamanan informasi yang baik untuk menjaga kerahasiaan dan keamanan informasi, dan dapat meningkatkan keamanan informasi atau informasi di era perkembangan teknologi informasi yang sangat pesat. Pesatnya perkembangan teknologi ini, banyak implikasi dan masalah baru muncul dalam penyampaian dan komunikasi informasi, hal ini dikarenakan setiap orang memiliki akses yang mudah terhadap media dan hal tersebut mempengaruhi keamanan informasi dan pesan pada media tersebut. Oleh karena itu, untuk melindungi pesan, kita dapat menggunakan enkripsi Caesar, yang relatif mudah diterapkan di PHP. Cara mengaplikasi pengamanan pesan pada penelitian ini dengan merancang aplikasi berbasis web menggunakan bahasa pemgrograman PHP dan HTML. Perlindungan pesan menggunakan algoritma enkripsi Caesar dengan mengubah setiap karakter dari pesan asli menjadi ciphertext. Karakter dalam teks biasa diganti dengan kunci yang ditentukan berdasarkan jumlah urutan abjad dari teks biasa. Dengan cara ini, pihak yang tidak berhak membacanya tidak dapat membaca pesan privasi tersebut dan pengguna dapat berinteraksi dengan pesan privasi dengan lebih bebas.

Kata kunci: caesar chiper, enkripsi, keamanan, pesan

Received April 07, 2023; Revised Mei 02, 2023; Accepted Juni 01, 2023
*Korespondensi penulis: harunalfirdaus@gmail.com

LATAR BELAKANG

Terdapat dua konsep utama dalam kriptografi, yaitu enkripsi dan dekripsi. Enkripsi adalah suatu proses dimana informasi/data yang akan dikirim diubah menggunakan algoritma tertentu menjadi bentuk yang hampir tidak dapat dikenali sebagai data aslinya. Dekripsi adalah kebalikan dari enkripsi, yaitu konversi bentuk yang disamarkan menjadi data asli (Azis 2018).

Banyaknya pengguna internet di era teknologi telah menjadi kebutuhan dan kewajiban untuk mendapatkan informasi dan memberikan informasi tanpa harus bertemu atau bertemu secara langsung, yang menyebabkan tumbuh dan lahirnya jejaring sosial. Ada banyak jejaring sosial yang menyediakan layanan hiburan yang mereka tawarkan seperti Facebook, G+, Twitter dan banyak lainnya. Meskipun demikian dalam hal keamanan pesan mereka tampaknya tidak memperhatikan lebih mendetail, hal ini menyebabkan banyak pihak yang mampu membaca pesan yang tidak semestinya mereka baca, hal ini dikarenakan lemahnya sistem kemaanan di jejaring sosial (Halimatusadiah and Insanudin 2016)

Proteksi atau keamanan yang digunakan jejaring sosial yang tersedia hanyalah proteksi login tanpa mempertimbangkan keamanan daripada surat-menyurat (*chat*). Dalam hal ini, metode keamanan diperlukan untuk mengamankan pesan di jejaring sosial terutama metode enkripsi memegang peranan yang sangat penting dalam mengenkripsi pesan. Didalam kajian ilmu kriptografi banyak sekali method enkripsisalah satunya Caesar chiper untuk mengamankan text dengan cara mengenkripsi pesan menggunakan key tertentu dan hanya orang yang memiliki dan mengetahui key nya saja yang dapat membuka pesan tersebut, tentu saja hal ini sangat berguna untuk pesan yang ingin di berikan keamanan atau pesan privasi.

KAJIAN TEORITIS

A. Aplikasi

Aplikasi berasal dari kata *application* yang artinya penerapan, penggunaan. Menurut istilah aplikasi adalah program siap pakai yang dirancang guna melaksanakan suatu fungsi bagi pengguna atau aplikasi yang lain dan dapat digunakan oleh sasaran yang dituju (Azis 2018).

e-ISSN: 2963-7805; p-ISSN: 2963-8208, Hal 64-76

Aplikasi adalah suatu program komputer yang dibuat untuk mengerjakan dan melaksanakan tugas khusus dari pengguna. Aplikasi merupakan rangkaian kegiatan atau perintah yang dieksekusi oleh komputer (Faruq 2015)

B. Kriptografi

Kriptografi berasal dari bahasa Yunani dan membagi bahasa menjadi dua bahasa, yaitu *crypto* dan *graphia*. *Crypto* berarti rahasia dan *graphia* berarti tulisan grafis. Menurut terminologi, kriptografi adalah ilmu dan seni menjaga keamanan pesan saat mengirim pesan dari satu tempat ke tempat lain (Azis 2018).

