BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 3, No 4, Desember 2022, Hal 367 - 373
ISSN 2722-0524 (media online)
DOI 10.47065/ bit.v3i1. 420
https://journal.fkpt.org/index.php/BIT

Perancangan Keamanan Data Pesan Dengan Menggunakan Metode Kriptografi Caesar Cipher

Radila Pratiwi, Lola Citra Utami, Rafli Bima Sakti, Triase
Fakultas sains dan Teknologi, Sistem Komputer, Universitas Islam Negeri Sumatera Utara, Medan, Indonesia
Email: [1]radilapratiwi03@gmail.com, [2]citralola09@gmail.com, [3]rafli.bimasakti@gmail.com, [4]*triase@uinsu.ac.id
Email Penulis Korespondensi: triase@uinsu.ac.id

Abstrak− Keamanan merupakan hal yang vital dalam segala aspek untuk menjaga informasi. Pada komputer atau laptop, pesan teks merupakan salah satu data penting yang perlu dilindungi oleh sistem keamanan data. Pada perangkat komputer atau laptop, keamanan data digunakan untuk menjaga keamanan data penting kita. data pribadi. Enkripsi digunakan untuk mencegah pihak yang tidak diundang membaca pesan. Selama proses deskripsi sedang digunakan, pesan dapat dibaca ulang oleh penerima yang dituju. Tingkat keamanan informasi pesan dapat ditingkatkan dengan mengenkripsi pesan teks. caesar cipher adalah metode untuk enkripsi yang membutuhkan sedikit usaha. Perangkat lunak Visual Basic 2010 mencakup implementasi algoritma Caesar Cipher. Deskripsi pesan dan desain aplikasi keamanan enkripsi hanya dapat digunakan pada komputer. Dengan mengubah pesan asli menjadi pesan rahasia melalui pergeseran kunci, penelitian ini telah memungkinkan pesan untuk dijaga

Kata Kunci: Chipertext; Caesar Chiper; Deskripsi; Enkripsi; Plaintext

Abstract− Security is vital in all aspects to protect information. On a computer or laptop, text messages are one of the important data that needs to be protected by a data security system. On a computer or laptop device, data security is used to maintain the security of our important data. personal data. Encryption is used to prevent uninvited parties from reading messages. As long as the description process is being used, the message can be re-read by the intended recipient. The security level of message information can be increased by encrypting text messages. caesar cipher is a method for encryption that requires minimal effort. The Visual Basic 2010 software includes the implementation of the Caesar Cipher algorithm. The message description and design of the encryption security application can only be used on computers. By turning the original message into a secret message through key shifting, this research has made it possible for the message to be safeguarded.

Keywords: Ciphertext; Caesar Chipper; Description; Encryption; Plaintex.

1. PENDAHULUAN

Kriptografi adalah sistem yang digunakan untuk keamanan data. Kemajuan teknologi pada saat ini sudah berkembang sangat pesat seperti memudahkan seseorang dalam bertukar data secara cepat. Semakin tin ggi tingkat teknologi komputer maka semakin tinggi tingkat ancaman keamanan teknologi tersebut.[1] Misalnya pencurian dan penyadapan yang menyebabkan data rusak, hilang bahkan disebar luaskan sehingga orang lain dapat melihat privasi kita. Salah satu cara untuk pengamanan data dapat dilakukan dengan menggunakan proses kriptografi caesar chiper tujuannya untuk merahasiakan pesan yang dikirim dan sekaligus menghindarkan pesan tersebut dari kecurigaan pihak lain yang tidak berkepentingan.[2] Pesan atau informasi keamanan dapat dipertahankan menggunakan kriptografi, baik saat dikirim melalui saluran komunikasi maupun saat disimpan di media penyimpanan. Kriptografi digunakan di hampir setiap aspek kehidupan modern untuk menjaga kerahasiaan dan keamanan informasi dengan menggunakan persamaan matematika dalam proses enkripsi dan dekripsi.[3]

