

Meningkatkan Keamanan Source Code Web Melalui Teknik Enkripsi dan Dekripsi Dengan Metode Reverse Cipher dan Caesar Cipher

Improving Web Source Code Security Through Encryption and Decryption Techniques Using Reverse Cipher and Caesar Cipher Methods

Faisal Harris¹, Ria Eka Sari²

¹Mahasiswa Universitas Potensi Utama, JL. KL. Yos Sudarso Km. 6,5 No. 3-A, Tanjung Mulia, Tj. Mulia, Kec. Medan Deli, Kota Medan, Sumatera Utara 20241 Indonesia

²Dosen Universitas Potensi Utama, JL. KL. Yos Sudarso Km. 6,5 No. 3-A, Tanjung Mulia, Tj. Mulia, Kec. Medan Deli, Kota Medan, Sumatera Utara 20241 Indonesia

Email : faisalharris27@gmail.com¹ , ladiespure@gmail.com²

ABSTRAK

Penelitian ini berfokus pada upaya untuk meningkatkan tingkat kerahasiaan Source Code Web, yang merupakan komponen penting dalam pengembangan aplikasi web. Source Code merupakan kumpulan pernyataan bahasa komputer yang memungkinkan komunikasi antara manusia dan komputer melalui perintah-perintah tertentu. Ancaman pencurian Source Code telah menjadi isu serius dalam dunia pengembangan aplikasi web. Pencurian Source Code dapat mengakibatkan dampak negatif yang signifikan, termasuk hilangnya kontrol, kerahasiaan, dan potensi kerugian finansial. Penelitian ini didasarkan pada pemahaman bahwa melindungi Source Code Web adalah kunci untuk memastikan keamanan, privasi, dan integritas aplikasi web. Untuk mencapai tujuan ini, peneliti menggabungkan dua metode enkripsi, yaitu Reverse Cipher dan Caesar Cipher. Metode Reverse Cipher digunakan sebagai dasar, yang melibatkan pembalikan urutan karakter dalam teks. Namun, peneliti menyadari bahwa metode ini mungkin kurang efektif jika teks rahasia pendek. Oleh karena itu, penelitian ini memperkuat kerahasiaan dengan menerapkan metode Caesar Cipher. Metode ini melibatkan pergeseran karakter dalam teks asli dengan sejumlah posisi tertentu dalam abjad. Hasil dari penggabungan kedua metode ini adalah tingkat kerahasiaan yang lebih baik untuk Source Code Web. Dengan meningkatnya kebutuhan akan perlindungan Source Code, penelitian ini memiliki relevansi yang signifikan dalam memastikan keamanan dan keberlanjutan aplikasi web. Peningkatan kerahasiaan Source Code Web dapat membantu mencegah akses tidak sah, modifikasi, atau penyalahgunaan data yang sensitif, serta melindungi kepentingan pemilik Source Code Web.

Kata Kunci : Enkripsi, Deskripsi, Reverse Cipher, Caesar Cipher, Source Code Web

ABSTRACT

This research focuses on efforts to increase the level of confidentiality of Web Source Code, which is an important component in web application development. Source Code is a collection of computer language statements that enable communication between humans and computers through certain commands. The threat of Source Code theft has become a serious issue in the world of web application development. Source Code theft can result in significant negative impacts, including loss of control, confidentiality, and potential financial loss. This research is based on the understanding that protecting Web Source Code is key to ensuring the security, privacy, and integrity of web applications. To achieve this goal, researchers combined two encryption methods, namely Reverse Cipher and Caesar Cipher. The Reverse Cipher method is used as a basis, which involves reversing the order of characters in the text. However, researchers realized that this method may be less effective if the secret text is short. Therefore, this research strengthens confidentiality by applying the Caesar Cipher method. This method involves shifting characters in the original text by a certain number of positions in the alphabet. The result of combining these two methods is a better level of confidentiality for Web Source Code. With the increasing need for Source Code protection, this research has significant relevance in ensuring the security and sustainability of web applications. Increasing the confidentiality of Web Source Code can help prevent unauthorized access, modification, or misuse of sensitive data, as well as protect the interests of Web Source Code owners.

Keywords : Encryption, Description, Reverse Cipher, Caesar Cipher, Web Source Code

1. PENDAHULUAN

Komputer dan teknologinya merupakan salah satu alat bantu yang paling tepat guna [1]. Perangkat lunak komputer yang memanfaatkan kemampuan komputer langsung untuk melakukan suatu tugas yang diinginkan pengguna [2]. Tuntutan kebutuhan akan informasi dan penggunaan komputer yang semakin banyak mendorong terbentuknya sebuah jaringan komputer yang mampu melayani berbagai kebutuhan tertentu [3], dengan berkembangnya menjadikan manusia bias berfikir kreatif, akan tetapi dapat meningkatkan kinerja teknologi sebelumnya [4]. Maka dari itu dibutuhkan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Keamanan data merupakan hal yang sangat penting dalam menjagakerahasiaan informasi terutama yang berisi informasi sensitif yang hanya boleh diketahui isinya oleh pihak yang berhak saja, akan sangat mudah disadap dan diketahui isi informasinya oleh pihak-pihak yang tidak bertanggung jawab [5].

Source Code adalah sebuah kumpulan pernyataan bahasa komputer yang dapat ditulis dan dibaca manusia. Dengan adanya Source Code, memungkinkan manusia berkomunikasi dengan komputer menggunakan perintah-perintah tertentu [6]. Biasanya aplikasi web yang akan dibuat terlebih dahulu diuji melalui localhost sebelum dihosting dengan menyimpan Source Code Web di perangkat komputer [7]. Masalah yang terjadi adalah jika data Source Code Web dicuri, maka pencuri dapat membuka isi datanya dan dapat menjual source code sehingga mendapatkan keuntungan tersendiri dan disisi lain jika terdapat data yang penting maka dapat merugikan pemilik Source Code Web. Oleh karena itu perlunya diterapkan keamanan dalam sebuah Source Code Web sehingga para pencuri informasi tidak dapat mencuri data yang terdapat di dalam Source Code Web dengan cara mengubah isi dari teks yang tersimpan di dalam Source Code Web menjadi rahasia.

