Sebatik Vol. 26 No. 2 Desember 2022
ISSN: 1410-3737(p) 2621-069X(e)

DOI:10.46984/sebatik.v26i2.2061

IMPLEMENTASI KRIPTOGRAFI PADA PENGAMANAN DATA PEMBAYARAN PIUTANG PELANGGAN MENGGUNAKAN *VIGENERE CIPHER*

Risna[1)], **Yusni Amaliah**[2)], dan **Selly Yunita**[3)]

[1,2,3]Sistem Informasi, STMIK PPKIA Tarakanita Rahmawati
[1,2,3]Jl. Yos Sudarso No. 8, Tarakan, 77111
E-mail: nurrisna098@gmail.com[1)], lily@ppkia.ac.id[2)], selly@ppkia.ac.id[3)]

ABSTRAK

Keamanan data merupakan sebuah bentuk untuk memproteksi hal penting dalam hal ini data, dari manipulasi atau penyalahgunaan oleh orang-orang yang tidak berwenang. CV Harapan Kaltim Abadi merupakan distributor yang bergerak dibidang peralatan dan kosmetika yang belum memiliki metode pengamanan data pembayaran pelanggan, sehingga sangat rentan terhadap manipulasi dan memungkinkan terjadinya kebocoran data dan manipulasi data. Solusi yang dapat digunakan untuk mencegah hal tersebut yaitu ilmu kriptografi, yaitu ilmu penyandian data. *Vigenere Cipher* ialah salah satu metode dalam kriptografi. Metode ini mengubah kalimat asli melalui urutan *Caesar cipher* mengacu pada huruf dalam kata kunci. Proses enkripsi pada penelitian ini menggunakan *Vigenere Cipher* yang menerapkan metode kriptografi kunci simetris. Proses enkripsi dan deskripsi dalam kriptografi dengan kata kunci simetris hanya membutuhkan satu kunci. Kunci yang digunakan dalam proses enkripsi dan deskripsi adalah kunci yang sama. *Plaintext* berubah menjadi *ciphertext* dengan kata-kata yang tidak dapat dipahami. Pada proses deskripsi, *ciphertext* berubah kembali menjadi *plaintext*, yaitu teks yang dapat dibaca kembali. Berdasarkan penerapan dan proses uji coba yang dilakukan dalam penelitian ini, metode *Vigenere Cipher* telah berhasil mengamankan data pembayaran piutang pelanggan berupa *file* Microsoft Excel yang berisi satu sampai dua lembar dokumen. Tahapan penyandian atau enkripsi dan pengembalian atau deskripsi dilakukan dengan menggunakan karakter yang berisi non-huruf kapital, huruf kapital dan simbol sesuai dengan jumlah karakter pada *keyboard*.

Kata Kunci: *Kriptografi, Enkripsi, Dekripsi, Vigenere Cipher, Keamanan Data*

1. PENDAHULUAN

Keamanan data yaitu langkah untuk menjaga atau melindungi data dari hal-hal yang tidak diinginkan seperti penyalahgunaan yang dibuat oleh pihak yang tidak berwenang baik pihak asing atau pihak di dalam Lembaga tersebut. Pada zaman digital, komunikasi dengan jaringan menjadi penting dimana komunikasi dengan media jaringan membuat proses yang terjadi menjadi lebih efektif dan efisien. (Sopiandi & Jabbar, 2020). Dalam merancang sebuah keamanan sistem komputer, pastilah dibutuhkan pula metode pengamanan untuk data atau *file* di dalamnya. Apabila informasi diletakkan di dalam perangkat komputer yang digunakan untuk umum dan bersama, maka data tersebut sangat rawan untuk dimanipulasi. Keamanan informasi bersifat penting sehingga perlu penjagaan atau pengamanan terlebih apabila berhubungan dengan sebuah negara, hal-hal terkait bisnis sebuah perusahaan serta informasi yang lain yang dapat menyebabkan hal fatal apabila digunakan secara tidak benar oleh pihak yang tidak berwenang (Ziaurrahman dkk., 2019). Oleh karena itu, aspek-aspek yang terkait dengan keamanan sebuah data atau informasi haruslah diperhatikan dengan baik agar data tersebut tidak diselewengkan oleh pihak-pihak yang tidak bertanggung jawab. Metode kriptografi adalah salah satu teknik yang bisa digunakan untuk menjaga keamanan data (Surbakti & Subandi, 2018).

Teknik kriptografi (*cryptography)* adalah sebuah ilmu juga seni yang dapat melindungi pesan supaya aman. *"Crypto"* mempunyai arti rahasia atau *"secret"* sedangkan *"graphy"* sama dengan tulisan atau *"writing*". Orang atau pihak yang menerapkan kriptografi dikenal dengan *cryptographers*. *Cipher* merupakan alur logika kriptografi atau *cryptographic algorithm*. *Cipher* berupa formula matematika yang diterapkan dalam tahapan enkripsi dan deskripsi. Umumnya, rumus tahapan-tahapan untuk enkripsi dan deskripsi terkait secara matematis dengan cukup erat. (Aini dkk., 2020).

CV Harapan Kaltim Abadi merupakan distributor yang bergerak dibidang peralatan dan kosmetika. Pada perusahaan ini juga terjadi proses hutang-piutang. Piutang adalah salah satu substansi yang berharga karena piutang berhubungan dengan kas organisasi (Hastuti dkk., 2021). Data piutang pelanggan CV Harapan Kaltim Abadi tersimpan di dalam sebuah *file* Microsoft Excel. *File* Microsoft Excel berupa data piutang tersebut biasanya dikelola oleh seorang administrator dan dikirim

melalui email kepada pimpinan dengan tembusan ke beberapa pihak lain, yang berarti pihak-pihak selain pimpinan juga dapat mengunduh *file* tersebut sehingga sanggatlah rawan untuk dimanipulasi dan memungkinkan terjadinya kebocoran data, yaitu tersebarnya data kepada pihak lain yang tidak berkepentingan.

Berdasarkan latar belakang aktivitas pada perusahaan, permasalahan yang tengah dihadapi oleh CV Harapan Kaltim Abadi yaitu belum adanya aplikasi pengamanan pada data pembayaran piutang pelanggan, sehingga memungkinkan data tersebut dibaca oleh orang yang tidak berkepentingan, selain itu mudah untuk dimanipulasi sehingga keberadaan aplikasi untuk mengamankan dokumen ini sangat penting.

Dalam kriptografi, *vigenere cipher* merupakan teknik mengodekan kalimat dengan mengimplementasikan jajaran kode *Caesar* berlandaskan alfabet atau huruf yang ada dalam kunci (Arfandy dkk., 2022).

Penelitian berjudul Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma *Vigenere Cipher* pada tahun 2022, mengimplementasikan metode *Vigenere Cipher* untuk tahapan enkripsi *file* citra digital dan sukses diterapkan. Hal ini terbukti melalui angka uji validitas yang diperoleh dimana selalu mendapatkan skor kemiripan 100% antara *file* asli dengan *file* citra digital hasil enkripsi (Imam Riadi dkk., 2022).