Salah satu aspek terpenting dari sistem informasi saat ini adalah pesan. Pesan merupakan contoh proses yang melibatkan penggunaan teknologi dan ilmu pengetahuan yang berpotensi melipat gandakan teknologi dan tradisional, serta dilakukan oleh individu yang sedang mengambil data dari sistem informasi. Salah satu solusi untuk menjaga keamanan pesan yaitu dengan menggunakan caesar cipher dalam menjaga keamanan pesan.[4] Proses algoritma Caesar Cipher melibatkan perbandingan plaintext dan ciphertext ke arah positif atau negatif. Enkripsi merupakan salah satu pendekatan yang sering digunakan. Proses penyembunyian makna pesan melalui enkripsi mencegah orang yang tidak berkepentingan untuk memahaminya. Dengan menggunakan kriptografi, keamanan pesan dapat ditingkatkan sehingga orang tidak akan percaya bahwa pesan tersebut telah dienkripsi atau bahwa file tersebut tidak mengandung informasi rahasia.[5]. Prosedur penyandian pesan pada penelitian ini tetap berbasis komputer pada desktop. Diharapkan bahwa hasil penyandian pesan yang lebih baik akan dihasilkan dari penggabungan kedua algoritma ini. Dengan tujuan agar cenderung menjadi media pembelajaran bagi masyarakat atau civitas akademika. Dalam hal ini kami mengambil pesan sebagai alat komunikasi seperti SMS. Siapa yang tidak mengetahui SMS. Aplikasi yang sering dipakai banyak orang baik dari anak anak maupun orang dewasa. SMS adalah sebuah aplikasi yang digunakan untuk mengirimkan pesan dan menerima pesan masuk berupa teks, sehingga banyak digunakan sebagai media komunikasi yang fleksibel. Isi SMS kebanyakan sangat bervariasi, bisa berupa pesan teks biasa atau pesan teks rahasia, seperti perjanjian yang akan dikirim ke perusahaan tertentu. Secara alami, pesan teks rahasia memerlukan tingkat keamanan yang tinggi, dengan data yang akan dikirim terlebih dahulu dienkripsi untuk melindungi pesan dari penyadapan.[6]

Aplikasi yang dibuat oleh penulis yaitu Visual Studio 2010 Menggunakan kriptografi one-time pad, untuk mengenkripsi dan mendekripsi data teks yang akan digunakan secara rahasia dan lebih mudah oleh pengguna di masa mendatang.[7].

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 3, No 4, Desember 2022, Hal 367 - 373
ISSN 2722-0524 (media online)
DOI 10.47065/ bit.v3i1. 420
https://journal.fkpt.org/index.php/BIT

Perlindungan data pada komputer dan sistem komunikasi merupakan pokok bahasan ilmu yang disebut keamanan data. Privasi (confidentiality), integritas (consistency), keaslian (authenticity), ketersediaan (availability), dan kontrol akses adalah semua komponen keamanan data[8]. Dari bahasa Yunani, kryptos, yang berarti "tersembunyi," dan graphein, yang berarti "menulis," kriptografi adalah seni dan ilmu yang membuat komunikasi menjadi tidak mungkin bagi siapa pun kecuali penerima yang dituju. Seni mengirim pesan diubah sehingga hanya penerima yang dapat memahaminya dikenal sebagai kriptografi. Proses mengubah pesan asli menjadi kode mengikuti seperangkat aturan dikenal sebagai kriptografi. Ini memastikan bahwa hanya pesan asli yang dapat diterima oleh pesan penerima yang memahami seperangkat aturan. Kriptografi menggabungkan metode, misalnya, ti microdots, konsolidasi kata-kata dengan gambar, dan cara lain untuk menyelundup data pergi. Kriptografi dapat dilakukan dengan berbagai cara, termasuk penggunaan sandi, kode, dan substitusi, sehingga hanya pihak berwenang yang dapat secara akurat melihat pesan yang sebenarnya. Informasi yang dikirim melalui jaringan komunikasi publik seperti telepon, microwave, atau satelit dapat dilindungi menggunakan kriptografi[9]. Ada empat komponen utama kriptografi:[10]

1. Khusus pesan yang dapat dibaca adalah plaintext.
2. Ciphertext, yang merupakan pesan acak atau kode yang tidak dapat dipahami.
3. Key, khususnya kunci yang diperlukan untuk melakukan metode kriptografi.
4. Algoritma, untuk lebih spesifik teknik yang akan dilakukan enkripsi dan decoding.

