E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 01 Nomor 02 September 2023

Peningkatan Pengamanan Pesan Pribadi Menggunakan Kriptografi Klasik Berbasis Algoritma Subtitusi Chiper

[1]Hildayanti Idrus

[1]Pendidikan Teknik Informatika dan Komputer, Universitas Negeri Makassar, Jl. A.P. Pettarani, Kota Makassar, Sulawesi Selatan
Email: hildayantiidrus806@gmail.com[1]

Received : 18 Juli 2023
Accepted : 29 Agustus 2023
Published : 25 September 2023

ABSTRAK

Pada zaman digital yang semakin berkembang ini, keamanan pesan atau informasi menjadi hal yang penting karena semakin banyak informasi atau pesan yang rentan diakses atau dibaca oleh orang lain yang tidak sah. Untuk melindungi privasi dan kerahasiaan informasi pribadi, diperlukan sistem keamanan pesan yang efektif dan terpercaya. Salah satu cara yang efektif adalah dengan menggunakan algoritma kriptografi seperti algoritma subtitusi chiper yang telah digunakan untuk mengamankan data. Implementasi sistem keamanan pesan atau informasi menggunakan algoritma subtitusi chiper dapat menjadi solusi yang efektif dan terpercaya untuk mengamankan pesan pribadi dari serangan dan akses yang tidak sah serta menjaga privasi dan kerahasiaan informasi pribadi. Penelitian ini menggunakan metode Studi Literatur, Analisa Sistem, Implementasi, dan Pengujian untuk menganalisis dan mengimplementasikan algoritma subtitusi chiper berbasis visual basic. Hasil penelitian ialah sebuah aplikasi berbasis Microsoft Visual Basic yang dapat melakukan enkripsi dan dekripsi pesan/teks. Algoritma subtitusi chiper menunjukkan bahwa pada proses enkripsi dan dekripsi dapat menjaga keamanan pesan yang telah di ujikan sehingga keamanan pesan lebih terjamin dan terjaga kerahasiaannya.

Kata Kunci: Kriptografi, Keamanan Data, Algoritma Subtitusi Chiper, Enkripsi, Dekripsi

ABSTRACT

In this growing digital age, message or information security is important because more and more information or messages are vulnerable to being accessed or read by unauthorized persons. To protect the privacy and confidentiality of personal information, an effective and reliable message security system is needed. One effective way is to use cryptographic algorithms such as the cipher substitution algorithm that has been used to secure data. Implementation of a message or information security system using a cipher substitution algorithm can be an effective and reliable solution for securing private messages from attacks and unauthorized access and maintaining the privacy and confidentiality of personal information. This study uses the method of Literature Study, System Analysis, Implementation, and Testing to analyze and implement a visual basic based cipher substitution algorithm. The result of this research is an application based on Microsoft Visual Basic that can encrypt and decrypt messages/texts. The cipher substitution algorithm shows that the encryption and decryption process can maintain the security of the message that has been tested so that message security is guaranteed and confidentiality is maintained.

Keywords: Cryptography, Data security, Cipher Substitution Algorithm, Encryption, Decryption

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 01 Nomor 02 September 2023

1. PENDAHULUAN

Dalam era digital seperti saat ini dimana semua hal dilakukan secara digital, sehingga keamanan pesan atau informasi sangatlah penting agar tidak dapat diakses oleh orang yang tidak bertanggung jawab (Murni et al., 2023). Baik itu pesan atau informasi yang penting dan bersifat pribadi dan harus di jaga keamanannya (Alasi & Fitriani, 2022). Pengamanan pesan atau informasi dilakukan untuk menjaga kerahasiaan, keutuhan dan keabsahan informasi. Pada proses pengiriman atau pertukaran pesan atau informasi harus dijamin bahwa pesan atau informasi tersebut tidak dapat diketahui oleh orang yang tidak berhak (Hidayah et al., 2023).

