

Paper

Implementasi Kriptografi Kombinasi Algoritma Reverse Cipher dan Algoritma Vigenere Cipher untuk Keamanan Pesan Teks Pada Aplikasi Catatan Berbasis Desktop

Author: Anggi Rizki, Sayuti Rahman, Arnes Sembiring

Implementasi Kriptografi Kombinasi Algoritma Reverse Cipher dan Algoritma Vigenere Cipher untuk Keamanan Pesan Teks Pada Aplikasi Catatan Berbasis Desktop

Anggi Rizki¹, Sayuti Rahman², Arnes Sembiring³

^{1,2,3} Universitas Harapan, Medan, Indonesia

¹anggirizki99@gmail.com, ²masay.rahman@gmail.com, ³arnessembiring@gmail.com

Abstrak- Keamanan dan kerahasiaan merupakan hal yang penting pada sistem informasi. Data yang bersifat rahasia tersebut diberi sistem keamanan agar tidak mudah terbaca atau diubah oleh orang-orang yang tidak bertanggung jawab. Keamanan data diperlukan baik saat data tersebut tersimpan sebagai file didalam komputer ataupun saat data tersebut dikirim melalui e-mail. Dalam hal ini kriptografi merupakan salah satu metode mengamankan data yang dapat digunakan untuk menjaga kerahasiaan data, keaslian data serta keaslian pengirim. Metode ini bertujuan agar informasi yang bersifat rahasia yang dikirim melalui telekomunikasi umum seperti LAN atau internet. Kriptografi biasanya dalam bentuk enkripsi dan dekripsi. Algoritma yang dipakai dalam aplikasi adalah algoritma reverse cipher dan vigenere cipher. Berdasarkan pembahasan dalam perancangan aplikasi catatan menggunakan kriptografi kombinasi reverse cipher dan vigenere Cipher dapat disimpulkan bahwa dengan mengkombinasi algoritma reverse cipher dan vigenere cipher sistem enkripsi dan dekripsidapat menjaga kerahasiaan data pribadi.

Kata Kunci: Keamanan data, Kriptografi, *Reverse cipher*, *Vigenere cipher*

Abstract- Security and confidentiality are important in information systems. The confidential data is given a security system so that it is not easily read or changed by irresponsible people. Data security is required both when the data is stored as a file on the computer or when the data is sent via e-mail. In this case cryptography is one method of securing data that can be used to maintain data confidentiality, data authenticity and the authenticity of the sender. This method aims for confidential information to be sent via public telecommunications such as LAN or the internet. Cryptography is usually in the form of encryption and decryption. The algorithms used in the application are reverse cipher and vigenere cipher algorithms. Based on the discussion in designing a note application using a combination of reverse cipher and vigenere cipher cryptography, it can be concluded that by combining the reverse cipher and vigenere cipher algorithms, the encryption and decryption system can maintain the confidentiality of personal data.

