JNATIA Volume 3, Nomor 3, Mei 2025 p-ISSN: 2986-3929
Jurnal Nasional Teknologi Informasi dan Aplikasinya e-ISSN: 3032-1948

Perancangan Sistem Enkripsi Pesan Teks Menggunakan Enkripsi RSA dan Caesar Cipher

I Nyoman Arista Wisnawa[a1], I Made Widiartha[a2]

Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam,
Universitas Udayana
Jalan Raya Kampus UNUD, Bukit Jimbaran, Kuta Selatan, Badung, Bali, Indonesia
[1]ariswisnawa46@gmail.com
[2]madewidiartha@unud.ac.id

Abstract

The development of communication methods has changed a lot in the current digital era, people who initially communicated face-to-face or through a mail are starting to be communicating through the internet. Nowadays, people more often exchange information on social media. The increasingly widespread internet infrastructure makes it easier for people to access social media without being limited by place or time. The vast digital world certainly requires a way to secure the information circulating through the internet. The vulnerability of data on the internet to hacking and leaks makes it important to have strong security measures to protect sensitive data from unauthorized access. Encryption plays an important role in overcoming this problem. Encryption is the process of changing text data into another form that cannot be understood without knowing the correct decryption key. This research applies two different encryption methods to secure text data, utilizing a combination of the Caesar cipher and RSA algorithms to strengthen data security. The proposed system offers enhanced protection against potential security breaches, ensuring data confidentiality and integrity.

Keywords: *Encryption, Caesar cipher, RSA, Text data, Security*

1. Pendahuluan

Pesan merupakan suatu objek penting dalam komunikasi yang berisi suatu pesan yang ingin disampaikan. Komunikasi sendiri merupakan proses pertukaran informasi oleh komunikator ke komunikan secara lisan maupun tertulis. Komunikasi telah mengalami perkembangan seiring berjalannya waktu. Pada awalnya, komunikasi hanya dapat dilakukan dengan lisan secara tatap muka, tetapi seiring perkembangan zaman, manusia mulai melakukan komunikasi menggunakan surat hingga akhirnya memasuki era digital.

Pada era digital ini, komunikasi lebih sering dilakukan melalui internet menggunakan media sosial. Hal ini dikarenakan dengan menggunakan media sosial, masyarakat tidak terbataskan oleh jarak dan waktu lagi. Pada tahun 2024, secara global, pengguna internet rata-rata menghabiskan waktunya untuk bermedia sosial adalah sebanyak 143 menit perhari [1]. Di Indonesia sendiri, KIC (*Katadata Insight Center*) dan Kominfo (Kementerian Komunikasi dan Informatika) mengatakan bahwa media sosial yang sering digunakan pada tahun 2021 adalah aplikasi WhatsApp diikuti dengan Facebook lalu Instagram. Data ini didapat dengan melakukan survey. Jika dijabarkan, ada sebanyak 27,6% responden yang sangat sering menggunakan aplikasi WhatsApp dan sebanyak 52% berkata bahwa mereka sering menggunakan WhatsApp dalam sehari. 16,6% jarang serta 3,8% masuk ke dalam kategori sangat jarang dalam konteks menggunakan aplikasi WhatsApp dalam kehidupan sehari-hari [2].

Dengan begitu banyaknya pengguna yang bertukar informasi pada media sosial, tentunya dibutuhkan suatu cara untuk dapat mengamankan data pesan untuk menjaga kerahasiaan dan keamanan data. Solusi untuk permasalahan ini salah satunya dengan mengenkripsi pesan yang akan dikirim. Menurut KBBI, enkripsi berarti tulisan berupa kode atau sandi. Enkripsi dapat dikatakan sebagai sebuah proses mengubah suatu data atau teks menjadi suatu bentuk yang