Karena adanya pemikiran untuk mengamankan data, maka lahirlah ilmu khusus yang mempelajari tentang kamanan data tersebut. Dalam sejarah terciptanya ilmu ini, ada banyak cara dalam mengamankan data secara tradisional, misalnya saja seperti pesan singkat yang ditulis di kertas panjang yang digulung pada sebuah kayu (scytale), dan apabila gulungan kertas tersebut dibuka, maka pesan akan berbentuk huruf-huruf sandi yang sulit dimengerti. Pada zaman yang lebih modern, ilmu keamanan data ini sudah dikenal dengan kriptografi (Hidayah et al., 2023).

Teknik yang bisa digunakan untuk mengamankan data adalah Teknik kriptografi (Serdano et al., 2019). Dimana kriptografi merupakan salah satu cabang ilmu yang sangat berperan penting dalam pengamanan data atau ilmu yang mempelajari tentang bagaimana sebuah data atau pesan tetap dijaga kerahasiaannya. Dimana kerahasiaan data dijaga agar data tersebut terhindar dari pihak-pihak yang tidak berhak yang mungkin membaca data tersebut (Widarma et al., 2019).

Kriptografi memiliki dua proses yang sangat penting dimana yaitu proses enkripsi dan deskripsi. Enkripsi merupakan mengubah data atau disebut juga plaintext kedalam kriptografi menjadi sebuah kode-kode acak yang tidak dapat dibaca yang dapat disebut cipertext (Muhammad & Bengkulu, 2020). Sedangkan deksripsi yaitu mengubah data yang telah di enkripsi menjadi data awal sehingga dapat dibaca oleh penerima data atau pesan (Widarma et al., 2019). Kriptografi memiliki teknik matematika yang berhubungan dengan aspek keamanan informasi, kuat lemahnya metode kriptografi tidak terletak pada hasil enkripsi atau ciphertext, melainkan pada kunci yang digunakan (Budi et al., 2019).

Salah satu algoritma kunci simetris adalah subtitusi cipher. Subtitusi Cipher adalah algoritma klasik yang menggunakan abjad. Caranya adalah dengan mengganti (menyulih atau mensubstitusi) setiap karakter dengan karakter lain dalam susunan abjad (alfabet). Misalnya, tiap huruf disubstitusi dengan huruf ketiga berikutnya dari susunan abjad (Utomo et al., 2019).

Pada Penelitian sebelumnya yaitu membuat sistem Informasi inventory yang digunakan melakukan enkripsi terhadapa data yang akan di simpan pada database sehingga kerahasiaan data lebih terjamin (Susianto & Mustika, 2019). Proses enkripsi yang dilakukan yaitu dengan melakukan enkripsi pada nama obat yang tersimpan kedalam sistem *inventory* dengan menggunakan *key* tertentu dengan memanfaatkan algoritma kripstografi caesar cipher, PHP dan database MySQ.

Pada Penelitian sebelumnya yaitu menggunakan algoritma Caesar chipper dan vigenere cipher untuk membuat aplikasi kriptografi berbasis android yang dapat melakukan enkripsi dan dekripsi (Utomo et al., 2019), Yang perlu diperhatikan adalah pemakaian karakter yang tepat agar proses enkripsi dan dekripsi dapat berjalan dengan optimal, karena jika karakter yang dipakai berada di luar batasan karakter yang digunakan maka karakter tersebut tidak dapat dienkripsi dan dekripsi.

Pada penelitian sebelumnya yaitu membuat sebuah sistem untuk mengamankan data pada pengarsipan surat menggunakan kriptografi klasik (Fajri et al., 2015), dengan menggunakan gabungan dari metode vigenere cipher dan shift *cipher/Caesar cipher*. Hasil dari penelitian ini adalah memiliki kemampuan lebih dalam *record database* karena menggunakan 2 metode yaitu vigenere dan shift, sehingga sangat sulit untuk dibaca isi dari *record* tersebut dan untuk kekurangan nya untuk menampilkan waktu dalam proses enkripsi.