Pada penelitian yang berjudul Pengamanan *File* Dokumen Menggunakan Metode Substitusi dan *Vigenere Cipher* yang dilakukan di tahun 2019, mengatakan bahwa program metode kriptografi dapat diterapkan pada basis data MySql serta mendapatkan *output file* yang telah dienkripsi atau rahasia yang secara kualitas tidak berbeda dari *file* awal. Proses pengamanan dilakukan dengan melakukan pengamanan pada isi teks yang ada di dalam *file* tersebut. (Budi dkk., 2019).

Sebuah penelitian yang dilakukan pada tahun 2020, menggunakan versi *vigenere cipher* yang telah ditingkatkan dengan menggunakan tabel modifikasi untuk mencakup karakter selain alfabet A-Z (Nahar & Chakraborty, 2020).

Penelitian yang dilakukan pada tahun 2022 yang mengamankan dokumen teks dengan menerapkan algoritma kriptografi klasik yang salah satunya adalah *vigenere cipher* mengatakan bahwa aplikasi yang ditanamkan metode dapat berjalan dengan baik dan menghasilkan *ciphertext* juga *plaintext* yang sesuai. Selain itu, pengujian juga menggunakan kunci yang berbeda pada tahapan pengodean dan pengembalian yang menghasilkan hasil dekripsi yang tidak sesuai atau tidak bisa dikembalikan ke bentuk semula. Hal ini membuktikan bahwa *vigenere cipher* sebagai salah satu algoritma kriptografi simetri membutuhkan satu kunci yang sesuai pada saat tahapan enkripsi serta deskripsi (Simatupang, 2022).

Sebuah penelitian pada tahun 2022, menerapkan metode *Vigenere Cipher* untuk mengamankan data penggajian. Keluaran yang diperoleh dari penelitian ini adalah pengamanan data membuat tingkat kekhawatiran terhadap kebocoran gaji berkurang dan algoritma *vigenere cipher* yang dinilai cukup aman untuk digunakan dalam mengamankan data penggajian (Syahputra dkk., 2022).

Berdasarkan penelitian-penelitian yang pernah dilakukan, penelitian ini akan membuat sebuah aplikasi pengamanan data, yaitu dengan melakukan enkripsi terhadap *file* Microsoft Excel yang berisi data pembayaran piutang pelanggan pada CV Harapan Kaltim Abadi dengan menggunakan teknik pengamanan data yaitu kriptografi dengan metode *Vigenere Cipher*. Bagian yang berkepentingan dapat melakukan enkripsi pada dokumen Excel sehingga isi dokumen akan teracak menjadi bentuk yang tidak beraturan dan hanya bisa di deskripsi atau di kembalikan ke bentuk semula oleh bagian yang mengetahui kunci pada saat melakukan enkripsi *file*.

Penelitian ini memutuskan untuk menggunakan kriptografi alih-alih dengan mengunci *file* atau pun steganografi karena apabila hanya dengan mengunci *file*, maka ketika kata sandi dapat ditebak, isi di dalam dokumen akan terekspos seperti pada dokumen aslinya sehingga tingkat keamanan masih kurang. Kriptografi adalah salah satu bentuk yang lebih umum dibandingkan dengan steganografi dimana isi dokumen disisipkan pada bentuk *file* lain, mengingat dokumen juga akan dibaca oleh pimpinan sebagai orang yang awam dengan steganografi atau pun tipe *file* yang lain, oleh karena itu dipilihlah kriptografi dengan mengamankan isi teks di dalam dokumen dibandingkan mengubah tipe *file* melalui enkripsi dimana kriptografi dengan metode ini mudah diterapkan dan diterima tetapi keamanan yang dihasilkan cukup baik.

Diharapkan melalui sistem ini, isi di dalam dokumen akan di acak menjadi bentuk karakter yang tidak berarti sehingga tidak dapat dipahami artinya walaupun dibuka. Selain itu, pada penelitian kali ini, semua lembar kerja yang ada pada dokumen akan digabungkan menjadi satu lembar kerja yang sama pada saat di enkripsi untuk mengecoh dan mencegah penyalahgunaan oleh pihak yang tidak berwenang karena isi dokumen yang tidak dapat dipahami yang belum pernah dicoba pada penelitian sebelumnya.

2. RUANG LINGKUP

Adapun penelitian ini dibatasi oleh hal-hal berikut, dokumen yang dienkripsi adalah data piutang pelanggan berupa *file* Microsoft Excel, karakter yang dienkripsi adalah huruf, angka, dan simbol dengan total 94 karakter, dan kunci enkripsi serta deskripsi bersifat simetri.

3. BAHAN DAN METODE

Bahan dan metode yang dipakai dalam proses penelitian antara lain:

3.1 Keamanan Data

Pengertian keamanan data ialah sebuah upaya untuk menjaga dan memberi jaminan kepada tiga bagian paling penting dalam dunia sistem komputer dan informasi, antara lain kerahasiaan, keutuhan, dan ketersediaan data. Bagian yang pertama berarti pengguna dunia digital terjaga keamanannya atau privasinya di saat beraktivitas yang berhubungan dengan internet, baik pada perangkat pribadi, komputer ataupun perangkat genggam. Bagian kedua atau keutuhan data berarti pengguna dunia digital memperoleh data yang riil tanpa hasil modifikasi atau pengubahan oleh orang lain di tengah prosesnya. Sedangkan aspek yang terakhir yaitu ketersediaan data berarti pengguna dunia digital dapat memperoleh informasi Ketika diinginkan tanpa ada halangan oleh orang lain. (Rg dkk., 2018).

3.2 Piutang

Hak perusahaan yang dipegang oleh orang lain disebut piutang. Piutang berperan sentral bagi sebuah perusahaan, baik perusahaan jasa juga dagang. Piutang umumnya muncul karena adanya penjualan baik barang ataupun jasa. (Fauzia, 2020).

3.3 Kriptografi

Kriptografi disebutkan sebagai teknik yang mencoba untuk menutupi pesan pada mulanya. Kemudian dijelaskan bahwa kriptografi adalah teknik yang berlandaskan pada perhitungan matematika untuk menjaga keamanan, kerahasiaan, keutuhan, dan keaslian data. Dengan demikian, kriptografi pada saat ini bukan hanya menyembunyikan pesan tetapi lebih bertujuan untuk menjaga keamanan informasi. (Karman & Nurhasan, 2019).

Kriptografi mempunyai dua aspek utamanya, antara lain enkripsi dan deskripsi. Enkripsi atau penyandian berarti mentransformasikan data atau informasi ke bentuk yang tidak dapat diidentifikasi layaknya bentuk awal dengan menerapkan metode tertentu. Di sisi lain, deskripsi yaitu mengembalikan bentuk yang telah diacak tersebut ke bentuk data atau informasi semula. (Permana, 2018). Proses enkripsi dan deskripsi dikendalikan oleh kunci yang di inputkan (Aung dkk., 2019)

Komponen-komponen yang digunakan dalam kriptografi adalah *plaintext*, *ciphertext*, *encryption*, *decryption*, *cipher*, dan *key*.