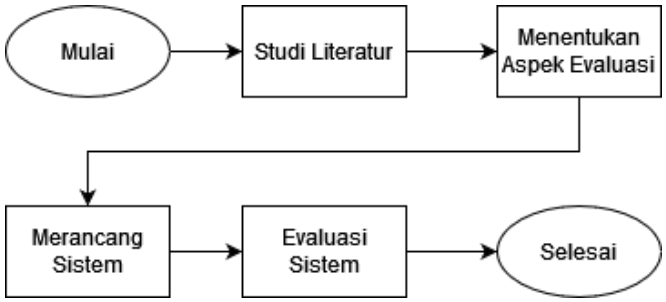
p-ISSN: 2986-3929
e-ISSN: 3032-1948

tidak dapat dimengerti tanpa mengetahui metode dekripsi yang tepat. Beberapa metode yang dapat digunakan seperti algoritma RSA dan *Caesar Cipher*. Sebelumnya telah terdapat beberapa penelitian-penelitian yang membahas penggunaan dari metode-metode tersebut. Salah satunya adalah pengimplementasian algoritma caesar cipher untuk mengamankan data yang ditulis oleh Febrianingsih dan Hafiz (2019). Aplikasi yang dikembangkan peneliti dapat menyamarkan file sehingga tidak dapat dipahami sehingga membuat keamanan data menjadi terjamin [3]. Pada penelitian ini penulis akan menggunakan gabungan dari metode enkripsi *caesar cipher* dan RSA untuk memperkuat tingkat keamanan pesan.

2. Metode Penelitian

2.1. Alur Penelitian

Untuk membuat sistem enkripsi, ada beberapa langkah-langkah yang diikuti oleh penulis. Pertama, penulis melakukan studi pustaka untuk mempelajari teori-teori yang nantinya akan digunakan pada sistem enkripsi. Setelah itu, penulis menentukan aspek-aspek yang akan digunakan untuk mengevaluasi sistem yang dirancang. Kemudian penulis merancang sistem serta melakukan evaluasi pada sistem. Gambar 1 berikut merupakan flowchart dari alur penelitian.



Gambar 1. Flowchart Alur Penelitian

2.2. Studi Literatur

a. Kriptografi

Dalam kriptografi, kita akan mempelajari teknik-teknik untuk melakukan pengamanan terhadap suatu data, menjaga kerahasiaan data, serta integritas data [4]. Kriptografi menerapkan disiplin ilmu matematika tingkat lanjut dalam melakukan pengamanan terhadap data ataupun informasi yang akan dikirim ke penerima [5]. Pengamanan data salah satunya dapat dilakukan dengan mengenkripsi data.

Enkripsi merupakan proses menyamarkan suatu informasi ke dalam bentuk yang tidak dapat dibaca tanpa mengetahui kunci khusus yang digunakan. [6]. Untuk mengembalikan *ciphertext* menjadi *plaintext*, sang penerima dari data harus melakukan proses dekripsi terhadap *ciphertext* yang diterima. Dekripsi merupakan proses pengembalian *ciphertext* ke bentuk semula (*plaintext*) sehingga dapat dibaca dan dipahami. Untuk melakukan deskripsi biasanya dibutuhkan kunci (*key)* yang digunakan dalam proses enkripsi. Kunci atau *key* adalah sebuah *keyword* yang dipakai untuk melakukan enkripsi atau dekripsi [5]. Penerapan *key* dalam enkripsi dan dekripsi dapat berbeda tergantung dari kategori enkripsi tersebut.

Kategori enkripsi ada dua, yaitu enkripsi simetris dan enkripsi asimetris. Enkripsi simetris menggunakan 1 *key* yang sama dalam mengenkripsi maupun dekripsi data. Sedangkan enkripsi asimetris menggunakan dua *key* yang berbeda, yaitu *public key* (kunci publik) dan *private key* (kunci privat) dalam proses enkripsi dan dekripsi. Enkripsi asimetris tergolong baru dibandingkan enkripsi simetris [5].