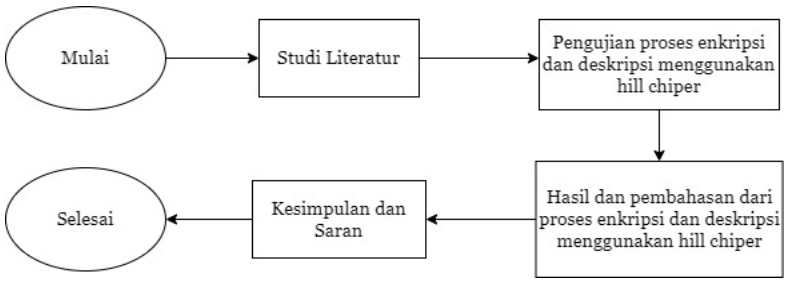
Kriptografi mempunyai tujuan untuk memberikan administrasi keamanan, yang disebut perspektif keamanan, antara lain[11]:

1. Sebuah layanan yang disebut sebagai kerahasiaan yang dirancang untuk mencegah pihak supaya tidak berwenang membaca pesan.
2. Layanan yang dikenal sebagai "integritas data" memastikan bahwa pesan tidak diubah atau diubah dengan cara apa pun selama transmisi.
3. Bantuan dan otentikasi adalah layanan terkait yang menentukan kebenaran pihak yang berkomunikasi.
4. Non-repudiation berfungsi sebagai pencegah belas kasihan dari entitas yang berkomunikasi.

Proses mengubah pesan asli menjadi kode mengikuti seperangkat aturan dikenal sebagai kriptografi. Ini memastikan bahwa hanya pesan asli yang dapat diterima oleh pesan penerima yang memahami seperangkat aturan.
Algoritma caesar cipher adalah metode pengkodean berbasis substitusi pertama yang pernah dikembangkan. Caesar menggeser setiap huruf dalam pesan atau mengubah huruf menjadi angka untuk menjaga keamanan data yang dikirim[12]. Untuk menyandikan sebuah pesan, hanya perlu mencari huruf yang ingin disandikan dengan alfabet biasa, kemudian tuliskan huruf sesuai dengan alfabet sandi. Untuk memecahkan sandi tersebut gunakan hal sebaliknya. Contoh caesar chipper yaitu: Plainteks: “JURUSAN SISTEM INFORMASI” Chipertext: “MXUXVDP VLVWHP LQIRUPDVL

2. METODOLOGI PENELITIAN

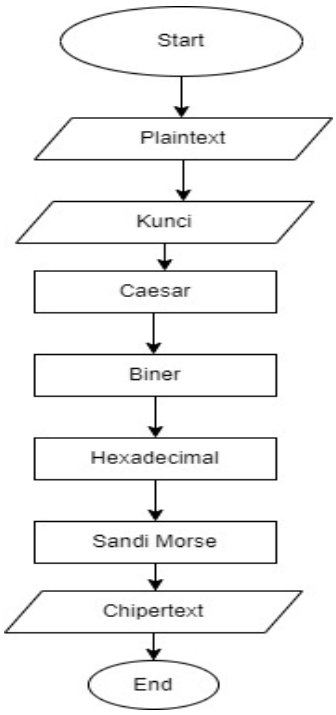
Metode penelitian pada penyusunan menggunakan studi literatur yaitu Mengumpulkan bahan-bahan referensi baik buku, artikel, makalah maupun situs internet mengenai algoritma Hill Cipher, Deskripsi , Enkripsi, dan teknik deskripsi dan enkripsi pada hill chiper. antara lain:



Gambar 1. Alur Penelitian

Dalam studi literatur, tahap ini melibatkan pengumpulan data dari buku, jurnal internasional, jurnal nasional, dan jurnal lokal, serta jurnal yang diterbitkan di negara lain.Adapun metode yang penulis pakai yaitu caesar cipher: Caesar cipher adalah salah satu metode enkripsi terbaik dan paling terkenal. Algoritma Caesar Cipher digunakan dalam kriptografi. Simetris yang digunakan sejauh ini sebelum kunci sistem kriptografi publik ditemukan adalah kriptografi klasik yang ada dalam berbagai bentuk, dianggap optimal karena kesederhanaannya. Caesar cipher adalah jenis substitusi sandi di mana setiap huruf plaintext diganti dengan huruf dengan banyak tetap posisi di bawah alfabet[11]. Istilah "single cipher alfabet" adalah nama lain untuk metode ini. Julius Caesar adalah orang pertama yang menggunakan sandi Caesar. Caesar mengkodekan informasi dengan mengatur ulang urutan abjad dari setiap huruf informasi menjadi tiga huruf baru[13].