Keywords: *Data security*, *Cryptography*, *Reverse cipher*, *Vigenere cipher*

1. PENDAHULUAN

Keamanan dan kerahasiaan merupakan hal yang penting pada sistem informasi [1]. Data yang bersifat rahasia tersebut diberi sistem keamanan agar tidak mudah terbaca atau diubah oleh orang-orang yang tidak bertanggung jawab. Keamanan data diperlukan baik saat data tersebut tersimpan sebagai *file* didalam komputer ataupun saat data tersebut dikirim melalui e-mail. Keamanan pesan teks adalah satu cara untuk melindungi pesan teks dari ancaman, baik dalam bentuk kesengajaan maupun tidak disengaja. Mengatasi ancaman keamanan teks perlu diketahui dalam suatu pengiriman pesan, dan antisipasi penulis adalah membuat aplikasi enkripsi dan deskripsi dalam sebuah pesan text yang dimana pesan text asli diubah dalam bentuk sandi yang disebut dengan kriptografi. Kriptografi bertujuan untuk menyamarkan data atau informasi yang dikomunikasikan [2]. Pada penelitian yang dilakukan [1], Untuk melindungi dan menjaga rahasia data untuk menghindari orang yang tidak berhak mendapatkan informasi ini, yaitu menggunakan metode kriptografi. Kriptografi memiliki beberapa metode ataupun algoritma. Salah satu metode kriptografi yang dapat digunakan adalah metode *Reverse cipher*. Agar mencapai tingkat keamanan yang lebih tinggi, metode dikombinasi dengan metode RSA yang menggunakan kunci public dan memiliki keamanan yang tinggi. Pada penelitian yang dilakukan [3] dijelaskan hasil penelitian menunjukkan bahwa isi *file* dapat terenkripsi menggunakan algoritma *Vigenere cipher* yang bersifat sistem substitusi *multi-alphabet*, yaitu dengan sistem sandi *Caesar* tetapi dengan pergeseran alphabet yang berlainan disesuaikan dengan kata kunci. Maksudnya yaitu sistem sandi substitusi merupakan penyandian dengan cara

menggantikan huruf-huruf/teks aslinya dengan huruf-huruf sandi. Berdasarkan penelitian terkait maka tujuan dari penelitian ini adalah untuk membangun sebuah aplikasi catatan berbasis desktop menggunakan kombinasi kriptografi algoritma *reverse cipher* dan algoritma *vigenere cipher*.

2. METODE PENELITIAN

2.1 Keamanan Data

Keamanan dan kerahasiaan pesan merupakan hal yang sangat penting dalam berkomunikasi melalui internet karena jaringan tersebut rawan kejahatan dengan menyebarkan keburukan seseorang kepada yang tidak berhak untuk mengetahui informasi. Pengguna komputer yang ingin datanya tidak diketahui pihak yang tidak berwenang selalu berusaha menyiasati cara mengamankan informasi yang akan dikomunikasikan atau disimpan. Sehingga perlindungan terhadap kerahasiaan data semakin meningkat, salah satu caranya adalah dengan enkripsi data. Enkripsi adalah proses mengubah pesan asli menjadi karakter yang tidak dapat dibaca. Ada beberapa algoritma enkripsi yang umum digunakan seperti Block Cipher, Stream Cipher, Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES), dan sebagainya[4].

2.2 Kriptografi

Kriptografi dapat didefinisikan sebagai seni maupun ilmu yang menghasilkan pesan yang rahasia. Sebuah pesan asli yang disebut *plaintext* disandikan menjadi pesan tersandi yang disebut sebagai *ciphertext* melalui proses enkripsi dan *ciphertext* dipulihkan menjadi *plaintext* kembali melalui proses dekripsi[5]. Dari paparan awal dapat dirangkum bahwa kriptografi bertujuan untuk memberi layanan keamanan. Yang dinamakan aspek-aspek keamanan yaitu[6]:

- a. Kerahasiaan (*confidentiality*)
Adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak.
- b. Integritas data (*data integrity*).
Adalah layanan yang menjamin bahwa pesan masih asli atau belum pernah dimanipulasi selama pengiriman.
- c. Otentikasi (*authentication*).
Adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication*).
- d. *Non-repudiation*
Adalah layanan untuk menjaga entitas yang berkomunikasi melakukan penyangkalan.