b. Caesar Cipher

Caesar cipher atau biasa dikenal juga dengan nama *shift cipher* atau *substitusi cipher* merupakan metode enkripsi teks yang awalnya berasal Romawi. Dipopulerkan pertama kali oleh Julius Caesar yang merupakan seorang pimpinan militer serta politikus Romawi dengan menggeser setiap huruf pada alphabet sebanyak 3 kali [7]. Julius awalnya mencetuskan metode ini untuk kepentingan pengiriman pesan kepada para sekutunya dengan tujuan agar musuh tidak dapat mengetahui pesan yang dikirim [8]. Pada dasarnya, metode ini bekerja dengan menggeser setiap huruf alphabet sebanyak yang diinginkan dengan rentang 1 sampai 25. Rentang tersebut didapatkan dari jumlah huruf pada alphabet dikurangi 1. Pada tabel 1 merupakan contoh dari pergeseran yang dilakukan:

Tabel 1. Contoh penggeseran huruf sebanyak 3 kali

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
Misalkan geser 3 kali, A = D
D E F G H I J K L M N O P Q R S T U V W X Z Y A B C

Dapat dilihat pada tabel, jika misalnya huruf digeser sebanyak 3 kali maka A akan menjadi D, B menjadi E, dan seterusnya. Untuk mengembalikan pesan ke bentuk aslinya (dekripsi) sebenarnya tidak begitu rumit, hanya saja membutuhkan waktu jika misalnya pergeseran dilakukan sangat banyak. Hal ini dikarenakan proses dekripsi harus dilakukan dengan mencoba setiap kemungkinan pergeseran yang dilakukan. Itu merupakan salah satu kelemahan dari metode enkripsi ini. Proses enkripsi dan dekripsi secara umum dapat dirumuskan berturut-turut sebagai dengan persamaan berikut:

$$C(P) = (IP + K)\ mod\ 26 \quad (1)$$

$$P(C) = (IC + K)\ mod\ 26 \quad (2)$$

Rumus tersebut diterapkan secara berulang untuk setiap huruf pada pesan yang dikirim. Dengan keterangan sebagai berikut:

- *C* merupakan *Ciphertext,* teks setelah dilakukan enkripsi
- *P* merupakan *Plaintext*, teks asli sebelum dienkripsi ataupun sesudah didekripsi
- *IP* merupakan indeks dari setiap huruf pada *plaintext* yang dikirim
- *IC* merupakan indeks dari setiap huruf pada *ciphertetx* yang dikirim
- *K* merupakan banyaknya pergeseran yang dilakukan atau biasa disebut dengan *key*

c. Algoritma Rivest-Shamir-Adleman (RSA)

Algoritma Rivest-Shamir-Adleman atau disingkat sebagai RSA merupakan jenis enkripsi yang menggunakan *asymmetric key system*. Jenis enkripsi ini menggunakan dua kunci yang berbeda untuk melakukan proses enkripsi dan dekripsinya. Pada algoritma enkripsi RSA sendiri memerlukan kunci publik dan kunci privat. Kunci publik merupakan kunci yang dapat dibagikan ke orang lain sedangkan kunci privat tidak boleh diketahui oleh sembarangan orang, harus dirahasiakan terutama untuk pihak yang tidak sah [7]. Algoritma ini susah untuk dipecahkan karena sistem enkripsinya yang menggunakan pemfaktoran bilangan prima yang besar [9].

Kunci publik ada 2, dilambangkan dengan *n* dan *e*. Untuk kunci privat berjumlah satu, umumnya dilambangkan dengan *d*. Selain kunci publik dan kunci privat tersebut, ada

beberapa variabel yang juga harus dimiliki untuk menerapkan algoritma RSA. Tabel 2 merupakan penjelasan dari setiap variabel yang digunakan:

Tabel 2. Variabel yang diperlukan

Simbol	Penjelasan
p	Simbol *p* merupakan bilangan prima yang diambil secara acak. Nilai dari *p* diharapkan cukup besar setidaknya 300-digit atau lebih
q	Simbol *q* merupakan bilangan prima yang diambil secara acak. Nilai dari *q* diharapkan cukup besar setidaknya 300-digit atau lebih
n	Nilai n merupakan nilai yang nantinya akan menjadi modulus. Nilai n didapatkan dengan mengalikan p dan q
ϕ(*n*)	ϕ(*n*) atau *phi of n* merupakan banyaknya bilangan yang kurang dari *n* dan berkoprima terhadap *n*
e	Merupakan eksponen untuk proses enkripsi. Variabel e bernilai kurang dari n dan lebih dari 2
d	Merupakan eksponen untuk proses dekripsi

