

Analisis Tambahan Keamanan Password Menggunakan Algoritma Vigenere Cipher Berdasarkan Kunci Dan Tabula Recta untuk Keamanan Data Koperasi Ara Cahayani Gayo

Sandi Refinda¹, Pristiwati Fitriani²

¹²Program Studi Teknik Informatika, STMIK Logika, Medan, Indonesia

Email: ¹1703R002@logika.ac.id, ²pristiwatifitriani@logika.ac.id

Email Penulis Korespondensi: ¹1703R002@logika.ac.id

Abstrak—Algoritma klasik substitusi yang masih banyak digunakan untuk penyandian pesan sekarang yaitu algoritma Vigenere cipher. Vigenere cipher merupakan salah satu metode peng-enkripsi-an teks alphabet menggunakan seri lain dari Caesar cipher yang berdasarkan suatu kunci. Pada skripsi ini penulis mencoba menerapkan algoritma vigenere cipher untuk tambahan keamanan password. Penelitian ini bertujuan untuk menerapkan algoritma vigenere cipher untuk mengamankan sebuah password didalam database, perancangan sistem untuk mendapatkan output dilakukan dengan enkripsi password pada database dengan algoritma Vigenere cipher. Dengan menerapkan algoritma ini diharapkan dapat Mengamankan password pada sebuah database dengan menggunakan teknik penyandian algoritma vigenere cipher dan Aplikasi yang dirancang dapat melakukan penyandian password dengan algoritma Vigenere cipher yang memiliki kunci telah terenkripsi sehingga dapat diterapkan dalam file teks yang ada pada database.

Kata Kunci: Tambahan Keamanan; Password; Algoritma Vigenere Cipher;

Abstract—The classic substitution algorithm that is still widely used for encoding messages today is the Vigenere cipher algorithm. Vigenere cipher is a method of encrypting alphabetic text using another series of Caesar ciphers based on a key. In this thesis the author tries to apply the vigenere cipher algorithm for additional password security. This study aims to apply the vigenere cipher algorithm to secure a password in the database, the system design to get the output is done by encrypting the password in the database with the Vigenere cipher algorithm. By applying this algorithm, it is expected to be able to secure passwords in a database using the encryption technique of the Vigenere cipher algorithm and the designed application can encode passwords with the Vigenere cipher algorithm which has an encrypted key so that it can be applied to a text file in the database.

Keywords: Additional Security; Password; Vigenere Cipher Algorithm;

1. PENDAHULUAN

Koperasi Ara Cahayani Gayo (ACG) berdiri pada 13 Maret oleh 25 pengusaha kopi dan petani dari Kabupaten Bener Meriah dan Aceh Tengah, Provinsi Aceh. Koperasi ACG semula beralamat di Kampung Karang Rejo, Kecamatan Bukit, Kabupaten Bener Meriah, kemudian berpindah alamat ke Dusun Cubung Jaya, Kampung Tawar Bengi, Kecamatan Bandar.

Salah satu metode pengamanan sistem informasi yang umum diketahui oleh banyak orang adalah password. Tanpa disadari password mempunyai peranan penting dalam mengamankan informasi-informasi yang sifatnya pribadi (*confidential*). Pada beberapa aplikasi yang berhubungan dengan piranti lunak, seperti HP, kartu ATM, dll. Ada juga sistem pengamanannya yang fungsinya mirip dengan password, biasa dikenal sebagai Kode PIN. Walaupun hanya terdiri dari angka, namun kegunaannya sama seperti password, yaitu untuk mengaman-kan informasi. Informasi yang disimpan tersebut biasanya sudah berbentuk digital[1].