Menurut [7] Kriptografi klasik merupakan kriptografi yang disebut sebagai kriptografi kunci tunggal atau kriptografi simetris yang menggunakan kunci sama untuk Enkripsi maupun Dekripsi. Kriptografi klasik merupakan kriptografi yang digunakan pada zaman dahulu sebelum komputer ditemukan atau sudah ditemukan namun secanggih sekarang. Kriptografi ini melakukan pengacakan huruf pada kata terang / *plaintext*. Algoritma kriptografi klasik memiliki ciri diantaranya berbasis karakter dan menggunakan kunci simetri. Dalam kriptografi klasik, teknik enkripsi yang digunakan yaitu kunci simetris dimana kunci dekripsi sama dengan kunci simetris seperti yang dapat dilihat pada gambar 1. [8]



Gambar 1. Proses Enkripsi Dekripsi

sumber :[8]

2.3 Reverse Cipher

Kriptografi *Reverse cipher* merupakan kriptografi klasik yang menggunakan transposisi yaitu mengganti satu huruf dengan huruf yang lain. Algoritma ini adalah contoh yang paling sederhana dari kriptografi transposisi yaitu mengubah suatu kalimat dengan menuliskan setiap kata secara terbalik[9].

Contoh kriptografi *Reverse cipher* sebagai berikut:

Plainteks : SAYA BERMAIN BOLA

Cipherteks : AYAS NIAMREB ALOB

2.4 Vigenere Cipher

Vigenère cipher adalah salah satu algoritma kriptografi klasik yang diperkenalkan pada abad 16 atau kira-kira pada tahun 1586. Algoritma kriptografi ini dipublikasikan oleh seorang diplomat dan juga kriptologis yang berasal dari Prancis, yaitu Blaise de Vigenère, namun sebenarnya algoritma ini telah digambarkan sebelumnya pada buku *La Cifra del Sig.* Giovan Batista Belaso, sebuah buku yang ditulis oleh Giovan Batista Belaso, pada tahun 1553 [10]. Pada buku *Everyday Cryptography* (Martin, 2015), mengatakan bahwa *vigenere cipher* adalah sebuah metode dari *Enkripsi* teks alfabetik menggunakan serangkaian penyandian berbasis *caesar* pada huruf-huruf dari sebuah kata kunci, dan merupakan bentuk sederhana dari substitusi *polyalphabetic*. Berikut ini rumus Enkripsi dan Dekripsi *Vigenere Cipher*:

Enkripsi : $C_i = P_i + k_i \text{ mod } 26$

Dekripsi : $P_i = C_i - k_i \text{ mod } 26$

C_i : *Ciphertext*

P_i : *Plaintext*

k_i : *Key* atau kunci

Berbeda dengan *caesar cipher*, *inputkey vigenere cipher* berupa sebuah kata yang merupakan rangkaian huruf.

2.5 Java

Java adalah bahasa pemrograman yang populer, yang pertama kali dikembangkan lewat sebuah proyek bernama "*The Green Project*" yang dibentuk oleh *Sun Microsystems*[11]. Bahasa pemrograman ini bersifat *multiplatform* yakni bahasa ini dapat digunakan di berbagai *platform*, seperti *desktop*, *android* dan bahkan untuk sistem operasi Linux. Dilansir dari *w3school*, java dapat digunakan untuk beberapa hal, diantaranya adalah aplikasi *mobile*, aplikasi *desktop*, aplikasi *web*, *serverweb* dan aplikasi server, *game*, dan koneksi *database*.

3. HASIL DAN PEMBAHASAN

Sebelum melakukan proses perancangan sistem, maka perlu dilakukan analisis sistem terlebih dahulu. Analisis sistem merupakan suatu tahapan untuk mengidentifikasi masalah dan segala kebutuhan yang akan diterapkan dalam sistem. Hal ini dilakukan agar dapat membantu dalam proses perancangan sistem sehingga tidak terjadi kesalahan dan sistem yang dibangun optimal sesuai dengan masalah yang akan diselesaikan. Analisis proses digunakan untuk menjelaskan proses kerja dari metode/algoritma untuk menyelesaikan permasalahan yang ada. Proses-proses yang dilakukan untuk menghasilkan aplikasi catatan yang tersandi yaitu berdasarkan bagaimana pembuatan aplikasi catatan tersebut. Perhitungan secara matematis dilakukan sebagai penggambaran proses yang akan terjadi pada metode ini yang didalamnya terdapat algoritma reverse cipher dan vigenere cipher.