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 3, No 4, Desember 2022, Hal 367 - 373
ISSN 2722-0524 (media online)
DOI 10.47065/ bit.v3i1. 420
https://journal.fkpt.org/index.php/BIT



Gambar 2. Flowchart Enkripsi Pesan Teks.

Caesar Cipher digunakan untuk membuat ciphertext dengan cara berikut[5]:

a. Menentukan besarnya karakter shift yang digunakan untuk mengubah plainteks menjadi ciphertext.
b. Pergeseran yang telah ditentukan mengubah karakter swap pada plaintext menjadi ciphertext.

Jumlah pergeseran huruf, yang dalam hal ini adalah 3, itu merupakan kuncinya. Tabel substitusi dibuat dengan menggeser alfabet yaitu tiga huruf:

Tabel 1. Subsitusi

Plaintext	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Chipertext	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Oleh karena itu Plainteks menggantikan D untuk huruf A, E untuk huruf B, dan seterusnya. Dengan secara matematis mengkodekan setiap huruf alfabet dengan bilangan bulat, menggeser tiga huruf mengubah teks P menjadi teks sandi C dengan melakukan operasi modulo berikut:[14][15]

$$C=P+K \bmod n \qquad (1)$$

Ket:
C: Chipertext
P: Plaintext
K: Kunci
Mod: Modulus
N: Jumlah Abjad yaitu 26

Dengan operasi kebalikannya, penerima pesan menerima ciphertext sekali lagi, yang secara matematis persamaan nya dapat dinyatakan sebagai berikut:

$$P=C-K \bmod n \qquad (2)$$

Dengan keterangan:
P: Plaintext
C: Chipertext
K: Kunci
Mod: Modulus
N: Jumlah Abjad yaitu 26
Penerima pesan dapat mengubah nomor pesan kembali ke huruf setelah ciphertext kembali ke plaintext yang setara

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 3, No 4, Desember 2022, Hal 367 - 373
ISSN 2722-0524 (media online)
DOI 10.47065/ bit.v3i1. 420
https://journal.fkpt.org/index.php/BIT

3. HASIL DAN PEMBAHASAN

3.1 Proses Enkripsi

Prosedur yang mengubah kode yang dapat dipahami (plaintext) menjadi kode yang tidak dapat dipahami (ciphertext). Misalkan diketahui plaintext sebagai berikut :[16]

"JURUSAN SISTEM INFORMASI"

Dengan menyandikan setiap huruf bilangan bulat A=0, B=1, C=2, dan Z=25, persamaan berikut dapat digunakan untuk menggeser secara matematis tiga huruf alfabet dari teks biasa P menjadi teks sandi C, yang setara dengan melakukan operasi modulo:

Kunci: 3

Rumus:

$$C = P + K \; mod \; 26 \qquad (3)$$

J: 9 + 3 mod 26 = 12 mod 26: "M"
U: 20 + 3 mod 26 = 23 mod 26: "X"
R: 17 + 3 mod 26 = 20 mod 26: "U"
U: 20 + 3 mod 26 = 23 mod 26: "X"
S: 18 + 3 mod 26 = 21 mod 26: "V"
A: 0 + 3 mod 26 = 3 mod 26: "D"
N: 13 + 3 mod 26 = 16 mod 26: "Q"
S: 18 + 3 mod 26 = 21 mod 26: "V"
I: 8 + 3 mod 26 = 11 mod 26: "L"
S: 18 + 3 mod 26 = 21 mod 26: "V"
T: 19 + 3 mod 26 = 22 mod 26: "W"
E: 4 + 3 mod 26 = 7 mod 26: "H"
M: 12 + 3 mod 26 = 15 mod 26: "P"
I: 8 + 3 mod 26 = 11 mod 26: "L"
N: 13 + 3 mod 26 = 16 mod 26: "Q"
F: 5 + 3 mod 26 = 8 mod 26: "I"
O: 14 + 3 mod 26 = 17 mod 26: "R"
R: 17 + 3 mod 26 = 20 mod 26: "U"
M: 12 + 3 mod 26 = 15 mod 26: "P"
A: 0 + 3 mod 26 = 3 mod 26: "D"
S: 18 + 3 mod 26 = 21 mod 26: "V"
I: 8 + 3 mod 26 = 11 mod 26: "L"

Kemudian diperoleh *ciphertext:* MXUXVDQ VLVWHP LQIRUPDVL

3.2 Proses Deskripsi

Proses mengubah kode dari tidak dapat dipahami (ciphertext) menjadi dapat dimengerti (plaintext) adalah kebalikan dari enkripsi[17].