Kriptografi dikenal dan dipakai cukup lama sejak kurang lebih tahun 1900 sebelum masehi. Kriptografi sendiri berasal dari kata “Crypto” yang berarti rahasia dan “graphy” yang berarti tulisan [8]. Salah satu metode kriptografi yang bisa digunakan adalah metode Reverse Cipher, dikenal sebagai metode Caesar Cipher dengan pergeseran 1, adalah sebuah teknik enkripsi sederhana yang melibatkan pembalikan urutan karakter dalam teks asli [9]. Caesar Cipher adalah salah satu bentuk enkripsi yang sangat sederhana dan mudah dimengerti [10]. Namun, tingkat keamanannya rendah karena terdapat hanya sedikit variasi pergeseran yang mungkin digunakan, sehingga mudah untuk didekripsi melalui metode percobaan dan kesalahan [11].

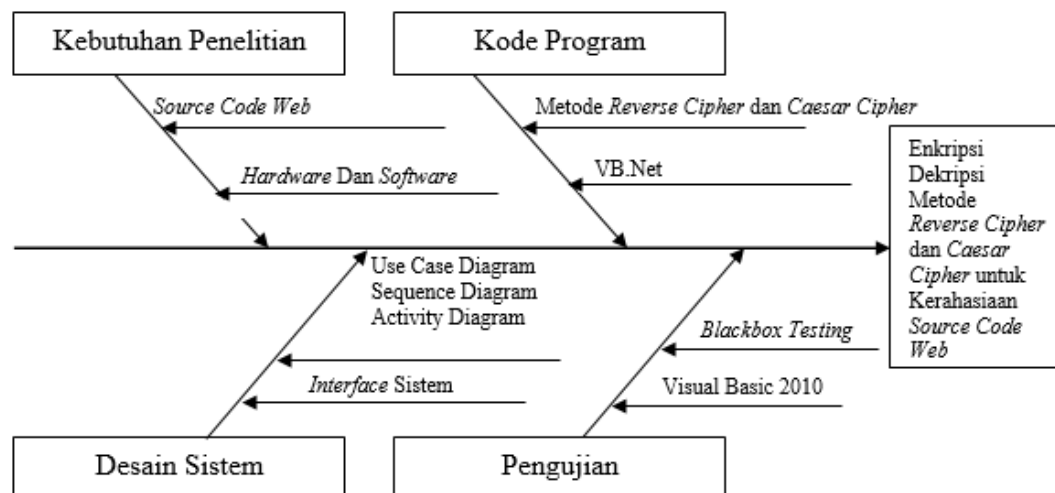
Beberapa penelitian terdahulu, Penelitian yang mengangkat judul “Rancang Bangun Sistem Keamanan RFID Tag menggunakan Metode Caesar Cipher pada Sistem Pembayaran Elektronik”. Dari hasil pengujian diperoleh bahwa tag dapat digunakan untuk menyimpan data berupa nilai nominal uang dan dari sistem yang telah direalisasikan nilai nominal uang tersebut dapat ditambah atau dikurang jumlahnya dari Rp 0 – Rp 4.294.967.295 [12]. Penelitian yang mengangkat judul “Peningkatan Keamanan Kriptografi Caesar Cipher dengan Menerapkan Algoritma Kompresi “Stout Codes””. Dalam penelitian ini algoritma yang digunakan algoritma kriptografi klasik yaitu Caesar Cipher yang dikombinasikan dengan algoritma kompresi Stout Codes. Hasil chiperteks Caesar Cipher kemudian dilakukan kompresi dengan menerapkan algoritma Stout Codes [13]. Penelitian yang mengangkat judul “Rancang Bangun Aplikasi Penyembunyian Pesan QRCode Dengan Menggunakan Metode Caesar Cipher Berbasis Android”. Cara kerja kata sandi Caesar Cipher yang di ilustrasikan dengan menghubungkan dua set alfabet. Dimana kata sandi disusun dengan cara menggeser huruf dari kanan atau ke kiri dengan angka tertentu (sesuai kunci). Untuk meningkatkan keamanan kerahasiaan pesan, digunakan QRCode [14]. Penelitian yang mengangkat judul “Kombinasi Metode Stream Cipher Dan

Caesar Cipher Dalam Pengamanan Data Kredit Customer (Studi Kasus : PT. ACE HARDWARE)”. Stream cipher merupakan cipher yang menggeser urutan alphabet sehingga urutan alphabetnya berubah dan dikombinasikan dengan metode caesar cipher atau sandi geser, sandi ini termasuk sandi substitusi dimana setiap huruf pada teks terang (plaintext) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alphabet. Pada Caesar cipher, tiap huruf disubstitusi dengan huruf ketiga berikutnya dari susunan alphabet yang sama [15].

2. METODE

Tahapan penelitian ini dapat direpresentasikan dalam sebuah diagram Fishbone, yang membantu menguraikan proses penelitian menjadi sejumlah tahapan yang kunci. Tahap awal adalah perencanaan, di mana peneliti menentukan topik, ruang lingkup, dan tujuan penelitian. Selanjutnya, literatur penelitian melibatkan pengumpulan dan analisis literatur yang relevan. Tahapan perancangan mencakup pemilihan metode penelitian dan perancangan eksperimen, sementara pengumpulan data adalah implementasi metode yang telah dirancang. Data yang terkumpul kemudian dianalisis dalam tahap analisis data, dengan hasilnya diinterpretasikan dan disajikan sebagai temuan penelitian.

Setelah itu, tahap kesimpulan melibatkan evaluasi hasil penelitian, implikasi temuan, dan menyimpulkan hasil akhir penelitian. Tahapan publikasi melibatkan penulisan laporan penelitian dan mempublikasikannya di berbagai media ilmiah. Selanjutnya, evaluasi penelitian mencakup evaluasi proses dan hasil penelitian. Terakhir, dalam tahapan lanjutan, peneliti merencanakan tindakan lanjut, seperti penelitian lanjutan atau implementasi hasil penelitian dalam praktik. Diagram Fishbone ini membantu dalam pemahaman yang lebih baik tentang proses penelitian dan membantu peneliti dalam perencanaan, pelaksanaan, dan evaluasi penelitian secara komprehensif. Tahapan dalam penelitian ini dapat di modelkan pada diagram *Fish Bone*. Adapun beberapa tahapan yang digunakan dalam penelitian ini adalah sebagai berikut:



Gambar 1. Diagram Fish Bone Metodologi Penelitian

Keterangan:

1. Analisis Kebutuhan

Tahap awal penelitian ini melibatkan analisis kebutuhan yang sangat penting untuk menentukan persiapan yang diperlukan. Peneliti menganalisis kebutuhan utama, termasuk data Source Code Web yang akan digunakan sebagai subjek penelitian, serta persyaratan perangkat keras (hardware) dan perangkat lunak (software) yang diperlukan untuk mendukung penelitian ini. Analisis ini menjadi landasan untuk merancang sistem dan memastikan bahwa semua sumber daya yang diperlukan tersedia.