3.1 Proses Enkripsi

Tahap ini dilakukan dengan menggunakan algoritma *reverse cipher* terlebih dahulu dan setelahnya menggunakan algoritma *vigenere cipher* yang akan dilakukan untuk meng-*enkripsi* pesan asli (*plaintext*) pengirim.

Tabel 1. Vigenere Cipher dalam bentuk angka

Sumber : [2]

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
!	"	#	\$	%	&	'	()	*	+	,	-	.	/	0	1	2	3	4
20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
5	6	7	8	9	:	;	<	=	>	?	@	A	B	C	D	E	F	G	H
40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	[\
60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
]	^	_	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
80	81	82	83	84	85	86	87	88	89	90	91	92	93						
q	r	s	t	u	v	w	x	y	z	{		}	~						

Diketahui sebuah *plaintext* yaitu "PERHITUNGAN" dengan kunci "ANGKA". Maka untuk mendapatkan *ciphertext*nya terlebih dahulu penulis akan mengubah *plaintext* tersebut ke dalam algoritma *reverse cipher*.

Plaintext : PERHITUNGAN

Ciphertext : NAGNUTIHREP

Setelah diubah dalam bentuk *reverse cipher*, kita akan melakukan *enkripsi* ke dalam bentuk *vigenere cipher*.

Plaintext : NAGNUTIHREP

Kunci : ANGKA

Penulis memilih kata "ANGKA" sebagai kunci yang akan digunakan untuk melakukan proses *enkripsi* menggunakan algoritma *vigenere cipher*, sehingga proses kata "ANGKA" akan mengikuti banyak karakter *ciphertext* yang didapat.

Plaintext : NAGNUTIHREP

Kunci : ANGKA

Karena metode yang diterapkan pada *vigenere cipher* adalah dengan menyusun kunci yang panjangnya akan disesuaikan dengan panjang *plaintext*nya. Maka kunci akan mengalami perulangan sampai banyak karakter yang terdapat pada *plaintext*nya.

Plaintext: NAGNUTIHREP

Kunci : ANGKAANGKA

Selanjutnya kita akan *enkripsi* dengan formula algoritma *vigenere cipher* yaitu:

$$C_i = (P_i + K_i) \bmod 94$$

Dengan penjelasan:

C_i = nilai desimal karakter *ciphertext* ke- i

P_i = nilai desimal karakter *plaintext* ke- i

K_i = nilai desimal karakter kunci ke- i

$$C_1 = N + A = (45 + 32) \bmod 94 = 77 = n$$

$$C_2 = A + N = (32 + 45) \bmod 94 = 77 = n$$

$$C_3 = G + G = (38 + 38) \bmod 94 = 76 = m$$

$$C_4 = N + K = (45 + 42) \bmod 94 = 87 = x$$

$$C_5 = U + A = (52 + 32) \bmod 94 = 84 = u$$

$$C_6 = T + A = (51 + 32) \bmod 94 = 83 = t$$

$$C_7 = I + N = (40 + 45) \bmod 94 = 85 = v$$

$$C_8 = H + G = (39 + 38) \bmod 94 = 77 = n$$

$$C_9 = R + K = (49 + 42) \bmod 94 = 91 = |$$

$$C_{10} = E + A = (36 + 32) \bmod 94 = 68 = e$$

$$C_{11} = P + A = (47 + 32) \bmod 94 = 79 = p$$

Sehingga *ciphertext* yang didapat adalah nmxutv|ep

3.2 Proses Dekripsi

Pada tahap ini penulis akan melakukan Proses *dekripsi* untuk memecahkan *ciphertext* yang akan kembali menjadi *plaintext*. Diketahui sebuah *ciphertext* yaitu “nmxutvn|ep” dengan kunci yang sama yaitu “ANGKA”. Maka untuk mendapatkan *plaintext*nya kembali penulis akan mengubah *ciphertext* tersebut ke dalam algoritma *vigenere cipher* terlebih dahulu.

