

PENGGUNAAN ALGORITMA VIGENERE CIPHER SEBAGAI KEAMANAN SISTEM PADA USAHA KECIL MENENGAH

Alief Fathul Habibie¹, Fahmi Zahary², Muara Nataryda Lubis³, dan Mardiah Nasution⁴.

^{1,2,3,4}Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara.
email: alieffathul.habibie@gmail.com¹, Fahmizaharyyy@gmail.com², muaranatarida17@gmail.com³,
mardiahnst.logika@gmail.com⁴

Abstrak— Perkembangan teknologi saat ini dan segala aktivitas manusia sangat bergantung pada kemajuan teknologi. Setiap aspek kehidupan modern diwujudkan secara digital. Hal ini berimplikasi pada pertumbuhan data dan informasi yang terus meningkat. Di Indonesia, kriptografi juga dikenal sebagai bagian dari pengkodean, yang secara bahasa mengacu pada seni melindungi data dan informasi dari pihak yang tidak diinginkan selama dalam perjalanan dan penyimpanan. Oleh karena itu, karena masalah keamanan dan kerahasiaan informasi sangat penting dalam suatu organisasi atau individu, maka diperlukan prosedur untuk menjaga dan melindungi kerahasiaan data informasi tersebut. Tentu saja, orang yang tidak berwenang tidak dapat melihat atau mengumpulkan informasi yang sangat penting ini. Badan Pusat Statistik membuat perbedaan sistematis tentang usaha rumah tangga, usaha bisnis kecil, menengah, dan besar berdasarkan jumlah tenaga kerja yang ada didalamnya. Ada beberapa aplikasi kriptografi yang mungkin diterapkan dalam lingkungan Bisnis kecil menengah tersebut diantaranya sudah dapat diterapkan seperti mengenkripsi pada password, file, dan email.

Kata Kunci: Keamanan, Kriptografi, Usaha Kecil Menengah, vigenere cipher.

Abstract— Current technological developments and all human activities depend heavily on technological advances. Every aspect of modern life is realized digitally. This has implications for the growth of data and information that continues to increase. In Indonesia, cryptography is also known as part of coding, which linguistically refers to the art of protecting data and information from unwanted parties during transit and storage. Therefore, because the issue of security and confidentiality of information is very important in an organization or individual, procedures are needed to maintain and protect the confidentiality of the information data. Of course, non-masters cannot see or gather this vital information. The Central Statistics Agency makes systematic distinctions between household businesses, and small, medium, and large businesses based on the number of workers in them. There are several cryptographic applications that might be applied in this small and medium business environment, some of which can already be applied, such as encrypting passwords, files, and e-mails.

Keywords - Security, Cryptography, Small and Medium Enterprises, vigenere cipher.

I. PENDAHULUAN

Ada berbagai macam definisi Usaha Kecil Menengah di Indonesia yang diakui oleh semua departemen, instansi pemerintah, serta swasta yang ada di Indonesia. Dengan adanya penghasilan yang diuntungkan sebesar 1 milyar digolongkan dalam usaha kecil, dan usaha dengan hasil penjualan antara Rp. 1-50 milyar digolongkan dalam usaha menengah, maka pemerintah menggalakkan bahwa peran usaha kecil menengah di Indonesia harus terus maju. Saat ini, hanya Badan Pusat Statistik yang membuat perbedaan sistematis tentang usaha rumah tangga, usaha kecil, menengah dan besar berdasarkan jumlah tenaga kerja. Dari lingkup UKM, sumber dayanya meliputi sumber daya manusia dan infrastruktur TI serta biaya. Dalam konteks penelitian ini ada beberapa aplikasi enkripsi yang dapat diimplementasikan di lingkungan UKM. Menerapkan aplikasi enkripsi seperti itu akan lebih murah dan mudah bagi UKM yang sudah memiliki departemen TI sendiri. Aplikasi enkripsi yang dapat diterapkan antara lain enkripsi password, file, dan email.

Enkripsi adalah salah satu cabang dari kriptografi. Enkripsi adalah proses mengubah data teks atau informasi menjadi bentuk teks lain yang tidak dapat dipahami. Dalam kriptografi sendiri terdapat kunci simetris dan asimetris. Ada beberapa algoritma yang dapat digunakan untuk enkripsi menggunakan kunci simetris, tiga di antaranya adalah Caesar cipher, Vigenere cipher, serta affine Cipher.