Kriptografi terbagi ke dalam dua bagian. Bagian tersebut yaitu kriptografi algoritma klasik dan algoritma modern. Sesuai namanya, kriptografi dengan algoritma klasik adalah metode yang telah ada jauh sebelum terciptanya komputer (Utomo dkk., 2019).

Berdasarkan kunci enkripsi dan deskripsinya, kriptografi dikelompokkan ke dalam dua tipe yaitu, kriptografi simetri dan asimetri. Kriptografi simetri dapat dikenal dengan kritografi algoritma klasik, karena kunci yang digunakan dalam penyandian dan proses pengembaliannya adalah sama. Sedangkan kriptografi asimetri juga dikenal kriptografi dengan kunci publik, dimana kunci dalam proses penyandian dan pengembaliannya adalah tidak sama (Putri dkk., 2018). *Vigenere cipher* dikategorikan sebagai metode dengan algoritma simetri karena kunci yang digunakan dalam proses enkripsi dan deskripsi sama. Algoritma simetri bekerja dengan waktu yang lebih cepat dibandingkan algoritma asimetri ketika mengenkripsi data dengan jumlah yang besar (Saju dkk., 2021)

3.4 *Vigenere Cipher*

Vigenere cipher merupakan sebuah teknik yang dapat digunakan untuk menutupi kekurangan metode substitusi tunggal. Dalam tiap-tiap baris pada tabel *vigenere* berarti hasil *ciphertext* yang didapat dari *Caesar cipher*, dimana setiap karakter pada *plaintext* bergeser berdasarkan nilai angka pada karakter kuncinya. Kunci pada metode ini akan disesuaikan dengan panjangnya karakter yang diamankan (Widarma dkk., 2019). Kunci yang digunakan merupakan sebuah kata atau susunan dari beberapa huruf. Kunci yang digunakan dalam proses penyandian akan diubah ke bentuk numerik berdasarkan tabel yang dipakai. Di lain sisi kalimat yang akan dienkripsi juga diubah ke dalam bentuk numerik berdasarkan acuan pada tabel yang sama (Afandi & Nurhayati, 2021). Kunci pada metode *Caesar cipher* dan *vigenere cipher* menerapkan pola yang berbeda. Kunci pada *Caesar chiper* terdiri dari satu nilai saja sedangkan kunci pada *vigenere* terdiri dari sebuah atau beberapa kata sehingga tiap-tiap karakter *plaintext* dapat dihitung dengan pasangan kunci yang berbeda-beda untuk dienkripsi (Amrulloh & Ujianto, 2019). Oleh karena itu, algoritma ini dikelompokkan sebagai metode substitusi *polyalphabetic* (Safii & Vidy, 2018). Keuntungan yang diperoleh dari menggunakan metode ini adalah memperoleh level keamanan yang sama dengan metode segolongannya tanpa menggunakan tahapan yang rumit dan kompleks (Konyar & Solak, 2021) . Model matematis enkripsi algoritma ini dapat dituliskan dalam persamaan (1) (Widarma dkk., 2019):

$$Enkripsi\ (Ci) = Pi + Ki \bmod 26 \qquad (1)$$

Dimana Ci adalah karakter *ciphertext* yang akan dihasilkan. Pi adalah nilai numerik dari karakter *plaintext*, Ki adalah nilai numerik dari tiap karakter kunci. Sedangkan 26 adalah jumlah dari banyaknya karakter yang dipakai dalam proses enkripsi dan dapat menyesuaikan sesuai kebutuhan penelitian. Kemudian model matematis untuk deskripsi algoritma ini dapat dilihat dalam persamaan (2) (Widarma dkk., 2019):

$$Dekripsi\ (Pi) = Ci - Ki \bmod 26 \qquad (2)$$

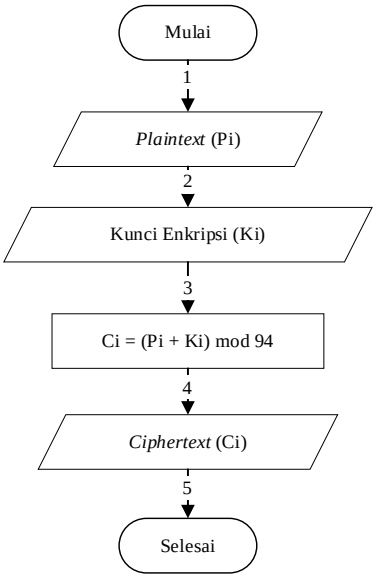
Dimana Pi adalah karakter *plaintext* yang akan dihasilkan. Ci adalah nilai numerik dari karakter *ciphertext*, Ki adalah nilai numerik dari karakter kunci, dan 26 adalah jumlah dari banyaknya karakter yang dipakai dalam proses dekripsi. *Vigenere Cipher* secara

klasik hanya menggunakan 26 karakter dari A-Z untuk enkripsi dan deskripsi (Rizal dkk., 2019). Namun, seiring berkembangnya zaman, hal ini mengalami modifikasi.

Jumlah karakter yang dipakai dalam penelitian ini adalah 94 karakter dengan menggunakan tabel karakter sendiri agar keamanan data lebih terjamin karena tidak ada pihak yang mengetahui nilai karakter kecuali penulis. Sehingga rumus enkripsi dalam penelitian ini menjadi seperti persamaan (3):

$$Enkripsi\ (Ci) = Pi + Ki \bmod 94 \quad (3)$$

Alur metode *vigenere cipher* yang diterapkan dalam penelitian ini dapat dilihat pada gambar 1.

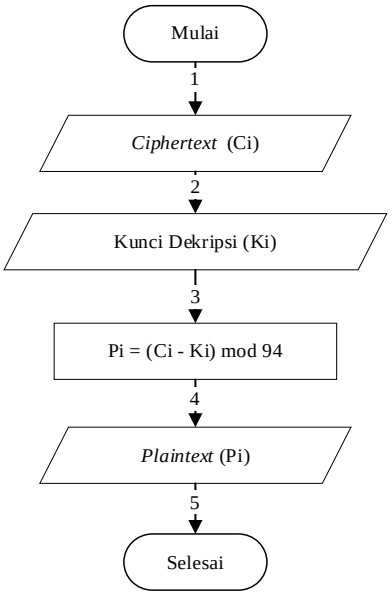


Gambar 1. Alur Enkripsi *Vigenere Cipher*

Sedangkan model matematika deskripsi dalam penelitian ini menjadi seperti persamaan (4):

$$Dekripsi\ (Pi) = Ci - Ki \bmod 94 \quad (4)$$

Alur deskripsi metode *vigenere cipher* dalam penelitian ini dapat dilihat pada gambar 2.



Gambar 2. Alur Deskripsi *Vigenere Cipher*

Tabel karakter yang dijadikan acuan dalam penelitian ini dapat dilihat pada Tabel 1.