Plaintext : nmxutvn|ep

Ciphertext : ANGKA

Karena metode yang diterapkan pada *vigenere cipher* adalah dengan menyusun kunci yang panjangnya akan disesuaikan dengan panjang *plaintext*nya. Maka kunci akan mengalami perulangan sampai banyak karakter yang terdapat pada *plaintext*nya.

Plaintext: n n m x u t v n | e p

Kunci : A N G K A A N G K A A

Selanjutnya kita akan despkripsi dengan formula algoritma *vigenere cipher* yaitu:

$P_i = (C_i - K_i) \bmod 94$; untuk $C_i \geq K_i$

Dengan penjelasan:

C_i = nilai desimal karakter *ciphertext* ke- i

P_i = nilai desimal karakter *plaintext* ke- i

K_i = nilai desimal karakter kunci ke- i

$C_1 = n - A \bmod 94 = 77 - 32 \bmod 94 = 45 = N$

$C_2 = n - N \bmod 94 = 77 - 45 \bmod 94 = 42 = A$

$C_3 = m - G \bmod 94 = 76 - 38 \bmod 94 = 38 = G$

$C_4 = x - K \bmod 94 = 87 - 42 \bmod 94 = 45 = N$

$C_5 = u - A \bmod 94 = 83 - 32 \bmod 94 = 51 = U$

$C_6 = t - A \bmod 94 = 85 - 32 \bmod 94 = 53 = T$

$C_7 = v - N \bmod 94 = 85 - 35 \bmod 94 = 40 = I$

$C_8 = n - G \bmod 94 = 77 - 38 \bmod 94 = 39 = H$

$C_9 = | - K \bmod 94 = 91 - 42 \bmod 94 = 49 = R$

$C_{10} = e - A \bmod 94 = 79 - 32 \bmod 94 = 47 = E$

$C_{11} = p - A \bmod 94 = 79 - 32 \bmod 94 = 47 = P$

Sehingga *plaintext* yang didapat adalah NAGNUTIHREP.

Setelah diubah dalam bentuk *vigenere cipher* kita akan melakukan *dekripsi* ke dalam bentuk *reverse cipher*.

Plaintext : NAGNUTIHREP

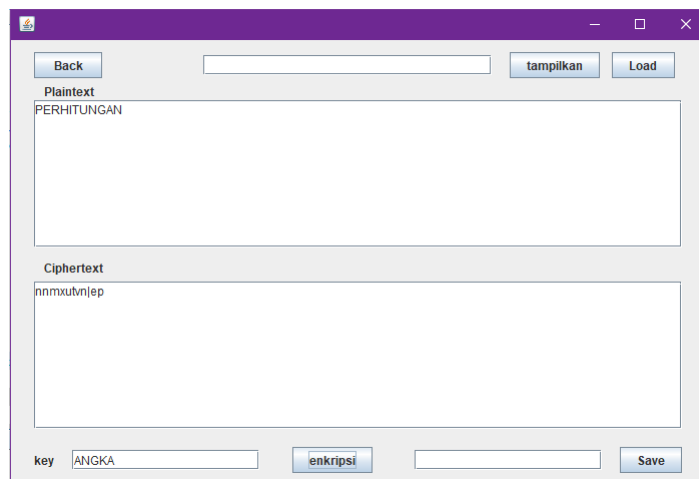
Ciphertext : PERHITUNGAN

3.3 Implementasi Sistem

Tahap implementasi sistem merupakan tahap dimana aplikasi yang dirancandijalankan. Tahap ini menunjukkan apakah setiap proses dapat berjalan dengan baik danmampu memberikan hasil yang diharapkan. Pada proses perancangan aplikasi menggunakan *Netbeans* ditampilan dalam bentuk form-form yang menjadi sarana bagi pengguna untukmelakukan implementasi.