II. LANDASAN TEORI

Adapun landasan teori yang penulis ambil untuk menunjang penelitian ini diantaranya;

Penelitian yang dilakukan oleh (Buyung Solihin Hasugian, 2017) membahas mengenai kriptografi secara umum dimana berdasarkan sifat kuncinya, kriptografi dibagi menjadi dua, yaitu kriptografi simetris dan kriptografi asimetris. Metode penelitiannya dengan menggunakan metode tinjauan literatur (library research) yaitu penelitian yang didasarkan pada pendapat ahli dan hasil-hasil penelitian terdahulu. Serta kesimpulan akhir dari penelitian ini yaitu, pengguna diberikan ID dan

password untuk mengakses sistem yang ada. Kata sandi dienkripsi untuk mencegah akses tidak sah ke sistem, misalnya pencurian data penting.[1]

Penelitian (Nizar Alam Hamdani dan Galih Abdul Fatah, tahun 2018) dimana penelitian ini membahas tentang Perencanaan sistem informasi strategis perlu menjadi bagian dari perencanaan strategis perusahaan. Rencana strategis sistem informasi ini disusun sebagai strategi untuk memenangkan persaingan sehingga dapat meningkatkan kinerja bisnis UKM. Tujuan dari penelitian ini adalah mengembangkan pada sebuah strategi untuk menggambarkan tujuan sistem dan arsitektur teknis yang akan diterapkan di UKM. Metode yang digunakan dalam penelitian ini adalah metode Strategic Planning Information System (SPIS) dari John Ward dan Joe Peppard (Ward & Peppard). Hasil yang diharapkan dalam perencanaan sistem teknologi informasi sangat berguna bagi UKM tentang bagaimana memanfaatkan informasi organisasinya dengan baik. Berdasarkan hasil tersebut, UKM harus memiliki kemampuan dalam menerapkan teknologi informasi untuk menjadikannya sebuah inovasi untuk pengembangan usaha.[2]

Penelitian (Budi Iskandar dan Agus Umar Hamdani, 2017) dimana penelitian ini membahas tentang Perusahaan PT. XYZ membutuhkan sistem informasi yang cepat dan akurat untuk dapat meningkatkan proses pengiriman barang ke pelanggan. Penelitian ini mensimulasikan pada sebuah sistem usulan yang disesuaikan dengan kebutuhan pengguna. Pada penelitian ini, penulis menganalisis dan memodelkan sistem yang diusulkan menggunakan metode object-oriented analysis and design (OOAD), mengembangkan aplikasi menggunakan Microsoft Visual Net 2010 dan database SQL Server 2008, serta mengujinya menggunakan teknik pengujian black-box Sistem yang diusulkan dilengkapi dengan skor evaluasi untuk pengujian. Sistem menggunakan skala Likert. Hasil akhir dari penelitian ini adalah sebuah model sistem informasi freight forwarder berbasis desktop yang diharapkan dapat membantu manajemen dalam memberikan pelayanan terbaik kepada pelanggan.[3]

Penelitian (Imam Wahyu Utomo, dkk. 2019) dimana penelitian ini membahas mengenai

Kriptografi adalah suatu cara yang dapat digunakan untuk menjaga kerahasiaan dan keamanan informasi dari orang yang tidak berkepentingan. Metode caesar cipher dan vigenere cipher adalah metode enkripsi klasik yang tergolong lemah bila diterapkan masing-masing. Penelitian ini menghasilkan aplikasi untuk melakukan enkripsi dan dekripsi teks berbasis android sehingga dapat digunakan di mana saja.[4]

Penelitian (Veny Cahya Hardita dan Eka Wahyu Sholeha 2021) dimana penelitian ini membahas mengenai Konsep agar sebuah informasi penting tidak dapat diketahui oleh pihak yang tidak memiliki hak dapat dilakukan dengan cara membuat kerahasiaan dari data dan informasi menggunakan kriptografi. Keamanan pada vigenere cipher bergantung pada jumlah kunci yang digunakan semakin banyak jumlah kunci maka semakin luas ruang kunci. Keunggulan dari penelitian ini yaitu menerapkan kombinasi vigenere cipher dan caesar cipher pada vigenere cipher tidak hanya menggunakan satu kunci saja tetapi menggunakan dua kunci dalam pengamanannya serta menggunakan hasil keluaran berupa simbol bukan huruf untuk memperkuat pengamanannya isi pada suatu pesan.[5]

