SNASTIKOM 2020
Program Studi Teknik Informatika, Fakultas Teknik dan Komputer, Universitas Harapan Medan
website: www.snastikom.com

IMPLEMENTASI KOMBINASI KRIPTOGRAFI TEKNIK SUBSTITUSI DAN TEKNIK TRANSPOSISI DALAM PENGAMANAN PESAN TEKS

Sabrina Alwi Hamdah
Universitas Harapan Medan, Jl. HM Jhoni No. 70 Medan, sabrinahamdah88@gmail.com

Herlina Harahap
Universitas Harapan Medan, Jl. HM Jhoni No. 70 Medan, herlinaharahap66@gmail.com

Ari Usman
Universitas Harapan Medan, Jl. HM Jhoni No. 70 Medan, ariusman09@gmail.com

Abstract

Cryptography is one of the right solutions to overcome wiretapping, piracy or theft of data or information from people who do not have access rights to such data. So that the data is still guaranteed its integrity, confidentiality, and accuracy. Therefore, the aim of this research is to build a text message security application using a combination of classical cryptography substitution techniques and algorithms reverse cipher. In terms of data security techniques, many cryptographic methods can be used. These cryptographic methods have their own techniques and methods. One of the cryptographic methods that can be used is the substitution technique method. But if you only use the substitution technique method, the security of text data is very weak. So to achieve a higher level of security this method is combined with the transposition technique method. In this study, the cryptography used is a combination of classical cryptography substitution techniques and classical cryptography transposition techniques, namely the Caesar cipher algorithm and the algorithm reverse cipher. In testing the algorithm caecar cipher, the process of encryption and decryption of messages is only carried out on uppercase (A-Z) and lowercase (a-z) characters. Based on the security analysis, it is found that the encryption or decryption process uses a substitution 468,235,319, 2,147,483,622, and 2,147,483,623 The encryption process and the decryption process of the algorithm caecar cipher can be done if the result of the calculation of the key input is not more than the capacity of the data type used, namely the data type integer.

Keywords:
Cryptography; Caesar Cipher; Reverse Cipher

Abstrak

Kriptografi merupakan salah satu solusi yang tepat untuk mengatasi penyadapan, pembajakan ataupun pencurian data atau informasi dari orang-orang yang tidak memiliki hak akses terhadap data tersebut. Sehingga data tersebut masih terjamin keutuhannya, kerahasiaannya, dan keakuratannya. Maka dari itu, tujuan penelitian ini adalah untuk membangun sebuah aplikasi pengamanan pesan teks menggunakan kombinasi kriptografi klasik teknik substitusi dan algoritma reverse cipher. Dalam hal teknik pengamanan data, banyak metode kriptografi yang dapat digunakan. Metode - metode kriptografi tersebut mempunyai teknik dan cara tersendiri. Salah satu metode kriptografi yang bisa digunakan adalah metode teknik substitusi. Tetapi jika hanya menggunakan metode teknik substitusi saja keamanan data teks sangatlah lemah. Maka untuk mencapai tingkat keamanan yang lebih tinggi metode ini dikombinasikan dengan metode teknik transposisi. Dalam penelitian ini, kriptografi yang digunakan adalah kombinasi kriptografi klasik teknik substitusi dan kriptografi klasik teknik transposisi yaitu algoritma caesar cipher dan algoritma reverse cipher. Pada pengujian algoritma caecar cipher, proses enkripsi dan dekripsi pesan hanya dilakukan pada karakter huruf kapital (A-Z) dan huruf kecil (a-z). Berdasarkan analisa keamanan diperoleh bahwa pada proses enkripsi atau proses dekripsi menggunakan kunci substitusi 468.235.319, 2.147.483.622, dan 2.147.483.623 proses enkripsi dan proses dekripsi algoritma caecar cipher dapat dilakukan jika hasil perhitungan kunci yang diinputkan tidak lebih dari kapasitas tipe data yang digunakan yaitu tipe data integer.

