SKANIKA: Sistem Komputer dan Teknik Informatika
Volume 5, Nomor 2, Juli 2022, Halaman 240-254 ISSN:2721-4788

Enkripsi Database Sistem Informasi Helpdesk Dengan Algoritme Kriptografi AES-128 dan Vigenere Chiper

Muhammad Apit Ruswandi[1], Windarto[2]
[1,2]Fakultas Teknologi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta, Indonesia
E-mail: [1]1711520088@student.budiluhur.ac.id, [2]windarto@budiluhur.ac.id*
(* : corresponding author)

Abstrak

Teknologi informasi mempunyai manfaat untuk membantu dan memudahkan manusia dalam melakukan segala hal dalam berbagi komunikasi. Pada masa pandemi, PT. Royal Audrey Megah salah satu perusahaan yang menerapkan program *Work From Home* (WFH). Untuk mempertahankan kualitas *support* yang baik dalam layanan *hosting,* divisi *Customer Service* dan *IT Support* dapat mengakses aplikasi *helpdesk* yang terhubung ke *internet*. Aplikasi yang dapat diakes dari *internet* membawa banyak manfaat bagi penggunanya, tak luput juga dengan dampak negatifnya. Mengingat hal tersebut, maka data menjadi aset yang sangat berharga dan harus dilindungi. Pegamanan data bisa dilakukan salah satunya dengan cara mengamankan dari sisi *database*. Pengamanan *database* dapat dilakukan dengan menerapkan kriptografi simetris *Advance Encryption Standard* (AES) dan *Vigenere*. Tujuan dari penelitian ini adalah untuk meminimalisir terjadinya kebocoran *database* dan penyalahgunaan oleh pihak-pihak yang tidak bertanggung jawab. Teknik kriptografi yang digunakan adalah metode *Advanced Encryption Standard* (AES) dan *vigenere*. Dari hasil implementasi diperoleh kesimpulan bahwa aplikasi mampu mengamankan data dalam database yang dienkripsi sehingga dapat meminimalisir terjadinya penyalahgunaan atau manipulasi data oleh orang-orang yang tidak memiliki wewenang atas data tersebut.

Kata kunci: Kriptografi, Algoritme AES-128, Vigenere, Database

Abstract

Information technology has benefits to help and make it easier for humans to do everything in sharing communication. During the pandemic, PT. Royal Audrey Megah is one of the companies implementing Work From Home (WFH). To maintain a good quality of support in hosting services, the Customer Service and IT Support division can access helpdesk application through the internet connection. Applications that can be accessed from the internet bring many benefits to their users, even though not spared from their negative impacts. Given this, data is a very valuable asset and must be protected. Data security can be done, one of which is by securing from the database side. Database security can be done by implementing symmetric cryptography Advance Encryption Standard (AES) and Vigenere. The purpose of this study is to minimize the occurrence of database leaks and misuse by irresponsible parties. The cryptographic techniques used are the Advanced Encryption Standard (AES) and vigenere methods. From the results of the implementation, it was concluded that the application is able to secure data in an encrypted database so that it can minimize the occurrence of misuse or manipulation of data by people who do not have authority over the data.

Keywords: Cryptography, AES-128 Algorithm, Vigenere, Database

1. PENDAHULUAN

Desember 2019 COVID-19 atau *Corona Virus Deaseases* mulai mewabah di Wuhan China. Pada awal tahun 2020 penyebaran virus ini semakin pesat ke beberapa negara termasuk ke Indonesia. Pandemi COVID-19 secara resmi dinyatakan telah menyebar di Indonesia pada 2 Maret 2020, dengan dua kasus positif pertama [1]. Kemudian WHO (World Health Organization atau Badan Kesehatan Dunia) secara resmi mendeklarasikan virus corona (COVID-19) sebagai pandemi pada tanggal 9 Maret 2020 [2]. Langkah pencegahan yang dilakukan oleh pemerintah Indonesia guna mengurangi resiko penularan virus corona lebih luas, maka pemerintah mengeluarkan himbauan agar bekerja dari rumah atau *Work Form Home (WFH).* Langkah ini diambil untuk mendukung kebijakan *social distancing.* Tentunya hal ini

sangat berdampak langsung pada perekonomian negara karena banyak aktivitas diluar rumah berkurang secara signifikan. PT. Royal Audrey Megah salah satu perusahaan swasta yang mendukung program pemerintah dalam penerapan Social Distancing. Dimana program tersebut mengharuskan karyawan untuk bekerja dari rumah atau *Work From Home (WFH)*. Namun dalam kondisi tersebut PT. Royal Audrey Megah ingin mempertahankan kualitas support pada layanan *hosting* yang dikerjakan oleh divisi *Customer Service* dan *IT Support*. Divisi tersebut mengharuskan operatornya mengakses aplikasi *helpdesk* yang berbasis pada jaringan komputer lokal atau hanya bisa diakes dari kantor. Aplikasi *helpdesk* ini menjadi media penghubung antara *Customer Service* dengan bagian *IT Support* untuk menyampaikan informasi keluhan *client* yang selanjutnya keluhan tersebut akan diproses oleh bagian *IT Support*. Keluhan tersebut berupa informasi data seperti permintaan spesifikasi *hardware dedicated server, source code, lisence key software* berbayar, dan lain sebagainya. Data-data tersebut akan disimpan dalam server lokal. Akan tetapi dimasa pandemi ini dimana pekerjaan dilakukan dari rumah *(work from home)*, maka aplikasi *helpdesk* yang digunakan haruslah dapat diakes melalui internet. Aplikasi yang dapat diakes dari internet membawa banyak manfaat bagi penggunanya, tak luput juga dengan dampak negatifnya. Salah satu dampak negatifnya adalah keamanan data dimana data menjadi aset yang sangat berharga dan harus dilindungi. Untuk melakukan pengamanan data salah satu caranya dapat dilakukan dengan cara mengamankan dari sisi *database*. Fungsinya agar data tidak mudah dilihat dan disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab.

Dalam prosesnya penelitian ini mengacu pada beberapa penelitian terdahulu yang masih berkaitan dengan penggunaan algoritme Advance Encryption Standard (AES) atau algoritme Vigenere. Berikut diuraikan beberapa tinjauan pustaka dari beberapa penelitian sebelumnya berkaitan dengan kriptografi dengan penggunaan metode yang beragam.

Penelitian yang dilakukan oleh Dian Widyawan dan Imelda [3] dengan judul Pengamanan File Menggunakan Kriptografi Dengan Metode AES-128 Berbasis WEB di Komite Nasional Keselamatan Transportasi pada tahun 2021 mendapat bahwa Komite Nasional Keselamatan Transportasi membutuhkan kerahasiaan data dalam melakukan investigasi. Untuk itu penelitian yang dilakukan oleh Dian Widyawan dan Imelda dilakukan untuk menghasilkan suatu aplikasi yang dapat membantu dalam mengamankan data. Teknik pengamana data yang dilakukan adalah dengan menggunakan kriptografi dengan metode Advanced Encryption Standard (AES). Metode kriptografi *Advanced Encryption Standard* (AES) adalah standar ekripsi kunci simetris dengan menggunakan kunci yang dapat berukuran 128 bit, 192 bit, ataupun 256 bit. Adapun tahapan perancangan aplikasi dalam penelitian ini menggunakan metode *waterfall*. Penelitian ini memberikan hasil bahwa aplikasi yang dibangun mampu mengamankan file hasil investigasi di Komite Nasioanal Keselamatan Transportasi dari file yang semula berbentuk *plaintext* menjadi file yang berbentuk *chipertext*.