2. Perancangan Sistem

Dalam tahap ini, peneliti merancang sistem yang akan digunakan dalam penelitian. Untuk itu, peneliti menggunakan pemodelan UML (Unified Modeling Language) yang mencakup pengembangan use case diagram, activity diagram, dan sequence diagram. Use case diagram digunakan untuk mengidentifikasi aktor-aktor yang terlibat dalam sistem dan fungsionalitas yang akan dikembangkan. Activity diagram membantu menggambarkan alur kerja atau proses yang akan diimplementasikan dalam sistem, sementara sequence diagram digunakan untuk mengilustrasikan interaksi antara berbagai komponen dalam sistem.

3. Penulisan Kode Program

Tahap ini mencakup implementasi nyata dari sistem yang dirancang. Peneliti menggunakan bahasa pemrograman Visual Basic 2010 untuk mengembangkan aplikasi yang akan digunakan dalam penelitian. Selama tahap ini, kode program akan ditulis, struktur sistem akan dibangun, dan fitur-fitur yang telah direncanakan akan diimplementasikan.

4. Pengujian

Pengujian merupakan tahap penting untuk memastikan bahwa sistem yang dibangun berfungsi dengan baik dan sesuai dengan persyaratan. Pengujian program dilakukan menggunakan dua metode: pertama, pengujian program secara lokal dengan menggunakan localhost, yang memungkinkan peneliti untuk memastikan bahwa aplikasi beroperasi dengan benar dalam lingkungan lokal. Kedua, pengujian teori menggunakan blackbox testing, yang bertujuan untuk memverifikasi bahwa aplikasi bekerja sesuai yang diharapkan tanpa memperhatikan rincian implementasi internalnya.

5. Hasil

Hasil dari penelitian ini adalah pengembangan aplikasi "Enkripsi Dekripsi Metode Reverse Cipher dan Caesar Cipher untuk Kerahasiaan Source Code Web." Aplikasi ini merupakan produk akhir dari tahapan sebelumnya dan dapat digunakan untuk mengamankan Source Code Web, menjaga kerahasiaan data, dan mencegah akses yang tidak sah. Dengan demikian, penelitian ini berhasil mencapai tujuan utamanya dan memberikan solusi untuk meningkatkan keamanan Source Code Web.

3. HASIL DAN PEMBAHASAN

Masalah yang terjadi adalah Isi Source Code Web tidak diterapkan kerahasiaan data sehingga penelitian ini membuat beberapa solusi pemecahan masalah yaitu:

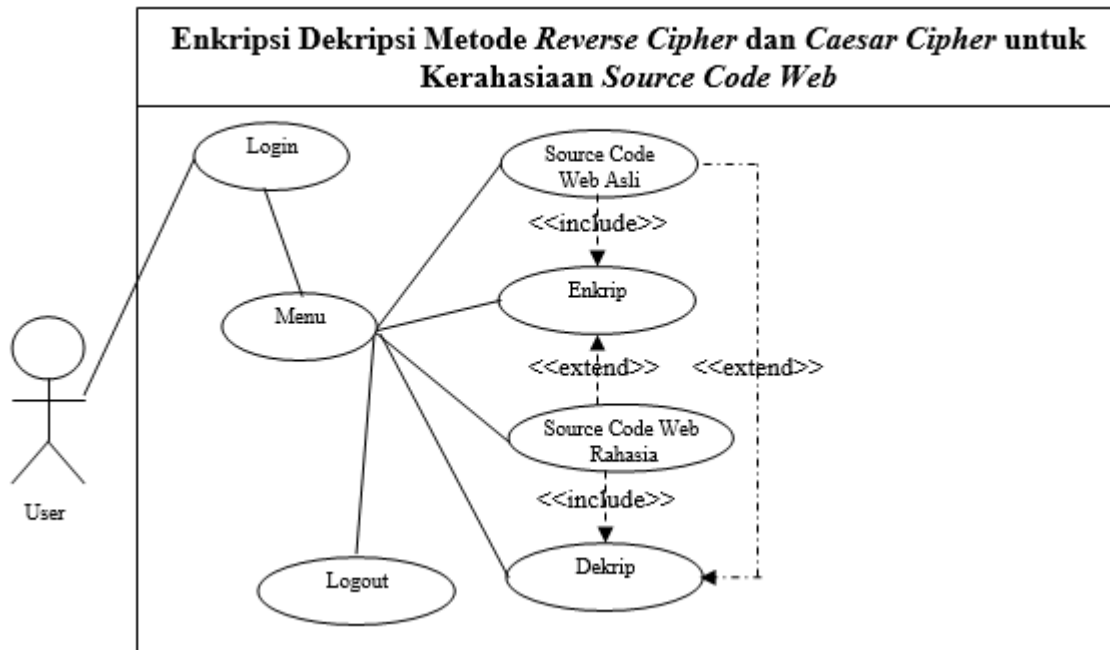
1. Menggunakan metode Reverse Cipher untuk membalikkan kalimat pada source code asli.
2. Menggunakan metode Caesar Cipher untuk mengubah source code asli menjadi rahasia.
3. Membuat aplikasi yang menerapkan metode Reverse Cipher dan Caesar Cipher untuk merahasiakan source code.

A. Desain Sistem

Dalam rancangan sistem ini, peneliti menggunakan berbagai bentuk diagram dari Unified Modeling Language (UML) untuk merinci dan menggambarkan berbagai aspek sistem. Pertama, Use Case Diagram digunakan untuk mengidentifikasi aktor-aktor yang terlibat dalam sistem dan fungsi-fungsi yang akan dieksekusi oleh sistem. Diagram ini memberikan pandangan tingkat tinggi tentang interaksi antara pengguna dan sistem. Penggunaan berbagai jenis diagram UML ini memungkinkan peneliti untuk merancang sistem dengan lebih teliti dan rinci, memahami interaksi antara komponen-komponen utama, serta merinci struktur data yang diperlukan. Hal ini memberikan pandangan menyeluruh tentang sistem yang akan dikembangkan, memudahkan komunikasi antara tim pengembangan, dan memastikan bahwa sistem yang dihasilkan sesuai dengan kebutuhan penelitian.