Kata Kunci:
Kriptografi; Caesar Cipher; Reverse Cipher.

1. PENDAHULUAN

Perkembangan dan pemanfaatan teknologi informasi dalam membantu pekerjaan diberbagai organisasi maupun pekerjaan pribadi. Dalam suatu sistem informasi, keamanan telah menjadi aspek yang sangat penting. Betapa pentingnya informasi tersebut dikirim dan diterima oleh orang yang berkepentingan. Apabila informasi itu disadap atau dibajak oleh orang yang tidak berhak, informasi akan tidak berguna ditengah proses pengirimannya.

Informasi dibagi menjadi dua bagian yaitu informasi yang besifat pribadi dan umum.Informasi yang bersifat pribadi maksudnya informasi yang terkandung hanya untuk satu orang sedangkan informasi yang bersifat umum yaitu informasi yang dapat diketahui oleh orang banyak. Adapun perjalanan informasi tersebut tidak luput dari gangguan-gangguan pihak yang tidak berhak. Salah satu ilmu untuk menjaga keamanan dan kerahasiaan data atau informasi yaitu kriptografi.

Kriptografi merupakan seni atau ilmu untuk menjaga keamanan data. Konsep kriptografi bermula dari zaman tradisional hingga modern. Secara umum ada dua jenis kriptografi, yaitu tradisional/klasik dan modern[1], [2]. Algoritma kriptografi klasik digunakan sejak sebelum era komputerisasi dan kebanyakan menggunakan teknik kunci simetris. Metode menyembunyikan pesannya adalah dengan teknik substitusi atau transposisi atau keduanya. Teknik substitusi adalah menggantikan karakter dalam *plaintext* menjadi karakter lain yang hasilnya adalah *ciphertext*. Sedangkan transposisi adalah teknik mengubah *plaintext* menjadi *ciphertext* dengan cara permutasi karakter. Kombinasi kedua teknik ini secara kompleks adalah yang melatarbelakangi terbentuknya berbagai macam algoritma kriptografi modern. Contoh algoritma kriptografi klasik yaitu: *Caesar Cipher*, *Vigenere Cipher*, dan *Hill Cipher* [3], [4]. Algoritma substitusi tertua yang diketahui adalah *caesar cipher* yang digunakan oleh kaisar Romawi, Julius Caesar untuk menyandikan pesan yang ia kirim kepada para gubernurnya [5]. *Reverse cipher* adalah salah satu contoh yang paling sederhana dari kriptografi transposisi yaitu mengubah suatu kalimat dengan menuliskan setiap kata secara terbalik [6].

Pada penelitian yang dilakukan Priyono (2016) membangun sebuah aplikasi pengamanan pesan teks menggunakan kriptografi klasik teknik substitusi yaitu algoritma *caesar cipher* dan Algoritma *Vigenere Chiper*. Aplikasi yang dibangun menggunakan bahasa pemrograman *Microsof*t *Visual Basic .Net 2008*. Pada penelitian tersebut, peneliti tidak mengkombinasikan kedua algoritma yang dipakai, melainkan dengan memilih salah satu algoritma yang ingin digunakan untuk mengamankan pesan.

Pada penelitian yang dilakukan Yusfrizal (2019) melakukan kombinasi algoritma *reverse cipher* dan algoritma RSA (*Rivest-Shamir-Adleman*) yang diiplementasikan dalam bentuk aplikasi enkripsi dan dekripsi teks berbasis *android* untuk mengamankan pesan. Pada penelitian tersebut, peneliti mengkombinasikan kedua algoritma dengan dua kali proses enkripsi dan dekripsi. Pertama menekan tombol enkripsi algoritma *reverse cipher* kemudian dienkripsi lagi dengan menekan tombol enkripsi algoritma RSA. Dan untuk proses dekripsinya, dengan cara melakukan hal yang sama.