Penelitian yang dilakukan oleh Basyiah dan Fahmy Syahputra [4] dengan judul Perancangan Aplikasi Penyadian Pesan Teks Mengunakan Vigenere Chiper dan Algoritme Elgamal pada tahun 2017 mendapati bahwa salah satu fasilitas yang disediakan oleh ponsel pintar adalah pengiriman pesan teks melalui fasilitas *Short Message Service* (SMS). Informasi yang dikirimkan melalui SMS mungkin saja berupa data yang penting dimana tidak semua pihak boleh mengetahuinya. Beberapa risiko yang dapat mengancam keamanan pesan dalam layanan SMS antara lain *SMS Spoofing, Snooping SMS*, dan *SMS Interception*. Sistem keamanan pesan berupa teks dapat dilakukan salah satunya dengan kriptografi. Dengan menggunakan berbagai macam algoritme kriptografi tulisan yang bermakna akan diubah menjadi tidak bermakna. Untuk mengamankan data, maka dalam penelitian ini Basyiah dan Fahmy Syahputra menerapkan algoritme ElGamal dan Vigenere Chiper. Algoritme ElGamal menggunakan 2 kunci yang berbeda dalam mengenkripsi dan mendekripsi yaitu kunci publik untuk enkripsi dan kunci privat untuk dekripsi. Sedangkan dalam algoritme vigenere chiper hanya menggunakan satu kunci baik untuk mengenkripsi maupun mendekripsi pesan. Dari hasil penelitian tersebut diperoleh kesimpulan bahwa aplikasi penyandian pesan teks menggunakan algoritme ElGamal dan Vigenere Chiper dapat membantu mengamankan pesan

teks dikirimkan oleh pengguna ponsel pintar.

Penelitian yang dilakukan oleh Laila Mustika [5] dengan judul Implementasi Algoritme AES Untuk Pengamanan Login dan Data Customer Pada E-Commerce Berbasis Web pada tahun 2020 mendapati bahwa saat ini banyak kejahatan siber yang mengincar website komersial seperti pada bidang E-Commerce. Untuk itu dibutuhkan beberapa pengamanan pada data saat login. Hal ini disebabkan oleh karena data yang digunakan pada saat melakukan *login* merupakan data yang sangat penting dan bersifat rahasia karena tidak boleh semua orang mengetahui. Selain data yang digunakan untuk *login,* data yang cukup penting untuk diamankan dari akses illegal adalah data pelanggan *(customer),* tentunya pengamanan data ini bertujuan untuk mencegah perubahan dan perusakan data agar data tidak disalahgunakan oleh pihak yang tidak bertanggung jawab seperti untuk melakukan penipuan dan lain sebagainya. Untuk menyelesaikan masalah tersebut, penelitian ini dilakukan dengan tujuan untuk mengamankan data *login* dan data *customer*. Dalam penelitian ini Laila Mustika menerapkan algoritme kriptografi AES (Advanced Encryption Standard) dengan panjang blok 128 bit untuk mengamankan data. Algoritme dipilih dengan alasan bahwa algoritma ini lebih mudah dalam implemetasinya pada memori yang berukuran kecil, selain itu juga dari sisi biaya lebih murah. Hasil dari penelitian ini didapatkan bahwa penerapan Algoritme AES dalam mengamankan data *login* dan data *customer* menjadikan *website e-commerce* lebih aman dan diharapkan kepercayaan *customer* terhadapat *website e-commerce* bertambah dengan meningkatnya keamanan website.

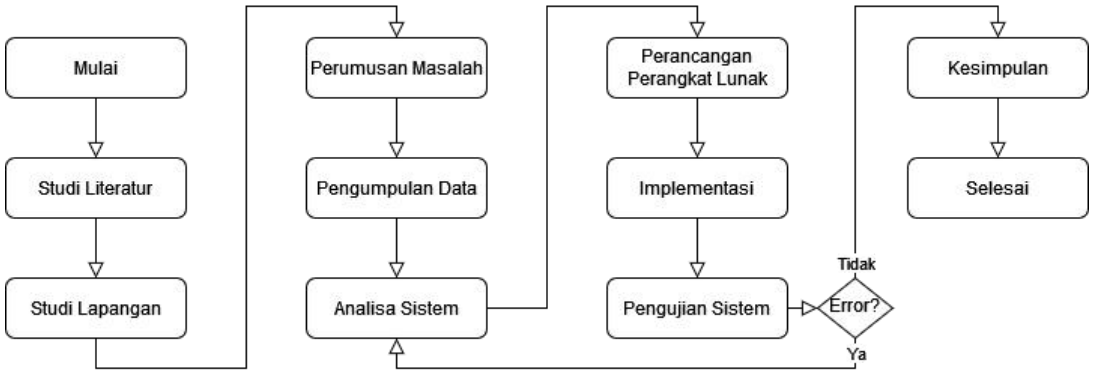
Penelitian yang dilakukan oleh Jaka Prayudha, Saniman, Ishak [6] dengan judul Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES) pada tahun 2020 mendapati bahwa data gaji PT. Capella Medan merupakan salah satu data yang bersifat rahasia yang hanya dapat dilihat oleh bendahara dan kepala kantor. Hal tersebut dilakukan agar data gaji karyawan tidak disalahgunakan atau dimanipulasi oleh orang-orang yang tidak berhak sehingga menimbulkan kerugian baik bagi karyawan maupun perusahaan. Berdasarkan hal tersebut, diperlukan sebuah metode untuk mengamankan data. Adapun metode yang dapat dilakukan untuk mengamankan data adalah dengan melakukan penyandian dan pengacakan terhadap data yang akan diamankan, dalam hal ini data gaji karyawan. Salah satu metode untuk menyandikan data adalah dengan menyandikan data yang diinginkan dengan menggunakan suatu algoritme kriptografi. Dalam penelitian ini, algoritme kriptografi yang digunakan adalah algoritme *Advanced Encryption Standard* (AES). Melalui proses pengujian yang telah dilakukan, penelitian ini memberikan hasil bahwa data gaji karyawan dapat diamankan dengan baik sehingga dapat menghindari terjadinya manipulasi dan penyalahgunaan data gaji karyawan oleh pihak yang tidak memiliki wewenang atas data tersebut.