Sehingga dengan penjabaran referensi penelitian sebelumnya diatas, maka penulis tertarik untuk menggunakan algoritma kunci simetris yakni dengan metode vigenere cipher. Dengan harapannya untuk menjaga keamanan informasi yang dikirim dapat lebih aman dan menghindari risiko terjadinya pencurian informasi. Penelitian yang dibuat untuk mengamankan data para pegawai di sektor bisnis usaha kecil menengah tentu perlu digalakkan dan mulai dibangun oleh para pihak IT yang mereka miliki, agar para karyawan yang bekerja merasa data informasi mereka terjaga dari pihak yang tidak berhak untuk mengetahuinya.

III. METODE PENELITIAN

Adapun metode yang dilakukan dalam penelitian ini, sebagai berikut :

A. Studi Pustaka

Pada penelitian ini penyusun menggunakan pendekatan secara kualitatif. Dimana penulis meninjau literatur (library research) untuk memahami fenomena yang terjadi sebenarnya dengan mengumpulkan data menggunakan studi pustaka yang nantinya dapat membantu penulis dalam menyelesaikan proposal penelitian ini. Data ini dapat berupa bahan-bahan pendukung seperti teori-teori serta konsep yang digunakan dari literatur penelitian terdahulu.

B. Pengumpulan Data

Sebagai sarana bahan pendukung yang sangat berguna bagi penulis untuk mencari informasi atau mengumpulkan data yang diperlukan dalam penelitian ini, penulis menggunakan cara-cara pengumpulan data sebagai berikut:

1. Pengamatan (Observation)

Metode ini dilakukan dengan cara mengamati secara langsung mengenai objek penelitian yang bertujuan untuk mengumpulkan data kongkrit yang diperlukan dalam penulisan dan perancangan penelitian, selain itu untuk mendapatkan data-data penunjang, serta penulis melakukan pengamatan secara langsung pada kasus pengantaran makanan empek-empek lumpia di Kota Medan.

2. Wawancara (Interview)

Pada metode ini peneliti akan melakukan wawancara atau melakukan kegiatan tanya jawab dengan pengembang bisnis makanan rumahan empek-empek lumpia ini untuk nantinya akan dikembangkan sistem pengamanan data pembeli pada detail pembelian. Mengenai masalah yang diangkat dalam penelitian ini yang nantinya dianggap dapat memberikan keterangan yang akurat mengenai hal-hal yang berhubungan dengan masalah yang akan dibahas dalam penelitian ini.

C. Analisis Sistem dan Pengambilan Tindakan

Pada tahap ini penyusun akan melakukan analisis terhadap data apa saja yang diperlukan untuk merancang sistem yang nantinya digunakan untuk mengenkripsi dan mendekripsi data dari para user pembeli makanan empek-empek lumpia. Analisis ini bertujuan untuk mengambil tindakan terhadap permasalahan yang terjadi terhadap sistem informasi dalam proses menjaga keamanan serta pada saat pengambilan data.

D. Evaluasi

Pada tahap ini akan dilakukan penyimpulan terhadap penelitian yang sudah dilakukan.

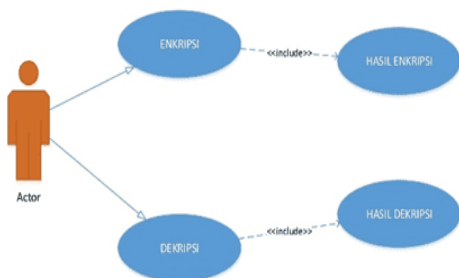
IV. HASIL DAN PEMBAHASAN

A. Pemodelan Rancangan Sistem

Adapun pemodelan yang digunakan untuk merancang sistem nantinya dengan menggunakan :

1. Use Case Diagram

Dalam kasus yang diambil dalam penelitian ini pada usaha kecil menengah yaitu pada usaha bisnis empek-empek lumpia yang ada di Kota Medan. Dengan menggunakan pemodelan use case digram untuk menjabarkan tentang fitur yang akan dipakai pada sistem. Use case diagram digunakan untuk menggambarkan hal-hal apa saja yang nantinya bisa digunakan oleh aktor/pengguna dari sistem. Pada gambar 1 akan ditunjukkan tampilan dari use case diagram pada sistem aplikasi kriptografi dalam penelitian ini.