Keamanan password adalah mengamankan sebuah password yang tersimpan di dalam *database*, Password perlu diamankan karena jika password diketahui oleh pihak yang tidak berkepentingan atau yang tidak berhak maka data penting dan lainnya akan dicuri. Metode tambahan keamanan password untuk pengguna perlu dijelaskan yang aman bahkan jika penyusup dapat membaca data sistem, dan dapat mengutak-atik atau menguping komunikasi antara pengguna dan sistem. Password digunakan sebagai salah satu otentikasi yang diketahui oleh pemakai[2]. Otentikasi adalah cara masuk ke dalam sistem berdasarkan *username* dan password. Untuk itu, biasanya sebelum kita masuk atau ingin membuka sesuatu yang bersifat pribadi, alangkah baiknya jika ada otentikasi dahulu. Hal-hal yang biasanya menggunakan password adalah *login* untuk masuk ke sebuah aplikasi, email, *messenger*, *operating system*, *database*[3], dokumen[4], USB dan hal-hal lain yang memiliki informasi bernilai tinggi. Oleh karena itu, untuk mendapatkan informasi yang bernilai tersebut banyak orang melakukan berbagai macam cara untuk menembus password, hal ini sering dinamakan *hacking*. Semakin kuat sistem keamanan informasi yang digunakan, semakin canggih pula teknik *hacking* yang digunakan. Salah satunya adalah dengan cara *Brute Force Attack*. Dengan cara ini, dapat diestimasi berapa lama waktu yang dibutuhkan untuk dapat password yang diinginkan.

Semakin panjang dan bervariasi password yang digunakan, semakin lama waktu yang dibutuhkan untuk memperolehnya. Untuk menghindari hal tersebut terjadi, para pengguna password seharusnya mengerti kebijakan password (*policy*) dan mengetahui password seperti apa yang dapat dikatakan baik dan kuat, karena password digunakan untuk mengamankan suatu informasi. Jadi, dapat dikatakan bahwa password sudah menjadi bagian dalam kehidupan kita[5]. Diharapkan untuk ke depannya, pengamanan informasi yang sifatnya pribadi tersebut dapat lebih terjaga dan memiliki otentikasi yang kuat dan tahan terhadap gangguan. Masyarakat pun dapat lebih peduli terhadap perkembangan sistem pengamanan informasi dan akan terus memperbaikinya. Seberapa jauh orang mengerti penggunaan password yang baik, seberapa penting informasi yang ingin diamankan, dan hal-hal apa saja yang diproteksi dengan menggunakan password. Salah satu agar tidak terjadi pencurian data password penulis meneliti algoritma vigenere cipher untuk menyandikan password tersebut di dalam sebuah database[6].

Sehingga data yang ada di dalam database berbeda dengan data password sesungguhnya, sekalipun adanya sebuah pencurian data maka pihak yang tidak berkepentingan tak akan dapat mengetahui password secara langsung. Dalam penyandian tersebut menggunakan fungsi kunci dan tabula recta. Tabula recta adalah tabel abjad persegi, yang setiap barisnya dibuat dengan menggeser yang sebelumnya ke kiri.

2. METODOLOGI PENELITIAN

Adapun metodologi penelitian yang digunakan adalah dengan memadukan dan menunjang kepada tujuan dan sasaran studi. Untuk lebih jelasnya diuraikan secara berikut :

2.1. Metode Pengamatan (Observasi)

Pada tahap ini penulis mengkaji metode-metode yang penulis gunakan dalam penulisan skripsi ini yaitu metode algoritma vigenere cipher. Pengkajian juga akan dikembangkan kepada kemampuan dan juga karakteristik dari algoritma vigenere cipher dalam kemampuannya mengamankan data password pada proses enkripsi dan deskripsi data.

2.1.1. Kriptografi

Kriptografi adalah cabang ilmu yang membahas mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi[7]. Pada dasarnya kriptografi sendiri sudah digunakan jauh sebelum konsep komputer dikenal[8][9]. Kriptografi, selama berabad-abad, telah menjadi seni yang dipraktikkan oleh banyak orang yang telah merancang teknik ad hoc untuk memenuhi beberapa persyaratan keamanan informasi[10]. Dua puluh tahun terakhir telah menjadi masa transisi bagi kriptografi dimana sebelumnya kriptografi hanyalah sebuah form atau bentuk dan sekarang telah pindah dari seni menjadi sebuah cabang ilmu. Sekarang ada beberapa konferensi ilmiah internasional yang ditujukan khusus untuk kriptografi dan juga organisasi ilmiah internasional, International Association for Cryptologic Research (IACR), yang bertujuan untuk mendorong penelitian di area tersebut. Dalam jaman dimana virus dan hacker atau penyadapan elektronik dan penipuan elektronik merupakan sesuatu yang wajar dan sering terjadi, maka tidaklah salah kalau keamanan adalah yang faktor terpenting dalam sebuah sistem yang terkoneksi dengan internet ataupun jaringan lokal. Didalam sebuah metode kriptografi ada dua proses yang merupakan fitur utama dari metode kriptografi manapun. Berikut penjelasan dari proses-proses tersebut.