Dengan demikian, tujuan penilitian pengamanan pesan pribadi menggunakan kriptografi berbasis algoritma subtitusi cipher yang digunakan untuk melakukan enkripsi dan dekripsi agar dapat menjadi solusi yang efektif dan terpercaya untuk mengamankan pesan selama proses pertukaran data dari orang yang tidak berhak serta menjaga kerahasiaan data agar tetap aman.

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 01 Nomor 02 September 2023

2. PENELITIAN TERKAIT

Keamanan pesan telah menjadi hal penting dalam proses pertukaran informasi saat ini. Salah satu cara menjaga informasi agar tidak diketahui oleh siapapun kecuali pihak yang memiliki akses dapat dilakukan dengan cara membuat konsep kerahasiaan data. Untuk menjaga keamaanan data dapat menggunakan kriptografi (Diana, 2022). Dengan menggunakan teknik enkripsi dan deskripsi. Salah satu teknik enkripsi yang umum digunakan adalah algoritma subtitusi cipher.

Pesan (*message*) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah (*plaintext*) atau teks jelas (*cleartext*)(Alasi & Fitriani, 2022). Agar pesan tidak dapat dimengerti maknanya oleh pihak lain yang tidak berkepentingan, maka pesan perlu disandikan kebentuk lain yang tidak dapat dipahami. Bentuk pesan yang tersandi disebut cipherteks (*ciphertext)* atau kriptogram (*cryptogram*) (Batubara, 2019). Cipherteks harus dapat ditransformasikan kembali menjadi plaintext semula agar dapat diterima dan bisa.

Subtitusi Cipher adalah algoritma klasik yang menggunakan abjad. Cara kerja algoritma ini yaitu mengenkripsi plaintext pada pesan dengan cara menggeser huruf pada pesan tersebut sampai nilai kunci pada urutan alphabet sehingga pesan tidak dapat dibaca oleh orang lain, pesan dapat diubah dengan metode caesar dan dengan pergeseran kunci untuk keamanan dari isi pesan (Susianto & Mustika, 2019). Fungsi enkripsi serta dekripsi Setelah di implementasikan dapat tidak dapat memperoleh plaintext. Berfungsi dengan baik dimana plainteks awal sebelum di enkripsi sama dengan plainteks akhir hasil dari fungsi dekripsi (Alasi, 2019).

Kriptografi merupakan salah satu bidang ilmu yang mempelajari tentang menjaga keamanan pesan dalam proses pengiriman dengan menggunakan metode penyandian tertentu dengan tujuan agar informasi yang termuat dalam pesan tersebut tidak diambil dan disalahgunakan oleh orang lain (Hidayah et al., 2023).

Ada empat tujuan mendasar dari ilmu kriptograpi ini juga merupakan aspek keamanan informasi yaitu: Kerahasiaan adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi. Integritas data adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubtitusian data lain kedalam data yang sebenarnya. Autentikasi adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasiitu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian isi datanya, waktu pengiriman.

Kriptografi adalah sebagai ilmu untuk menjaga sebuah kerahasiaan data. Namun pada pengertian modern kriptografi terdiri dari dua kegiatan yang saling berkaitan (Fachri & Sembiring, 2020). dua proses tersebut disebut enkripsi dan deskripsi (Lestari et al., 2019). Kriptografi memiliki 4 komponen utama yaitu: Plaintext, yaitu pesan yang dapat dibaca. Ciphertext, yaitu pesan sandi/ pesan acak yang tidak bisa dibaca. Key, yaitu kunci untuk melakukan Teknik kriptografi. lgoritma, yaitu metode untuk melakukan enkripsi dan dekripsi.

Proses menyandikan plainteks menjadi cipherteks disebut enkripsi (encryption) atau enciphering. Sedangkan proses mengembalikan cipherteks menjadi plainteks disebut dekripsi (decryption) atau deciphering (Hidayah et al., 2023).