Gambar 1. Use Case Diagram Sistem Kriptografi

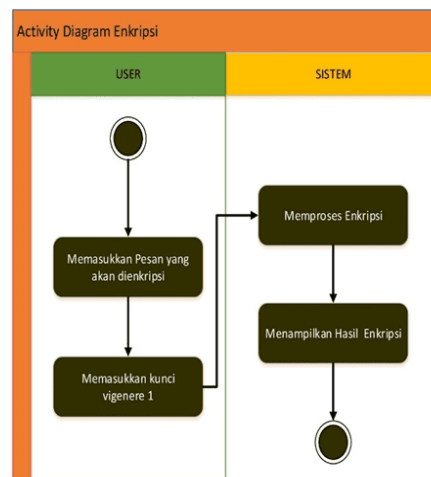
Pada Gambar 1 menampilkan use case diagram yang dibangun. Dijelaskan pada gambar tersebut bahwa seorang aktor yang nantinya seorang kurir pengirim barang berupa makanan itu akan diberikan kunci dari pegawai UKM empek-empek lumpia agar dapat mengakses sistem secara keseluruhan. Hal yang dapat dilakukan oleh aktor tersebut adalah dengan mengenkripsi dan dekripsi data berupa lembar tampilan alamat pengiriman beserta nama pembeli yang akan dituju. Setelah melakukan enkripsi atau dekripsi, sistem akan menampilkan hasil dari enkripsi atau dekripsi yang telah dilakukan oleh si aktor.

2. Activity Diagram

Activity diagram adalah model dari proses yang terjadi dalam sistem. Berikut adalah diagram aktivitas sistem kriptografi pada penelitian ini:

1. Activity Diagram Enkripsi

Activity Diagram enkripsi menjelaskan aktivitas dari aktor yang melakukan proses enkripsi data untuk metode vigenere cipher dengan alur seperti Gambar 2 berikut.

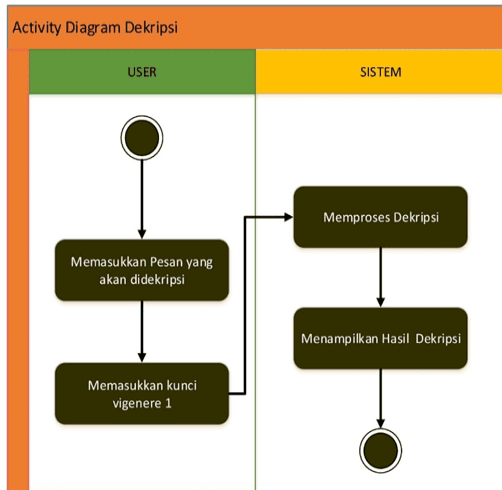


Gambar 2. Activity Diagram Enkripsi

Gambar 2 menampilkan activity diagram enkripsi, dari Gambar 2 user dapat memasukkan pesan yang akan dienkripsi kemudian ia akan menginputkan kunci vigenere yang diberikan oleh pegawai empek-empek lumpia nantinya. Setelah itu sistem akan memproses enkripsi dan menampilkan hasil enkripsinya berupa Penerima, no. hp, alamat, Pengirim, dan jumlah barang yang dikirimkan.

2. Activity Diagram Dekripsi

Activity Diagram dekripsi menjelaskan tentang activity diagram dari proses dekripsi. Gambaran yang ditampilkan pada proses dekripsi digambarkan pada Gambar 3 berikut.



Gambar 3. Activity Diagram Dekripsi

Gambar 3 menampilkan activity diagram dekripsi, dimana user atau kurir pengirim barang dapat menginputkan pesan yang ingin di dekripsi dan memasukkan kunci yang dibuat oleh pegawai empek-empek lumpia. Setelah itu sistem akan memprosesnya dan kemudian akan menampilkan hasil dari dekripsi sistem tersebut.