Berdasarkan penelitian terkait di atas maka tujuan dari penelitian ini adalah untuk membangun sebuah aplikasi pengamanan pesan teks menggunakan kombinasi kriptografi klasik teknik substitusi dan algoritma *reverse cipher*.

a. Algoritma Caesar Cipher

Sebelum ada komputer, kriptografi dilakukan menggunakan pensil dan kertas. Algoritma kriptografi *(chiper)* yang digunakan dinamakan algoritma klasik. Algoritma klasik adalah algoritma berbasis karakter. Dimana enkripsi dan dekripsi dilakukan pada setiap karakter pesan. Pada dasarnya, algoritma kriptografi klasik dapat dikelompokkan kedalam dua macam cipher yaitu [5]:

1. Cipher Substitusi (*Substitution Ciphers*)
2. Cipher Transposisi (*Transposition Ciphers*)

Dalam *Cipher* Substitusi setiap unit plainteks diganti dengan satu unit cipherteks. Satu unit berarti satu huruf, pasangan huruf, atau kelompok lebih dari dua huruf. Algoritma substitusi tertua yang diketahui adalah *caesar cipher* yang digunakan oleh kaisar Romawi, Julius Caesar untuk menyandikan pesan yang ia kirim kepada para gubernurnya[5].

Mengemukakan bahwa langkah-langkah yang dilakukan untuk membentuk *chipertext* pada algoritma *caesar cipher* adalah menentukan besarnya pergeseran karakter yang digunakan dalam membentuk *plaintext* ke *ciphertext*, menukarkan karakter pada *ciphertext* menjadi *plaintext* dengan berdasarkan pada pergeseran yang telah ditentukan sebelumnya, dapat dinyatakan dengan fungsi enkripsi dan fungsi dekripsi sebagai berikut[7], [8]:

Fungsi enkripsi:

$C = E(P) = (p+K) \bmod 26$

Fungsi dekripsi:

$P = D(C) = (c-K) \bmod 26$

Dimana:

P : Plaintext

C : Ciphertext
K : Kunci
E : Enkripsi
D : Dekripsi
p : Urutan alphabet *plaintext*
c : Urutan alphabet *ciphertext*

b. Algoritma Reverse Cipher

Algoritma *reverse cipher* merupakan contoh kriptografi klasik yang menggunakan transposisi yaitu mengganti satu huruf dengan huruf lain. Algoritma ini adalah contoh yang paling sederhana dari kriptografi transposisi yaitu mengubah suatu kalimat dengan menuliskan setiap kata secara terbalik [6].

Contoh algoritma *reverse cipher* sebagai berikut:

Plaintext : SAYA SEDANG MAKAN NASI
Ciphertext : AYAS GNADES NAKAM ISAN

2. HASIL DAN PEMBAHASAN

a. Pengujian Dengan Kunci 468.235.319

Pada pengujian pesan teks dengan menggunakan kunci substitusi 468.235.319, dapat dilihat pada Gambar 1, Gambar 2, Gambar 3, dan Gambar 4.

																									ENKRIPSI
Alfabet Kapital	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	JUMLAH
Urutan ASCII	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	468.235.344
Chiphertext	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	KUNCI
Urutan ASCII	84	85	86	87	88	89	90	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	468.235.319
Alfabet Kecil	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	JUMLAH
Urutan ASCII	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	468.235.344
Chiphertext	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	
Urutan ASCII	116	117	118	119	120	121	122	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	

Gambar 1. Proses Perhitungan Enkripsi Kunci 468.235.319

Pada Gambar 1, dapat dilihat proses perhitungan enkripsi kunci 468.235.319 untuk *plaintext* huruf "A" *ciphertext*nya "T", untuk *plaintext* huruf "B" *ciphertext*nya "U", untuk *plaintext* huruf "C" *ciphertext*nya "V" dan seperti itu seterusnya.