1. Use Case Diagram

Perancangan dimulai dari identifikasi aktor dan bagaimana hubungan antara aktor dan *use case* didalam sistem. Perancangan *Use Case Diagram* dapat dilihat pada gambar berikut:



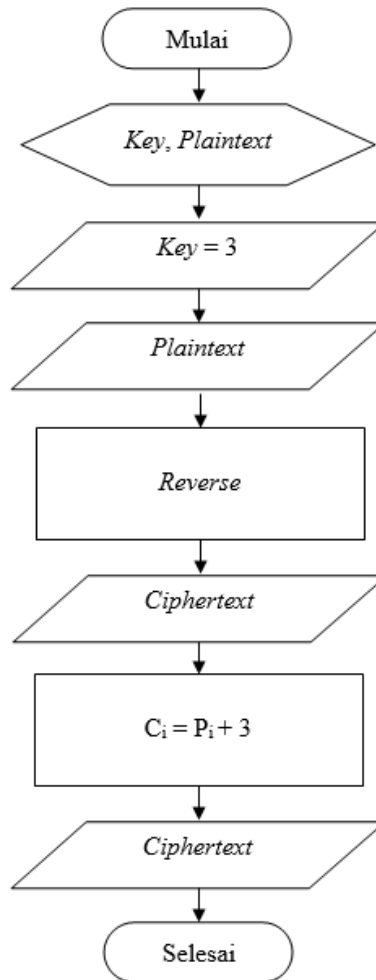
Gambar 2. Use Case Enkripsi Dekripsi Metode Reverse Cipher dan Caesar Cipher untuk Kerahasiaan Source Code Web

B. Penerapan Metode

Dalam penelitian ini, metode enkripsi yang digunakan untuk mendapatkan pesan rahasia adalah metode Reverse Cipher dan Caesar Cipher. Reverse Cipher digunakan untuk mengubah pesan asli (plaintext) dengan cara membalikkan urutan karakter, sehingga pesan tersebut menjadi ciphertext. Misalnya, huruf "A" akan menjadi "Z," "B" menjadi "Y," dan seterusnya. Metode ini adalah salah satu cara sederhana untuk mengubah pesan sehingga menjadi sulit dibaca bagi mereka yang tidak memiliki pengetahuan tentang perubahan urutan karakter ini. Selain Reverse Cipher, penelitian ini juga memanfaatkan metode Caesar Cipher. Metode ini melibatkan pergeseran karakter dalam pesan asli sebanyak sejumlah posisi tertentu dalam alfabet atau set karakter yang digunakan. Ini berarti, jika peneliti mengambil contoh pergeseran sebanyak 3 karakter, maka setiap karakter dalam pesan akan digantikan oleh karakter yang terletak tiga langkah ke kanan dalam alfabet. Metode Caesar Cipher ini memberikan lapisan tambahan dalam perlindungan pesan rahasia. Kombinasi kedua metode ini, yaitu Reverse Cipher dan Caesar Cipher, memberikan tingkat keamanan yang lebih baik dalam mengamankan pesan rahasia, seperti Source Code Web, sehingga menjadikan penelitian ini relevan dalam konteks keamanan data dan pengembangan aplikasi web. Penelitian ini bertujuan untuk menjaga kerahasiaan data yang sensitif dan mencegah akses yang tidak sah ke dalam Source Code Web.. Berikut ini adalah rumus enkrip dari metode Caesar Cipher:

$$C_i = P_i + 3 \dots \dots \dots (1)$$

Flowchart metode enkrip dapat dilihat sebagai berikut:



Gambar 3. Flowchart Enkrip Metode Reverse Cipher dan Caesar Cipher

Langkah-langkah metode *Reverse Cipher* untuk enkrip dapat dilihat sebagai berikut:

1. Buat pesan untuk di enkrip.
2. Lakukan penukaran tiap karakter pesan.

Plaintext : POTENSI

Ciphertext : ISNETOP

ASCII control characters				ASCII printable characters												Extended ASCII characters											
DEC	HEX	Simbolo ASCII		DEC	HEX	Simbolo	DEC	HEX	Simbolo	DEC	HEX	Simbolo	DEC	HEX	Simbolo	DEC	HEX	Simbolo	DEC	HEX	Simbolo	DEC	HEX	Simbolo	DEC	HEX	Simbolo
00	00h	NULL		(carácter nulo)	32	20h	espacio	64	40h	@	96	60h	`	128	80h	Ç	160	A0h	á	192	C0h	À	224	E0h	Ó		
01	01h	SOH		(inicio encabezado)	33	21h	!	65	41h	A	97	61h	a	129	81h	Ù	161	A1h	â	193	C1h	Á	225	E1h	Ô		
02	02h	STX		(inicio texto)	34	22h	"	66	42h	B	98	62h	b	130	82h	Ú	162	A2h	ã	194	C2h	Â	226	E2h	Õ		
03	03h	ETX		(fin de texto)	35	23h	#	67	43h	C	99	63h	c	131	83h	Û	163	A3h	ä	195	C3h	Ã	227	E3h	Ö		
04	04h	EOT		(fin transmisión)	36	24h	\$	68	44h	D	100	64h	d	132	84h	Ü	164	A4h	å	196	C4h	Ä	228	E4h	Ø		
05	05h	ENQ		(enquiry)	37	25h	%	69	45h	E	101	65h	e	133	85h	Ý	165	A5h	æ	197	C5h	Å	229	E5h	Ù		
06	06h	ACK		(acknowledgement)	38	26h	&	70	46h	F	102	66h	f	134	86h	ÿ	166	A6h	ß	198	C6h	ä	230	E6h	Þ		
07	07h	BEL		(timbre)	39	27h	'	71	47h	G	103	67h	g	135	87h	ÿ	167	A7h	¸	199	C7h	å	231	E7h	ß		
08	08h	BS		(retroceso)	40	28h	(	72	48h	H	104	68h	h	136	88h	ÿ	168	A8h	¸	200	C8h	æ	232	E8h	¸		
09	09h	HT		(tab horizontal)	41	29h	)	73	49h	I	105	69h	i	137	89h	ÿ	169	A9h	¸	201	C9h	¸	233	E9h	¸		
10	0Ah	LF		(salto de línea)	42	2Ah	*	74	4Ah	J	106	6Ah	j	138	8Ah	ÿ	170	AAh	¸	202	CAh	¸	234	EAh	¸		
11	0Bh	VT		(tab vertical)	43	2Bh	+	75	4Bh	K	107	6Bh	k	139	8Bh	ÿ	171	ABh	¸	203	CBh	¸	235	EBh	¸		
12	0Ch	FF		(form feed)	44	2Ch	,	76	4Ch	L	108	6Ch	l	140	8Ch	ÿ	172	ACH	¸	204	CDh	¸	236	EBh	¸		
13	0Dh	CR		(retorno de carro)	45	2Dh	.	77	4Dh	M	109	6Dh	m	141	8Dh	ÿ	173	ADh	¸	205	CDh	¸	237	EDh	¸		
14	0Eh	SO		(shift Out)	46	2Eh	:	78	4Eh	N	110	6Eh	n	142	8Eh	ÿ	174	ACh	¸	206	CEh	¸	238	EEh	¸		
15	0Fh	SI		(shift In)	47	2Fh	/	79	4Fh	O	111	6Fh	o	143	8Fh	ÿ	175	AFh	¸	207	CFh	¸	239	EFh	¸		
16	10h	DLE		(data link escape)	48	30h	0	80	50h	P	112	70h	p	144	90h	ÿ	176	B0h	¸	208	D0h	¸	240	F0h	¸		
17	11h	DC1		(device control 1)	49	31h	1	81	51h	Q	113	71h	q	145	91h	ÿ	177	B1h	¸	209	D1h	¸	241	F1h	¸		
18	12h	DC2		(device control 2)	50	32h	2	82	52h	R	114	72h	r	146	92h	ÿ	178	B2h	¸	210	D2h	¸	242	F2h	¸		
19	13h	DC3		(device control 3)	51	33h	3	83	53h	S	115	73h	s	147	93h	ÿ	179	B3h	¸	211	D3h	¸	243	F3h	¸		
20	14h	DC4		(device control 4)	52	34h	4	84	54h	T	116	74h	t	148	94h	ÿ	180	B4h	¸	212	D4h	¸	244	F4h	¸		
21	15h	NAK		(negative acknowle.)	53	35h	5	85	55h	U	117	75h	u	149	95h	ÿ	181	B5h	¸	213	D5h	¸	245	F5h	¸		
22	16h	SYN		(synchronous idle)	54	36h	6	86	56h	V	118	76h	v	150	96h	ÿ	182	B6h	¸	214	D6h	¸	246	F6h	¸		
23	17h	ETB		(end of trans. block)	55	37h	7	87	57h	W	119	77h	w	151	97h	ÿ	183	B7h	¸	215	D7h	¸	247	F7h	¸		
24	18h	CAN		(cancel)	56	38h	8	88	58h	X	120	78h	x	152	98h	ÿ	184	B8h	¸	216	D8h	¸	248	F8h	¸		
25	19h	EM		(end of medium)	57	39h	9	89	59h	Y	121	79h	y	153	99h	ÿ	185	B9h	¸	217	D9h	¸	249	F9h	¸		
26	1Ah	SUB		(substitute)	58	3Ah	:	90	5Ah	Z	122	7Ah	z	154	9Ah	ÿ	186	BAh	¸	218	DAh	¸	250	FAh	¸		
27	1Bh	ESC		(escape)	59	3Bh	;	91	5Bh	[	123	7Bh	{	155	9Bh	ÿ	187	BBh	¸	219	DBh	¸	251	FBh	¸		
28	1Ch	FS		(file separator)	60	3Ch	<	92	5Ch	\	124	7Ch	}	156	9Ch	ÿ	188	BCh	¸	220	DCh	¸	252	FCh	¸		
29	1Dh	GS		(group separator)	61	3Dh	=	93	5Dh	]	125	7Dh	}	157	9Dh	ÿ	189	BDh	¸	221	DDh	¸	253	FDh	¸		
30	1Eh	RS		(record separator)	62	3Eh	>	94	5Eh	^	126	7Eh	~	158	9Eh	ÿ	190	BEh	¸	222	DEh	¸	254	FEh	¸		
31	1Fh	US		(unit separator)	63	3Fh	?	95	5Fh	_				159	9Fh	ÿ	191	BFh	¸	223	DFh	¸	255	FFh	¸		
127	20h	DEL		(delete)																							

Gambar 4. Daftar ASCII

Ubah *plaintext* menjadi ASCII:

I = 73
S = 83
N = 78
E = 69
T = 84
O = 79
P = 80

Langkah-langkah metode *Caesar Cipher* untuk enkrip dapat dilihat sebagai berikut:

1. Masukkan *plaintext* untuk di enkrip.
2. Ubah pesan per karakter dan kunci ke dalam kode *ascii*.
3. Lakukan proses penjumlahan 3 terhadap *ascii* pesan pada tiap karakter.

Berikut ini adalah rumus enkrip dari metode *Caesar Cipher*:

$$P_i = C_i + 3 \dots \dots \dots (2)$$

Proses enkripsi:

$$C_i = P_i + K_i$$

$$I = 73 + 3 = 76 = L$$

$$S = 83 + 3 = 86 = V$$

$$N = 78 + 3 = 81 = Q$$

$$E = 69 + 3 = 72 = H$$

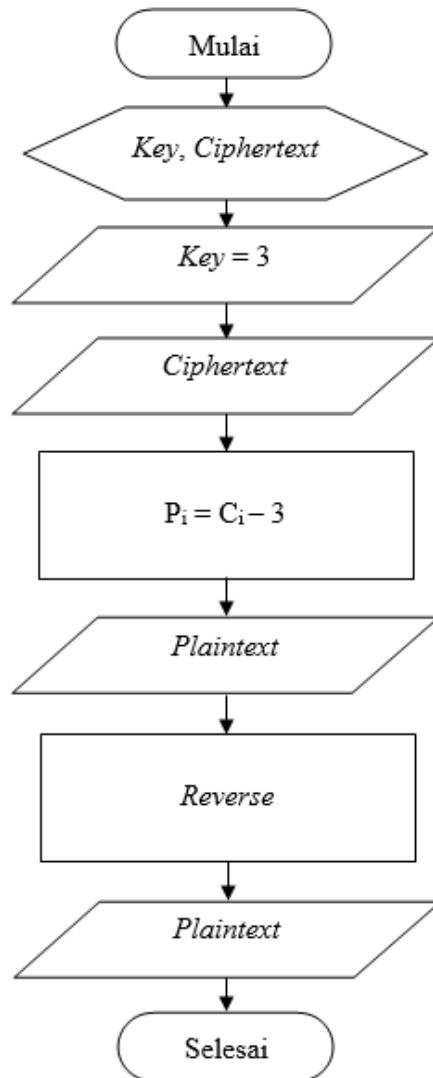
$$T = 84 + 3 = 87 = W$$

$$O = 79 + 3 = 82 = R$$

$$P = 80 + 3 = 83 = S$$

Ciphertext: LVQHWRS

Flowchart metode dekrip dapat dilihat sebagai berikut:



Gambar 5. Flowchart Dekrip Metode Caesar Cipher

Langkah-langkah metode *Caesar Cipher* untuk dekrip dapat dilihat sebagai berikut:

1. Masukkan *ciphertext* untuk di dekrip.
2. Ubah pesan per karakter dan kunci ke dalam kode *ascii*.
3. Lakukan proses pengurangan 3 terhadap *ascii* pesan pada tiap karakter.

