JAINS (Journal of Artificial Intelligence and Network Systems)
Vol. 1 No. 1, September 2025

SUPER ENKRIPSI PENGGUNAKAN ALGORITMA CAESAR CIPHER, AFFINE CIPHER DAN RSA UNTUK KEAMANAN DATA

Abas Rifai[1)], Bagaskara Dwi Rizky[2)], Muhammad Rangga Habibie[3)], Achmad Fauzi[4)]

[1,2,3,4)]STMIK Kaputama
Jl. Veteran No. 4A – 9A, Binjai, Sumatera Utara, Telp: (061)8828840, Fax: (061)8828845
Email: abasrifai321@gmail.com

ABSTRACT

In the ever-evolving digital era, data security has become one of the most important components. With the increasing amount of information technology, safeguarding sensitive information has become a major issue. This is especially true in the fields of communication, banking, and government. Cryptographic techniques are one of the effective ways to maintain data confidentiality. Allowing data to be encrypted, cryptography enables only authorized individuals to access it. This study examines how the combination of three cryptographic algorithms, Caesar Cipher, Affine Cipher, and RSA, results in a super encryption method. Caesar Cipher and Affine Cipher are used for initial encryption, and RSA, which is a modern algorithm with a higher level of security, is used to strengthen the layer of protection. The results of this method show that the combination of the three algorithms can enhance the security of text data by leveraging each of them. It is hoped that this super encryption technique can help address the increasingly complex data security issues in the current digital era.

Keywords : *Affine_Cipher, Caesar_Cipher, Data_security, RSA, Super_Encryption.*

1. PENDAHULUAN

Dalam era digital saat ini, keamanan data adalah komponen yang sangat penting. Berbagai industri, seperti komunikasi, perbankan, dan pemerintahan, menghadapi masalah besar dalam melindungi informasi sensitif seiring dengan peningkatan penggunaan teknologi informasi. Teknik kriptografi adalah salah satu cara yang efektif untuk menjaga kerahasiaan data.

Kriptografi mengenkripsi data sehingga hanya orang yang berwenang yang dapat mengaksesnya. Caesar Cipher, Affine Cipher, dan RSA adalah beberapa algoritma kriptografi yang paling umum digunakan. Ini adalah algoritma klasik yang mudah digunakan, tetapi memiliki tingkat keamanan yang relatif terbatas. RSA (Rivest-Shamir-Adleman) adalah algoritma modern yang lebih kompleks yang menawarkan tingkat keamanan yang lebih tinggi melalui penerapan kunci asimetris.

Dalam penelitian ini, kami menciptakan metode penyandian super enkripsi dengan menggabungkan algoritma enkripsi Caesar Cipher, Affine Cipher, dan RSA. Kami menggunakan keunggulan masing-masing algoritma ini untuk meningkatkan keamanan data teks. Data terenkripsi awal dibuat dengan Caesar Cipher dan Affine Cipher pada tahap awal. Output kemudian diproses menggunakan algoritma RSA untuk memberikan lapisan perlindungan tambahan.

2. METODOLOGI PENELITIAN

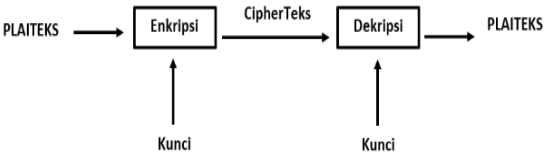
2.1 Kriptografi

Bahasa Yunani "kriptografi" berasal dari kata "cryptos", yang berarti "rahasia," dan "graphein", yang berarti "tulisan." Jadi, "tulisan rahasia" adalah definisi kriptografi. Istilah ini memiliki banyak definisi dalam literatur yang berbeda. Kriptografi adalah seni dan ilmu yang bertujuan untuk melindungi keamanan pesan, menurut Scheneier Bruce (1996)[1].

Kriptografi adalah disiplin ilmu yang berusaha menjaga kerahasiaan pesan dengan menyandikannya dalam bentuk yang tidak dapat dipahami. Enkripsi dan dekripsi adalah dua proses utama dalam kriptografi. Proses enkripsi dan dekripsi dilakukan menggunakan berbagai jenis kunci, sehingga pesan yang telah dienkripsi dapat dengan mudah dibaca dan dipahami oleh siapa pun. Istilah "plaintext" digunakan untuk menggambarkan proses ini. Selain itu, ciphertext adalah istilah yang digunakan untuk menggambarkan pesan yang telah diubah menjadi bentuk yang tidak dapat dibaca. Berbagai istilah sering digunakan dalam proses ini [2].