Algoritma kriptogarfi disebut juga cipher, yaitu aturan untuk enkripsi dan dekripsi, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Beberapa cipher memerlukan algoritma yang berbeda untuk enciphering dan deciphering (Susianto & Mustika, 2019). Konsep matematis yang mendasari algoritma kriptografi adalah relasi antara dua buah himpunan yang berisi elemen - elemen plainteks dan himpunan yang berisi cipherteks. Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen- elemen antara dua himpunan tersebut (Utomo et al., 2019).

Caesar, atau sandi geser, kode Caesar atau Geseran Caesar adalah salah satu teknik enkripsi paling terkenal. Sandi ini termasuk sandi substitusi dimana setiap huruf pada teks terang (plaintext) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet (Susianto & Mustika, 2019). Pada teknik Caesar cipher ada dua deretan baris alphabet yang disusun, pada deratan barispertama berisikan urutan alphabet A-Z dan pada deretan kedua berisikan alphabet sandi untuk mengenkripsi pergesaran dari plaintext.

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES
Progressive Information, Security, Computer, and Embedded System

PISCES Volume 01 Nomor 02 September 2023

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
Ciphertext	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

Gambar 1. Tabel Subtitusi Cipher

Caranya adalah dengan mengganti (menyulih atau mensubstitusi) setiap karakter dengan karakter lain dalam susunan abjad (alfabet)(Hidayah et al., 2023) Jadi, huruf a pada plaintetx disubstitusikan dengan D, huruf b disubstitusi dengan E, demikian seterusnya. Pergeseran huruf tersebut besifat siklik, jadi huruf x digeser menjadi A, huruf y menjadi B, dan huruf z menjadi C. Karena hanya ada 26 huruf abjad, maka pergeseran huruf yang mungkin dilakukan adalah dari 0 sampai 25 (Fajri et al., 2015).

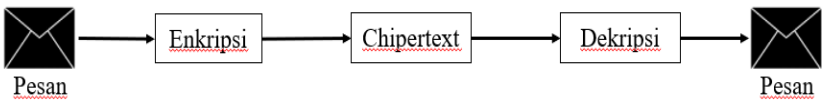
3. METODE PENELITIAN

Metodologi penelitian berisi rencana dan tahapan atau gambaran dari penelitian yang akan dilakukan, sehingga menghasilkan hasil sesuai yang diharapkan. Adapun tahapan penelitiannya yaitu, Studi Literatur, Analisis Sistem, Implementasi, dan Pengujian. Metode penelitian berisi tahapan dari penelitian yang dilakukan antara lain:

Studi Literatur, melakukan pencarian literatur mengenai proses enkripsi dan deskripsi algoritma subtitusi cipher untuk memahami konsep, prinsip, kelebihan, dan kekurangan masing-masing topik. Studi literatur ini sebagai referensi dalam melakukan penelitian kedepannya. Analisis Sistem, tahap ini berguna untuk menganalisis mengenai kebutuhan sistem keamanan dalam hal ini maka dilakukan perangkuman penelitian-penelitian sebelumnya mengenai penggunaan algoritma subtitusi cipher untuk proses enkripsi dan dekripsi. Implementasi, pada tahap ini, di implementasikan algoritma subtitusi cipher untuk proses enkripsi dan dekripsi untuk mengamankan informasi atau pesan untuk menjamin keamanan data. Pengujian, pada Tahap ini dilakukan uji coba untuk memastikan algoritma subtitusi cipher berjalan dengan baik dan tidak terjadi kesalahan, dimana dapat melakukan enkripsi dan dekripsi.