Berkaitan dengan begitu banyaknya kasus-kasus yang terjadi terhadap penyalahgunaan data serta merujuk pada beberapa tinjauan literatur penelitian sebelumnya, maka untuk meminimalkan terjadinya tindakan penyalahgunaan data oleh pihak yang tidak berkepentingan diperlukanlah metode yang dapat menjaga keamanan data apabila terjadi kebocoran data. Metode yang dapat digunakan untuk menjaga keamanan informasi yakni dengan cara menyandikan informasi yang diinginkan dengan menerapkan ilmu kriptografi. Kriptografi adalah seni menjaga keamanan informasi dengan mengubah suatu informasi yang dapat dipahami menjadi suatu bentuk yang tidak dapat dipahami oleh penerima yang tidak diinginkan. Pesan asli yang dapat dibaca manusia disebut sebagai teks biasa *(plaintext)*, kemudian pesan ini diubah menggunakan algoritme tertentu atau serangkaian operasi matematika menjadi sesuatu yang akan terlihat seperti bahasa yang tidak jelas *(chipertext)* [7]. Terkait dengan hal tersebut, maka dalam penelitian ini difokuskan pada bagaimana cara mengamankan data pada *database* di aplikasi *helpdesk* di PT. Royal Audrey Megah yang pernah mengalami kebocoran data khususnya pada tabel tiket dan tabel karyawan. Untuk membatasi ruang lingkup penelitian, penelitian ini dibatasi pada penyandian *field problem_summary, problem_detail, nama, email* yang berada di tabel karyawan dan table tiket pada *database* sistem *helpdesk*. Algoritma kriptografi yang dipakai untuk menyandikan field tersebut adalah algoritma *Advance Encryption*

Standard (AES) yang dikombinasikan dengan algoritma *Vigenere*.

2. METODE PENELITIAN

Metode penelitian digunakan sebagai pedoman dalam melakukan penelitian ini agar penelitian yang dilakukan tidak menyimpang dari tujuan utamanya. Tahapan penelitian yang dilakukan dapat dilihat pada gambar 1.



Gambar 1. Alur penerapan metode

Dari diagram alur yang ditampilkan pada gambar 1 dapat dijelaskan bahwa penelitian ini dilakukan dalam beberapa tahapan. Tahapan-tahapan dalam penelitian ini dapat diuraikan pada pembahasan berikut ini.

Studi literatur merupakan alat bantu mempelajari konsep yang akan digunakan untuk membangun sistem dalam penelitian ini. Studi dapat dilakukan dengan mempelajari beberapa referensi seperti buku teks, jurnal, karya tulis maupun diktat kuliah yang terkait dengan penelitain yaitu kriptografi algoritme *Advanced Encryption Standard* (AES) dan algoritme *Vigenere*. Dengan dipelajarinya studi ini, penulis mendapatkan dasar referensi yang baik untuk menyelesaikan permasalahan yang akan diteliti.

Studi Lapangan merupakan studi kasus untuk mempelajari lebih dalam untuk mengetahui permasalahan yang ada pada data aplikasi *Helpdeks*, yang kemudian akan dirangkum menjadi masalah penelitian.

Perumusan Masalah merupakan tahap dalam menentukan masalah yang diambil dari tahap sebelumnya, yaitu bagaimana mengamankan data pada tabel karyawan dan tiket dengan mengimplementasikan kriptografi algoritme *Advanced Encryption Standard* (AES) dan algoritme *Vigenere*.

Pengumpulan data merupakan tahap dalam pengumpulan data menurut masalah yang ditentukan dari tahap sebelumnya. Beberapa tahapan yang dapat dilakukan yaitu melakukan wawancara dan melakukan observasi. Wawancara dilakukan kepada pihak yang berkaitan dengan masalah dan program untuk mendapat informasi dalam membangun penelitian. Sementara observasi dilakukan dengan mengamati secara langsung prosedur pada sistem yang sedang berjalan.

Identifikasi permasalahan dilakukan guna menyelesaikan permasalahan dalam penelitian ini. Tahapan yang dilakukan dalam mengidentifikasi permasalahan yakni dengan menganalisis data, menganalisis penerapan algoritme, dan menganalisis sistem. Pada tahapan analisis data dilakukan dengan cara mengelompokkan data sesuai dengan jenisnya dan mendeskripsikan data sebagai bantuan untuk membangun program yang lebih baik. Sementara itu pada tahapan analisis penerapan algoritme dilakukan guna menjelaskan bagaimana implementasi algoritme kriptografi yang digunakan yakni algoritme *advanced encryption standard* (AES) dan algoritme *vigenere.* Pada tahapan ini dilakukan penentuan kunci sebagai salah satu proses kriptografi untuk enkripsi dan dekripsi data. Kemudian tahapan berikutnya yakni proses enkripsi dan proses dekripsi. Tahapan analisis sistem merupakan tahap untuk

mengimplementasi pengamanan pada data yang dienkripsi sebelum data disimpan ke dalam sebuah basis data.

Perancangan perangkat lunak merupakan tahap perancangan antarmuka, rancangan pendukung, serta hasil dari analisis sistem tahap sebelumnya yang akan diintegrasikan dengan program. Beberapa rancangan pendukung yang dimaksud adalah proses login, proses tambah data, dan proses modifikasi data.

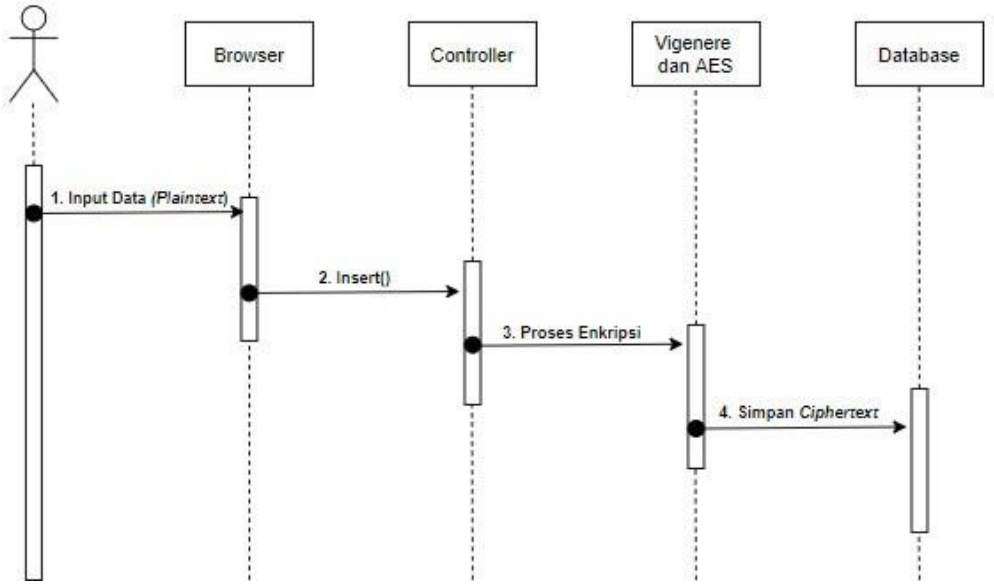
Implementasi merupakan proses pengerjaan atau pembuatan sistem aplikasi sesuai dengan rancangan yang telah ditentukan sebelumnya. Dalam tahap pembuatan ini, penulis merancang sistem aplikasi berbasis web dengan framework *codeigniter* menggunakan bahasa pemograman PHP untuk sistem dan algoritme *Advanced Encryption Standard* (AES) dan algoritme *Vigenere*, lalu perangkat lunak DBMS yaitu MySQL.