2.2 Caesar Cipher

Sebelum sistem kriptografi berbasis kunci publik muncul, algoritma Caesar Cipher banyak digunakan dalam sistem kriptografi simetris. Caesar Cipher mengubah setiap karakter menjadi karakter baru dengan menggesernya beberapa tempat ke kiri atau ke kanan, tergantung arah pergeseran karakter tersebut. Ini adalah salah satu jenis cipher substitusi. Metode Caesar Cipher memiliki kelebihan karena dapat menyamarkan pesan sehingga hanya orang yang mengirim dan menerima yang tahu sandi yang digunakan. Namun, metode ini tidak dapat mengenkripsi atau mendekripsi pesan yang terdiri dari beberapa kalimat atau rumus kompleks[3]. Cara kerja Caesar Cipher mengikuti cara seperti gambar dibawah ini.



Gambar 1. Cara Kerja Teknik Caesar Cipher

2.2.1 Proses Caesar Cipher

Teknik penyandian Caesar Cipher mengubah jumlah pergeseran huruf dalam teks asli berdasarkan jumlah kunci yang digunakan. Dalam proses enkripsi dan dekripsi, algoritma Caesar Cipher terdiri dari dua rumus.

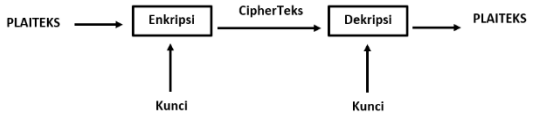
Dalam Caesar Cipher, enkripsi dapat dilakukan dengan menggunakan operator aritmetika modulo 255, yang sesuai dengan tabel ASCII. Rumus matematis yang diperlukan untuk mengenkripsi karakter P dengan mengubah K adalah sebagai berikut:

Enkripsi: C = E(P) = (P+K) Mod 255
Dekripsi: P = D(C) = (C-K) Mod 255

Dengan C sebagai ciphertext, P sebagai plaintext, K sebagai kunci rahasia, E(P) sebagai proses enkripsi, dan D(C) sebagai proses dekripsi.

2.3 Affine Cipher

Pengembangan dari Caesar Cipher, Affine Cipher mengolah plainteks dengan mengalikannya dengan nilai dan menambahkan pergeseran. Pengembangan aplikasi dengan Affine Cipher yang menggunakan kriptografi adalah salah satu metode terbaik untuk menjaga kerahasiaan informasi, dan hal ini sangat penting. [4]. Affine Cipher digambarkan seperti dibawah ini.



Gambar 2. Cara Kerja Teknik Affine Cipher

2.3.1 Proses Affine Cipher

Persamaan berikut dapat digunakan untuk melakukan proses enkripsi plaintext menggunakan algoritma affine cipher[5].

$$C = (mP + b)\ mod\ n$$

Keterangan :
C = ciphertext
P = plaintext
n = jumlah alfabet
m = bilangan bulat yang relatif prima terhadap n
b = nilai pergeseran

Algoritma cipher Affine memungkinkan proses dekripsi apabila terdapat invers dari m (mod n), yang diwakili sebagai m^{-1} (mod n). Menurut penjelasan Munir

2.4 Rivest Shamir Adlemen(RSA)

RSA diciptakan oleh Tiga peneliti dari Massachusetts Institute of Technology (MIT) Ron Rivest, Adi Shamir, dan Leonard Adleman membangun RSA pada tahun 1976. Metode kriptografi RSA membedakan kunci enkripsi dan dekripsi[6]. Berikut ini adalah penjelasan mengenai cara pembentukan kunci RSA :

1. Dua bilangan prima yang berbeda, p dan q, dipilih secara acak, dengan syarat $p \neq q$. Nilai kedua bilangan prima ini sebanding dengan tingkat keamanan yang lebih tinggi.
2. Nilai n = p*q adalah modulus untuk perhitungan kunci publik dan privat.
3. Nilai φ(n) dapat dihitung dengan menggunakan rumus φ(n) = (p – 1) * (q – 1), yang menjaga kerahasiaannya.
4. Berdasarkan ketentuan bahwa 1 < e < φ(n) dan GCD (greater common divisor) (φ(n), e) = 1, kita dapat menghitung nilai e.