Gambar 2. Enkripsi Dengan Kunci 468.235.319

Alfabet Kapital	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
Urutan ASCII	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
Plaintext	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
Urutan ASCII	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	65	66	67	68	69	70	71
Alfabet Kecil	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
Urutan ASCII	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122
Plaintext	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
Urutan ASCII	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	97	98	99	100	101	102	103

DEKRIPSI
JUMLAH
(468.235.294)
KUNCI
468.235.319
JUMLAH
(468.235.294)

Gambar 3. Proses Perhitungan Dekripsi Kunci 468.235.319

Pada Gambar 3, dapat dilihat proses perhitungan dekripsi kunci 468.235.319 untuk *ciphertext* huruf "A" *plaintext*nya "H", untuk *plaintext* huruf "B" *ciphertext*nya "I", untuk *plaintext* huruf "C" *ciphertext*nya "J" dan seperti itu seterusnya.

Gambar 4. Dekripsi Dengan Kunci 468.235.319

Pada Gambar 2 dan Gambar 4, dapat dilihat kunci yang diinput dapat digunakan untuk proses enkripsi dan juga proses dekripsi. Serta hasil proses dekripsi sesuai dengan *plaintext* yang diinputkan.

Tabel 1. Pengujian Enkripsi Dengan Kunci 468.235.319

NO.	*Plaintext*	Kunci	Hasil Yang Diharapkan	Kesim-pulan
1.	Berapakah hasil (40 x 5) + 200 – 50 + (100 : 2) ?	468.235.319	Menampilkan *ciphertext caesar cipher*, dan *reverse cipher*.	Sesuai

Tabel 2. Pengujian Dekripsi Dengan Kunci 468.235.319

NO.	*Ciphertext*	Kunci	Hasil Yang Diharapkan	Kesim-pulan
1.	atdtitkxU eblta 04(q)5 + 002 – 05 + 001(:)2 ?	468.235.319	Menampilkan *plaintext reverse cipher*, dan *caesar cipher*.	Sesuai

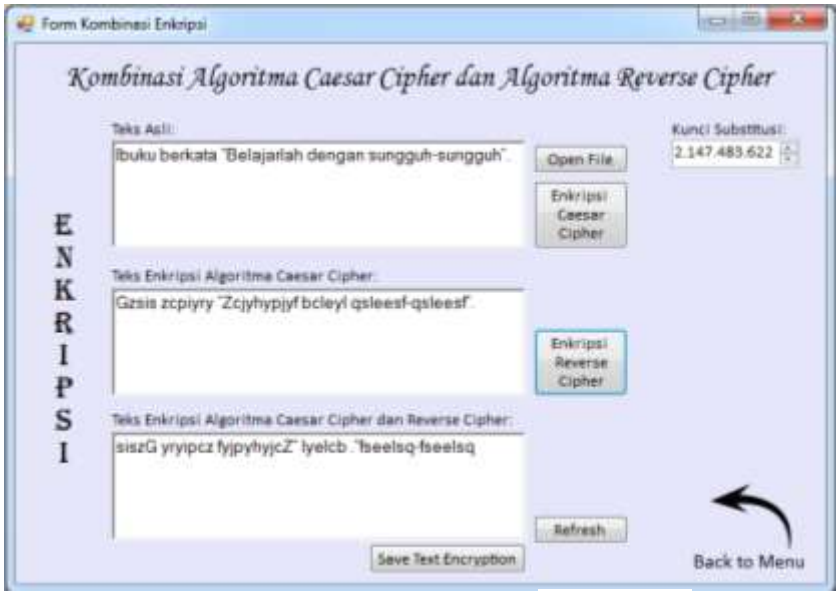
b. Pengujian Dengan Kunci 2.147.483.622

Pada pengujian pesan teks dengan menggunakan kunci substitusi 2.147.483.622, dapat dilihat pada Gambar 5, Gambar 6, Gambar 7 dan Gambar 8.