Chipertext: "MXUXVDQ VLVWHP LQIRUPDVL"

Persamaan berikut memungkinkan penerima pesan untuk mendekripsi ciphertext:

Kunci: 3

Rumus:

$$P = C - K \; mod \; 26 \qquad (4)$$

P1: 12 – 3 mod 26 = 9 Mod 26: "J"

P2: 23 – 3 mod 26 = 20 Mod 26: "U"

P3: 20 – 3 mod 26 = 17 Mod 26: "R"

P4: 23 – 3 mod 26 = 20 Mod 26: "U"

P5: 21– 3 mod 26 = 18 Mod 26: "S"

P6: 3 – 3 mod 26 = 0 Mod 26: "A"

P7: 16 – 3 mod 26 = 13 Mod 26: "N"

P8: 21 – 3 mod 26 = 18 Mod 26: "S"

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 3, No 4, Desember 2022, Hal 367 - 373
ISSN 2722-0524 (media online)
DOI 10.47065/ bit.v3i1. 420
https://journal.fkpt.org/index.php/BIT

P9: 11 – 3 mod 26 = 8 Mod 26: "I"

P10: 21 – 3 mod 26 = 18 Mod 26: "S"

P11: 22 – 3 mod 26 = 19 Mod 26: "T"

P12: 7 – 3 mod 26 = 4 Mod 26: "E"

P13: 15 – 3 mod 26 = 12 Mod 26: "M"

P14: 11 – 3 mod 26 = 8 Mod 26: "I"

*P15:*16 – 3 mod 26 = 13 Mod 26: "N"

P16: 8 – 3 mod 26 = 5 Mod 26: "F"

P17: 17 – 3 mod 26 = 14 Mod 26: "O"

P18: 20 – 3 mod 26 = 17 Mod 26: "R"

P19: 15 – 3 mod 26 = 12 Mod 26: "M"

P20: 3 – 3 mod 26 = 0 Mod 26: "A"

P21: 21 – 3 mod 26 = 18 Mod 26: "S"

P22: 11 – 3 mod 26 = 8 Mod 26: "I"

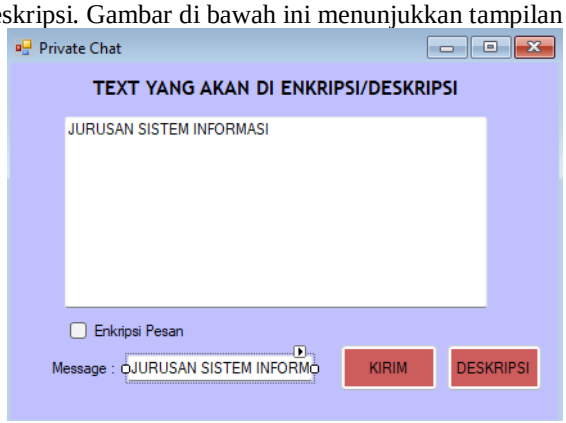
Maka *Plaintext* yang di dapat adalah: "JURUSAN SISTEM INFORMASI"

3.3. Hasil

Secara konseptual, desain ini menjelaskan bagaimana sistem bekerja. Selain merancang bentuk tampilan layar, desain antarmuka juga menentukan dokumen sumber untuk memasukkan data dan memproses data tersebut menjadi keluaran yang dapat digunakan pengguna.

a. Menu Utama

Menu utama adalah tampilan daftar yang memungkinkan Anda membuat beberapa elemen, seperti pesan pribadi, enkripsi pesan, kirim, dan deskripsi. Gambar di bawah ini menunjukkan tampilan menu utama.