Kriptografi merupakan suatu metode yang digunakan untuk mengamankan informasi sehingga hanya pengguna yang disebutkan yang dapat membaca melalui penggunaan kode rahasia. Tujuan utama dari kriptografi adalah untuk menjaga keutuhan, kerahasiaan, dan autentikasi dari seluruh sumber daya informasi (Alasi 2019).

Dalam kriptografi terdapat dua tahapan, yaitu enkripsi dan dekripsi. Proses enkripsi melibatkan pengubahan teks asli menjadi sebuah susunan karakter atau simbol yang tidak dapat dipahami oleh manusia. Proses ini dapat menghasilkan sebuah pesan yang susunan karakternya jauh berbeda dari teks aslinya. Sedangkan tahapan kedua yaitu dekripsi, merupakan kebalikan dari proses enkripsi. Pada tahapan ini, susunan karakter atau simbol acak yang dihasilkan dari proses enkripsi dapat disusun kembali ke bentuk teks asli agar dapat dibaca oleh penerima yang berhak. Tujuan dari proses dekripsi adalah untuk mengembalikan pesan yang telah diubah oleh proses enkripsi menjadi bentuk aslinya (Ridho, Mutia, and Sinaga 2022).

Bruce Scheiner dalam bukunya yang berjudul Applied Cryptography mendefinisikan kriptografi sebagai ilmu pengetahuan dan seni dalam menjaga keamanan pesan-pesan. Meskipun masih sederhana, konsep kriptografi telah digunakan sejak lama oleh manusia di berbagai peradaban seperti Mesir dan Romawi (Azis 2018).

Menurut Hayaty (2020) terdapat prinsip-prinsip yang mendasari kriptografi yakni:

1) *Confidentiality* (kerahasiaan) mengacu pada tindakan menjaga informasi agar tetap rahasia dengan membatasi hak akses seseorang, yang paling umum dilakukan melalui penggunaan enkripsi. Tujuannya adalah untuk membatasi akses terhadap informasi sesuai dengan tingkat kerahasiaannya dan melindungi data atau informasi dari pihak yang tidak bertanggung jawab agar tidak diketahui.

2) *Integrity* (keaslian) merujuk pada upaya memastikan bahwa data atau informasi yang dimiliki tetap utuh dan tidak berubah tanpa sepengetahuan pemilik informasi. Tingkat kepercayaan terhadap suatu informasi dapat ditentukan berdasarkan tingkat keaslian yang dipertahankan. Dalam menjaga integritas terdapat dua mekanisme keamanan, yaitu mekanisme *preventif* dan mekanisme *detektif*. Mekanisme *preventif* (pencegahan) adalah kontrol akses yang dirancang untuk mencegah data diubah. Sedangkan mekanisme *detektif* (pendeteksi) adalah mendeteksi dan memperkirakan perubahan yang akan atau sedang dilakukan oleh orang lain.
3) *Authentication* (keotentikan) adalah layanan yang terkait dengan proses pengenalan, baik itu otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun autentikasi keaslian data atau informasi.
4) *Availability* (ketersediaan) Berkaitan dengan ketersediaan informasi saat dibutuhkan. Artinya informasi harus selalu tersedia dan dapat diakses dengan cepat oleh pengguna ketika dibutuhkan.

Biasanya, proses enkripsi dan dekripsi memerlukan penggunaan kunci, yaitu sejumlah informasi rahasia. Beberapa mekanisme enkripsi menggunakan kunci yang sama untuk enkripsi dan dekripsi, sementara mekanisme lain menggunakan kunci yang berbeda untuk kedua proses tersebut. Dua tipe dasar dari teknologi kriptografi adalah *symmetric* (*secret/private key*) *cryptography* dan *asymmetric* (*public key*) *cryptography*. Pada *symmetric key cryptography* (kriptografi kunci simetris), baik pengirim maupun penerima memiliki kunci rahasia yang umum. Pada *asymmetric key cryptography* (kriptografi kunci asimetris), pengirim dan penerima masing-masing berbagi kunci publik dan privat (Azis 2018).