Berikut ini adalah rumus dekrip dari metode *Caesar Cipher*:

$$P_i = C_i - 3 \dots\dots\dots (3)$$

Contoh proses dekrip:

C: LVQHWRS

Solusi:

Ubah *plaintext* menjadi ASCII:

Proses dekrip:

$$P_i = C_i - K_i$$

$$L = 76 - 3 = 73 = I$$

$$V = 86 - 3 = 83 = S$$

$$Q = 81 - 3 = 78 = N$$

$H = 72 - 3 = 69 = E$
 $W = 87 - 3 = 84 = T$
 $R = 82 - 3 = 79 = O$
 $S = 83 - 3 = 80 = P$
Ciphertext: ISNETOP

Langkah-langkah metode *Reverse Cipher* untuk dekrip dapat dilihat sebagai berikut:

1. Masukkan *ciphertext* untuk di dekrip.
2. Lakukan penukaran tiap karakter pesan.

Contoh proses dekrip:

Ciphertext : ISNETOP

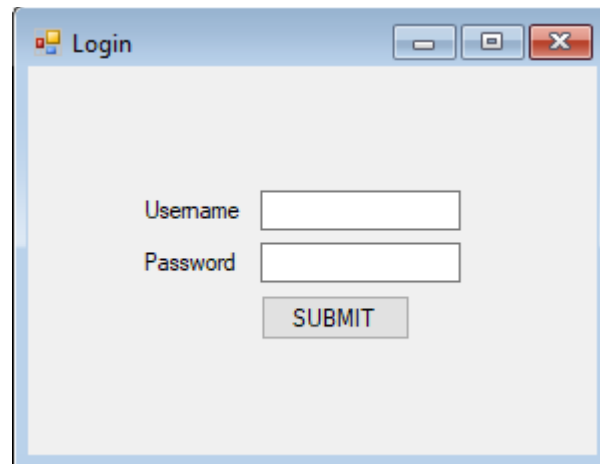
Plaintext : POTENSI

C. Tampilan Hasil

Aplikasi Enkripsi Dekripsi Metode *Reverse Cipher* dan *Caesar Cipher* untuk Kerahasiaan *Source Code Web* memiliki tampilan sebagai berikut:

1. Tampilan Hasil *Form Login*

Tampilan Hasil *Form Login* berfungsi menampilkan *form login*. Adapun Tampilan Hasil *Form Login* dapat dilihat pada gambar berikut:

A screenshot of a web browser window displaying a login form. The window has a title bar with the text 'Login' and standard minimize, maximize, and close buttons. The form itself is centered and contains two text input fields. The first field is labeled 'Username' and the second is labeled 'Password'. Below these fields is a button labeled 'SUBMIT'.

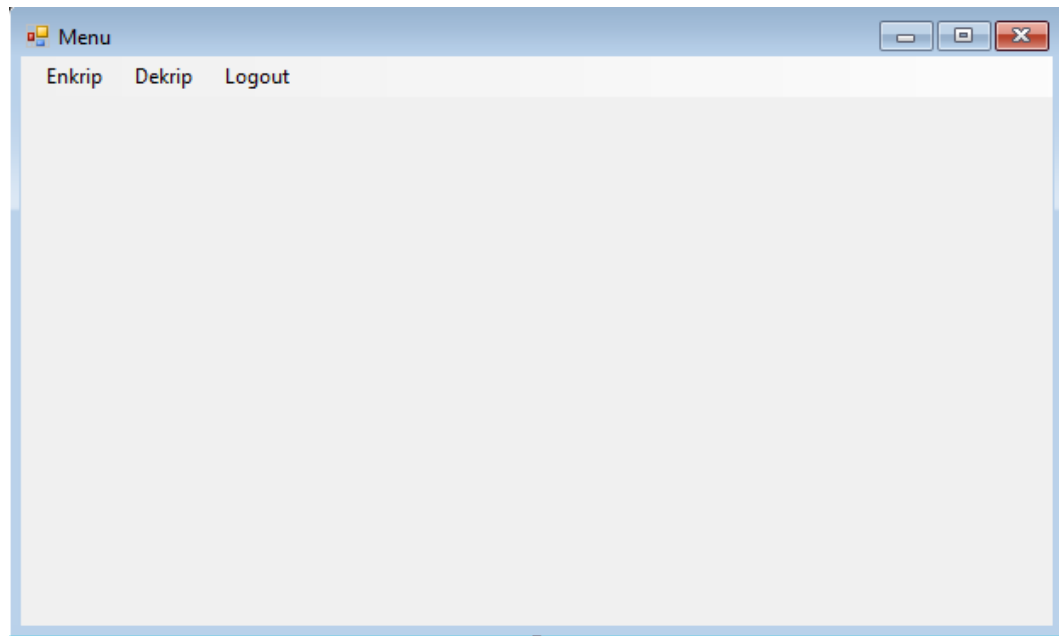
Gambar 6. Tampilan Hasil *Form Login*

Keterangan:

Gambar diatas merupakan tampilan *form login* untuk akses masuk aplikasi ke menu utama jika pengguna memasukkan sandi dengan benar.