5. Nilai d ditentukan sebagai bilangan bulat dengan memastikan bahwa (d * e) mod φ(n) = 1. Dengan kata lain, d dapat ditemukan dengan menggunakan rumus d = (1 + k * φ(n). Selanjutnya, berbagai nilai dicoba untuk menemukan nilai d yang memenuhi syarat tersebut.

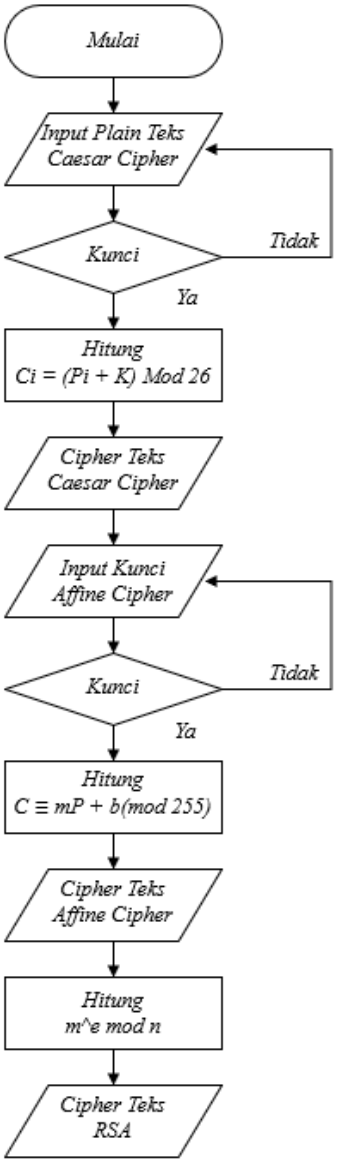
3. HASIL DAN PEMBAHASAN

3.1 Diagram Flowchart

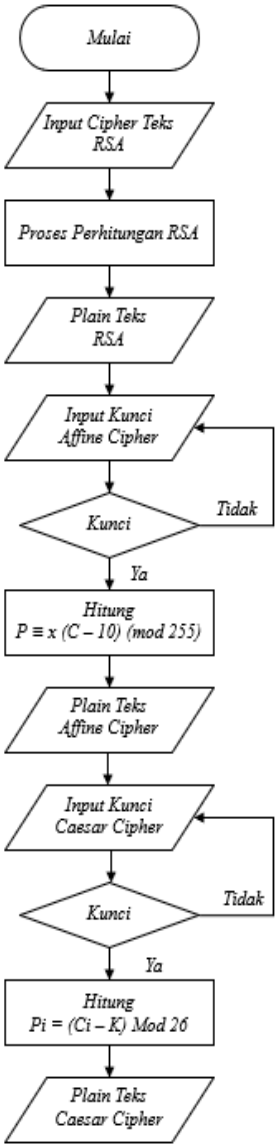
Dalam penelitian ini, kami ingin menggunakan teknik penyandian super yang menggabungkan Caesar Cipher, Affine Cipher, dan RSA. Pertama, kami akan mengenkripsi teks plaintext dengan Caesar Cipher, yang merupakan teknik sederhana yang mengubah setiap huruf dalam teks dalam posisi tertentu. Setelah Caesar Cipher menghasilkan cipher, teks kemudian akan dienkripsi kembali dengan Affine Cipher, yang merupakan teknik yang lebih kompleks yang mengubah setiap huruf dalam teks ke posisi tertentu.

Selanjutnya, teknik penyandian RSA (Rivest–Shamir–Adleman) akan mengenkripsi teks yang telah disandi dengan metode Affine Cipher. RSA adalah kriptografi asimetris yang menggunakan pasangan kunci publik dan privat untuk mengenkripsi dan mendekripsi data, menghasilkan lapisan keamanan yang sangat kuat.

Teks sandi yang dibuat menggunakan algoritma RSA yang paling baru akan didekripsi dengan kunci privat yang tepat selama proses dekripsi. Tujuan dari langkah ini adalah untuk mendapatkan hasil enkripsi sebelumnya yang dibuat oleh Affine Cipher. Kemudian, hasil dekripsi ini akan diproses kembali dengan menggunakan teknik penyandian kedua, Affine Cipher, dengan parameter kunci yang sesuai. Pada akhirnya, teknik Caesar Cipher akan digunakan untuk mendekripsi hasil dekripsi yang baru ke bentuk plaintext asli. Kami berharap dapat meningkatkan keamanan data secara signifikan dengan menggabungkan tiga metode penyandian ini. Selain itu, upaya pemecahan enkripsi tanpa mengetahui kunci yang tepat akan menghadirkan tantangan yang lebih besar.