Pengujian sistem merupakan tahap yang dibutuhkan untuk menjamin sistem yang telah dibuat sesuai dengan perancangan dan analisis sehingga sistem berjalan dengan baik secara fungsional, berjalan sesuai dengan tujuan, dan menghasilkan *output* yang diharapkan. Metode pengujian sistem yang akan digunakan adalah metode *Blackbox Testing*.

Pada tahap ini diambil kesimpulan akhir, berdasarkan hasil pengujian dan beberapa tahap yang telah dilakukan. Hal ini dilakukan guna mengetahui apakah implementasi kriptografi algoritme *Advanced Encryption Standard* pada sistem telah berjalan sesuai harapan.

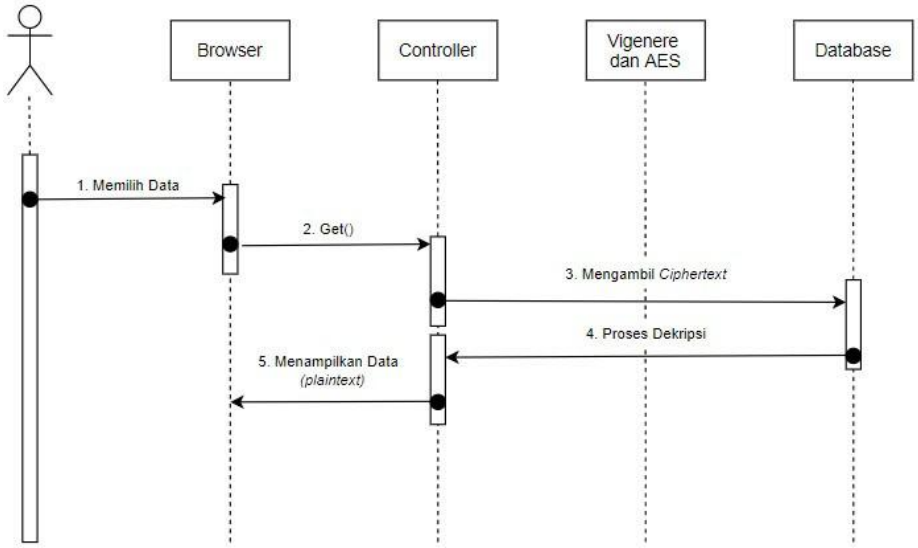
3. HASIL DAN PEMBAHASAN

Untuk dapat memahami proses pada proses pengembangan sistem helpdesk dengan menerapkan algoritma AES-128 dan Vigenere akan digambarkan dalam bentuk *Unified Modeling Language* (UML). *Unified Modeling Language* (UML) adalah sebuah bahasa pemodelan untuk tujuan yang umum. Tujuan UML adalah sebagai standar dalam menggambarkan sistem yang dirancang [8]. Gambar.2 menjelaskan proses enkripsi yang terjadi didalam sistem *helpdesk*.



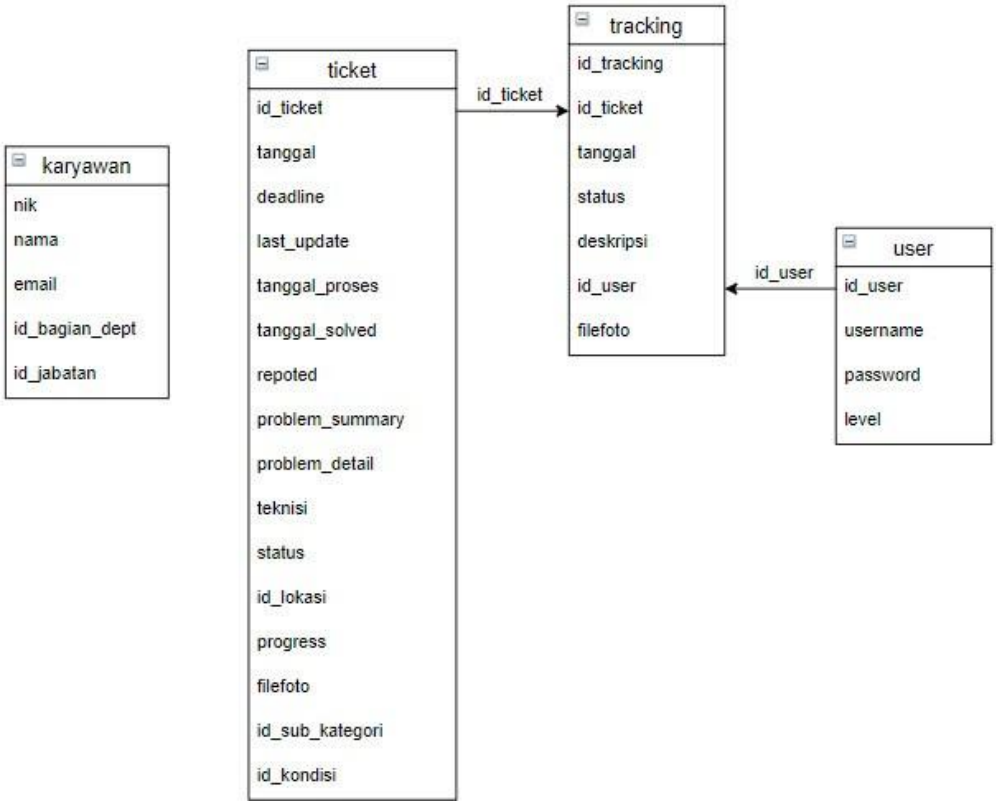
Gambar 2. Sequence Diagram Enkripsi

Gambar 3 menjelaskan proses dekripsi yang terjadi didalam sistem helpdesk



Gambar 3. Sequence Diagram Enkripsi

Gambar 4. adalah *Logical Record Structure* (LRS) yang menggambarkan basis data yang akan digunakan dalam pengembangan sistem.



Gambar 4. *Logical Record Structure*

Pada tahapan implementasi algoritme kriptografi ke dalam sistem helpdesk akan digunakan algoritme *vigenere* dan AES 128. Dimana langkah pertama adalah enkripsi *plaintext* dengan menggunakan algoritme *vigenere*. *Chipper text* hasil dari enkripsi dengan algoritme vigere akan dienkripsikan kembali dengan menggunakan algoritme AES 128.

Vigenère cipher adalah jenis substitusi *cipher* yang digunakan untuk enkripsi data dimana struktur *plaintext* asli agak tersembunyi dalam *ciphertext* dengan menggunakan beberapa macam substitusi *chiper monoalphabetic*. Kunci kode menentukan substitusi mana

yang akan digunakan untuk mengenkripsi setiap simbol *plaintext*. Sandi yang dihasilkan dikenal juga sebagai polialfabetik, yang telah memiliki sejarah penggunaan yang panjang. Perbedaan utama terletak pada bagaimana kunci digunakan untuk memilih di antara beberapa kumpulan aturan substitusi monoalfabetik. Sandi ini ditemukan pada tahun 1553 oleh kriptografer Italia Giovan Battista Bellaso tetapi selama berabad-abad dikaitkan dengan kriptografer Prancis abad ke-16 Blaise de Vigenère, yang merancang sandi serupa pada tahun 1586 [9].