1) Algoritma Kriptografi Simetris

Algoritma kriptografi simetris adalah algoritma kriptografi yang menggunakan kunci enkripsi dan dekripsi yang sama. Saat mengirim pesan menggunakan algoritma ini, pesan penerima harus diberi tahu kunci untuk pesan tersebut agar dapat mendekripsi pesan yang diterima. Keamanan dari pesan yang dikirim dengan algoritma ini bergantung pada kunci yang digunakan. Jika kunci tersebut diketahui oleh orang lain, orang tersebut dapat melakukan enkripsi dan dekripsi pesan (Syam and Pramusinto 2018).

Sebelum mengirim pesan, pengirim dan penerima harus dilarang menggunakan kunci tertentu yang sama dan kunci tersebut harus dirahasiakan dari pihak yang tidak

berkepentingan. Karena kunci rahasia tersebut, algoritma ini disebut juga sebagai algoritma kunci privat atau kunci rahasia (*secret-key algorithm*) (Azis 2018).

2) Algoritma Kriptografi Asimetris

Algoritma kriptografi asimetris juga dikenal sebagai algoritma kunci publik, karena kunci yang digunakan untuk enkripsi dan dekripsi berbeda. Meskipun kunci publik dapat diketahui oleh siapa saja, namun sulit untuk mengetahui kunci privat yang digunakan. Pada umumnya proses enkripsi dilakukan menggunakan kunci publik (*public key*) sementara prose dekripsi dilakukan menggunakan kunci privat (*private key*) (Azis 2018).

Kunci memainkan peran yang sangat penting dalam proses enkripsi dan dekripsi, selain algoritma yang digunakan. Oleh karena itu, menjaga kerahasiaan kunci sangatlah krusial, karena jika kunci tersebut terbongkar, maka isi pesan dapat dengan mudah diketahui oleh pihak yang tidak dimilikinya.

C. Caesar Chiper

Julius Caesar, seorang kaisar Romawi, menemukan metode sandi sandi Caesar pada masa lalu. Algoritma ini awalnya digunakan untuk menyandikan pesan militer yang dikirim kepada panglima perang dan juga untuk pesan resmi lainnya (Bancin et al. 2023).

Caesar Cipher merupakan suatu algoritma cipher substitution yang memanfaatkan perubahan huruf dengan modulo 26. Biasanya, metode ini digunakan pada informasi yang bersifat khusus. Pada Caesar cipher, setiap huruf disamarkan dengan huruf yang berada tiga tempat di belakangnya pada susunan alfabet yang sama. Dalam hal ini, kunci terdiri dari pergeseran huruf tertentu menjadi huruf lainnya (Aditya et al. 2023).

Adapun beberapa pengertian yang harus diketahui dalam kriptografi caesar yaitu:

1) Pesan Teks

Pesan adalah data atau informasi yang mudah dipahami oleh penerima pesan. Dalam arti lain, pesan adalah teks yang belum dienkripsi atau disandikan (Mira, Purnomo, and Sembiring 2022).

2) Enkripsi

Menurut Anggriani dkk (2019) enkripsi merupakan sebuah proses yang melibatkan penggunaan algoritma khusus untuk mengubah data atau informasi menjadi suatu format yang hampir tidak dapat dikenali atau diidentifikasi sebagai informasi aslinya. Plaintext atau teks biasa merujuk pada informasi atau pesan yang dikirim dalam format yang mudah dibaca atau dalam bentuk aslinya.