Gambar 3. Proses Enkripsi Penyandian Super



Gambar 4. Proses Dekripsi Penyandian Super Enkripsi

3.2 Uji Coba Perhitungan

Untuk menguji penerapan metode penyandian super Caesar Cipher, Affine Cipher, dan RSA, kami mencoba perhitungan menggunakan salah satu studi kasus di bawah ini.

Seseorang ingin mengirimkan pesan penting kepada rekannya tanpa khawatir isi pesan akan jatuh ke tangan orang lain. Ia menyandikan teks dengan metode penyandian seperti Caesar Cipher, Affine Cipher dan RSA untuk menjamin kerahasiaan.

- Pesan yang dikirim adalah “SUNSET”
- Kunci yang diterapkan dalam teknik penyandian Caesar Cipher adalah angka "5".
- Kunci yang digunakan untuk teknik penyandian Affine Cipher adalah “7”.

a) Selanjutnya, tahap pertama penyandian dilakukan dengan teknik Caesar Cipher, yang menghasilkan teks cipher dari hasil penyandian, seperti yang ditunjukkan pada gambar di bawah ini. Teknik ini menggunakan representasi bilangan ASCII.

$Plain\ teks = \boldsymbol{SUNSET}$

$Kunci = 5$

Tabel 1. Proses Enkripsi Caesar Cipher

S	U	N	S	E	T
83	85	78	83	69	84

Berdasarkan tabel di atas, setiap karakter akan digeser sesuai dengan jumlah kunci yang telah ditetapkan, yaitu 5 posisi. Oleh karena itu, rumus berikut digunakan untuk melakukan enkripsi dengan metode Caesar Cipher:

$$Ci = (Pi + K)\ Mod\ 255$$

C1 = (83+5)mod 255
= 88 mod 255
= 88 (X)
C2 = (85+5)mod 255
= 90 mod 255
= 90 (Z)
C3 = (78+5)mod 255
= 83 mod 255
= 83 (S)
C4 = (83+5)mod 255
= 88 mod 255
= 88 (X)
C5 = (69+5)mod 255
= 74 mod 255
= 74 (J)
C6 = (84+5)mod 255
= 88 mod 255
= 89 (Y)

Oleh karena itu, teks yang dibuat dengan menggunakan metode penyandian Caesar Cipher adalah **XZSXJY**

b) Selanjutnya, teks cipher yang dihasilkan dari proses penyandian Caesar Cipher akan dienkripsi dengan menggunakan teknik penyandian Affine Cipher, yang dilakukan dengan

menggunakan rumus berikut:C ≡ (m · P + b) mod n

Tabel 2. Proses Enkripsi Affine Cipher

X	Z	S	X	J	Y
88	90	83	88	74	89

Rumus yang digunakan untuk enkripsi dalam metode penyandian affine cipher adalah sebagai berikut: Dengan parameter n=255, m=7 (di mana m adalah bilangan relatif prima terhadap n), dan b=10 (bilangan bebas). Dalam metode penyandian affine cipher, rumus berikut digunakan untuk enkripsi:

Plainteks : XZSXJY (88, 90, 83, 88, 74, 89)
n = 255
m = 7
b = 10

Enkripsi: C ≡ 7P + 10 (mod 255)
P_1=88→C_1≡7.88+10≡626≡116 (mod255)(‘t’)
P_2=90→C_2≡7.90+10≡640≡130 (mod255)(‘,’)
P_3=83→C_3≡7.83+10≡591≡81 (mod255)(‘Q’)
P_4=88→C_4≡7.88+10≡626≡116 (mod255)(‘t’)
P_5=74→C_5≡7.74+10≡18≡116(mod255)
(‘DC2’)
P_6=89→C_6≡7.89+10≡633≡123(mod255)(‘{‘)

Dengan menggunakan teknik penyandian Affine Cipher, teks yang dihasilkan adalah **t,Q tDC2{**

c) Pada langkah ketiga, metode penyandian RSA digunakan untuk mengenkripsi teks cipher yang dihasilkan dari proses penyandian Affine Cipher.