2.1.2. Enkripsi

Proses enkripsi sendiri adalah sebuah perombakan suatu data menjadi bentuk data yang sama sekali tidak dapat dikaitkan dengan data awal sebelum di enkripsi[11][12]. Proses enkripsi biasanya merupakan sebuah operasi yang terikat dengan algoritma awal dari sebuah kriptografi dan tidak akan keluar dari algoritma dasar, jadi berdasarkan penjelasan diatas maka bisa diambil kesimpulan mengenai proses enkripsi yaitu sebuah proses pengamanan data yang digunakan untuk merubah entiti awal dari sebuah data menjadi bentuk yang sama sekali tidak merepresentasikan bentuk awal dari data sebelum data di enkripsi[13].

2.1.3. Deskripsi

fungsi dekripsi yang mengembalikan data yang telah dienkripsi kembali ke bentuk awal sebelum proses enkripsi adalah fitur yang harus dimiliki oleh semua metode kriptografi[14]. Pengembalian bentuk data ini dilakukan untuk mengembalikan kemampuan data untuk menampilkan kembali informasi yang terdapat didalamnya. Jadi berdasarkan penjelasan diatas dapat disimpulkan bahwa dekripsi adalah proses pengembalian data ke bentuk awal sebelum dienkripsi untuk mengembalikan *read ability* (sifat data untuk dapat dibaca atau pengekstrakan informasi) dari data tersebut menggunakan kebalikan proses dari enkripsi.

2.1.4. Algoritma Vigenere Cipher dan Tabula Recta

Di kriptografi, tabula recta adalah tabel abjad persegi[15], yang setiap barisnya dibuat dengan menggeser baris sebelumnya ke kiri, tabel ini yang diterapkan dalam proses pembentukan enkripsi dan deskripsi pada vigenere cipher. Istilah ini ditemukan oleh penulis dan biarawan Jerman Johannes Trithemius pada 1508, dan digunakan dalam miliknya Sandi trithemius. Sandi Trithemius diterbitkan oleh Johannes Trithemius dalam bukunya Polygraphia, yang dianggap sebagai karya terbitan pertama kriptologi[16]. Di dalam tubuh Tabula Recta, setiap alfabet bergeser satu huruf ke kiri dari huruf di atasnya. Ini membentuk 26 baris alfabet bergeser, diakhiri dengan alfabet yang dimulai dengan Z (seperti yang ditunjukkan pada gambar). Terpisah dari 26 huruf ini adalah baris tajuk di bagian atas dan kolom tajuk di sebelah kiri, masing-masing berisi huruf-huruf alfabet dalam urutan AZ.

2.2. Analisa dan Perancangan Sistem

Pada tahap ini dilakukan analisa terhadap metode algoritma vigenere cipher. Analisa juga akan dikembangkan pada inti sari proses enkripsi penjadwalan kunci rotasi enkripsi. Selanjutnya mengembangkan sebuah aplikasi menggunakan Visual Basic dengan platform ini dianggap sebagai platform yang tepat dan mampu mengolah data keamanan password dan menerima implementasi algoritma kriptografi vigenere cipher.

2.3. Pengujian Aplikasi

Pada tahap ini dilakukan analisa terhadap metode algoritma vigenere cipher. Analisa juga akan dikembangkan pada intisari proses enkripsi penjadwalan kunci rotasi enkripsi. Selanjutnya mengembangkan sebuah aplikasi

menggunakan Visual Basic dimana platform ini dianggap sebagai platform yang tepat dan mampu mengolah data keamanan password dan menerima implementasi algoritma kriptografi vigenere cipher.