Tabel 1. Tabel Karakter

Desimal Nilai	Karakter	Desimal Nilai	Karakter
0	1	48	m
1	2	49	n
2	3	50	o
3	4	51	p
4	5	52	q
5	6	53	r
6	7	54	s
7	8	55	t
8	9	56	u
9	0	57	v
10	A	58	w
11	B	59	x
12	C	60	y
13	D	61	z
14	E	62	~
15	F	63	!
16	G	64	@
17	H	65	#
18	I	66	$
19	J	67	%
20	K	68	^
21	L	69	&
22	M	70	*
23	N	71	(
24	O	72	)
25	P	73	-
26	Q	74	+
27	R	75	=
28	S	76	{
29	T	77	}
30	U	78	|
31	V	79	[
32	W	80	]
33	X	81	\

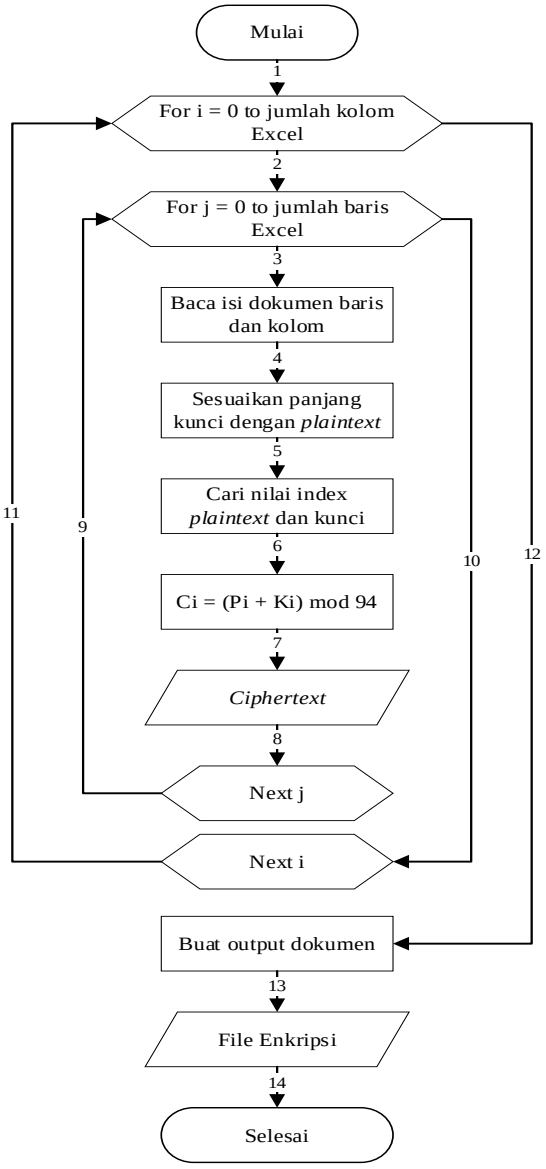
34	Y	82	:
35	Z	83	“
36	a	84	;
37	b	85	‘
38	c	86	<
39	d	87	>
40	e	88	?
41	f	89	,
42	g	90	.
43	h	91	/
44	i	92	_
45	j	93	[spasi]
46	k		
47	l		

Proses perhitungan *vigenere cipher* dimulai dengan menyesuaikan panjang kunci dengan panjang *plaintext*. Setelah itu, tiap-tiap karakter pada *plaintext* akan diterjemahkan ke nilai desimalnya sesuai dengan tabel karakter yang telah dibuat. Begitu juga dengan kunci. Karakter pertama dari *plaintext* akan berpasangan dengan karakter pertama dari kunci, kemudian lanjut ke perhitungan matematis dengan rumus enkripsi. Begitu seterusnya. Setelah didapatkan hasil dari perhitungan matematis, angka tersebut akan diterjemahkan kembali menjadi karakter berdasarkan referensi pada tabel acuan. Karakter yang didapatkan itulah yang menjadi *ciphertext* atau hasil enkripsi. Proses deskripsi juga berjalan sama seperti enkripsi tetapi menggunakan persamaan matematis untuk deskripsi.

Setelah melakukan perhitungan terhadap data, berikutnya metode akan di aplikasikan ke dalam aplikasi lalu selanjutnya yaitu menguji sistem yang telah dibuat untuk mengecek apakah algoritma yang ditanamkan ke dalam sistem telah berjalan dengan sesuai.

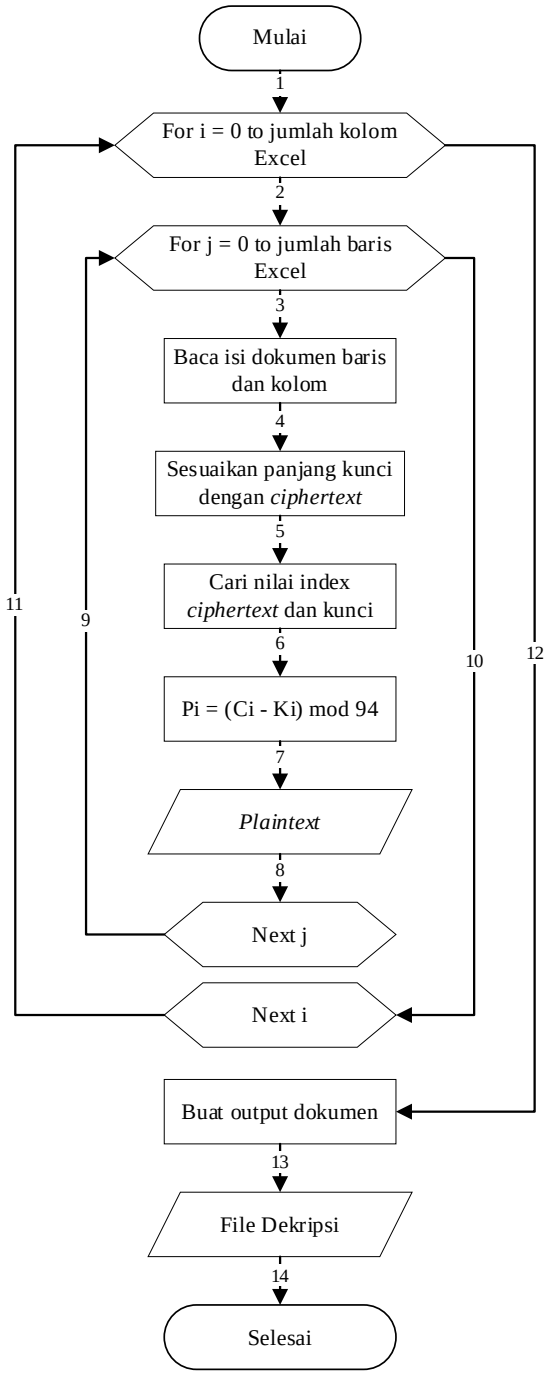
4. PEMBAHASAN

Berikut merupakan bagan jalannya tahapan enkripsi pada dokumen Excel yang dapat dilihat pada gambar 3.



Gambar 3. Alur Enkripsi

Sedangkan alur proses deskripsi pada dokumen Excel dapat dilihat pada gambar 4.