B. Metode Pengembangan Sistem

1. Metode Vigenere Cipher

Vigenere cipher adalah contoh terbaik dari sandi huruf majemuk “manual”. Algoritme ini diterbitkan oleh diplomat Prancis (dan kriptografer) Blaise de Vigenere pada abad ke-16, meskipun Giovan Batista Belaso pertama kali mendeskripsikannya pada tahun 1553 dalam bukunya La Cifra del Sig. vigenere cipher diterbitkan pada tahun 1586, tetapi algoritme tersebut tidak diketahui secara luas hingga 200 tahun kemudian, ketika penemu sandi tersebut menyebutnya Vigenere cipher. Sandi ini dipecahkan oleh Babbage dan Kaszysky pada pertengahan abad ke-19. Vigenere cipher digunakan oleh pasukan Konfederasi selama Perang Saudara Amerika.

Dalam vigenere cipher terdapat tabel dengan huruf alfabet disetiap baris bujursangkarnya, dimana huruf-huruf itu menyatakan ciphertext yang diperoleh dengan Caesar cipher yang mana jumlah pergeseran huruf dalam plaintext nya itu ditentukan oleh nilai numerik pada huruf kunci tersebut, yaitu (A = 0, B = 1, C = 2, D = 3, E = 4, ..., Z = 25).

Bujursangkar vigenere dipakai untuk memperoleh ciphertext dengan menggunakan kunci yang sebelumnya sudah ditentukan.

	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
A	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
B	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	A
C	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
D	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	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	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
H	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
I	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	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	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
T	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
U	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	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	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
Y	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
Z	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

Gambar 4. Bujur Sangkar Vigenere

Jika panjang kuncinya lebih pendek dari pada panjang plaintekstnya, maka kuncinya akan diproses untuk melakukan pengulangan penggunaannya (sistem periodik). Bila panjang kunci adalah m, maka periodenya dikatakan m.

2. Perancangan Antarmuka

Nantinya dari pihak penjualan akan membuat nota pengiriman sesuai detail dari pembeli termasuk didalamnya Pengirim, Penerima, No. HP pengirim dan Penerima, serta alamatnya. Hal inilah yang nantinya akan dijaga kerahasiaannya oleh pihak penjualan empek-empek lumpia untuk tidak mencetak bentuk fisik [6]berupa plaintekstnya secara langsung, sehingga pesan informasi yang disampaikan akan berbentuk

acak dan sulit dibaca oleh orang awam. Seperti pada gambar 5 berikut.[6]

Jasa Pengiriman Cepat Antar	
Penerima : No. HP : Alamat :	
Pengirim : No. HP : Alamat : Jumlah :	
Total Biaya :	Kode Pembayaran :

Gambar 5. Lembar Informasi Pengiriman

Setelah pihak toko memperoleh informasi dari pembeli yang melakukan transaksi, maka pihak toko perlu melakukan konfirmasi dengan pihak pembeli untuk nantinya data yang mereka kirimkan tidak dalam bentuk informasi umum yang bisa dibaca oleh semua orang seperti data pengiriman paket pada umumnya. Tentunya hal ini dilakukan untuk menjaga kerahasiaan informasi pembeli agar tidak di salah gunakan. Dengan penerapan ini maka dari pihak toko empek-empek

lumpia medan juga memberikan jaminan garansi agar barang sampai kepada pihak konsumennya secara langsung. Selanjutnya setelah pihak toko memperoleh orderan yang masuk maka mereka akan mencetak lembar pengiriman yang bentuk plaintextnya masih utuh karena belum dilakukan enkripsi data, seperti tampilan pada Gambar 6 berikut.

Jasa Pengiriman Cepat Antar	
Penerima : Suci	
Jasa Pengiriman Cepat Antar	
Penerima : Suci No. HP : 082165839878 Alamat : Medan Kota-Sumatera Utara, Medan, Jalan Gajah Mada	
Pengirim : Toko Empek-empek Lumpia Medan No. HP : 08135258477490 Alamat : Medan Sunggal-Sumatera Utara, Medan, Jalan Abadi Jumlah : 3 Pcs Barang : Empek-empek Lumpia Matang	
Total Biaya : Rp 150.000,00	Kode Pembayaran : ZA32BB90TU

Gambar 6. Lembar Informasi Pengiriman Sebelum di Enkrpsi

Setelah pihak toko melakukan enkripsi pada data informasi pembeli nantinya mereka akan memberikan konfirmasi berupa email ataupun telpon kepada pembeli bahwa lembar informasi pengirimannya nanti yang akan mereka terima bentuknya akan acak dan tidak dapat dibaca karena toko empek-empek lumpia ingin menjaga kerahasiaan dari data pembeli dan hanya pihak kurir saja yang dapat mengetahui isi didalam format lembar informasi pengiriman barang yang mereka antar. Berikut adalah contoh hasil enkripsi secara periodik pada Lembar Informasi Pengiriman Pembeli di Toko Empek-empek lumpia medan.