Vigenere Cipher berisi alfabet yang dituliskan dalam 26 baris, masing-masing baris digeser ke kiri dari baris sebelumnya membentuk ke-26 kemungkinan sandi *caesar* setiap huruf disediakan dengan menggunakan baris yang berbeda-beda sesuai kunci yang diulang [4]. Gambar.5 menunjukkan tabel vigenere dalam 26 urutan alphabet.

Gambar 5. Vigenere Table [10]

Untuk memahami langkah enkripsi dengan kedua algoritme tersebut, akan diilustrasikan pada setiap tahapan berikut. Pada tahap awal, disiapkan 1 buah *plaintext* dengan 2 buah kunci yang digunakan untuk masing-masing algoritme. Dapat dilihat pada table.1 adalah table *plaintext* dan kunci.

Tabel 1. Tabel Plaintext dan Key

Plaintext	A	P	I	T	R	U	S	W	A	N	D	I	U	B	L	R
keyVIG	T	U	G	A	S	A	K	H	I	R	T	U	G	A	S	A
keyAES	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6

Tahap selanjutnya *plaintext* akan di enkripsi menggunakan algoritme *Vigenere* dengan panjang *key* mengikuti panjang *plaintext* yang dapat dilihat pada tabel.2. *Plaintext* dan kunci akan diproses menggunakan formula

C*i* = (P*i* + K*i*) mod 26

Tabel 2. Tabel *Plaintext* dan *Key Vigenere*

Plaintext	A	P	I	T	R	U	S	W	A	N	D	I	U	B	L	R
keyVIG	T	U	G	A	S	A	K	H	I	R	T	U	G	A	S	A

Langkah enkripsi dengan menggunakan vigenere dijabarkan pada tabel.3

Tabel 3. Tabel Enkripsi Dengan *Vigenere*

C*i*	=	(A+T) mod 26	C*i*	=	(P+U) mod 26	Ci	=	(I+G) mod 26
	=	(0+19) mod 26		=	(15+20) mod 26		=	(8+6) mod 26
	=	19 mod 26 = 19		=	35 mod 26 =		=	14 mod 26 = 14
	=	**T**		=	**J**		=	O

Ci = (T+A) mod 26
= (19+0) mod 26
= 19 mod 26 = 19
= **T**

Ci = (R+S) mod 26
= (17+18) mod 26
= 35 mod 26 = 9
= **J**
=

Ci = (U+A) mod 26
= (20+0) mod 26
= 20 mod 26 = 20
= **U**

Ci = (S+K) mod 26
= (18+10) mod 26
= 28 mod 26 = 2
= **C**

Ci = (W+H) mod 26
= (22+7) mod 26
= 29 mod 26 = 3
= **D**

Ci = (A+I) mod 26
= (0+8) mod 26
= 8 mod 26 = 8
= **I**

Ci = (N+R) mod 26(13+17)
= mod 30 mod 26 = 4
= **E**
=

Ci = (D+T) mod 26
= (3+19) mod 26
= 22 mod 26 = 22
= **W**

Ci = (I+U) mod 26
= (8+20) mod 26
= 28 mod 26 = 2
= **C**

Ci = (U+G) mod 26
= (20+6) mod 26
= 26 mod 26 = 0
= **A**

Ci = (B+A) mod 26
= (1+0) mod 26
= 1 mod 26 = 1
= **B**

Ci = (L+S) mod 26
= (11+18) mod 26
= 29 mod 26 = 3
= **D**

Ci = (R+A) mod 26
= (17+0) mod 26
= 17 mod 26 = 17
= **R**

Tabel.4 memperlihatkan hasil dari enkripsi dari algoritme *vigenere* yang menghasilkan *chipertext.*

Tabel 4. Hasil Enkripsi Algoritme Vigenere

Chipertext Vigenere	T	J	O	T	J	U	C	D	I	E	W	C	A	B	D	R

Chipertext ini akan digunakan untuk tahapan enkripsi berikutnya dengan menggunakan algoritme AES-128 menggunakan kunci yang sudah ditentukan pada tabel.5

Tabel 5. *Chipertext Vigenere* Digunakan Untuk *Plaintext* AES

Plaintext	T	J	O	T	J	U	C	D	I	E	W	C	A	B	D	R
keyAES	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6

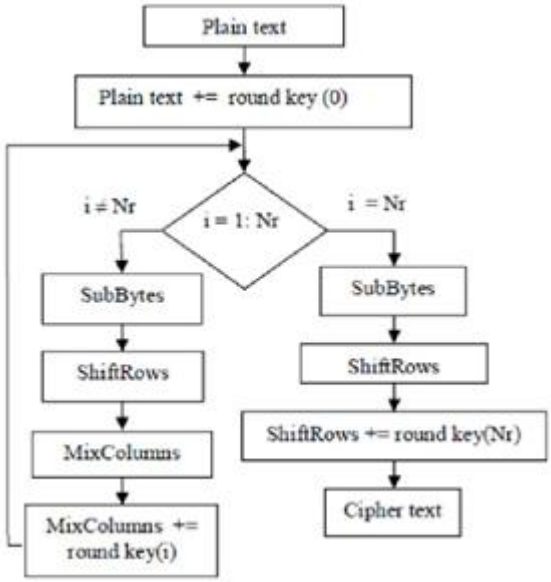
Algoritma Rijndael AES menggunakan kunci blok cipher simetris baik dalam enkripsi maupun dekripsi. Fitur utama Rijndael adalah kemampuannya untuk beroperasi pada berbagai ukuran kunci dan blok data. Ini memberikan fleksibilitas ekstra karena ukuran blok dan ukuran kunci mungkin 128, 192, atau 256 bit. Saat Rijndael menentukan tiga ukuran kunci, ada sekitar 3,4 x 1038 kemungkinan kunci 128-bit, 6,2 x 1057 kemungkinan kunci 192-bit dan 1,1 x 1077 kemungkinan kunci 256-bit. Pada awal enkripsi, input disalin ke dalam array. Algoritma enkripsi mengenkripsi satu blok data pada satu waktu untuk menghasilkan blok data terenkripsi dengan menggunakan kunci rahasia. Dekripsi hanyalah proses kebalikan dari enkripsi, dan setiap operasi adalah kebalikan dari proses enkripsi. Panjang blok data ditetapkan hingga 128 bit, sedangkan panjang kuncinya bisa 128, 192, atau 256 bit [11]. Setiap blok data disusun ulang dalam bentuk matriks. Algoritma AES adalah algoritma iteratif dan setiap iterasi. Jumlah byte dalam satu baris panjang kunci sudah ditentukan.