2. Tampilan Hasil *Form Menu*

Tampilan Hasil *Form Menu* berfungsi menampilkan *form menu*. Adapun Tampilan Hasil *Form Login* dapat dilihat pada gambar berikut:

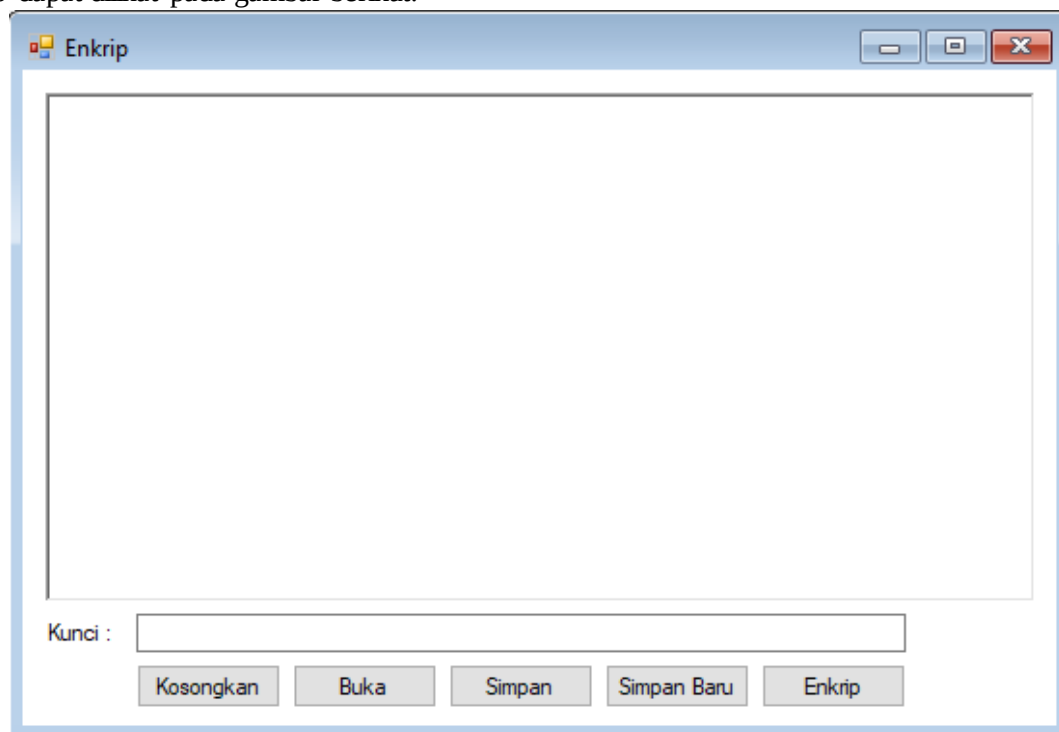
Gambar 7. Tampilan Hasil *Form* Menu

Keterangan:

Gambar diatas merupakan tampilan *form* menu yang terdiri dari dua *form* yaitu enkrip dan dekrip. Jika pengguna mengklik enkrip maka akan tampil *form* enkrip dan jika pengguna mengklik dekrip maka akan tampil *form* dekrip.

3. Tampilan Hasil *Form* Enkrip

Tampilan Hasil *Form* Enkrip berfungsi menampilkan *form* enkrip. Adapun Tampilan Hasil *Form* Enkrip dapat dilihat pada gambar berikut:

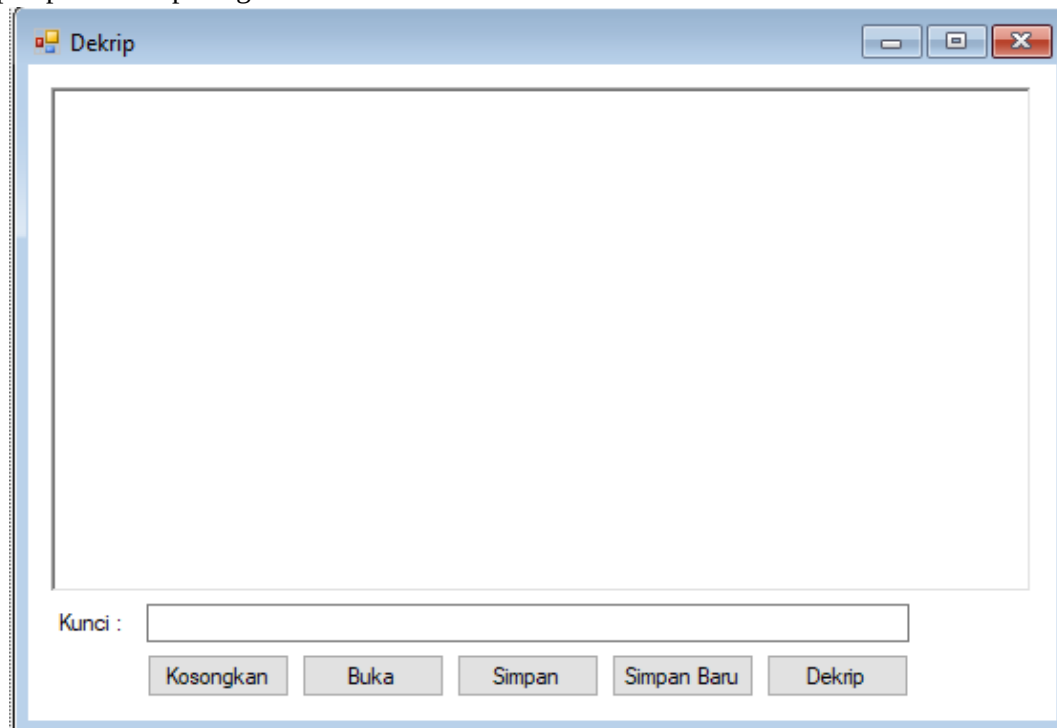
Gambar 8. Tampilan Hasil *Form* Enkrip

Keterangan:

Gambar diatas merupakan tampilan *form* enkrip dan untuk menggunakannya terlebih dahulu pengguna harus memilih data yang akan di enkrip maka akan tampil seluruh isi *Source Code Web*. Kemudian pengguna mengklik tombol Enkrip, maka isi teks *Source Code Web* akan menjadi teks rahasia.

4. Tampilan Hasil *Form* Dekrip

Tampilan Hasil *Form* Dekrip berfungsi menampilkan *form* dekrip. Adapun Tampilan Hasil *Form* Dekrip dapat dilihat pada gambar berikut:



Gambar 9. Tampilan Hasil *Form* Dekrip

Keterangan:

Gambar diatas merupakan tampilan *form* dekrip dan untuk menggunakannya terlebih dahulu pengguna harus memilih data yang akan di dekrip maka akan tampil seluruh isi *Source Code Web* yang ditampilkan. Kemudian pengguna mengklik tombol Dekrip, maka isi teks *Source Code Web* akan menjadi teks rahasia.

D. Kelebihan dan Kekurangan Sistem

Setiap sistem memiliki kelebihan dan kekurangan, berikut ini adalah kelebihan dan kekurangan sistem yang telah dibuat.