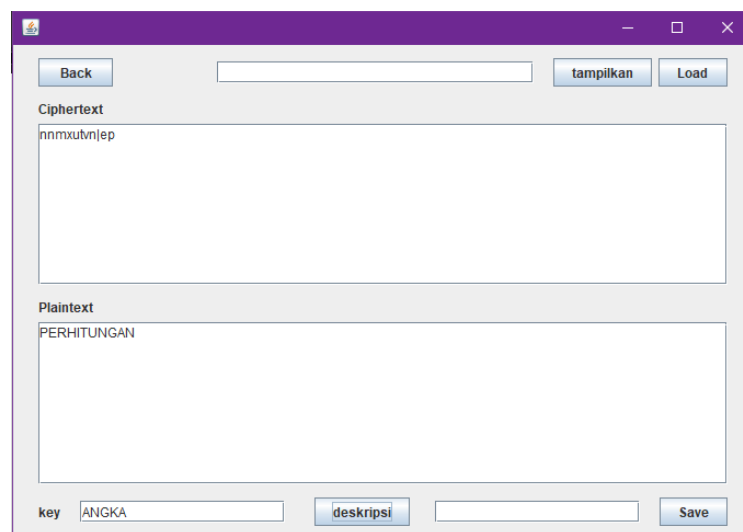
a. Tampilan Hasil

Tampilan hasil menjelaskan bagaimana tampilan dari aplikasi yang dirancang. Mulai dengan tampilan halaman awal, tampilan halaman nama, tampilan halaman judul, tampilan halaman materi dan tampilan halaman utama.



Gambar 2. Tampilan Hasil Enkripsi

Pada tampilan gambar 2. digambarkan bahwa pengguna mengisi pesan rahasia terlebih dahulu di *textboxplaintext*, kemudian masukkan kunci seperti yang terlihat pada *textbox key*, setelah mengisi kunci pengguna dapat menekan tombol enkripsi, maka hasil pesan rahasiayang disandikan akan tampil pada*textboxciphertext*.



Gambar 3. Tampilan Hasil Dekripsi

Pada tampilan gambar 3 digambarkan bahwa hasil *ciphertext* yang dihasilkan pada gambar 2 bisa dikembalikan lagi dalam bentuk pesan rahasia asli. Sebelumnya masukkan pesan rahasia sandi yang digambar 2 ke *textbox ciphertext*, setelah itu masukkan kunci yang sama seperti enkripsi sebelumnya pada *textbox key*, setelah mengisi kunci pengguna dapat menekan tombol dekripsi, maka hasil pesan rahasia yang asli akan tampil pada *textbox plaintext*.

b. Tabel pengujian

Tabel 2. Tabel Pengujian

Nama File	Text	Proses	Hasil	Keterangan
Plaintext 1	Kriptografi dapat didefinisikan sebagai seni maupun ilmu yang menghasilkan pesan yang rahasia	Enkripsi	V]QWR\k`N]8 aX`FO [X[N^VeYKPQ`T VXWFMRj VeUX [I`ZLZ bd\N TeQ^ [X[QT`XXLYRd [XcJ[TeQ^ N`cFSNi	Berhasil
Ciphertext 1	V]QWR\k`N]8 aX`FO	Dekripsi	Kriptografi dapat didefinisikan sebagai seni maupun ilmu yang menghasilkan pesan yang rahasia	Berhasil
Plaintext 2	Proses menyandikan plaintext menjadi ciphertext disebut Enkripsi	Enkripsi	`\cT]= [X[NO[XiSPZ aoUYYVX\U V[QOYRd aoUY]R_`NN alRJ^V[Vj`N]Xe5	Berhasil
Ciphertext 2	`\cT]= [X[NO[XiSPZ aoUYYVX\U V[QOYRd aoUY]R_`NN alRJ^V[Vj`N]Xe5	Dekripsi	Proses menyandikan plaintext menjadi ciphertext disebut Enkripsi	Berhasil
Plaintext 3	Pesan adalah data atau informasi yang dapat dibaca dan dimengerti maknanya	Enkripsi	[XcJ; UX\FON NkQI bXdF VjQR])^N TeQ^ aX`FO NZQGTQ [XT VkbJR[)]NO Np^FYXX]	Berhasil
Ciphertext 3	[XcJ; UX\FON NkQI bXdF VjQR])^N TeQ^ aX`FO NZQGTQ [XT VkbJR[)]NO Np^FYXX]	Dekripsi	Pesan adalah data atau informasi yang dapat dibaca dan dimengerti maknanya	Berhasil