N = L / (8 x Br) dimana, N adalah jumlah *byte*, L adalah panjang blok dalam bit, dan Br adalah jumlah baris dalam matriks array. Setiap putaran diulang 10 kali untuk kunci panjang

128-bit, 12 kali untuk kunci 192-bit dan 14 kali untuk kunci 256 bit dengan masing-masing 4, 6 dan 8 byte dalam deretan panjang kunci. Setiap putaran menggunakan empat transformasi dan *invers* tetapi pada iterasi terakhir tidak dilakukan transformasi *MixColumn*. Untuk menguraikan blok data di Rijndael, langkah Add *Round Key* dilakukan (meng-XOR-kan subkunci dengan blok) dengan sendirinya, kemudian melanjutkan putaran transformasi, dan kemudian putaran terakhir dengan langkah *MixColumn* dihilangkan. *Cipher* itu sendiri didefinisikan oleh langkah-langkah berikut:

- Penambahan Round Key awal;
- Iterasi sebanyak Nr-1;
- Iterasi akhir.

Gambar 6. menunjukkan alur algoritma Enkripsi AES.



Gambar 6. Algoritma Enkripsi AES [12]

Pada tahap awal enkripsi AES *Plaintext* dan *key* tersebut dikonversikan ke dalam bentuk *bit* menggunakan kode *ASCII* yang kemudian dikonversi kembali ke bentuk *hexsadesimal*. Setelah didapatkan kode heksa desimalnya, langkah selanjutnya adalah menggabungkannya dengan kunci AES menggunakan fungsi XOR. Langkah ini disebut dengan *AddRoundKey.* Tabel tabel.6 mengilustrasikan proses *AddRoundKey* antara *plaintext* dengan kunci AES.

Tabel 6. Proses AddRoundKey Antara *Plaintext* Dengan Kunci AES

Plaintext

54	4A	49	41
4A	55	45	42
4F	43	57	44
54	44	43	52

keyAES

31	35	39	33
32	36	30	34
33	37	31	35
34	38	32	36

54	4A	49	41
4A	55	45	42
4F	43	57	44
54	44	43	52

XOR

31	35	39	33
32	36	30	34
33	37	31	35
34	38	32	36

Untuk mengoperasikan XOR antara plaintext dengan kunci AES diperlukan perubahan

bentuk heksadesimal ke binary. Tabel 7 memperlihatkan langkah operasi XOR untuk tiap cell matriks.

Tabel 7. Operasi XOR Untuk Tiap Cell Matriks

54 : 01100100 31 : 00110001 XOR **01100101**	4A : 01001010 35 : 00110101 XOR **01111111**	49 : 01001001 39 : 00111001 XOR **01110000**	41 : 01000001 33 : 00110011 XOR **01110010**
4A : 01001010 32 : 00110010 XOR **01111000**	55 : 01010101 36 : 00110110 XOR **01100011**	45 : 01000101 30 : 00110000 XOR **01110101**	42 : 01000010 34 : 00110100 XOR **01110110**
4F : 01001111 33 : 00110011 XOR **01111100**	43 : 01000011 37 : 00110111 XOR **01110100**	57 : 01010111 31 : 00110001 XOR **01100110**	44 : 01000100 35 : 00110101 XOR **01110001**
54 : 01010100 34 : 00110100 XOR **01100000**	44 : 01000100 38 : 00111000 XOR **01111100**	43 : 01000011 32 : 00110010 XOR **01110001**	52 : 01010010 36 : 00110110 XOR **01100100**

Hasil dari operasi *XOR* antara *plaintext* dengan kunci AES dalam bentuk heksa desimal dapat dilihat pada tabel.8

Tabel 8. Tabel hasil *AddRoundKey*

65	7F	70	72
78	63	75	76
7C	74	66	71
60	7C	71	64

Langkah selanjutnya adalah melakukan proses *SubByte. SubBytes* adalah proses substitusi *byte* dengan menggunakan tabel *S- Box* seperti Gambar 2.12. Setiap elemen array pertama kali dibalik dan diproses melalui transformasi *affine*. Transformasi *SubBytes* dilakukan pada setiap *byte array*. Pada sebagian besar aplikasinya *SubBytes* dihitung terlebih dahulu dan disimpan dalam tabel pencarian yang disebut S-box 2 8 = 256 elemen [12]. Yang disubstitusikan adalah hasil dari proses *AddRoundKey.*

Tabel 9. Proses *SubByte*

65	7F	70	72
78	63	75	76
7C	74	66	71
60	7C	71	64

Proses SubBytes

4D	D2	51	40
BC	FB	9D	38
10	92	33	A3
D0	10	A3	43

Kemudian setelah mendapatkan hasil dari proses *SubByte*, tahapan selanjutnya adalah proses *ShiftRows. ShiftRows* adalah proses yang melakukan pergeseran pada setiap elemen blok atau tabel yang dilakukan pada setiap barisnya. Baris dalam *array* diputar. *Byte* di baris pertama tidak digeser sedangkan baris kedua, ketiga, dan keempat digeser ke kiri oleh satu *byte* secara berulang [12].

Tabel 10. Tabel *ShiftRows*

4D	D2	51	40
BC	FB	9D	38
10	92	33	A3
D0	10	A3	43

4D	D2	51	40
FB	9D	38	BC
33	A3	10	92
43	D0	10	A3

Setelah melakukan *ShiftRows,* tahap selanjutnya adalah mengalihkan hasil dari *ShiftRows* dengan matrix yang sudah ditentukan. Langkah ini disebut *MixColumns. MixColumns* adalah transformasi linier dan dilakukan pada *array* kolom demi kolom. Setiap *byte* yang ditransformasikan adalah kombinasi linier dari matriks [12].

Tabel.11 Tabel *MixColumns*

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

4D	D2	51	40
FB	9D	38	BC
33	A3	10	92
43	D0	10	A3

{ (02.4D) XOR (03.FB) XOR (01.33) XOR (01.43) } = FC

Hasil dari *MixColumns* dari tabel diatas disajikan pada tabel 12.

Tabel 12. Hasil *MixColumns*

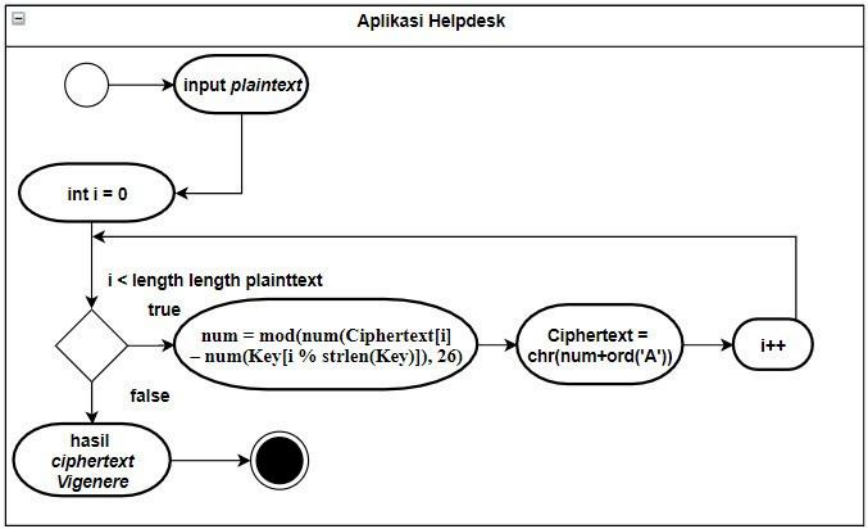
FC	70	EA	6E
B6	DD	01	2D
15	79	79	3D
99	E8	FB	B3

Pada tahap *AddRoundKey* setiap 128-bit putaran kunci dibagi menjadi 16 *byte* pada blok data. *AddRoundKey* adalah transformasi linier. Putaran kunci ditambahkan ke array dengan operasi Exclusive-OR (XOR) bitwise. Kunci digunakan sebagai *set* awal *byte* di setiap baris dan sisa *byte* dihasilkan dari kunci secara berulang [12]. Proses *AddRoundKey*, *SubBytes*, *ShiftRows* dan *MixColumns* dilakukan dengan cara yang sama hingga Round 10. Tetapi, ada perbedaan pada Round 10, dimana tidak terjadi *MixColumns* melainkan setelah mendapatkan hasil dari *ShiftRows* maka langsung masuk ke *AddRoundKey*. Berikut adalah hasil pada Round 10 atau Final.