Gambar 4. Alur Deskripsi

Sebagai contoh, terdapat sebuah *plaintext* yaitu TUNAI dengan kunci HKA789. Proses dimulai dengan penyesuaian panjang kunci dengan *plaintext* menjadi :

Plaintext = T U N A I
Kunci = H K A 7 8

Proses enkripsi dimulai dengan mencari nilai desimal dari setiap karakter dimana nilai desimal dari TUNAI adalah 29, 30, 23, 10, 18 dan nilai desimal dari HKA78 adalah 17, 20, 10, 6, 7. Selanjutnya yaitu hitung menggunakan rumus enkripsi seperti tercantum pada persamaan (3). Nilai desimal "T" akan berpasangan dengan nilai desimal kunci "H" dan seterusnya. Sebagai contoh,

Ci = Pi + Ki mod 94
= 29 + 17 mod 94
= 46 mod 94
= 46

Hasil 46 apabila diterjemahkan kembali ke karakter mengacu pada tabel karakter yang dipakai akan menghasilkan karakter "k". Begitu seterusnya hingga diperoleh *ciphertext* "koXGP". Hasil perhitungan enkripsi kata TUNAI dengan kunci HKA789 dapat dilihat pada tabel 2.

Tabel 2. Hasil Enkripsi TUNAI

Karakter		Index		Hasil Enkripsi	
Plaintext	Kunci	Plaintext	Kunci	Index	Karakter
T	H	29	17	46	k
U	K	30	20	50	o
N	A	23	10	33	X
A	7	10	6	16	G
I	8	18	7	25	P

Sedangkan untuk deskripsi, *ciphertext* yang akan di deskripsi adalah "koXGP" dengan kunci yang sama karena algoritma ini bersifat simetri yaitu HKA789. Langkah diawali dengan penyesuaian panjang *ciphertext* dengan panjang kunci menjadi

Ciphertexi = k o X G P
Kunci = H K A 7 8

Proses deskripsi dimulai dengan mencari nilai desimal dari setiap karakter dimana nilai desimal dari koXGP adalah 46, 50, 33, 16, 25 dan nilai desimal dari HKA78 adalah 17, 20, 10, 6, 7. Selanjutnya yaitu hitung menggunakan rumus deskripsi seperti pada persamaan (4). Nilai desimal "k" akan berpasangan dengan nilai desimal kunci "H" dan seterusnya, sebagai contoh:

Pi = Ci - Ki mod 94
= 46 - 17 mod 94
= 29 mod 94
= 29

Hasil 29 apabila diterjemahkan kembali ke karakter mengacu pada tabel karakter yang dipakai akan menghasilkan karakter "T". Begitu seterusnya hingga diperoleh *plaintext* "TUNAI". Hasil perhitungan deskripsi kata koXGP dengan kunci HKA789 dapat dilihat pada tabel 3.

Tabel 3. Hasil Deskripsi koXGP

Karakter		Index		Hasil Deskripsi	
Ciphertext	Kunci	Ciphertext	Kunci	Kunci	Plaintext
k	H	46	17	29	T
o	K	50	20	30	U
X	A	33	10	23	N
G	7	16	6	10	A
P	8	25	7	18	I

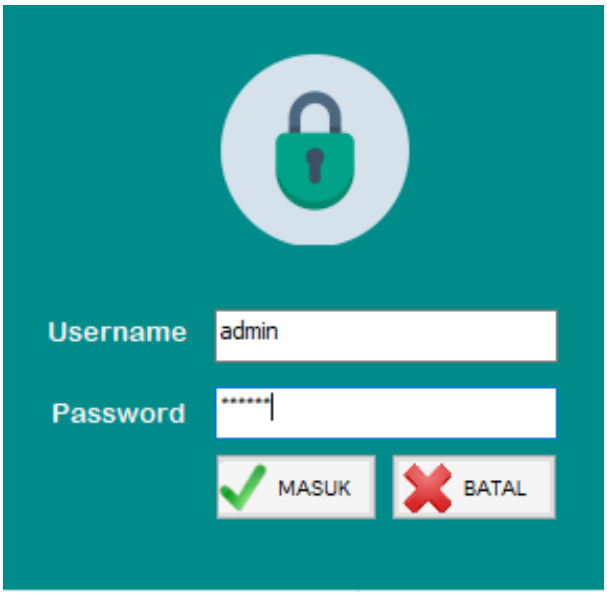
Selanjutnya, proses deskripsi akan dicoba menggunakan kunci yang berbeda dengan kunci pada saat enkripsi, yaitu "koXGP" dienkripsi dengan kunci "BAGUS" untuk membuktikan bahwa algoritma ini menerapkan kunci simetri yang dapat dilihat pada tabel 4.

Tabel 4. Hasil Deskripsi koXGP Menggunakan Kunci Berbeda

Karakter		Index		Hasil Deskripsi	
Ciphertext	Kunci	Ciphertext	Kunci	Kunci	Plaintext
k	B	46	11	35	Z
o	A	50	10	40	E
X	G	33	16	17	H
G	U	16	30	80	]
P	S	25	28	91	/

Berdasarkan hasil yang diperoleh, maka terbukti bahwa proses enkripsi dan deskripsi harus dilakukan dengan kunci yang simetri agar dokumen yang telah diamankan dapat kembali seperti dokumen asli.

Desain aplikasi dimulai dengan halaman yang paling pertama ketika aplikasi dijalankan yaitu halaman *login* yang dapat dilihat pada gambar 5.

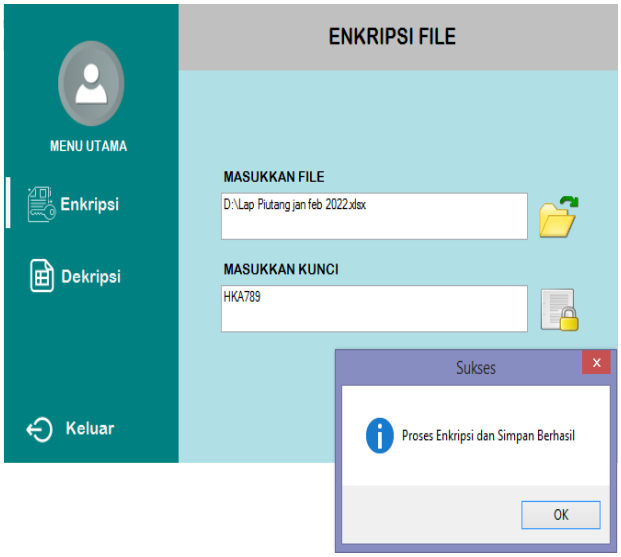


Gambar 5. Halaman *Login*

Ketika berada pada menu *login* pengguna harus mengetikkan nama *user* dan kata sandi yang sesuai. Apabila sesuai, maka pengguna akan diarahkan ke halaman berikutnya yaitu, menu. Halaman menu dapat dilihat pada gambar 6.