4. KESIMPULAN

Berdasarkan pembahasan dalam perancangan aplikasi catatan menggunakan kriptografi kombinasi *ReverseCipher* dan *VigenereCipher*, penulis dapat menyimpulkan sebagai berikut.

1. Dengan adanya aplikasi ini pengguna komputer akan lebih merasa aman jika pesan yang disimpan terlebih dahulu disandikan.
2. Dengan mengkombinasi algoritma reverse cipher dan vigenere cipher sistem enkripsi dan dekripsi tidak akan mudah untuk dipecahkan oleh pihak yang tidak berkepentingan.

DAFTAR PUSTAKA

- [1] Yusfrizal, "RANCANG BANGUN APLIKASI KRIPTOGRAFI PADA TEKS MENGGUNAKAN METODE REVERSE CHIPER DAN RSA BERBASIS ANDROID," *J. Tek. Inform. Kaputama*, vol. 3, no. 2, 2019.
- [2] M. Iqbal Afandi, "Implementasi Algoritma Vigenere Cipher Dan Atbash Cipher Untuk Keamanan Teks Pada Aplikasi Catatan Berbasis Android," 2020.
- [3] Fitria, "Pembuatan Aplikasi Kriptografi File Menggunakan Algoritma Vigenere Cipher," *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2013.
- [4] S. Rahman, I. Triana, S. Khairani, A. Yasir, and S. Sundari, "Rsa key development using fingerprint image on text message," *J. Phys. Conf. Ser.*, vol. 930, no. 1, 2017, doi: 10.1088/1742-6596/930/1/012037.
- [5] A. R. Santoso, A. Riski, and A. Kamsyakawuni, "Implementasi Algoritma Reversed Vigenere Encryption pada Pengamanan Citra," *Berk. Sainstek*, vol. 6, no. 2, p. 61, 2018, doi: 10.19184/bst.v6i2.9224.
- [6] N. Azis, "Perancangan aplikasi enkripsi dekripsi menggunakan metode caesar chiper dan operasi xor," *Ikraith-Informatika*, vol. 2, no. 1, pp. 1–9, 2018.
- [7] Rosdiana, "SEKURITAS SISTEM DENGAN KRIPTOGRAFI Oleh : Rosdiana, ST., M.Kom," pp. 21–32, 2014.
- [8] M. M. Amin, "Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks," *Pseudocode*, vol. 3, no. 2, pp. 129–136, 2017, doi: 10.33369/pseudocode.3.2.129-136.
- [9] A. Usman, "DAN TEKNIK TRANSPOSISI DALAM PENGAMANAN PESAN TEKS," pp. 209–216, 2020.
- [10] M. D. Irawan, "IMPLEMENTASI KRIPTOGRAFI VIGENERE CIPHER DENGAN PHP," vol. 1, pp. 11–21, 2017.
- [11] N. S. Sibarani, "Analisis Performa Aplikasi Native Android Menggunakan Bahasa Pemrograman Java dan Kotlin," *Researchget*, no. December, 2018, [Online]. Available: https://www.researchgate.net/publication/329525878_Analisis_Performa_Aplikasi_Android_Pada_Bahasa_Pemrograman_Java_dan_Kotlin.