Tabel 13. Hasil dari proses di putaran ke-10

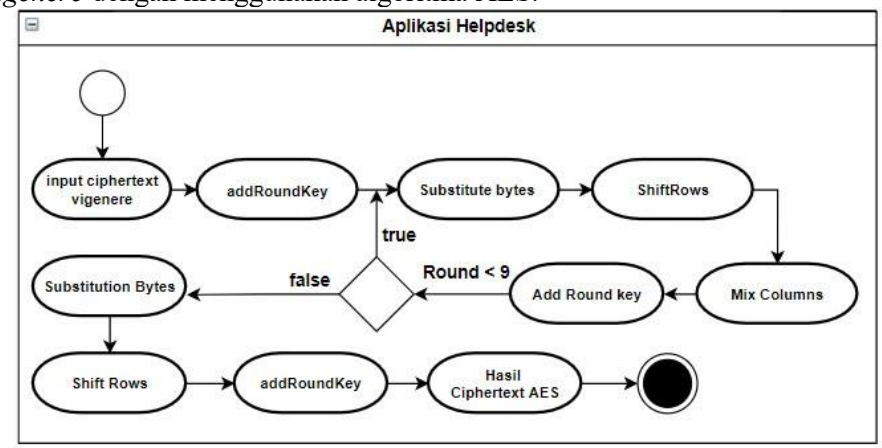
45	4D	07	3C
2E	E0	D7	93
FC	38	3E	D5
3F	A1	43	27

Untuk menjelaskan alur kegiatan dalam perancangan program, kemudian bagaimana proses berawal, lalu keputusan yang mungkin dihasilkan, dan bagaimana sistem akan berakhir digambarkan dalam bentuk aktivitas diagram [13]. Gambar 7 menjelaskan tentang diagram aktivitas awal dari proses enkripsi *plaintext* menjadi *ciphertext* dengan algoritme *vigenere.*



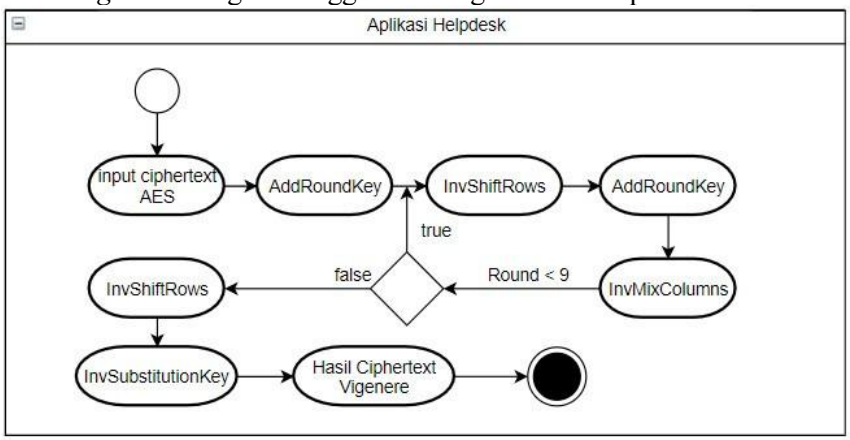
Gambar 7. Activity Diagram Proses Enkripsi Vigenere

Gambar 8 menjelaskan tentang diagram aktivitas proses enkripsi dari *ciphertext* hasil enkripsi *vigenere* dengan menggunakan algoritma AES.



Gambar 8. Activity Diagram Proses Enkripsi AES

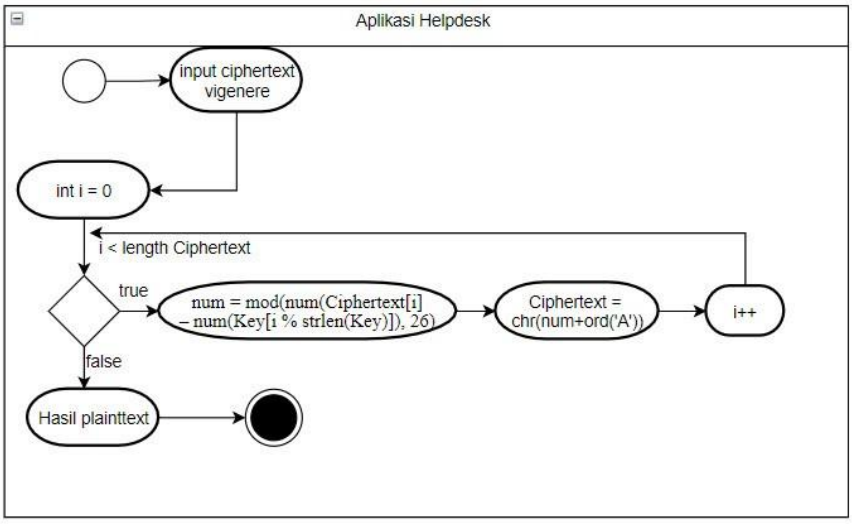
Diagram aktivitas pada gambar 9. menjelaskan tentang proses dekripsi dari *ciphertext AES* ke *ciphertext vigenere* dengan menggunakan algoritma dekripsi AES.



Gambar 9. Activity Diagram Proses Dekripsi AES

Diagram aktivitas pada gambar 10 menjelaskan tentang proses dekripsi dari *ciphertext*

vigenere ke *plaintext* dengan menggunakan algoritma dekripsi *vigenere*.



Gambar 10. Activity diagram proses dekripsi Vigenere

Bagian ini akan dibahas mengenai rangkaian uji coba aplikasi yang telah selesai dilaksanakan. Pengujian dilakukan cara *blackbox testing*, yakni dilakukan untuk menguji tampilan antarmuka perangkat lunak yang telah dibangun. Meskipun pengujian pada intinya digunakan untuk mencari kesalahan program, namun pengujian dengan cara *black-box* ini dapat digunakan untuk memperlihatkan bahwa setiap fungsi yang ada dapat dijalankan dengan baik seperti input dan output yang dapat dihasilkan secara tepat, serta integritas informasi diperlihara dengan baik [14].