Plainteks : SUCI
 Kunci : ENAK

Setiap huruf plainteks akan dienkrpsi dengan setiap huruf kunci dibawahnya. Untuk mengerjakan enkripsi dengan vigènere cipher, lakukan pada bujursangkar vigènere sebagai berikut : tarik garis vertical dari huruf plainteks ke bawah, lalu tarik garis mendatar dari huruf kunci ke kanan. Perpotongan dari kedua garis tersbut menyatakan huruf cipherteksnya.

Plainteks : SUCI
 Kunci : ENAK
 Cipherteks : WHCS

Plainteks	T	O	K	O	E	M	P	E
	K	E	M	P	E	K	L	U
	M	P	I	A	M	E	D	A
	N							
Kunci	E	N	A	K	E	N	A	K
	E	N	A	K	E	N	A	K
	E	N	A	K	E	N	A	K
	E							
Cipherteks	X	B	K	Y	I	Z	P	O
	O	R	M	Z	I	X	A	E
	Q	C	I	K	Q	R	D	K
	R							

Plainteks	M	E	D	A	N		S	U	N	
	G	G	A	L			S	U	M	A
	T	E	R	A			U	T	A	R
	A		M	E	D		A	N		J
	A	L	A	N			A	B	A	D
	I									
Kunci	E	N	A	K	E		N	A	K	
	E	N	A	K			E	N	A	K
	E	N	A	K			E	N	A	K
	E		N	A	K		E	N		A
	K	E	N	A			K	E	N	A
	K									
Cipherteks	Q	R	D	K	R		F	U	X	
	K	T	A	U			W	H	M	K
	X	R	R	K			Y	G	A	B
	E		Z	E	N		E	A		J
	K	P	N	N			K	F	N	D
	S									

Dari proses enkripsi pada tabel diatas maka nantinya hasil tampilan dari Lembar Informasi Pengiriman akan keluar seperti tampilan pada Gambar 7 berikut.



The screenshot shows a shipping form with the following details:

- Logo Toko:** Jasa Pengiriman Cepat Antar
- Penerima:** WHCS
- No. HP:** 082165839878
- Alamat:** QRDKR XODE-FUWEGEBE HTKVN, MOGNN, NNLKR TATEU MCGN
- Pengirim:** XBKY IZPOO-RMZIX AEQCIK QRDKR
- No. HP:** 08135258477490
- Alamat:** QRDKR FUXKTAU-WHMKXRRK YGABE, ZENEA, JKPNN KFNSD
- Jumlah:** 3 Pcs Barang: Empek-empek Lumpia Matang
- Total Biaya:** Rp 150.000,00
- Kode Pembayaran:** ZA32BB90TU

Gambar 7. Lembar Informasi Pengiriman Setelah di Enkripsi

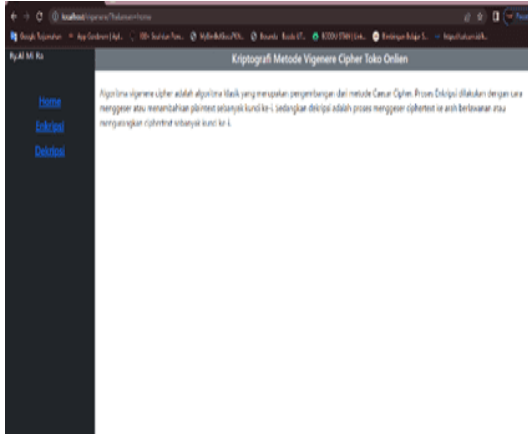
C. Implementasi Antarmuka (*Interface*)

Antarmuka pada aplikasi ini di implementasikan dengan perangkat Localhost yang dionlinekan dengan XAMPP. Implementasi antarmuka tiap-tiap menu dan diujicobakan pada tahap pengujian. Berikut ini adalah implementasi antarmuka dari aplikasi Enkripsi Vigenere Cipher.