Tabel 3. Proses Enkripsi RSA

t	,	Q	t	DC2	{
116	130	81	116	18	123

Rumus yang digunakan untuk melakukan enkripsi dalam metode RSA sebagai berikut:
Pemilihan dua angka prima p dan q
p= 23
q = 11
menghitung nilai n :
n = p x q = 23 x 11 = 253
nilai n digunakan dalam kunci publik dan private
menghitung nilai fungsi totien eular Φ(n) :
Φ(n) = (p - 1) x (q - 1) = (17 - 1) x (5 - 1) = 220
e = 13
mencari nilai d :
d.e mod Φn = 1
d.13 mod 220 = 1
17.13 mod 220 = 1
221 mod 220 = 1
1 = 1
maka, d = 17
Enkripsi :
Plainteks = t , Q t DC2 { (dari tabel 3 diatas)
Langkah pertama Plainteks = t , Q t DC2 { akan diubah ke tabel ASCII
t : 116
, : 130
Q : 81
t : 116
DC2: 18
{ : 123

c[0] = m^e mod n = 195 ^13 mod 253 = 139
c[1] = m^e mod n = 130^13 mod 253 = 212
c[2] = m^e mod n = 81^13 mod 253 = 75
c[3] = m^e mod n = 116^13 mod 253 = 139
c[4] = m^e mod n = 18^13 mod 253 = 2
c[5] = m^e mod n = 123^13 mod 253 = 41
Ubah ke dalam bentuk karakter ASCII
c[0] = 139 = ‹
c[1] = 212 = Ô
c[2] = 75 = K
c[3] = 139 = ‹
c[4] = 2 = SOH
c[5] = 41 =)

Dengan demikian, teks yang dihasilkan menggunakan metode penyandian RSA adalah "Ô K SOH".

d) Selanjutnya, teks Cipher yang dihasilkan dari proses penyandian RSA akan didekripsi dengan menggunakan rumus berikut:
$P = c^d \bmod n$

Tabel 4. Proses Dekripsi RSA

‹	Ô	K	‹	SOH	(
139	212	75	139	2	41

Dari tabel di atas, kita dapat melaksanakan proses dekripsi dengan menggunakan teknik RSA, yang dirumuskan sebagai P = c^d mod n. Untuk lebih jelas, teks ini ‹ Ô K ‹ SOH) akan diubah menjadi bentuk tabel ASCII.

‹ = 139
Ô = 212
K = 75
‹ = 139
SOH = 2

) = 41
p[0] = c^d mod n = 139^17 mod 253 = 116
p[1] = c^d mod n = 212^17 mod 253 = 130
p[2] = c^d mod n = 75^17 mod 253 = 81
p[3] = c^d mod n= 139^17 mod 253 = 116
p[4] = c^d mod n = 2^17 mod 253 = 18
p[5] = c^d mod n = 41^17 mod 253 = 123
Ubah ke dalam bentuk karakter ASCII
p[0] = t = 116
p[1] = , = 130
p[2] = Q = 81
p[3] = t = 116
p[4] = DC2 = 18
p[5] = { = 123

Dengan demikian, hasil dekripsi menggunakan metode penyandian RSA adalah **t,Q t DC2{**

e) Selanjutnya, dekripsi dilakukan dengan teknik penyandian Affine Cipher. Rumus yang digunakan untuk menggunakan Affine Cipher adalah:
$P \equiv m^{-1} (C - b) \pmod n$

Tabel 5. Proses Dekripsi Affine Cipher

t	,	Q	t	DC2	{
116	130	81	116	18	123

Dari tabel di atas, kita dapat melaksanakan proses dekripsi menggunakan teknik Affine Cipher dengan rumus yang telah disebutkan sebelumnya.
$P \equiv m^{-1} (C - b) \pmod n$
Mula – Mula hitung m^{-1} yaitu 7^{-1} (mod 255)
Dengan memecahkan 7 x ≡ 1 (mod 255)
Solusinya : x ≡ 73 (mod 255)
sebab 7 . 73 = 511 ≡ 1 (mod 255)
Jadi, P ≡ 73 (C – 10) (mod 255)

C_1=116→P_1≡73.(116–10)=7738≡88(mod 255)
C_2=130→P_2≡73.(130–10)=8760≡90(mod 255)
C_3=81→P_3≡73.(81–10)=5183≡83(mod 255)
C_4=116→P_4≡73.(116–10)=7738≡88(mod 255)
C_5=18→P_5≡73.(18–10)=584≡74(mod 255)
C_6=123→P_6≡73.(123–10)=8249≡89(mod 255)

Plainteks = X Z S X J Y
Maka hasil dekripsi yang dihasilkan dengan menggunakan metode penyandian Affine Cipher adalah X Z S X J Y

f) Langkah terakhir adalah mendekripsi hasil dari proses dekripsi Affine Cipher. Ini dilakukan dengan menggunakan rumus dekripsi dari metode Caesar Cipher.