3.1 Arsitektur Sistem

Sistem yang dibangun adalah sistem yang dapat melakukan proses enkripsi dan dekripsi terhadap pesan. Hal ini dilakukan untuk meningkatkan keamanan pesan terhadap akses oleh orang tidak berhak. Dimana setiap pesan akan dienkripsi dan didekripsi dengan algoritma algoritma subtitusi cipher sehingga pesan tidak dapat dibaca oleh orang lain. Adapun bentuk proses dari arsitektur sistem yang akan dibuat sebagai berikut:



Gambar 2. Arsitektur Sistem

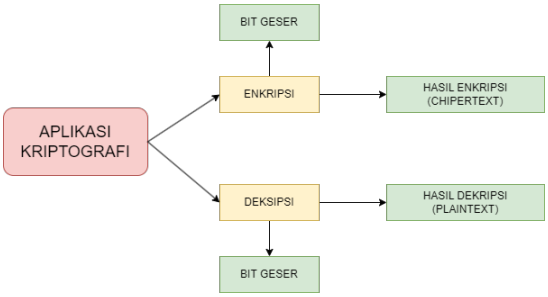
Penjelasan dari skema tersebut yaitu pesan yang telah dibuat akan di enkripsi menggunakan algoritma subtitusi cipher. Setelah di enkripsi maka pesan akan berbentuk chipertext dimana pesan tersebut tidak dapat dibaca dan dipahami jika belum dilakukan proses dekripsi. Selanjutnya pesan akan didekripsi untuk mengembalikan pesan asli sehingga pesan dapat di baca oleh penerima menggunakan algoritma seperti pada proses enkripsi sehingga pesan lebih terjamin keamanannya.

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 01 Nomor 02 September 2023

4. HASIL DAN PEMBAHASAN

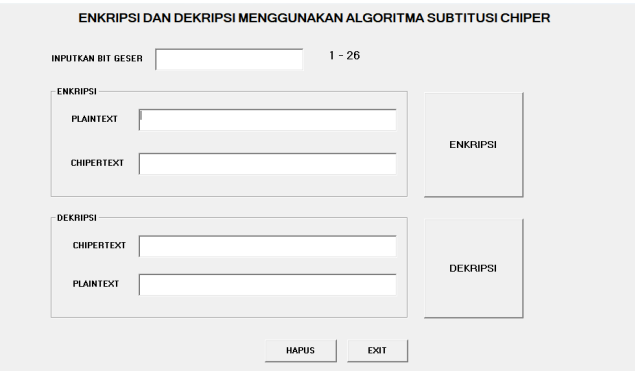
Aplikasi yang dirancang adalah sebuah aplikasi enkripsi dan dekripsi menggunakan Algoritma Subtitusi Cipher berbasis *Microsoft visual basic*, dalam aplikasi ini pengguna dapat melakukan enkripsi dan dekripsi pesan atau informasi. Pengujian dapat dilakukan dengan sebuah aplikasi enkripsi dan dekripsi Subtitusi Cipher melibatkan beberapa tahapan untuk mengetahui dan memastikan bahwa implemntasi Algoritma Subtitusi Cipher dapat berfungsi dengan benar serta dapat melindungi pesan atau informasi. Berikut gambara umum pengujian yang akan dilakukan:



Gambar 3. Desain Pengujian

4.1 Tampilan Aplikasi

Berikut tampilan aplikasi enkripsi dan dekripsi pesan pada gambar 4, dimana pada tampilannya terdapat beberapa fitur seperti enkripsi, dekripsi, hapus dan exit. Pada Tampilan enkripsi pengguna dapat melakukan enkripsi terhadap informasi yang dimiliki. Sedangkan pada Pada tampilan dekripsi pengguna dapat melakukan dekripsi terhadap ciphertext sehingga pesan yang telah di kodekan dapat di baca kembali oleh pengguna.



Gambar 4. Tampilan Aplikasi

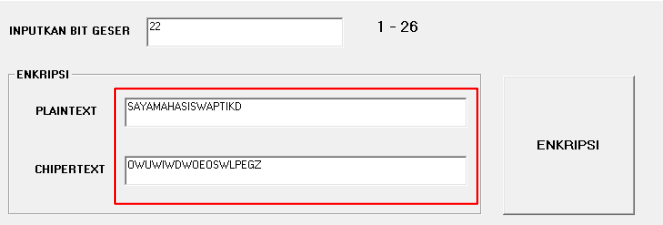
4.2 Enkripsi Pesan

Pada proses enkripsi informasi atau pesan dapat dilakukan dengan memasukkan pesan atau informasi yang ingin dienkripsi, lalu inputkan bit geser sesuai yang diinginkan seperti pada gambar 5. Selanjutnya tekan tombol enkripsi maka akan mengahasilkan chipertext yang tidak dapat di baca karena menggunakan kode-kode yang rumit.