Gambar 3. Menu Utama Pesan

b. Tulis Pesan

Di dalam menu tulis pesan ada terdapat sub menu dan tampilan. Berikut ini adalah tampilannya.

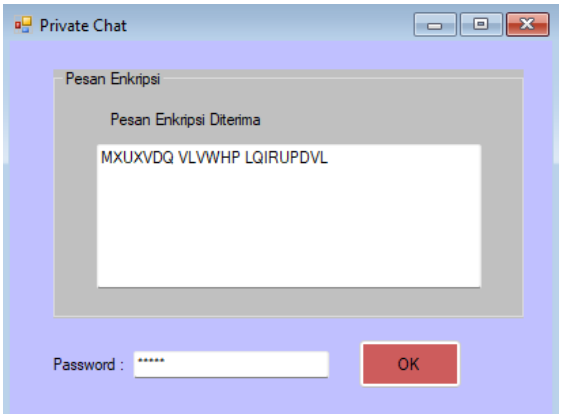
Gambar 4. Tulis Pesan

Jika pengguna melanjutkannya dengan mengklik kirim, pesan tersebut akan terkirim.

c. Pesan Enkripsi

Dalam menu kotak masuk akan terlihat list pesan yang masuk seperti gambar di bawah ini.

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 3, No 4, Desember 2022, Hal 367 - 373
ISSN 2722-0524 (media online)
DOI 10.47065/ bit.v3i1. 420
https://journal.fkpt.org/index.php/BIT



Gambar 5. Pesan Enkripsi

4. KESIMPULAN

Teknik enkripsi, seperti enkripsi caesar, dapat digunakan untuk mengimplementasikan keamanan pengiriman pesan. Dimana lawan pesan dapat mengubah proses pengiriman atau penerimaan pesan dengan menggunakan metode caesar dan pergeseran kunci untuk keamanan konten pesan. Menggunakan perangkat lunak Visual Basic 2010 untuk merancang aplikasi keamanan pesan yang menggunakan proses enkripsi dan dekripsi serta pergeseran kunci. Penulis lebih menekankan pada enkripsi dan dekripsi data dalam aplikasi data yang disimpan dengan aman. Berdasarkan hasil yang di peroleh telah selesai, upaya pengembangan menyarankan untuk memodifikasi cipher algoritma caesar kedalam bentuk morse, dimana pesan proses tidak boleh melebihi 30 karakter. Akibatnya, penelitian tambahan dapat memasukkan elemen program sehingga modifikasi algoritma caesar cipher ini dapat memuat pesan yang panjang. Enkripsi dan dekripsi pesan diharapkan akan lebih sering digunakan di masa mendatang dengan sistem penulis, terutama dalam hal keamanan pesan dengan algoritme kriptografi mutakhir. Selain itu, pesan ini dapat digunakan untuk mengirim pesan teks lebih aman di masa mendatang dengan menggabungkan kriptografi dan steganografi.

UCAPAN TERIMAKASIH

Terimakasih peneliti ucapkan kepada semua pihak yang telah mendukung dalam penelitian ini, harapannya hasil penelitian ini bisa menjadi bahan dasar dan acuan pembelajaran serta penelitian selanjutnya.