Tabel 6. Proses Dekripsi Caesar Cipher

X	Z	S	X	J	Y
88	90	83	88	74	89

Tabel di atas menunjukkan bahwa dengan menggunakan metode Caesar Cipher, kita dapat melakukan proses dekripsi pada hasil dekripsi Affine Cipher.
Rumus Dekripsi Caesar Cipher
$P = (C - K)\ Mod\ 255$
C1 = (88 - 5) mod 255
= 83 mod 255
= 83 (S)
C2 = (90 - 5)mod 255
= 85 mod 255
= 85 (U)
C3 = (83 - 5)mod 255
= 78 mod 255
= 78 (N)
C4 = (88 - 5)mod 255
= 83 mod 255
= 83 (S)
C5 = (74 - 5)mod 255
= 69 mod 255
= 69 (E)
C6 = (89 - 5)mod 255
= 83 mod 255
= 84 (T)

Dengan demikian, hasil akhir adalah kata "SUNSET", yang sesuai dengan pesan awal yang telah disandikan dengan metode penyandian super.

4. KESIMPULAN

Teknik super enkripsi yang menggabungkan algoritma kriptografi seperti Caesar Cipher, Affine Cipher, dan RSA telah terbukti memberikan perlindungan yang lebih baik terhadap data teks yang ingin diamankan. Lapisan perlindungan yang lebih kompleks dibentuk oleh kombinasi algoritma ini, sehingga menyulitkan penyerang untuk memasuki sistem. Proses dekripsi dilakukan dalam urutan yang terbalik, tetapi enkripsi

dilakukan secara berlapis dengan Caesar Cipher, Affine Cipher, dan RSA.

Pemilihan algoritma yang tepat dan implementasi yang teliti sangat penting untuk keberhasilan penerapan super enkripsi. Uji coba dengan teks "SUNSET" menunjukkan bahwa pesan dapat dienkripsi menjadi "XZSXJY" dan berhasil dikembalikan ke bentuk aslinya setelah proses dekripsi. Ini menunjukkan bahwa teknik super enkripsi efektif dalam melindungi data teks yang membutuhkan tingkat keamanan tambahan.

Namun, perlu diingat bahwa tidak ada sistem keamanan yang benar-benar kebal terhadap serangan. Meskipun super enkripsi memberikan perlindungan yang lebih tinggi, sistem ini masih dapat menghadapi ancaman yang terus berkembang. Oleh karena itu, melakukan evaluasi keamanan dan pembaruan sistem secara teratur sangat penting untuk memastikan bahwa keamanan data tetap terjaga.

DAFTAR PUSTAKA

[1] B. Silaban and T. Limbong, "Aplikasi Pembelajaran Pengenalan Kriptografi Algoritma Affine Cipher Dan Vigenere Cipher Menggunakan Metode Computer Assisted Instruction," MEANS (Media Informasi Analisa dan Sistem), pp. 93–99, Dec. 2017, doi: 10.54367/MEANS.V2I2.144.

[2] M. Azhari, J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," Jurnal Pendidikan Sains dan Komputer, vol. 2, no. 1, pp. 2809–476, 2022, doi: 10.47709/jpsk.v2i1.1390.

[3] A. Hasanah et al., "Implementasi Algoritma Caesar Cipher untuk Pengamanan Pesan Menggunakan Java NetBeans," Digital Transformation Technology, vol. 3, no. 1, pp. 11–19, May 2023, doi: 10.47709/DIGITECH.V3I1.2305.

[4] Nurjamiyah, "QUERY: Jurnal Sistem Informasi Implementasi Algoritma Affine Cipher untuk Keamanan Data Teks," 2020.

[5] I. N. Diana, "Algoritma Affine Cipher dan Modifikasi Affine Cipher, serta Kombinasinya dengan Cipher Transposisi Grup Simetri untuk Mengamankan Pesan Teks."

[6] N. Aulia Putri et al., "RESISTOR Journal | 61 Pengamanan Data Nilai Mahasiswa Menggunakan Algoritma Caesar Chiper dan RSA Berbasis Web", [Online]. Available: https://s.id/jurnalresistor