1. Kelebihan Sistem

Adapun kelebihan sistem yang telah dibuat diantaranya yaitu:

- Aplikasi yang telah dibuat dapat merahasiakan *source code web*.
- Aplikasi yang telah dibuat menggunakan kunci bebas sehingga memperkuat kerahasiaan data.
- Aplikasi dapat menyimpan hasil enkrip dan dekrip ke dalam *file source code web*.

2. Kekurangan Sistem

Adapun kekurangan sistem yang telah dibuat diantaranya yaitu:

- Aplikasi yang telah dibuat tidak menggunakan dua metode.
- Aplikasi yang telah dibuat tidak menggunakan kunci asimetris.
- Aplikasi yang telah dibuat tidak memiliki petunjuk penggunaan.

4. KESIMPULAN

Berdasarkan pembahasan dari bab-bab sebelumnya yang telah dilakukan maka dapat diambil beberapa kesimpulan sebagai berikut:

1. Hasil penelitian ini dapat menyelesaikan masalah ancaman dengan merahasiakan isi *Source Code Web* dari pencuri data
2. Hasil penelitian ini memberikan solusi yaitu dengan memberikan kerahasiaan pada isi *Source Code Web*.
3. Dengan menggunakan data teks dari *source code web* dan kunci yang ditentukan, kemudian data teks dari basis data dan kunci diubah menjadi ASCII sehingga selanjutnya dapat menerapkan metode *Reverse Cipher* dan *Caesar Cipher* untuk Kerahasiaan *Source Code Web* dengan aplikasi VB Net.
4. Hasil perhitungan metode antara aplikasi dan teori telah sesuai dan memiliki hasil yang sama.
5. Dengan menggunakan pemrograman *visual basic* 2010 maka dapat Aplikasi Enkripsi Dekripsi Metode *Reverse Cipher* dan *Caesar Cipher* untuk Kerahasiaan *Source Code Web*.

UCAPAN TERIMA KASIH

Penulis dengan tulus mengucapkan rasa terima kasih yang sebesar-besarnya kepada Universitas Potensi Utama atas bantuan yang diberikan dalam menyelesaikan karya tulis ilmiah ini.

REFERENSI

- [1] Saleh, A., Sari, R. E., & Orlando, J. M., (2020). "Pemanfaatan Penguasaan Komputer Dalam Menghadapi Ujian Berbasis Komputer Bagi Siswa". Jurnal TUNAS: Jurnal Ilmiah Pengabdian kepada Masyarakat, Vol 1 No 2, April, Page 85 – 89.
- [2] Agung, M., Roslina, & Sari, R. E., (2020). "Implementasi Aplikasi Pembuatan Chat". Jurnal FTIK, Vol. 1 No. 1.
- [3] Sari, R. E., Saleh, A., & Afandi, M. R., (2021). "Pemanfaatan Website Dalam Mengembangkan Kreativitas Siswa Di Dunia Usaha". Jurnal TUNAS: Jurnal Ilmiah Pengabdian kepada Masyarakat, Vol 2 No 2, April, Page 43 – 47.
- [4] Andrian, D., & Sari, R. E., (2020). "Perancangan Aplikasi Resep Masakan Khas Jawa Berbasis Android". Jurnal FTIK, Vol. 1 No. 1.
- [5] Nugroho, A. Y. H., Gunawan, H., Buyung, A. N., & Sari, R. E., (2022). "Penerapan Elgamal Guna Meningkatkan Keamanan Data Text dan Docx". IT Jourmale-ISSN: 2714-8831| p-ISSN: 2252-746X Vol. 10 No. 1 April 2022 Hal.76-86.
- [6] Padmanaba, A., Kumalasari, E., & Andayati, D., (2020). "Komparasi Penggunaan Framework Codeigniter Vs Php Native Pada Sistem Informasi Manajemen Surat Sekretariat Dprd Pemalang". Jurnal SCRIPT, Vol. 8 No. 1 Juni 2020.
- [7] Prahasti, Sapri, & Utami, F. H., (2022). "Aplikasi Pelayanan Antrian Pasien Menggunakan Metode FCFS Menggunakan PHP dan MySQL". Jurnal Media Infotama Vol.18 No.1 2022.
- [8] Shahnaz, & Destari, R. A., (2020). "Perancangan Aplikasi Enkripsi Dan Dekripsi Data Teks Dengan Menggunakan Metode Merkle Hellman". Jurnal FTIK, Vol. 1 No. 1.
- [9] Yusfrizal., (2019). "Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Cipher Dan Rsa Berbasis Android". Jurnal Teknik Informatika Kaputama (JTik) Vol. 3 , No. 2, Juli 2019.

- [10] Paskah, D. M., Puspasari, R., & Verina, W., (2020). "Perbandingan Metode Stream Dengan Metode Caesar Cipher Terhadap Pengiriman Pesan Pada Jaringan Wireless LAN". Jurnal FTIK, Vol. 1 No. 1.
- [11] Lumban, I. G., & Ekadiansyah, E., (2020). "Penerapan Metode Hill Cipher Dan Caesar Cipher Pada Aplikasi Wireless Lan Chatting". Jurnal FTIK, Vol. 1 No. 1.
- [12] Nataliana, D., & Hadiatna, F., & Fauzi, A., (2019). "Rancang Bangun Sistem Keamanan RFID Tag menggunakan Metode Caesar Cipher pada Sistem Pembayaran Elektronik". ELKOMIKA | ISSN (p): 2338-8323 | ISSN (e): 2459-9638 | Vol. 7 | No. 3 | Halaman 427 – 441 DOI : <http://dx.doi.org/10.26760/elkomika.v7i3.427> September 2019.
- [13] Mesran, & Darma, S. N., (2019). "Peningkatan Keamanan Kriptografi Caesar Cipher dengan Menerapkan Algoritma Kompresi "Stout Codes"". JURNAL RESTI(Rekayasa Sistem dan Teknologi Informasi)Vol. 4 No. 6 (2020) 1209 –1215.
- [14] Kartika, L., & Yudi., (2020). "Rancang Bangun Aplikasi Penyembunyian Pesan QRCode Dengan Menggunakan Metode Caesar Cipher Berbasis Android". Jurnal FTIK, Vol. 1 No. 1.
- [15] Hanafi A. S., & Haryanto, E. V., & Saleh, A., (2020). "Kombinasi Metode Stream Cipher Dan Caesar Cipher Dalam Pengamanan Data Kredit Customer (Studi Kasus : PT. ACE HARDWARE)". 4. Jurnal FTIK, Vol. 1 No. 1.