																									ENKRIPSI
Alfabet Kapital	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	**JUMLAH**
Urutan ASCII	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	2.147.483.647
Chiphertext	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	**KUNCI**
Urutan ASCII	89	90	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	2.147.483.622
Alfabet Kecil	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	**JUMLAH**
Urutan ASCII	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	2.147.483.647
Chiphertext	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	
Urutan ASCII	121	122	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	

Gambar 5. Proses Perhitungan Enkripsi Kunci 2.147.483.622

Pada Gambar 5, dapat dilihat proses perhitungan enkripsi kunci 2.147.483.622 untuk *plaintext* huruf "A" *ciphertext*nya "Y", untuk *plaintext* huruf "B" *ciphertext*nya "Z", untuk *plaintext* huruf "C" *ciphertext*nya "A" dan seperti itu seterusnya.



Gambar 6. Enkripsi Dengan Kunci 2.147.483.622

																									DEKRIPSI
Alfabet Kapital	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	**JUMLAH**
Urutan ASCII	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	(2.147.483.597)
Plaintext	C	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	**KUNCI**
Urutan ASCII	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	65	66	2.147.483.622
Alfabet Kecil	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	**JUMLAH**
Urutan ASCII	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	(2.147.483.597)
Plaintext	c	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	
Urutan ASCII	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	97	98	

Gambar 7. Proses Perhitungan Dekripsi Kunci 2.147.483.622

Pada Gambar 7, dapat dilihat proses perhitungan dekripsi kunci 2.147.483.622 untuk *ciphertext* huruf "A" *plaintext*nya "C", untuk *plaintext* huruf "B" *ciphertext*nya "D", untuk *plaintext* huruf "C" *ciphertext*nya "E" dan seperti itu seterusnya.

Gambar 8. Dekripsi Dengan Kunci 2.147.483.622

Pada Gambar 6 dan Gambar 8, dapat dilihat kunci yang diinput dapat digunakan untuk proses enkripsi dan juga proses dekripsi. Serta hasil proses dekripsi sesuai dengan *plaintext* yang diinputkan.

Tabel 3. Pengujian Enkripsi Dengan Kunci 2.147.483.622

NO.	*Plaintext*	Kunci	Hasil Yang Diharapkan	Kesim-pulan
1.	Ibuku berkata, "Belajarlah dengan sungguh-sungguh".	2.147.483.622	Menampilkan *ciphertext caesar cipher*, dan *reverse cipher*.	Sesuai

Tabel 4. Pengujian Dekripsi Dengan Kunci 2.147.483.622

NO.	*Ciphertext*	Kunci	Hasil Yang Diharapkan	Kesim-pulan
1.	siszG yryipcz fyjpyhyjcZ" lyelcb ."fseelsq-fseelsq	2.147.483.622	Menampilkan *plaintext reverse cipher*, dan *caesar cipher*.	Sesuai

c. Pengujian Dengan Kunci 2.147.483.623

Pada pengujian pesan teks dengan menggunakan kunci substitusi 2.147.483.623, dapat dilihat pada Gambar 9 dan Gambar 10.

Alfabet Kapital	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
Urutan ASCII	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
Chiphertext	Z	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
Urutan ASCII	90	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89
Alfabet Kecil	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
Urutan ASCII	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122
Chiphertext	z	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
Urutan ASCII	122	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121

ENKRIPSI
JUMLAH
2.147.483.648
KUNCI
2.147.483.623
JUMLAH
2.147.483.648

Gambar 9. Proses Perhitungan Enkripsi Kunci 2.147.483.623

Pada Gambar 9, dapat dilihat proses perhitungan enkripsi kunci 2.147.483.623 untuk jumlah perhitungan *plaintext* huruf "Z" adalah 2.147.483.648 yang berarti hasil perhitungan tersebut melebihi kapasitas tipe data integer.