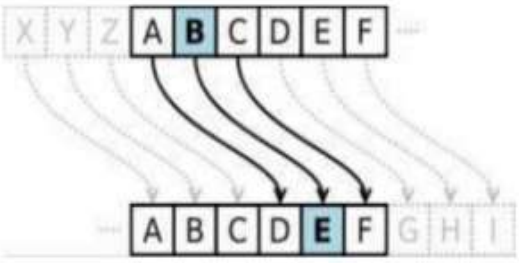
Dalam enkripsi Caesar cipher, karakter-karakter dalam pesan diubah menjadi nilai ASCII, kemudian dipindahkan sebanyak n karakter yang ditentukan dalam kunci enkripsi. Perpindahan ini dapat dilakukan dengan cara apapun (Alasi 2019).

3) Deskripsi

Menurut Ziliwu dkk (2022) deskripsi merupakan kegiatan yang bertujuan untuk mengembalikan pesan yang telah tersandi atau terenkripsi menjadi pesan asli atau plaintext. Proses mengembalikan isi pesan tersandi menggunakan kode yang telah ditentukan sebelumnya. Dekripsi merupakan kebalikan dari enkripsi, yang merupakan proses mengubah pesan asli menjadi pesan tersandi atau ciphertext. Proses mengubah plaintext menjadi ciphertext disebut enkripsi, sedangkan proses mengubah ciphertext menjadi plaintext disebut dekripsi.

Deskripsi Caesar Cipher dilakukan dengan mengambil nilai ASCII pada teks tersandi (cipher) dan kemudian melakukan pengurangan pergeseran sebanyak karakter kunci yang hanya diketahui oleh pengguna (Alasi 2019).

Sandi caesar atau juga dikenal dengan sandi geser merupakan salah satu teknik enkripsi yang paling terkenal dan mudah. Caesar Chiper termasuk jenis chiper substitusi yang paling sederhana dan banyak digunakan. Pada chiper ini, setiap huruf pada plaintex digantikan oleh huruf lain yang tetap pada posisi alfabet. Sebagai contoh, jika nilai pergeserannya adalah 3, maka huruf A akan digantikan oleh huruf D, huruf B menjadi huruf E, dan seterusnya. Proses pergeseran tersebut dapat dilihat pada gambar.3.



Gambar 1. Algoritma Caesar Chiper (Bancin et al. 2023)

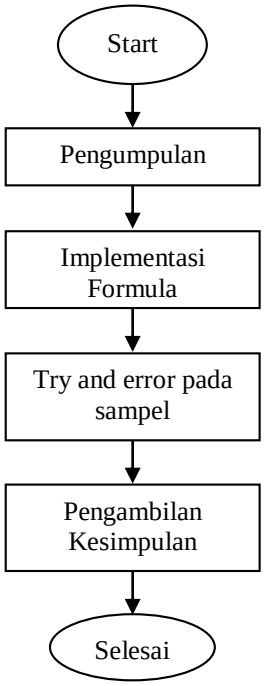
Pada gambar di atas, ditunjukkan sebuah proses pergeseran sebanyak 3 huruf yang dapat digambarkan dengan cara menyelaraskan antara plaintext dengan chipertext ke kiri atau ke kanan sebanyak pergeseran yang diinginkan. Sebagai ilustrasi, jika pergeseran dilakukan sebanyak 3 kali, maka plainteks "ABCDEFGHIJKLMNOPQRSTUVWXYZ" akan disandikan menjadi chiperteks "DEFGHIJKLMNOPQRSTUVWXYZABC".

Jurnal Teknik Mesin, Industri, Elektro Dan Informatika (JTMEI)
Vol.2, No.2 Juni 2023
e-ISSN: 2963-7805; p-ISSN: 2963-8208, Hal 64-76