1. Tampilan Menu Utama

Pada tampilan menu utama, terdapat pilihan menu yaitu Home yang menampilkan penjelasan singkat mengenai pengertian Vigenere Cipher, kemudian selanjutnya ada menu Enkripsi yang nantinya digunakan oleh User/Pegawai Empek-empek lumpia untuk mengenkripsi pesan dari pembeli berupa Nama, Alamat, Dll. Kemudian yang terakhir adalah menu Dekripsi yang fungsinya untuk mengembalikan pesan cipherteks menjadi plainteks untuk memudahkan proses pengantaran barang oleh kurir yang nantinya pihak pegawai toko akan memberikan kunci kepada pihak kurir. Berikut ini adalah tampilan menu utama pada Gambar 8.

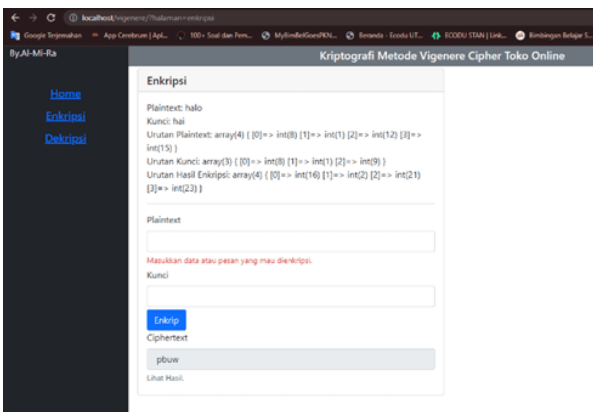
Plainteks	M	E	D	A	N		K	O	T	
	A		S	U	M		A	T	E	R
	A		U	T	A		R	A		M
	E	D	A	N						
Kunci	E	N	A	K	E		N	A	K	
	E		N	A	K		E	N	A	K
	E		N	A	K		E	N		A
	K	E	N	A						
Cipherteks	Q	R	D	K	R		X	O	D	
	E		F	U	W		E	G	E	B
	E		H	T	K		V	N		M
	O	G	N	N						



Gambar 8. Tampilan Halaman Depan

2. Tampilan Menu Enkripsi

Pada tampilan menu enkripsi memuat tabel plainteks yang nantinya digunakan untuk memasukkan teks asli dan akan diubah menjadi bentuk cipherteks dengan kunci yang diberikan. Seperti pada Gambar 9 berikut.

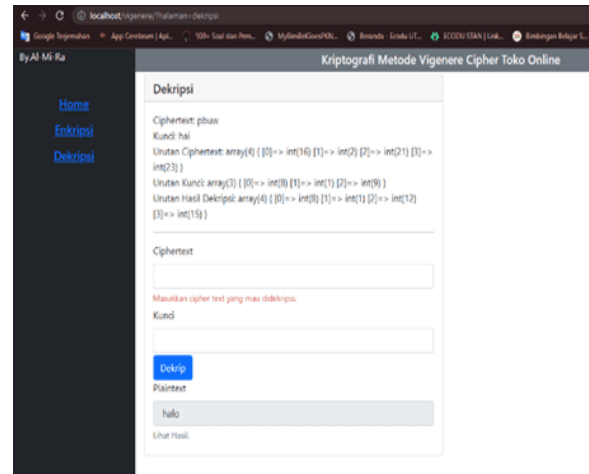


Gambar 9. Tampilan Halaman Enkripsi Teks

3. Tampilan Menu Dekripsi

Pada tampilan menu dekripsi ini memuat tabel chiperteks yang nantinya digunakan oleh kurir/user untuk mengubah cipherteks menjadi plainteks pesan kedalam bentuk aslinya. Tujuannya agar supaya kurir dapat dengan mudah mengetahui detail informasi dari pembeli. Namun disini pihak toko hanya memberikan bukti

screenshoot dari tampilan hasil dekripsi kepada kurir agar informasi tetap terjaga dan juga untuk aplikasi ini belum bisa diakses ataupun dionlinekan sehingga masih menggunakan XAMPP sebagai hosting untuk menjalankan programnya. Berikut adalah hasil tampilan halaman dekripsi pada Gambar 10,