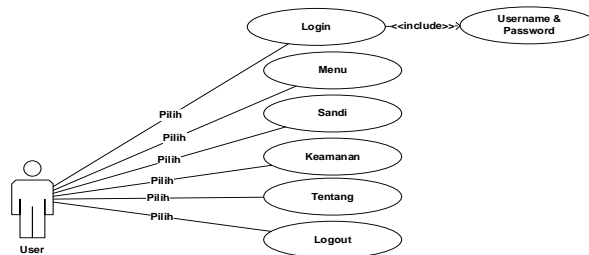
3. HASIL DAN PEMBAHASAN

3.1 Unified Modeling Language (UML)

Proses perancangan aplikasi menggunakan model *Unified Modeling Language* (UML) yang terdiri dari : *UseCase Diagram*, *SequenceDiagram*, *Activity Diagram* dan *Class Diagram*.

3.2 Use Case Diagram

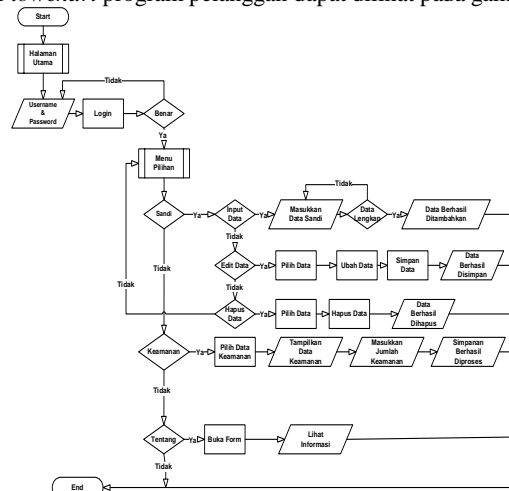
Use Case diagram digunakan untuk menggambarkan interaksi apa saja yang bisa dilakukan *user* kepada aplikasi yang akan dibangun. *UseCase diagram* dapat dilihat pada gambar



Gambar 1. Use Case Diagram

3.3 Flowchart Program

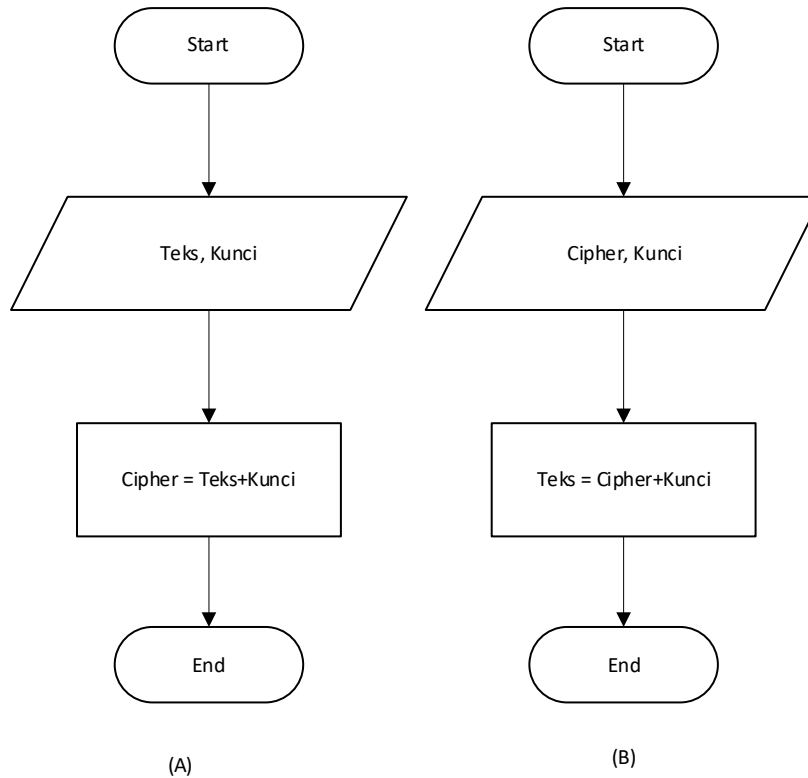
Berikut ini adalah gambar dari *flowchart program* dari sistem informasi koperasi berbasis visual studio pada koperasi ara cahayani gayo yang telah di bangun. *Flowchart* ini menggambarkan alur dari fungsi-fungsi yang dapat dilakukan admin pada aplikasi yang telah dibangun. *Flowchart program* pelanggan dapat dilihat pada gambar1. Flowchar Software



Gambar 2. Flowchart Program

3.4. Algoritma Vigenere Cipher

Algoritma *vigenere cipher* bekerja dengan menyandikan teks asli dengan menambah teks kunci menggunakan tabula recta. Sebaliknya mengembalikan teks asli dengan mengurangi teks kunci dengan teks sandi menggunakan tabula recta. Misal kata “Sandira” dikunci dengan “rafinda” maka akan menjadi “Jaslv”. Semua kata sandi nantinya akan tersimpan ke dalam *database* dan diamankan dalam *database*.