Setelah mengetahui apa saja variabel-variabel yang dibutuhkan, tentunya perlu untuk mengetahui juga rumus-rumus yang digunakan untuk membangkitkan atau mencari nilai dari variabel-variabel tersebut. Berikut merupakan rumus dari setiap variabel pada tabel 2 kecuali *p* dan *q* secara berturut-turut:

$$n = p \times q \tag{3}$$

$$\phi(n) = \phi(pq) = (p-1)(q-1) \tag{4}$$

$$e = FPB\big(e, \phi(n)\big) = 1;\ 2 < e < n \tag{5}$$

$$d = e \times d \equiv 1\ modulo\ \phi(n) \tag{6}$$

2.3. Gambaran Umum Sistem

Sistem enkripsi menerapkan dua buah metode enkripsi, yaitu Caesar cipher dan algoritma RSA. *Plaintext* terlebih dahulu di enkripsi dengan metode Caesar cipher. Hasil dari enkripsi tersebut kemudian akan dienkripsi lagi menggunakan algoritma enkripsi RSA. Setelah itu, sistem akan menghasilkan *ciphertext* akhir. Sedangkan pada proses dekripsi terjadi proses sebaliknya, sistem pertama-tama akan melakukan dekripsi dengan algoritma RSA. Hasil dari dekripsi tersebut kemudian akan dilakukan dekripsi dengan Caesar cipher untuk mencari *plaintext* yang asli.

Untuk melakukan enkripsi dan dekripsi tersebut, sistem meminta beberapa inputan dari user. Untuk enkripsi, sistem meminta *plaintext* yang akan di enkripsi dan *key* untuk melakukan *shifting*. Sedangkan, untuk melakukan dekripsi, sistem meminta *ciphertext* yang akan didekripsi, kunci privat, kunci publik, nilai n, dan *shifting key*. Output dari proses enkripsi berupa ciphertext akhir, kunci publik, kunci private, dan nilai n. Sedangkan, untuk proses dekripsi, outputnya adalah *plaintext* asli.

2.4. Penentuan Aspek Pengujian

Untuk mengetahui apakah sistem dapat mengamankan pesan teks sesuai yang diharapkan peneliti, perlu dilakukan pengujian kinerja sistem. Pengujian dilaksanakan dengan menguji aspek fungsi pada sistem. Pengujian dilakukan dengan melihat apakah:

a. Fungsi enkripsi dapat mengenkripsi plaintext yang diberikan oleh pengguna
b. Fungsi dekripsi dapat mendekripsi ciphertext akhir menjadi plaintext yang asli