Gambar 10. Enkripsi Dengan Kunci 2.147.483.623

Pada Gambar 10, dapat dilihat kunci yang diinput tidak melebihi batas kapasitas tipe data *integer*, tetapi ketika dilakukan proses perhitungan dan hasil perhitungan tersebut melebihi batas akhir tipe data *integer*. Kemudian sistem akan menampilkan sebuah pesan bahwa hasil perhitungan melebihi batas kapasitas. Maka tidak akan dilakukan proses enkripsi dan dekripsi.

Tabel 5. Pengujian Enkripsi Dengan Kunci 2.147.483.623

NO.	*Plaintext*	Kunci	Hasil Yang Diharapkan	Kesim-pulan
1.	Cari zona aman!	2.147.483.623	Menampilkan *ciphertext caesar cipher*, dan *reverse cipher*.	Tidak Sesuai

3. KESIMPULAN

Berdasarkan implementasi dari pengamanan pesan teks menggunakan kombinasi kriptografi klasik teknik substitusi dan algoritma *reverse cipher*, maka diperoleh kesimpulan sebagai berikut:

1. Bahwa sebuah aplikasi pengamanan pesan teks dapat diterapkan dengan menggunakan ilmu kriptografi dalam penyamaran atau penyandian pesan asli dengan kombinasi dua algoritma kriptografi klasik yang berbeda agar pesan teks tersebut tetap terjaga keaslianya.
2. Dengan penggabungan algoritma *reverse cipher*, dan algoritma *caesar cipher* sistem enkripsi akan semakin sulit untuk dipecahkan oleh pihak yang tidak memiliki hak akses.
3. Proses perhitungan pada enkripsi dan dekripsi algoritma *caesar cipher* tidak dilakukan jika hasil perhitungan melebihi rentang nilai antara -2.147.483.648 s/d 2.147.483.647.
4. Pada proses enkrpsi dan proses dekripsi algoritma *caesar cipher* ketepatan perhitungan sesuai dengan hasil yang didapat.

DAFTAR PUSTAKA

[1] A. Marisman and A. Hidayati, "Pembangunan Aplikasi Pembanding Kriptografi Dengan Caesar Cipher Dan Advance Encryption Standard (Aes) Untuk File Teks," *J. Penelit. Komun. dan Opini Publik*, vol. 19, no. 3, pp. 213–222, 2015.

[2] Y. Dwi Putri, R. Rosihan, and S. Lutfi, "Penerapan Kriptografi Caesar Cipher Pada Fitur Chatting Sistem Informasi Freelance," *JIKO (Jurnal Inform. dan Komputer)*, vol. 2, no. 2, pp. 87–94, 2019.

[3] S. Sumandri, "Studi Model Algoritma Kriptografi Klasik dan Modern," *Semin. Mat. dan Pendidik. Mat. UNY*, pp. 265–272, 2017.

[4] N. Azis, "Perancangan aplikasi enkripsi dekripsi menggunakan metode caesar chiper dan operasi xor," *Ikraith-Informatika*, vol. 2, no. 1, pp. 72–80, 2018.

[5] A. Pradipta, "Implementasi Metode Caesar Chiper Alphabet Majemuk Dalam Kriptografi Untuk Pengamanan Informasi," *Indones. J. Netw. Secur.*, vol. 5, no. 3, pp. 3–6, 2016.

[6] Y. Yusfrizal, "RANCANG BANGUN APLIKASI KRIPTOGRAFI PADA TEKS

MENGGUNAKAN METODE REVERSE CHIPER," *J. Tek. Inform. Kaputama*, vol. 3, no. 2, pp. 29–37, 2019.

[7] 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.

[8] I. Gunawan, "Kombinasi Algoritma Caesar Cipher dan Algoritma RSA untuk pengamanan File Dokumen dan Pesan Teks," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 2, no. 2, pp. 124–129, 2018.