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES
Progressive Information, Security, Computer, and Embedded System

PISCES Volume 01 Nomor 02 September 2023



Gambar 5. Tampilan Hasil Enkripsi

4.3 Dekripsi Pesan

Pada proses dekripsi seperti pada gambar 6, dapat dilakukan dengan memasukkan chipertext selanjutnya tekan tombol dekripsi untuk mendapatkan pesan atau informasi yang dapat dibaca dan dipahami.

Gambar 6. Tampilan Hasil Dekripsi

4.4 Pengujian Enkripsi dan Dekripsi

Untuk melakukan pengujian maka akan dilakukan uji coba dengan panjang pesan yang berbeda-beda dan input bit geser yang tidak sama setiap pesan, untuk melihat keberhasilan proses enkripsi dan dekripsi. Adapun hasil uji coba dapat dilihat pada tabel 1 berikut:

Tabel 1. Hasil Uji Coba Enkripsi dan Dekripsi

No.	Input Bit Geser	Plaintext (Enkripsi)	Chipertext	Plaintext (Dekripsi)
1.	22	SAYAMAHASISWAPTIKD	OWUWIWDWOEOSWLPEGZ	SAYAMAHASISWAPTIKD
2.	15	KEAMANANINFORMASI	ZTPBPCPCXCUDGBPHX	KEAMANANINFORMASI
3.	5	PENGERTIAN	UJSLJWYNFS	PENGERTIAN
4.	12	HAISAYAHILDAYANTI	TMUEMKMTUXPMKMZFU	HAISAYAHILDAYANTI
5.	8	PTIKD	XBQSL	PTIKD

Berdasarkan hasil proses enkripsi dan dekripsi dapat diketahui bahwa algoritma vigenere cipher berhasil melakukan enkripsi dan dekripsi dengan baik karena dapat melakukan pengkodean dan

mengembalikan pesan kebentuk semula sehingga pesan sulit untuk di baca jika telah dilakukan proses enkripsi karena pesan awal sangat jauh berbeda dengan pesan yang telah di enkripsi (chipertext).

5. KESIMPULAN DAN SARAN

Berdasarkan penelitian yang telah dilakukan, maka dapat ditarik kesimpulan yaitu, algoritma subtitusi cipher merupakan suatu algoritma dimana pada proses enkripsi dan dekripsi teks sangat sederhana karena caranya adalah dengan mengganti (menyulih atau mensubstitusi) setiap karakter dengan karakter lain dalam susunan abjad (alfabet). Dimana ciphertext yang dihasilkan berbeda dengan pesan asli sebelum di enkripsi sehingga keamanan pesannya lebih terjaga kerahasiaanya. Serta aplikasi ini dapat melakukan enkripsi dan dekripsi dimana kita tinggal memasukkan pesan atau informasi yang ingin kita enkripsi. Dan dapat pula melakukan dekripsi data agar data bisa dibaca kembali.

Berdasarkan hasil penelitian dan kesimpulan menganai aplikasi enkripsi dan dekripsi maka diajukan saran yaitu, aplikasi enkripsi dan dekripsi dapat melakukan enkripsi dan dekripsi berbagai file dokumen dan gambar. Serta aplikasi ini dapat menyediakan beberapa menu sehingga tampilan lebih menarik.

REFERENSI

Alasi, T. S. (2019). Implementasi Kriptografi Dengan Algoritma Ceasar Cipher Untuk Keamanan Data Microsoft Office Word Dan Excel. *Jurnal Informasi Komputer Logika*, *1*(2), 1–4. http://ojs.logika.ac.id/index.php/jikl/article/download/26/26

Alasi, T. S., & Fitriani, P. (2022). Peningkatan Keamanan untuk Password menggunakan Algoritma Vigenere Cipher. *Jurnal Mantik Penusa*, *6*(1), 1–10.