Gambar 3. Enkripsi dan Dekripsi Algoritma Vigenere Cipher

3.4.2 Perhitungan Algoritma Vigenere Cipher

jika plain adalah ‘Koperasi Ara Cahayani Gayo’ dan kunci adalah ‘Sandi Refinda’ maka proses enkripsi yang terjadi adalah sebagai berikut:

Plain : Koperasi Ara Cahayani Gayo

Key : Sandi Refinda

Cipher: Cochzrwn Ied Cshnbiem Llr

Pada contoh diatas kata teks yang ingin di kunci adalah “Koperasi Ara Cahayani Gayo”, kemudian kunci yang digunakan untuk proses keamanan dengan algoritma vigenere cipher adalah “Sandi Refinda”. Perhitungan pertama kali “K” disandikan dengan “S”. P_i dari “K” adalah 11 dan K_i dari “S” adalah 19. Jika dilihat dari perhitungan menggunakan tabula recta maka hasil yang didapat adalah “C” atau dengan nilai 3.

	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. Proses Enkripsi “K” dengan “S” Menghasilkan “C”

Adapun rumus dari enkripsi algoritma vigenere cipher seperti yaitu menggunakan persamaan, Sehingga dengan perhitungan sebagai berikut:

$$\begin{aligned}
 C_i &= (P_i + K_i) \bmod 27 \\
 &= (11 + 19) \bmod 27 \\
 &= 30 \bmod 27 = 3.
 \end{aligned}$$

Penulis menggunakan mod 27 karna nilai abjad 26 harus ditambah “spasi” sehingga menghasilkan 26 + 1 atau 27. Kemudian 3 jika dikembalikan ke nilai tabula recta akan menghasilkan nilai “C” begitu selanjutnya pada perhitungan algoritma vigenere cipher untuk enkripsi sebuah teks.

Selanjutnya untuk dekripsi dari sebuah *cipherteks* ke *plainteks* dilakukan dengan rumus $P_i = (C_i - K_i) + 27$. lebih jelas seperti berikut:

$$\begin{aligned} P_i &= (C_i - K_i) + 27 \\ &= (3 - 19) + 27 \\ &= (-16) + 26 = 11 \end{aligned}$$

Nilai 11 jika dilihat dari tabel Tabula Recta akan mengembalikan nilai ke “K”. begitu seterusnya untuk proses dekripsi dengan algoritma vigenere cipher.

Dalam melaksanakan implementasi dan pengujian sistem perangkat keras (hardware) dan perangkat lunak (software) yang digunakan adalah sebagai berikut :

1. Laptop



Gambar 5. Spesifikasi laptop yang digunakan

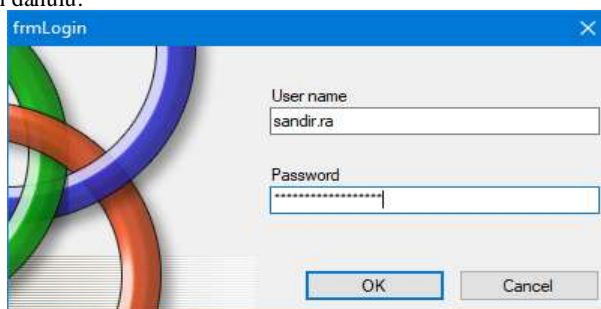
2. Perangkat Lunak (*Software*)
 - a. Sistem Operasi *Windows 10*
 - b. *DatabaseXampp*
 - c. *MicrosoftVisualStudio 2020*

3.5 Demontrasi Sistem

Demonstrasi program merupakan suatu langkah yang dilakukan untuk memperlihatkan atau menampilkan tampilan sebuah hasil dari data yang ada, dimana dalam hal ini data tersebut sudah dapat dijalankan menjadi sebuah *website*. Adapun beberapa tampilan yang dibuat oleh peneliti dalam tampilan penelitian ini. Tampilan serial monitor, Beriku adalah gambar dari tampilan – tampilan tersebut:

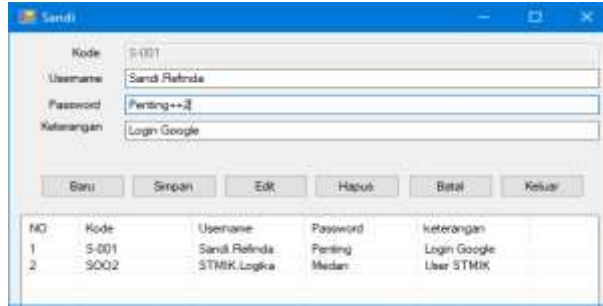
1. Tampilan From login

Halaman login merupakan halaman awal yang muncul saat user menggunakan aplikasi. Pada halaman ini, admin diharuskan untuk melakukan login terlebih dahulu.



Gambar 6. Tampilan form login

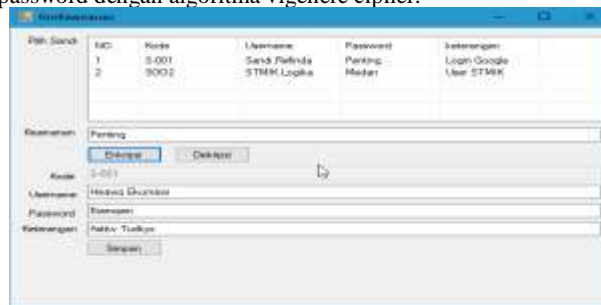
2. Tampilan From Sandi
Pada halaman ini, user dapat melakukan pengolahan data sandi.



Gambar 7. Tampilan form sandi

3. Tampilan From Enkripsi

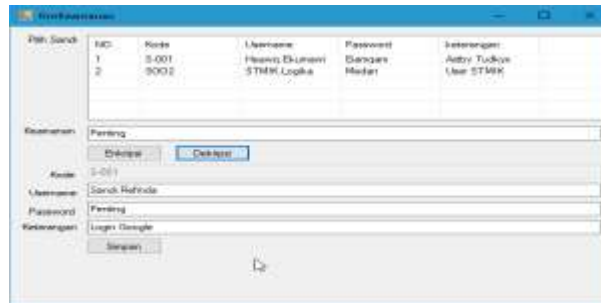
Form Enkripsi berguna untuk menyandikan file teks atau record data password dan lain-lain. Pada halaman ini, user dapat melakukan proses keamanan password dengan algoritma vigenere cipher.



Gambar 8. Tampilan form Enkripsi

4. Tampilan From Dekripsi

Form dekripsi merupakan proses kebalikan enkripsi, dari ciphertext diubah kembali ke plaintext dengan menggunakan fungsi matematis dan key atau kunci sebelumnya yang digunakan saat enkripsi



Gambar 9. Tampilan form Dekripsi

5. Tampilan From Tentang

Pada form ini, user dapat melihat pembuat dan info tentang pembuat aplikasi.



Gambar 10. Tampilan form Dekripsi

4. KESIMPULAN

Kesimpulan pada penelitian analisa tambahan keamanan password menggunakan algoritma vigenere cipher berdasarkan kunci dan tabula, Algoritma *viginerecipher* melakukan proses penyandian pada setiap *record* dari tabel *database* yang telah dipilih sebanyak sekali kali (secara sederhana) dengan nilai *substitusi* menerapkan tabula recta di setiap karakter *record* tergantung pada nilai hasil perkalian kunci dengan bilangan faktor pengali yang terbentuk. Kemudian, hasil akhir yang digunakan adalah hasil proses pengamanan dengan kunci hasilnya tidak memiliki kemiripan dengan *record* asli. Pembentukan kunci berdasarkan keputusan pengguna. Perlu diperhatikan bahwa kunci tidak boleh lupa.

UCAPAN TERIMAKASIH

Terima kasih disampaikan kepada Editorial Jurnal Informatika Logika, telah memeriksa dan menerbitkan penelitian ini, Ibu Pristiwati Fitriani yang selalu memberi motivasi untuk perkembangan. Penelitian ini merupakan luaran dari skripsi saat mengambil gelar sarjana ilmu komputer program studi teknik informatika yang di selesaikan di Medan, 18 November 2021.