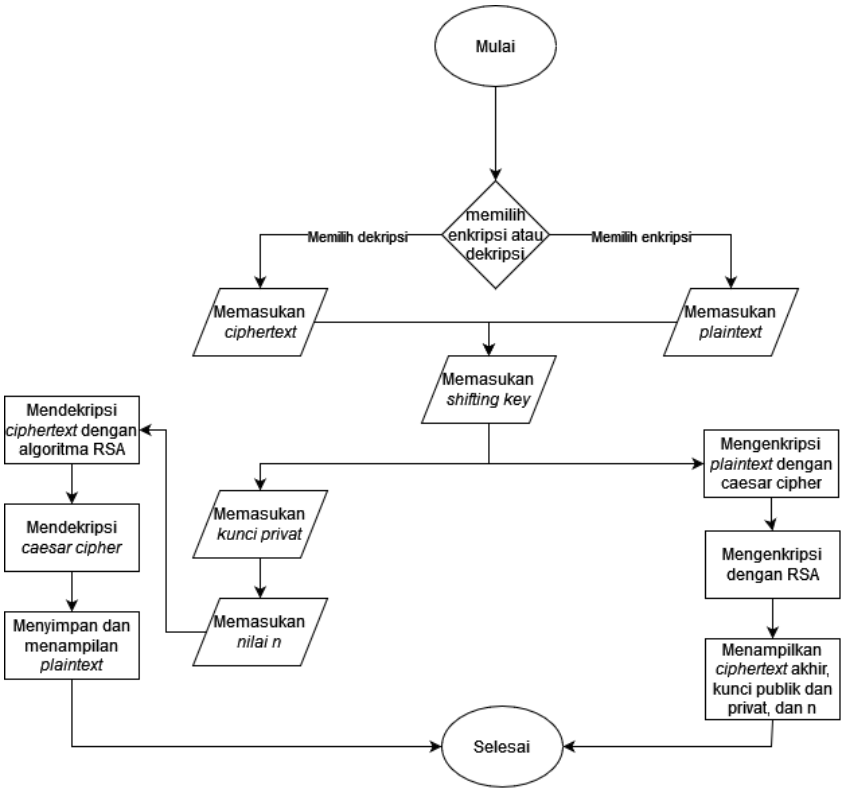
3. Hasil dan Pembahasan

3.1. Perancangan Sistem

Dalam membantu merancang sistem, penulis membuat flowchart alur sistem dan *pseudocode* fungsi-fungsi yang terdapat pada sistem. Flowchart membantu menjelaskan gambaran umum alur kerja dari sistem yang dirancang. Dari flowchart pada gambar 2, dapat dilihat bahwa saat pertama kali sistem dijalankan, user akan diminta memilih untuk melakukan enkripsi atau dekripsi.

Jika user memilih melakukan enkripsi, sistem akan meminta *input* berupa *plaintext* dan *shifting key*. *Shifting key* yang dapat dimasukan dari rentang 1-61, hal ini karena untuk melakukan enkripsi Caesar cipher menggunakan *dictionary* yang berisi huruf-huruf serta angka yang dapat dienkripsi oleh sistem, sistem akan mendeteksi setiap isi dari *dictionary* berdasarkan indeks yang dimulai dari 0. Setelah itu, sistem akan memproses *plaintext* untuk dienkripsi hingga menghasilkan *ciphertext* akhir. Terakhir, sistem akan menampilkan *ciphertext* akhir, kunci publik, kunci privat, serta nilai *n*.

Sedangkan untuk proses dekripsi, sistem pertama-tama akan meminta pengguna untuk memasukkan *ciphertext* yang akan didekripsi. Lalu secara berturut-turut meminta memasukkan shifting key, private key, dan n sebagai nilai modulus. Kemudian sistem melakukan dekripsi hingga menghasilkan *plaintext* asli. Gambar 2 menunjukan flowchart rancangan alur sistem.



Gambar 2. Flowchart alur sistem

Untuk memudahkan proses pengkodingan, penulis merancang *pseudocode* terlebih dahulu. *Pseudocode* dipisahkan per fungsi pada setiap metode. Pseudocode yang dibuat merupakan pseudocode umum, sehingga pada penerapannya nanti peneliti mungkin tidak berpatokan pada

p-ISSN: 2986-3929
e-ISSN: 3032-1948

pseudocode tersebut tetapi hanya sekedar sebagai referensi ataupun gambaran umum metode enkripsi. Pseudocode dapat dilihat pada tabel 3 dan 4 berikut:

Tabel 3. Pseudocode Caesar Cipher

Fungsi enkripsi Caesar Cipher

Make Caesar cipher dictionary
for letter in plaintext:
index = indeks letter
if index not -1:
newIndex = (index + key) % alphabetLenght
ciphertext = ciphertext + letters[newIndex]
else
ciphertext = ciphertext + letter
 	
return ciphertext

Fungsi dekripsi Caesar Cipher

for letter in ciphertext:
index = index letter
if index not -1:
newIndex = (index - key + alphabetLenght)) % alphabetLenght
plaintext = plaintext + letters[newIndex]
else
plaintext = plaintext + letter
 	