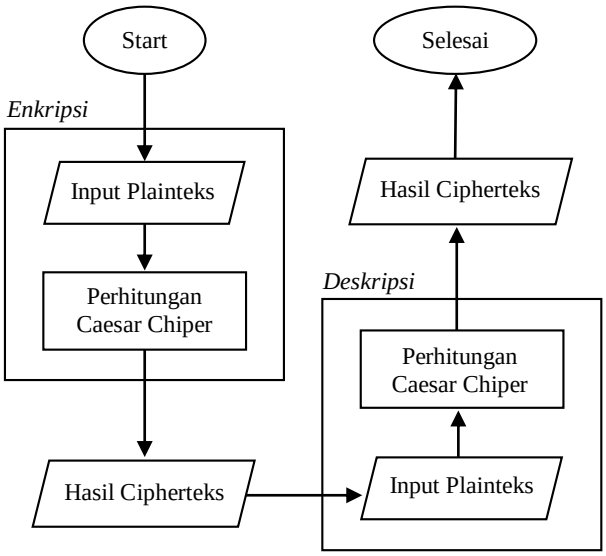
METODE PENELITIAN

Penelitian ini menggunakan literatur sebagai dasar referensi, kemudian melakukan eksperimen menggunakan rumus tertentu yang diakhiri dengan mendapatkan hasil akhir yang dapat disimpulkan berdasarkan hasil eksperimen tersebut. Objek sampel yang digunakan dalam eksperimen rumus pada penelitian ini diambil dari hasil enkripsi dengan menggunakan Caesar Cipher.

Penting untuk memperhatikan urutan penggunaan cipher dalam percobaan penelitian ini karena ada kemungkinan cipherteks tidak dapat didekripsi dan dikembalikan ke bentuk plaintext jika urutan cipher yang digunakan tidak benar atau acak. Jika cipherteks tidak dapat dikembalikan ke plaintext, maka penerima pesan tidak akan bisa membaca isi pesan asli yang dikirimkan, yang pada gilirannya dapat menyebabkan kegagalan dalam pengiriman dan penerimaan pesan.



Gambar 2. Diagram proses penelitian (Ridho et al. 2022)



Gambar 3. Flowchart Algoritma Caesar Cipher (Ridho et al. 2022)

HASIL DAN PEMBAHASAN

Dalam pembuatan rancangan ini, digunakan beberapa aplikasi, yaitu XAMPP, Visual Studio Code, dan Chrome untuk menampilkan hasil percobaan pada web. Bahasa yang digunakan dalam rancangan ini adalah php dan html. Sebuah proses yang melakukan perubahan sebuah kode dari yang bisa di mengerti (*plaintext*) menjadi sebuah kode yang tidak bisa di mengerti (ciphertext). Contoh kasus. Jika diberikan plaintext sebagai berikut:

Plaintext: “KEAMANAN JARINGAN”

Dengan menggunakan kunci 5, maka akan didapat ciphertext sebagai berikut:

Ciphertext: PJFRFSFS OFWNSLFS

Proses enkripsi pada Caesar Cipher dapat direperesentasikan menggunakan operator aritmetika modulo 26 setelah sebelumnya setiap huruf di transformasi kedalam angka, yaitu: A = 0, B = 1,…, Z = 25. Maka caesar cipher dirumuskan sebagai berikut: Proses enkripsi suatu huruf P dengan pergeseran K dapat dinyatakan secara matematis sebagai berikut:

Enkripsi C = E(P) = (P+K) mod 26

Dekripsi P = D(C) = (C − K) mod26

dengan C adalah ciphertext, P adalah plaintext, K adalah kunci rahasia, E(P) adalah enkripsi, dan D(C) adalah dekripsi.

Jurnal Teknik Mesin, Industri, Elektro Dan Informatika (JTMEI)
Vol.2, No.2 Juni 2023
e-ISSN: 2963-7805; p-ISSN: 2963-8208, Hal 64-76