REFERENCES

[1] F. Alfiah, R. Sudarji, and D. Taqiyyuddin Al Fatah, “Ciledug Raya, RT.10/RW.2, Petukangan Utara,” p. 12260, 2020.
[2] Bimrew Sendekie Belay, “No Titleהארץ” ,הכי קשה לראות את מה שבאמת לנגד העינים, vol. 3, no. 8.5.2017, pp. 2003–2005, 2022.
[3] L. Silalahi and A. Sindar, “Penerapan Kriptografi Keamanan Data Administrasi Kependudukan Desa Pagar Jati Menggunakan SHA-1,” J. Nas. Komputasi dan Teknol. Inf., vol. 3, no. 2, pp. 182–186, 2020, doi: 10.32672/jnkti.v3i2.2413.
[4] P. Priyono, “Penerapan Algoritma Caesar Cipher Dan Algoritma Vigenere Cipher Dalam Pengamanan Pesan Teks,” J. Ris. Komput., vol. 3, Nomor:, no. Algoritma Caesar Cipher, pp. 351–356, 2016.
[5] N. P. Ef endi, N. P. Efendi, and N. putra efendi, “Jurnal Pengamanan Aplikasi Pesan dengan Algoritma Caesar Chiper dan Affine Chiper,” 2021, [Online]. Available: http://dx.doi.org/10.31219/osf.io/y4acn
[6] R. R. A. Gurning, “Perancangan aplikasi pengamanan pesan dengan algoritma caesar chiper,” J. Pelita Inform. Budi Darma, vol. 6, no. 3, pp. 106–110, 2014.
[7] A. AGUSTIONO, “Pengembangan Pesan Text Menggunakan Kriptografi Untuk Keamanan Data Konsumen Pada Showroom Mobil Mitshubishi,” Kumpul. Karya Ilm. Mhs. …, 2021, [Online]. Available: https://journal.pancabudi.ac.id/index.php/fastek/article/download/1755/1597
[8] M. J. Hendra and S. Murniyanti, “Perancangan Aplikasi Keamanan Data Customer Pada Online Shop Dengan Menggunakan Metode Kriptografi RSA (Rivest , Shamir , Adleman) Dan,” no. x, 2020.
[9] N. Azis, “Perancangan Aplikasi Enkripsi Dekripsi Menggunakan Metode Caesar Chiper dan Operasi XOR,” Ikraith-Informatika, vol. 2, no. 1, pp. 72–80, 2018.

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 3, No 4, Desember 2022, Hal 367 - 373
ISSN 2722-0524 (media online)
DOI 10.47065/ bit.v3i1. 420
https://journal.fkpt.org/index.php/BIT

[10] M. D. Irawan, "Implementasi Kriptografi Vigenere Cipher Dengan Php," J. Teknol. Inf., vol. 1, no. 1, p. 11, 2017, doi: 10.36294/jurti.v1i1.21.
[11] A. A and D. Dasril, "Perancangan Aplikasi Pengamanan Data Menggunakan Algoritma XOR," J. Tek. Inform. Unika St. Thomas (JTIUST), Vol. 02 Nomor 02, Desember 2017, vol. 8, no. 1, pp. 61–69, 2017.
[12] M. A. F. Rachman, "Perancangan Aplikasi Memo Menggunakan Algoritma Kriptografi Caesar Cipher Dan Rsa Berbasis Android," Semin. Nas. Inov. dan Apl. Teknol. di Ind., pp. 121–127, 2018.
[13] M. H. Sandria, E. V. Haryanto, and A. Setiawan, "MENGGUNAKAN METODE RSA DAN CAESAR CIPHER BERBASIS ANDROID SMS Application Design Using RSA and Caesar Method Based On Android," pp. 13–24.
[14] B. Syahputra, "Perancangan Aplikasi Messanger Dengan Menerapkan Caesar Shift Berbasis Secret Sharing," J. Comput. Syst. Informatics …, vol. 1, no. 1, pp. 9–14, 2019, [Online]. Available: https://ejurnal.seminar-id.com/index.php/josyc/article/view/32
[15] I. Kombinasi Caesar Cipher dan Hill Cipher Menggunakan Modifikasi Sandi Morse Untuk Pengamanan Pesan Berbasis Teks et al., "Implementation of the Combination of Caesar Cipherand Hill Cipher Using Modified Morse Code forText-Based Message Security," vol. 3, no. 1, pp. 8–13, 2021.
[16] Hermansa, R. Umar, and A. Yudhana, "Pangamanan Pesan Menggunakan Kriptografi," J. Sains Komput. Mat. , vol. Vol 4, pp. 1–13, 2020.
[17] C Rizal, "Perancangan Server Kantor Desa Tomuan Holbung Berbasis Client Server," Bulletin of Information Technology (BIT), p.27-33, 2022.
[18] A. B. Nasution, "Implementasi Pengamanan Data Dengan Menggunakan Algoritma Caesar Cipher Dan Transposisi Cipher," J. Teknol. Inf., vol. 3, no. 1, p. 1, 2019, doi: 10.36294/jurti.v3i1.680.
[19] G. B. Minarto and M. Q. Khairuzzaman, "Penerapan Kriptografi Menggunakan Caesar Cipher Dan Vigenere Cipher," Enter, vol. 1, pp. 1–12, 2018, [Online]. Available: http://www.sisfotenika.stmikpontianak.ac.id/index.php/enter/article/view/787.