return plaintext

Tabel 4. Pseudocode Algoritma RSA

Fungsi enkripsi RSA

generate required key value
for ch in message:
convert ch to character code
ch append to message_encoded.
for ch in message_encoded:
encrypt ch
ch append to temp
‘, ’.join x in temp to ciphertext
 	
return ciphertext

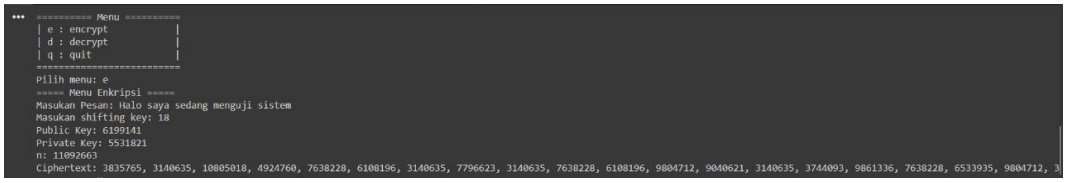
Fungsi dekripsi RSA

for ch in ciphertext:
decrypt ch
ch append to message_encoded
for ch in message_encoded:
convert ch to character code
ch append to message
 	
return message

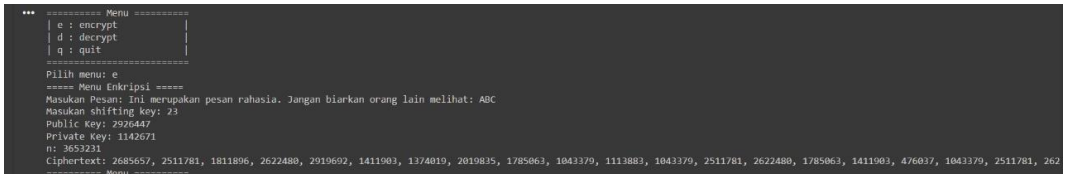
3.2. Pengujian Sistem

a. Fungsi Enkripsi

Fungsi enkripsi diuji coba dengan melakukan percobaan enkripsi dengan pesan. Hasil yang didapatkan menunjukan bahwa fungsi enkripsi dapat bekerja dengan baik dan mengeluarkan output, yaitu berupa ciphertext, kunci privat, kunci public, dan nilai modulus n seperti yang diharapkan. Gambar 3 dan 4 merupakan hasil percobaan yang dilakukan.



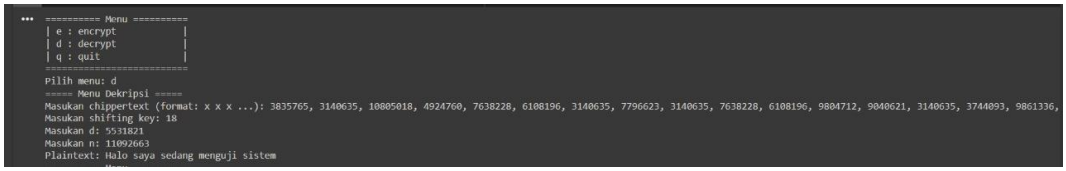
Gambar 3. Hasil percobaan fungsi enkripsi 1



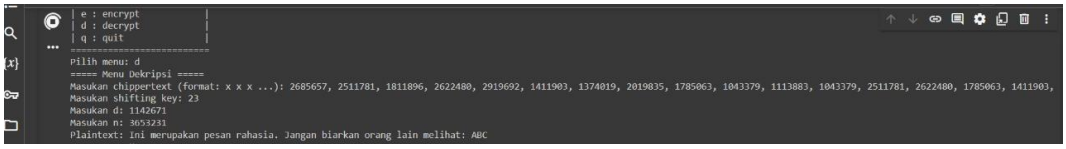
Gambar 4. Hasil perconaam fungsi enkripsi 2

b. Fungsi Dekripsi

Sama seperti fungsi enkripsi, fungsi dekripsi diuji coba dengan mendekripsi pesan. Dari percobaan yang dilakukan, fungsi dekripsi mampu melakukan proses dekripsi *ciphertext* sesuai dengan yang diharapkan. Fungsi dekripsi berhasil memecahkan *ciphertext* dan menampilkan *plaintext* semula. Berikut merupakan hasil percobaan fungsi dekripsi dapat dilihat pada gambar 5 dan gambar 6 berikut ini.