Gambar 4. Tampilan Interface Aplikasi

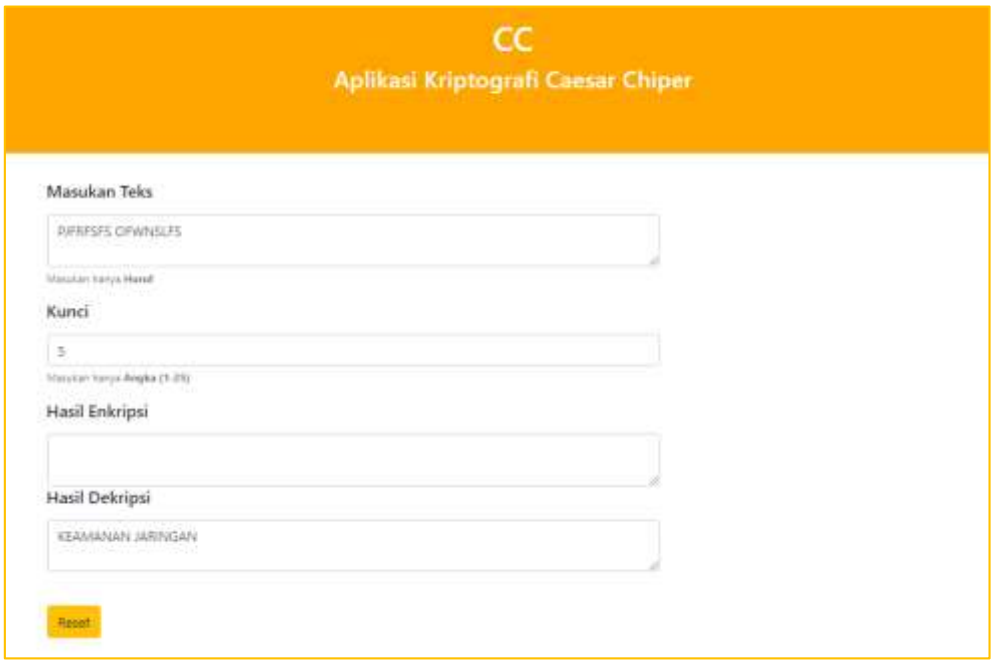
Tampilan utama untuk melakukan deskripsi dan enkripsi terdapat kolom untuk memasukkan teks atau pesan dan terdapat kolom kunci untuk memasukkan angka mulai dari 1-25. Kemudian terdapat tombol enkripsi dan tombol deskripsi untuk melakukan proses endkipsi atau deskripsi. Kemudian terdapat tombol batal untuk mereset semuanya.

Gambar 5. Tampilan Proses Enkripsi Pada Aplikasi

Ketika melakukan enkripsi pada kata KEAMANAN JARINGAN dan diberikan kunci 5, maka persamaan yang digunakan yaitu C = E(P) = (P+K) mod 26

K = E(10)= (10+5) mod 26 = 15 = P
E = E(4) = (4+5) mod 26 = 9 = J
A = E(0) = (0+5) mod 26= 5 = F
M = E(12) = (12+5) mod 26 = 17 = R
A = E(4) = (4+5) mod 26 = 9 = J
N = E(13) = (13+5) mod 26 = 18 = S
A = E(0) = (0+5) mod 26 = 5 = F
N = E(13) = (13+5) mod 26 = 18 = S...dst

Dari perhitungan enkripsi tersebut maka menghasilkan kata *PJFRFSFS OFWNSLFS.*



Gambar 6. Tampilan Proses Deskripsi Pada Aplikasi

Ketika melakukan deskripsi pada kata PJFRFSFS OFWNSLFS dan diberikan kunci 5, maka persamaan yang digunakan yaitu P = D(C) = (C − K) mod26

P = D(15) = (15-5) mod 26 = 10 = K
J = D(9) = (9-5) mod 26 = 4 = E
F = D(5) = (5-5) mod 26 = 0 = A
R = D(17) = (17-5) mod 26 = 12 = M
F = D(5) = (5-5) mod 26 = 0 = A
S = D(18) = (18-5) mod 26 = 13 = N
F = D(5) = (5-5) mod 26 = 0 = A

e-ISSN: 2963-7805; p-ISSN: 2963-8208, Hal 64-76

S = D(18) = (18-5) mod 26 = 13 = N ...dst

Dari perhitungan deskripsi tersebut maka menghasilkan kata KEAMANAN JARINGAN.

Hasil dan Analisa

Setelah menyelesaikan proses perangkat keras dan perangkat lunak, penulis melakukan pengujian program. Evaluasi hasil pengujian program menjadi penting dalam setiap pengembangan aplikasi untuk mengevaluasi dan memahami pelaporan yang telah dicapai oleh aplikasi yang dikembangkan. Penulis melakukan analisis program sebagai berikut:

1) Bahasa yang digunakan pada program ini adalah php dan html untuk pengembangan aplikasi web.
2) Program ini memungkinkan pengguna untuk melakukan enkripsi pesan dengan memasukkan kunci enkripsi menggunakan metode Caesar
3) Enkripsi pesan dilakukan dengan menggunakan 26 karakter huruf alfabet.
4) Metode enkripsi ini merupakan jenis cipher substitusi, dimana setiap huruf pada plaintext digantikan dengan huruf lain yang tetap pada posisi alfabet. Seperti pada contoh kata plaintext KEMANAN JARINGAN yang diubah ke ciphertext dengan kunci 5 maka menjadi PJFRFSFS OFWNSLFS. Meskipun demikian, metode ini masih rentan terhadap serangan brute force attack, yaitu serangan yang dilakukan dengan mencoba berbagai kemungkinan untuk menemukan kunci.