Batubara, M. I. (2019). Implementasi Algoritma One Time Pad (OTP) untuk Pengamanan Pesan Short Message Service (SMS). *MEANS (Media Informasi Analisa Dan Sistem)*, *4*(2), 193–199. https://doi.org/10.54367/means.v4i2.580

Budi, S., Purba, A. B., & Mulyana, J. (2019). *PENGAMANAN FILE DOKUMEN MENGGUNAKAN KOMBINASI*. *11*(28), 222–230.

Diana, I. N. (2022). Algoritma Affine Cipher dan Modifikasi Affine Cipher , serta Kombinasinya dengan Cipher Transposisi Grup Simetri untuk Mengamankan Pesan Teks. *KUBIK: Jurnal Publikasi Ilmiah Matematika*, *7*(1).

Fachri, B., & Sembiring, R. M. (2020). Pengamanan Data Teks Menggunakan Algoritma DES Berbasis Android. *Jurnal Media Informatika Budidarma*, *4*(1), 110. https://doi.org/10.30865/mib.v4i1.1700

Fajri, G. R., Ahmad, S., Saputra, R. K., & Sembiring, E. H. (2015). *KEAMANAN DATA PADA PENGARSIPAN SURAT MENGGUNAKAN METODE KRIPTOGRAFI KLASIK*. *2*(1), 61–72.

Hidayah, V. M., Mulyana, D. I., & Bachtiar, Y. (2023). Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian Pesan Teks. *Journal on Education*, *5*(3), 8563–8573. https://doi.org/10.31004/joe.v5i3.1647

Lestari, W. A., Tulloh, R., Novianti, A., & St, S. (2019). MEDIA PEMBELAJARAN INTERAKTIF ENKRIPSI CAESAR CIPHER , VIGENERE CIPHER , DAN ALGORITMA RSA Interactive Learning Media of Caesar Cipher , Vigenere Cipher , and RSA Algorithm Encryption. *EProceedings …*, *5*(3), 2912–2924. https://openlibrarypublications.telkomuniversity.ac.id/index.php/appliedscience/article/view/11296

Muhammad, A., & Bengkulu, U. M. (2020). *MENGGUNAKAN METODE ADVANCE VIGENERE*. *3*(3), 156–162.

Murni, I., Br pa, A. S., Lubis, B. R., & Ikhwan, A. (2023). Pengamanan Pesan Rahasia dengan Algoritma Vigenere Cipher Menggunakan PHP. *Journal on Education*, *5*(2), 3466–3476. https://doi.org/10.31004/joe.v5i2.1027

Serdano, A., Zarlis, M., Sawaluddin, & Hartama, D. (2019). Pengamanan Pesan Menggunakan Algoritma Hill Cipher Dalam Keamanan Komputer. *Jurnal Mahajana Informasi*, *4*(2), 1–5.

Susianto, D., & Mustika, D. (2019). MEMBANGUN SISTEM INFORMASI INVENTORY MENGGUNAKAN ALGORITMA CAESAR CIPHER SEBAGAI MEDIA ENKRIPSI (Studi Kasus: Klinik Ridho Husada).

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 01 Nomor 02 September 2023

Jurnal Cendikia, *18*(1), 309–315. https://jurnal.dcc.ac.id/index.php/JC/article/view/284

Utomo, I. W., Latifah, R., & Risanty, R. D. (2019). Aplikasi Kriptografi Berbasis Android Menggunakan Algoritma Caesar Cipher & Vigenere Cipher. *Jurnal Sistem Informasi, Teknologi Informasi Dan Komputer*, *9*(2), 142–149.

Widarma, A., Siregar, H. F., & Irawan, M. D. (2019). *Teknik Keamanan Data Menggunakan Vigenere Cipher Dan Electronic Code Book (ECB)*. *3*(September), 393–400.