Gambar 5. Hasil percobaan fungsi dekripsi 1



Gambar 6. Hasil percobaan fungsi dekripsi 2

4. Kesimpulan

Penggunaan dua metode enkripsi yang berbeda dalam mengamankan pesan teks dapat diterapkan pada sistem, yang dalam hal ini adalah metode Caesar cipher dan metode RSA. Penggabungan dua metode enkripsi dalam mengamankan data dapat menambah keamanan dari data tersebut dan mengurangi kerentanan dan juga kekurangan dari masing-masing metode. Metode Caesar cipher merupakan metode enkripsi yang paling cepat, tetapi memiliki kerentanan terhadap serangan *brute force,* serangan yang mencoba segala kemungkinan berkali-kali sampai menemukan kunci yang benar. Sedangkan metode RSA merupakan metode enkripsi yang cukup

kuat dan sulit dipecahkan. Menggabungkan dua metode ini dapat menghasilkan *ciphertext* yang kuat terhadap serangan dan sulit untuk dipecahkan. Dari hasil evaluasi, sistem telah dapat memenuhi tujuan awal peneliti, yaitu untuk melakukan enkripsi terhadap *plaintext* serta melakukan dekripsi kembali terhadap *ciphertext* yang dihasilkan untuk mengembalikan *ciphertext* ke *plaintext* awal.

Daftar Pustaka

[1] Dixon, S. J. “Daily time spent on social networking by internet users worldwide from 2012 to 2024,” Statista, 10 April 2024, [Online]. Tersedia: https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide/ [Diakses: 8 Mei 2024]

[2] Annur, C. M. “WhatsApp, Media Sosial Paling Sering Digunakan Publik untuk Berbagi Informasi,” databoks.katadata, 4 agustus 2022, [Online]. Tersedia: https://databoks.katadata.co.id/datapublish/2022/08/04/whatsapp-media-sosial-paling-sering-digunakan-publik-untuk-berbagi-informasi [Diakses: 8 Mei 2024]

[3] Febrianingsih, R., & Hafiz, A. "Implementasi Kriptografi Berbasis Caesar Chiper Untuk Keamanan Data." *Jurnal Informasi dan Komputer*, vol. 7, no. 2, 24 Oct. 2019, pp. 81-86, doi:10.35959/jik.v7i2.163.

[4] Ayuningtyas, M. E. “Apa itu Kriptografi: Pengertian, Jenis, dan Manfaat,” it.Telkomuniversity.ac.id, 24 April 2024, [Online]. Tersedia: https://it.telkomuniversity.ac.id/kriptografi-adalah/ [Diakses: 9 Mei 2024]

[5] Kurniawan, A. “Algoritma Enkripsi,” socs.binus.ac.id, 10 Desember 2018, [Online]. Tersedia: https://socs.binus.ac.id/2018/12/10/algoritma-enkripsi/ [Diakses: 9 Mei 2024]

[6] Azis, N. "Perancangan Aplikasi Enkripsi Dekripsi Menggunakan Metode Caesar Chiper dan Operasi Xor." *Ikraith Informatika*, vol. 2, no. 1, Mar. 2018, pp. 72-80.

[7] Holden, J. (2017). *The Mathematics of Secrets: Cryptography from Caesar Ciphers to Digital Encryption*. Princeton University Press.

[8] Churchhouse, R. F. (2002). *Codes and ciphers: Julius Caesar, the Enigma, and the internet*. Cambridge University Press.

[9] Sahara, R., Prastiawan, H., Rohman, A. "Implementasi Keamanan SMS dengan Algoritma Rsa pada Smartphone Android." *Jurnal Ilmiah Fifo*, vol. 9, no. 2, 2017, pp. 112-118, doi:10.22441/fifo.v9i2.2566.