Gambar 6. Halaman Menu

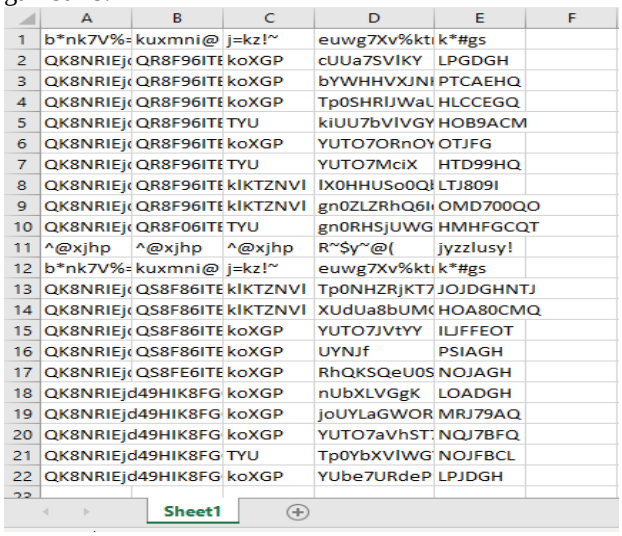
Pada halaman menu, pengguna dapat memilih untuk melakukan enkripsi dokumen baru atau deskripsi dokumen yang telah di enkripsi sebelumnya atau dapat juga memilih keluar. Apabila pengguna memilih enkripsi, maka pengguna akan diarahkan ke halaman enkripsi seperti pada gambar 7.



Gambar 7. Halaman Enkripsi

Pada halaman enkripsi, pengguna terlebih dahulu harus memasukkan dokumen berupa *file* Microsoft Excel. Setelah itu program akan meng*import* dokumen tersebut dan apabila berhasil maka akan muncul pesan. Selanjutnya yaitu mengetikkan kunci yang ingin digunakan dalam proses penyandian, lalu klik tombol enkripsi. Kemudian, akan tampil kotak pesan untuk menyimpan *file* hasil enkripsi dan notifikasi bahwa proses enkripsi berhasil. Apabila dokumen terdiri lebih dari satu lembar kerja, maka program akan otomatis menggabungkan semua lembar kerja menjadi satu dengan tujuan untuk mengecoh pihak-pihak yang kurang

berkepentingan. Contoh hasil enkripsi dapat dilihat pada gambar 8.

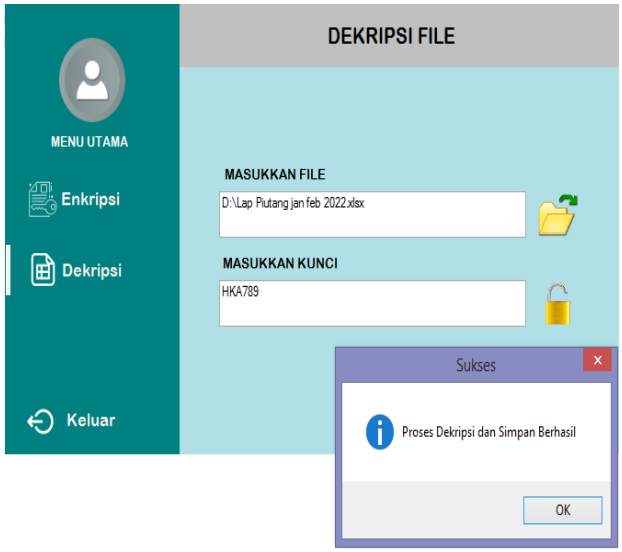


	A	B	C	D	E	F
1	b*nk7V%=	kuxmni@	j=kz!~	euwg7Xv%kt	k*#gs	
2	QK8NRIEj	QR8F96IT	koXGP	cUUa7SVIKY	LPGDGH	
3	QK8NRIEj	QR8F96IT	koXGP	bYWHHVXJN	PTCAEHQ	
4	QK8NRIEj	QR8F96IT	koXGP	Tp0SHRIJWa	HLCCEGQ	
5	QK8NRIEj	QR8F96IT	TYU	kiUU7bVIVGY	HOB9ACM	
6	QK8NRIEj	QR8F96IT	koXGP	YUTO7ORnOY	OTJFG	
7	QK8NRIEj	QR8F96IT	TYU	YUTO7MciX	HTD99HQ	
8	QK8NRIEj	QR8F96IT	kIKTZNVI	IX0HHUSo0Q	LTJ809I	
9	QK8NRIEj	QR8F96IT	kIKTZNVI	gn0ZLZRhQ6I	OMD700QO	
10	QK8NRIEj	QR8F06IT	TYU	gn0RHSjUWG	HMHFGCQT	
11	^@xjhp	^@xjhp	^@xjhp	R~$y~@(	jyzzlusy!	
12	b*nk7V%=	kuxmni@	j=kz!~	euwg7Xv%kt	k*#gs	
13	QK8NRIEj	QS8F86IT	kIKTZNVI	Tp0NHZRjKT7	JOJDGHNTJ	
14	QK8NRIEj	QS8F86IT	kIKTZNVI	XUdUa8bUM	HOA80CMQ	
15	QK8NRIEj	QS8F86IT	koXGP	YUTO7JVtYY	ILJFFEOT	
16	QK8NRIEj	QS8F86IT	koXGP	UYNJf	PSIAGH	
17	QK8NRIEj	QS8FE6IT	koXGP	RhQKSQeU0S	NOJAGH	
18	QK8NRIEjd	49HIK8FG	koXGP	nUbXLVGgK	LOADGH	
19	QK8NRIEjd	49HIK8FG	koXGP	joUYLaGWOR	MRJ79AQ	
20	QK8NRIEjd	49HIK8FG	koXGP	YUTO7aVhST	NQJ7BFQ	
21	QK8NRIEjd	49HIK8FG	TYU	Tp0YbXVIWG	NOJFBCL	
22	QK8NRIEjd	49HIK8FG	koXGP	YUbe7URdeP	LPJDGH	
23						

Sheet1

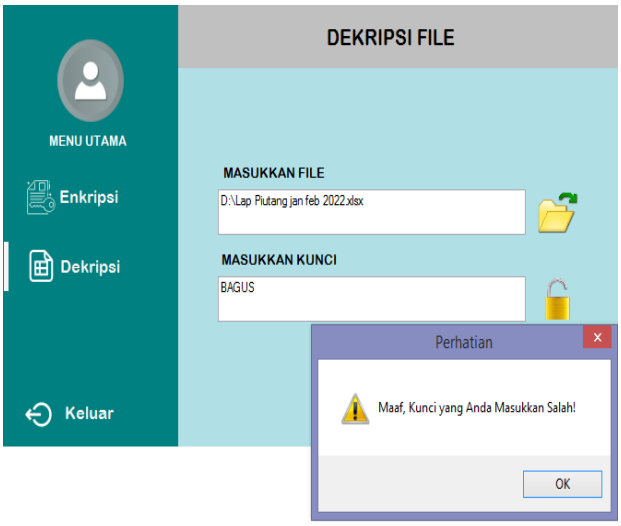
Gambar 8. Hasil Enkripsi

Setelah proses enkripsi, apabila pengguna ingin mengembalikan hasil enkripsi ke bentuk semula, maka pengguna dapat ke halaman deskripsi seperti pada gambar 9.