REFERENCES

- [1] M. Es-sabry *et al.*, "An efficient 32-bit color image encryption technique using multiple chaotic maps and advanced ciphers," *Egypt. Informatics J.*, vol. 25, p. 100449, 2024.
- [2] D. K. Maulana, S. M. Tanjung, R. S. Ritonga, and A. Ikhwan, "Penerapan Kriptografi Vigenere Cipher Pada Kekuatan Kata Sandi," *J. Sains dan Teknol.*, vol. 3, no. 1, pp. 47–52, 2023.
- [3] T. S. Alasi, "Penerapan Algoritma Algoritma Boyer Moore untuk Penyaringan Pesan dan Algoritma Hill Cipher dalam Keamanan Pesan Teks Berbasis Web Chat," *KAKIFIKOM Kumpul. Artik. Karya Ilm. Fak. Ilmu Komput.*, vol. 1, no. 2, pp. 73–79, 2019.
- [4] T. S. Alasi, J. Sembiring, R. Wanto, and V. H. Sitanggang, "Algoritma Blowfish Untuk Pengaman Pesan Teks," *J. Armada Inform.*, vol. 3, no. 1, 2019.
- [5] D. Purnamasari, D. Herlinudinkhaji, A. K. Dewi, and M. Z. Mauludin, "Foveal Avascular Zone Image Encryption using Pixel Scrambling Combination Technique for Medical Image Security," *J. INFOTEL*, vol. 16, no. 1, 2024.
- [6] I. Stepheng, C. A. Sari, E. H. Rachmawanto, and F. O. Isinkaye, "A Combination of Vigenere Cipher and Advanced Encryption Standard for Image Security," *Adv. Sustain. Sci. Eng. Technol.*, vol. 5, no. 3, p. 230305, 2023.
- [7] S. M. RAFI, Y. PVENKATASUBRAMANYAM, and A. SWATHI, "Deep Learning for Encryption-Decryption Techniques for Cloud Data Confidentiality".
- [8] E. Ndruru and T. S. Alasi, "Algoritma Tripple Des Dalam Pengamanan File Dengan Usb Flashdisk," *J. Inf. Komput. Log.*, vol. 2, no. 4, 2022.
- [9] R. Banoth and R. Regar, *Classical and Modern Cryptography for Beginners*. Springer Nature, 2023.
- [10] A. Singh, K. B. Sivangi, and A. N. Tuntu, "Machine Learning and Cryptanalysis: An In-Depth Exploration of Current Practices and Future Potential," *J. Comput. Theor. Appl.*, vol. 2, no. 1, pp. 27–42, 2024.
- [11] T. S. Alasi, R. Wanto, and V. H. Sitanggang, "Implementasi Kriptografi Algoritma Idea Pada Keamanan Data Teks Berbasis Android," *J. Inf. Komput. Log.*, vol. 2, no. 1, 2020.
- [12] C. Zhang and B. Du, "A fast piecewise image encryption scheme combining NC1DNSM and P-Box," *Integration*, vol. 88, pp. 328–342, 2023.
- [13] P. Fitriani and T. S. Alasi, "Pengamanan Pesan Dengan Teknik Steganografi Menggunakan Metode Least Significant Bit Pada Citra Digital," *J. Inf. Komput. Log.*, vol. 1, no. 2, 2019.
- [14] T. S. Alasi, "Algoritma Hill Cipher Untuk Kebenaran Informasi pada Gambar dalam Media Sosial," *J. Inf. Komput. Log.*, vol. 2, no. 2, 2021.
- [15] S. Garg, V. Jindal, H. Bhatia, R. Johari, and S. Gupta, "Community oriented socio-behavioural PentaPlicative Cipher Technique," *Egypt. Informatics J.*, vol. 24, no. 1, pp. 71–80, 2023.
- [16] T. S. Alasi and A. T. A. A. Siahaan, "Algoritma Vigenere Cipher Untuk Penyandian Record Informasi Pada Database," *J. Inf. Komput. Log.*, vol. 1, no. 4, 2020.