Gambar 10. Tampilan Halaman Dekripsi Teks

V. KESIMPULAN

Dari hasil pengujian yang telah dilakukan oleh penyusun mengenai kegunaan algoritma kriptografi dengan metode vigenere cipher berbasis web, maka dapat diambil kesimpulan sebagai berikut:

1. Dalam pembuatan Aplikasi Kriptografi Metode Vigenere Cipher pada Toko Online telah berhasil dijalankan dengan baik.
2. Dari hasil pengujian terhadap aplikasi tersebut diperoleh kesimpulan bahwa fungsi-fungsi yang terdapat didalam halaman web berjalan dengan baik dan sesuai dengan yang diharapkan, sehingga layak digunakan oleh pengguna atau end user.
3. Terdapat kekurangan dari aplikasi ini dimana Aplikasi Kriptografi Metode Vigenere Cipher pada Toko Online ini belum dapat di online kan, dikarenakan ia dapat berjalan dengan bantuan XAMPP sebagai localhostnya. Sehingga jika pihak kurir hanya mendapatkan

tampilan berupa foto/screenshot dari pihak toko empek-empek lumpia. Jadi yang mengatur semua pemrograman pada aplikasi ini berdasar pada pihak Toko Empek-empek Lumpia di Kota Medan.

UCAPAN TERIMAKASIH

Alhamdulillah, puji syukur penulis panjatkan kehadiran Allah SWT karena atas limpahan rahmat dan karunia-nya sehingga jurnal ini dapat terselesaikan. Tak lupa pula penulis mengirimkan salam dan shalawat kepada Nabi Besar Muhammad SAW yang telah membawa umat islam ke jalan yang diridhoi Allah SWT.

Jurnal yang berjudul “Penggunaan Algoritma Vigenere Cipher Sebagai Keamanan Sistem pada Usaha Kecil Menengah” merupakan tugas mata kuliah Keamanan Aset Informasi. Terwujudnya jurnal ini tidak lepas dari partisipasi dan bantuan berbagai pihak. Oleh karena itu, penulis ingin menyampaikan terima kasih yang seluas-luasnya kepada:

1. Ibu Raissa Amanda Puteri, S.Kom, M.Ti. Selaku dosen pengampu pada mata kuliah keamanan aset informasi yang telah mengembangkan tugasnya sebagai dosen untuk memberikan masukan, bimbingan dan motivasi yang membangun kepada penulis hingga jurnal ini terselesaikan dengan baik.
2. Kepada ibu Mardiah Nasution, S.Kom, M.Kom. sebagai dosen pembimbing untuk membantu memberikan arahan, informasi, dan masukkan motivasi.

DAFTAR PUSTAKA

- [1] E. S. Han and A. goleman, daniel; boyatzis, Richard; Mckee, “Peranan Kriptografi Sebagai Keamanan Sistem Informasi Pada Usaha Kecil Dan Menengah,” *J. Chem. Inf. Model.*, vol. 53, no. 9, p. 2, 2019.
- [2] N. A. Hamdani and G. A. Fatah, “Perencanaan Strategis Sistem Informasi pada Usaha Kecil dan Menengah,” *J. Petik*, vol. 4, no. 2, pp. 167–172, 2018, doi: 10.31980/jpetik.v4i2.382.
- [3] B. Iskandar and A. U. Hamdani, “Jasa Pengiriman Barang Studi Kasus : PT. XYZ,” *STMIK AMIKOM Yogyakarta*, vol. 1, no. 2, pp. 67–72, 2017.
- [4] I. W. Utomo, R. Latifah, and R. D. Risanty, “Aplikasi Kriptografi Berbasis Android Menggunakan Algoritma Caesar Cipher & Vigenere Cipher,” *J. Sist. Informasi, Teknol. Inf. dan Komput.*, vol. 9, no. 2, pp. 142–149, 2019.
- [5] V. C. Hardita and E. W. Sholeha, “Penerapan Kombinasi Metode Vigenere Cipher, Caesar Cipher Dan Simbol Baca Dalam Mengamankan Pesan,” *J. SAINTEKOM*, vol. 11, no. 1, pp. 34–43, 2021, doi: 10.33020/saintekom.v11i1.202. “1625-277-3303-1-10-20210508.”
- [6]