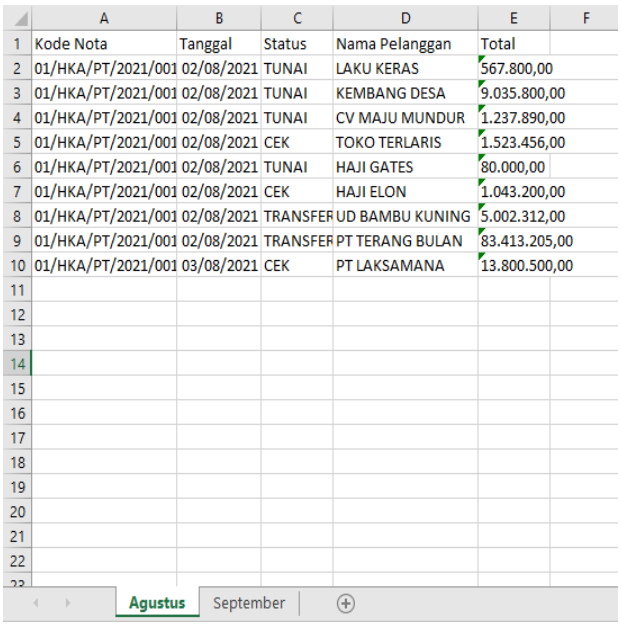
Gambar 9. Halaman Deskripsi

Pada halaman deskripsi, pengguna pada awalnya akan diminta untuk memasukkan dokumen hasil enkripsi. Setelah dokumen berhasil dimasukkan, pengguna harus memasukkan kunci yang digunakan dalam tahapan deskripsi. Sesuai dengan pembuktian bahwa metode ini membutuhkan kunci yang simetri, maka sistem telah dirancang agar tidak dapat melakukan deskripsi jika kunci berbeda. Sehingga, kunci yang di entri harus sama dengan kunci yang digunakan dalam proses enkripsi. Apabila tidak sama, maka proses deskripsi tidak dapat dilakukan dan akan muncul pesan yang dapat dilihat pada gambar 10.



Gambar 10. Kunci Deskripsi Tidak Sesuai

Jika proses deskripsi berhasil, akan tampil kotak dialog untuk menyimpan hasil deskripsi. Setelah itu dokumen hasil deskripsi sudah dapat pengguna buka seperti semula. Apabila dokumen enkripsi merupakan hasil penggabungan dari beberapa lembar kerja, setelah di deskripsi, dokumen akan kembali seperti semula sesuai jumlah lembar kerja yang ada. Contoh hasil deskripsi dapat dilihat pada gambar 11.



	A	B	C	D	E	F
1	Kode Nota	Tanggal	Status	Nama Pelanggan	Total	
2	01/HKA/PT/2021/001	02/08/2021	TUNAI	LAKU KERAS	567.800,00	
3	01/HKA/PT/2021/001	02/08/2021	TUNAI	KEMBANG DESA	9.035.800,00	
4	01/HKA/PT/2021/001	02/08/2021	TUNAI	CV MAJU MUNDUR	1.237.890,00	
5	01/HKA/PT/2021/001	02/08/2021	CEK	TOKO TERLARIS	1.523.456,00	
6	01/HKA/PT/2021/001	02/08/2021	TUNAI	HAJI GATES	80.000,00	
7	01/HKA/PT/2021/001	02/08/2021	CEK	HAJI ELON	1.043.200,00	
8	01/HKA/PT/2021/001	02/08/2021	TRANSFER	UD BAMBU KUNING	5.002.312,00	
9	01/HKA/PT/2021/001	02/08/2021	TRANSFER	PT TERANG BULAN	83.413.205,00	
10	01/HKA/PT/2021/001	03/08/2021	CEK	PT LAKSAMANA	13.800.500,00	
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						

Agustus | September

Gambar 11. Hasil Deskripsi

Pada hasil deskripsi, dokumen yang semula telah dienkripsi menjadi karakter-karakter yang tidak berarti dan tidak dapat dimengerti telah berhasil dikembalikan menjadi dokumen yang sama seperti dokumen asli.

Penelitian ini menggunakan metode pengujian *blackbox* untuk mengetahui keberhasilan aspek fungsionalitas dalam sistem yang dibangun. Hasil pengujian *blackbox testing* dapat dilihat pada tabel 5.

Tabel 5. Hasil *Blackbox Testing*

No.	Aktivitas	Keterangan	Hasil
1	*Login*	Aplikasi akan membuka halaman awal dan apabila *login* berhasil maka tampil halaman menu.	Berhasil
2	Memilih menu enkripsi	Aplikasi akan menampilkan halaman enkripsi.	Berhasil
3	Memasukkan *file* ke dalam aplikasi	Aplikasi akan membaca dan menampung isi *file.*	Berhasil
4	Memasukkan kunci dan melakukan enkripsi	Aplikasi akan menghasilkan *ciphertext* yang sesuai dan mengeluarkannya dalam bentuk *file* Excel yang isinya telah terenkripsi serta mampu menggabungkan beberapa lembar kerja menjadi satu.	Berhasil
5	Memilih menu deskripsi	Aplikasi akan menampilkan halaman deskripsi.	Berhasil
6	Memilih *file* yang ingin di deskripsi	Aplikasi akan membaca dan menampung isi *file*.	Berhasil
7	Memasukkan kunci dan melakukan deskripsi	Aplikasi akan mampu mengecek kesesuaian kunci dan apabila sesuai, aplikasi menghasilkan *plaintext* yang benar dan dikeluarkan dalam bentuk *file* Excel serta mengembalikan dokumen dengan jumlah lembar kerja aslinya.	Berhasil
8	Memilih menu "Keluar"	Aplikasi akan tertutup.	Berhasil

Melalui pengujian ini, didapatkan hasil bahwa aplikasi dan aspek fungsionalitas sistem berjalan semestinya dan sesuai yang diharapkan.

5. KESIMPULAN

Berdasarkan tahapan penelitian yang dilakukan, penerapan ilmu kriptografi pada dokumen Microsoft Excel yang berisi informasi piutang pelanggan telah berhasil diterapkan sehingga tidak mudah diselewengkan oleh pihak yang tidak berkepentingan. Dokumen dapat dienkripsi dan dikembalikan ke bentuk asal seperti pada dokumen awal yang dibuktikan oleh hasil pengujian *blackbox testing*, dimana sistem berjalan dengan baik dan sesuai harapan. Akan tetapi, terdapat kekurangan dimana terbentuk sebuah pola karena setiap kata pada isi dokumen di enkripsi dengan kunci yang sama. Pengamanan data pada dasarnya adalah mencegah pihak tidak berkepentingan mengakses atau mengubah data. Keberadaan aplikasi ini dapat mencegah hal tersebut, namun kejujuran pemegang kunci pengamanan juga perlu mendapatkan perhatian.

6. SARAN

Saran untuk penelitian ini agar ke depannya proses enkripsi dapat dilakukan dengan metode yang berbeda sebagai pembanding, atau dilakukan dengan menggabungkan dua metode untuk memperoleh persentase keamanan yang lebih tinggi. Kemudian diharapkan agar proses enkripsi dapat dilakukan dengan kunci yang dinamis, dalam arti setiap kata dalam satu dokumen diamankan menggunakan kunci yang berbeda-beda agar pola yang dibentuk tidak sama sehingga pemecahan menjadi lebih rumit. Proses enkripsi juga dapat dicoba untuk melakukan pengamanan pada tipe *file* tersebut bukan pada isi di dalam dokumen tersebut sehingga pihak yang tidak berkepentingan menjadi terkecoh dengan tipe *file* yang telah berubah akibat proses enkripsi. Selain itu, diharapkan proses enkripsi dilakukan pada dokumen yang memiliki gambar ataupun grafik, sehingga pengamanan data akan menjadi lebih maksimal.