KESIMPULAN DAN SARAN

Dengan meninjau sejarah, cara kerja, dan cara mendeskripsikan Caesar Cipher, dapat disimpulkan bahwa metode ini mudah diimplementasikan pada PHP dan dapat digunakan untuk mengamankan pesan di jejaring sosial. Dengan menerapkan metode ini, privasi pesan kita dapat terjaga dan kita dapat lebih bebas dalam berkomunikasi dengan pesan yang bersifat rahasia.

DAFTAR REFERENSI

Aditya, Febri, Mohammad Rizky, Revano Arya Saputra, and Fikri Abei. 2023. "Sistem Login Menggunakan Caesar Chipper Berbasis Web Login System Using Web-Based Caesar Chipper." 2(1):267–71.

Alasi, Tomy Satria. 2019. "Implementasi Kriptografi Dengan Algoritma Ceasar Cipher Untuk Keamanan Data Microsoft Office Word Dan Excel." *Jurnal Informasi Komputer Logika* 1(2):1–4.

Angriani, Husni, and Yeni Saharaeni. 2019. "Implementasi Algoritma Caesar Cipher Pada Keamanan Data Sistem E-Voting Pemilihan Ketua Organisasi Kemahasiswaan." *Inspiration: Jurnal Teknologi Informasi Dan Komunikasi* 9(2):123. doi: 10.35585/inspir.v9i2.2499.

Azis, Nur. 2018. "Perancangan Aplikasi Enkripsi Dekripsi Menggunakan Metode Caesar Chiper Dan Operasi XOR." *Ikraith-Informatika* 2(1):72–80.

Bancin, Haryanzelina, Mira Aripin, Sabrina Putri, and Adnan Buyung. 2023. "Implementasi Kriptografi Dengan Metode Caesar Cipher Untuk Mengamankan Data File Di Javanetbeans." *Jurnal Pendidikan, Sains Dan Teknologi* 2(1):17–22.

Faruq, Umar Al. 2015. "Rancang Bangun Aplikasi Rekam Medis Poliklinik Universitas Trilogi." *Jurnal Informatika* 9(1):1017–27.

Halimatusadiah, Aida, and Entik Insanudin. 2016. "Implementasi Kriptografi Metode Caesar Chiper Pada Chating Berbasis Web." *Caesar Cipher Chating* 1(20):1–5.

Hayaty, Nurul. 2020. *Buku Ajar: Sistem Keamanan*.

Mira, Hindriyanto Dwi Purnomo, and Irwan Sembiring. 2022. "Modifikasi Algoritma Caesar Cipher Pada Kode ASCII Dalam Meningkatkan Keamanan Pesan Teks." *Journal of Information Technology* 2(1):16–22. doi: 10.46229/jifotech.v2i1.293.

Ridho, Abdurrahman, Cut Mutia, and Amelia Putri Sinaga. 2022. "Analisis Enkripsi Dan Dekripsi Cipher Teks Menggunakan Kombinasi Gronsfeld Cipher Dengan Reverse Cipher." *Jurnal Teknik Informatika Kaputama (JTIK)* 6(1).

Syam, T. B., and W. Pramusinto. 2018. "Aplikasi Enkripsi Email Dengan Algoritma Gost Dan Caesar Cipher Berbasis Web Pada Ppsdm Universitas Terbuka." *Skanika* 1(3):919–24.

Ziliwu, Krisma Budi, Andi Maslan, and Hendri Kremer. 2022. "IMPLEMENTASI CAESAR CIPHER PADA ALGORITMA KRIPTOGRAFI DALAM PENYANDIAN PESAN WHATSAPP." *Comasie* 7(2):117–25.