7. DAFTAR PUSTAKA

Afandi, M. I., & Nurhayati, N. (2021). Implementasi Algoritma Vigenere Cipher Dan Atbash Cipher Untuk Keamanan Teks Pada Aplikasi Catatan Berbasis Android. *IT (INFORMATIC TECHNIQUE) JOURNAL*, *8*(1), 30–41.

Aini, F. N., Amiroch, S., & Chandra, N. E. (2020). Penggunaan Algoritma Vigenere Cipher dan RSA (Rivest-Shamir-Adleman) Untuk Keamanan Data Pembelian di PT Lamongan Marine Industry. *Unisda Journal of Mathematics and Computer Science (UJMC)*, *6*(01), 39–46.

Amrulloh, A., & Ujianto, E. I. H. (2019). Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher. *Jurnal CoreIT*, *5*(2), 71–77.

Arfandy, D., Simanjuntak, M., & Pasaribu, T. (2022). Penerapan Metode Vigenere Chiper untuk Mengamankan Data Text. *JUKI: Jurnal Komputer Dan Informatika*, *4*(1), 48–54.

Aung, T. M., Naing, H. H., & Hla, N. N. (2019). A complex transformation of monoalphabetic cipher to polyalphabetic cipher: (Vigenère-Affine Cipher). *International Journal of Machine Learning and Computing*, *9*(3), 296–303.

Budi, S., Purba, A. B., & Mulyana, J. (2019). PENGAMANAN FILE DOKUMEN MENGGUNAKAN KOMBINASI METODE SUBTITUSI DAN VIGENERE CIPHER. *ILKOM Jurnal Ilmiah*, *11*(3), 222–230.

Fauzia, K. (2020). Perancangan Sistem Informasi Akuntansi Piutang Usaha Berbasis Web Menggunakan PHP dan MySQL. *Jurnal Tekno Kompak*, *14*(2), 80–85.

Hastuti, H., Burhany, D. I., Rufaedah, Y. R., Mai, M. U., & Rochendi, H. R. (2021). EVALUASI EFEKTIVITAS SISTEM PENGENDALIAN INTERN PIUTANG PADA PERGURUAN

TINGGI NEGERI (SUATU STUDI KASUS). *Jurnal Riset Akuntansi*, *13*(1), 75–87.

Riadi, I., Fadlil, A., & Tsani, F. A. (2022). Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher. *JISKA (Jurnal Informatika Sunan Kalijaga)*, *7*(1), 33–45.

Karman, J., & Nurhasan, A. (2019). PERANCANGAN SISTEM KEAMANAN DATA INVENTORY BARANG DI TOKO NANDA BERBASIS WEB MENGGUNAKAN METODE KRIPTOGRAFI VIGENERE CIPHER. *Jurnal Teknologi Informasi MURA*, *11*(1), 29–36.

Konyar, M. Z., & Solak, S. (2021). Efficient data hiding method for videos based on adaptive inverted LSB332 and secure frame selection with enhanced Vigenere cipher. *Journal of Information Security and Applications*, *63*, 103037.

Nahar, K., & Chakraborty, P. (2020). A modified version of Vigenere cipher using 95× 95 table. *International Journal of Engineering and Advanced Technology (IJEAT)*, *9*(5), 1144–1148.

Permana, A. A. (2018). Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android. *JURNAL Al-AZHAR INDONESIA SERI SAINS DAN TEKNOLOGI*, *4*(3), 110–115.

Putri, G. G., Setyorini, W., & Rahayani, R. D. (2018). Analisis Kriptografi Simetris AES dan Kriptografi Asimetris RSA pada Enkripsi Citra Digital. *ETHOS (Jurnal Penelitian Dan Pengabdian)*, *6*(2), 197–207.

Rg, A. S., Azanuddin, S., & Halim, J. (2018). Security Serial Number Product Pada PT. Dayamega Pratama Medan Dengan Menggunakan Metode Merkle Hellman. *Jurnal Cyber Tech*, *1*(1), 151–161.

Rizal, A., Utomo, D. S. B., Rihartanto, R., Hiswati, M. E., & Haviluddin, H. (2019). Modified key using multi-cycle key in vigenere cipher. *Int. J. Recent Technol. Eng*, *8*(2S11), 2600–2606.

Safii, M., & Vidy, V. (2018). KRIPTOGRAFI MONOALFABETIK DAN POLIALFABETIK APLIKASI DAN KOMPARASI DALAM PENGAMANAN DATABASE BANK SOAL. *Sebatik*, *22*(1), 1–9.

Saju, S. H., Haque, S. M., & Lingcon, L. H. (2021). A Hybrid Cryptographic Scheme of Modified Vigenère Cipher using Randomized Approach for Enhancing Data Security. *International Journal of Computer Applications*, *183*(2), 1–8.

Simatupang, L. D. (2022). Pengamanan Dokumen Teks Dengan Menerapkan Kombinasi Algoritma Kriptografi Klasik. *Jurnal Teknik Informatika UNIKA Santo Thomas*, *7*(1), 133–140.

Sopiandi, I., & Jabbar, A. (2020). Studi Komparasi Al-Goritma Keamanan Data Menggunakan Kriptografi Vigenere Chiper Dan Rivest Shamir Adleman (Rsa). *INFOTECH Journal*, *6*(2), 51–56.

Surbakti, J. S., & Subandi, S. (2018). APLIKASI PENGAMANAN DATABASE KEUANGAN BERBASIS DESKTOP MENGGUNAKAN ALGORITMA RC4 DAN VIGENERE CIPHER. *SKANIKA*, *1*(1), 237–242.

Syahputra, Y. H., Azlan, A., & Girsang, L. A. (2022). Pengamanan Data Penggajian Menggunakan Vigenere Cipher Pada Mom's Kitchen Medan. *J-SISKO TECH (Jurnal Teknologi Sistem Informasi Dan Sistem Komputer TGD)*, *5*(1), 1–6.

Utomo, I. W., Latifah, R., & Risanty, R. D. (2019). Aplikasi Kriptografi Berbasis Android Menggunakan Algoritma Caesar Cipher & Vigenere Cipher. *Jurnal Sistem Informasi, Teknologi Informasi Dan Komputer*, *9*(2), 142–149.

Widarma, A., Siregar, H. F., & Irawan, M. D. (2019). Teknik Keamanan Data Menggunakan Vigenere Cipher Dan Electronic Code Book (ECB). *J-SAKTI (Jurnal Sains Komputer Dan Informatika)*, *3*(2), 393–400.

Ziaurrahman, M., Utami, E., & Wibowo, F. W. (2019). Modifikasi Kriptografi Klasik Vigenere Cipher Menggunakan One Time Pad Dengan Enkripsi Berlanjut. *Jurnal Informatika Dan Teknologi Informasi*, *4*(1), 63–68.