Tabel 14. *Black Box* Pada Aplikasi Website

No	Skenario Pengujian	Test Case	Hasil yang diharapkan	Hasil Pengujian	Kesim-pulan	Hasil Akurasi
1.	Menampilkan semua data tiket diterima	1.Klik menu tiket diterima	Layar menampilkan data tiket yang telah didekripsi	Sesuai Harapan	*Valid*	100%
2.	Menampilkan semua data detail tiket	1.Klik menu tiket diterima 2.Klik detail tiket	Layar menampilkan data detail tiket yang telah di dekripsi	Sesuai Harapan	*Valid*	100%
3.	Menampilkan semua data daftar tiket	1.Klik menu daftar tiket	Layar menampilkan data daftar tiket yang telah di dekripsi	Sesuai Harapan	*Valid*	100%
4.	Menampilkan data semua karyawan	1.Klik menu karyawan	Layar menampilkan data karyawan yang telah di dekripsi	Sesuai Harapan	*Valid*	100%

5.	Menambah data karyawan	1. Klik menu karyawan 2. Pilih menu tambah karyawan	Data karyawan berhasil di enkripsi ke database	Sesuai Harapan	*Valid*	100%
6.	Mengubah data karyawan	1. Klik menu karyawa 2. Pilih tombol ubah data berdasarkan id 3. Input form ubah data 4. Klik submit	1. Menampil-kan hasil data karya-wan yang telah di dekripsi 2. data berhasil diubah lalu di enkripsi ke database	Sesuai Harapan	*Valid*	100%
7.	Menampilkan data akun pengguna	1. klik menu akun pengguna	Layar menam-pilkan data akun pengguna yang telah di dekripsi	Sesuai Harapan	*Valid*	100%
8.	Menambah data tiket baru	1. Klik menu buat tiket	Data tiket berhasil di buat lalu di enkripsi ke database	Sesuai Harapan	*Valid*	100%
9.	Melihat tabel dalam database dengan SQLinjection	1. Menginject database dengan tools SQLmap	Melihat database pada tabel yang terenkripsi	Sesuai Harapan	*Valid*	100%

Setelah dilakukan analisa dari hasil pengujian aplikasi kriptografi dengan cara membandingkan hasil fungsi enkripsi dan dekripsi, ditemukan beberapa hasil yaitu sistem memiliki beberapa kelebihan yaitu sistem *helpdesk* hanya membutuhkan *browser*. Selain itu, tampilan antar muka yang sederhana memudahkan penggunanya dalam menggunakan sistem ini. Hasil dari implementasi algoritma vigenere dan AES berhasil mengenkripsi basis data sistem *helpdesk.* Namun masih terdapat beberapa kekurangan yaitu hanya mengenkripsi pada *field* yang ditentukan. Hasil dari enkripsi membuat ukuran file pada database menjadi lebih besar. Database tidak bisa diimport jika kunci algoritme berbeda dari sebelumnya. Masih ada kemungkinan kunci algoritme dicari dengan celah *SQL injection*.

4. KESIMPULAN DAN SARAN

Berdasarkan hasil implementasi algoritma pada program yang telah dibuat serta berdasarkan hasil analisa yang telah dilakukan, maka dapat disimpulkan bahwa algoritme AES-128 dan *vigenere* berhasil di implementasikan pada aplikasi *helpdesk* yang dikembangkan dengan menggunakan bahasa pemrograman PHP dan menggunakan basis data *MySQL* untuk mengamankan basis data pada *field* yang telah ditentukan. Selain menarik kesimpulan, beberapa saran dapat diajukan yang mungkin bisa menjadikan pertimbangan dalam pengembangan aplikasi yakni perlu adanya peningkatan pada teknik enkripsi dan teknik dekripsi database sehingga dapat mengenkripsi dan mendekripsi database secara maksimal.

DAFTAR PUSTAKA

[1] A. G. Hanggara, "Jakarta Response to COVID-19 Outbreak: A Timeline," 2020. https://corona.jakarta.go.id/en/artikel/linimasa-kebijakan-penanganan-pandemi-covid-19-di-jakarta (accessed Jun. 23, 2022).

[2] -, "Apa yang dimaksud dengan pandemi?," *COVID19.GO.ID*, 2021. https://covid19.go.id/tanya-jawab?search=Apa yang dimaksud dengan pandemi (accessed Jun. 23, 2022).

[3] D. Widyawan and I. Imelda, "Pengamanan File Menggunakan Kriptografi Dengan Metode AES-128 Berbasis Web di Komite Nasional Keselamatan Transportasi," *Skanika*, vol. 4, no. 1, pp. 15–22, 2021, doi: 10.36080/skanika.v4i1.2216.

[4] Basyiah and F. Syahputra, "Perancangan Aplikasi Penyandian Pesan Teks Menggunakan Vigenere Chiper dan Algoritma Elgamal," *MEANS (Media Informasi Analisa dan Sistem)*, 2018. .

[5] L. Mustika, "Implementasi Algoritma AES Untuk Pengamanan Login dan Data Customer Pada E-Commerce Berbasis Web," *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 1, p. 148, 2020, doi: 10.30865/jurikom.v7i1.1943.

[6] J. Prayudha, Saniman, and Ishak, "Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES)," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 18, no. 2, p. 119, 2019, doi: 10.53513/jis.v18i2.150.

[7] J. Fruhlinger, "What is cryptography? How algorithms keep information secret and safe," *CSO*, 2022. https://www.csoonline.com/article/3583976/what-is-cryptography-how-algorithms-keep-information-secret-and-safe.html (accessed Jun. 23, 2022).

[8] T. Chakraborty, "Unified Modeling Language (UML) | An Introduction," *GeeksForGeeks*, 2019. https://www.geeksforgeeks.org/unified-modeling-language-uml-introduction/ (accessed Jun. 23, 2022).

[9] G. J. Simmons, "Vigenère cipher," *Encyclopedia Britannica*. https://www.britannica.com/topic/Vigenere-cipher (accessed Jun. 23, 2022).

[10] "Vigenère Table," *Encyclopædia Britannica*. https://www.britannica.com/topic/Vigenere-cipher#/media/1/628637/1284 (accessed Jun. 23, 2022).

[11] Federal Information Processing Standards Publication 197, *Announcing the ADVANCED ENCRYPTION STANDARD (AES)*. Gaithersburg: National Institute of Standards and Technology, 2001.

[12] N. K. Jharbade and R. Shrivastava, "Network based Security model using Symmetric Key Cryptography (AES 256– Rijndael Algorithm) with Public Key Exchange Protocol (Diffie-Hellman Key Exchange Protocol)," *Int. J. Comput. Sci. Netw. Secur.*, vol. 12, no. 8, pp. 69–73, 2015.

[13] A. Ansori, "Pengertian Activity Diagram : Tujuan, Simbol, dan Contohnya," *Ansoriweb*, 2022. https://www.ansoriweb.com/2020/03/pengertian-activity-diagram.html (accessed Jun. 24, 2022).

[14] J. D. Susatyono, "Teknik Pengujian Black-box Testing dan White-box Testing," *Universitas STEKOM*, 2021. http://sistem-komputer-s1.stekom.ac.id/informasi/baca/Teknik-Pengujian-Black-box-Testing-dan-White-box-Testing/38db21cd8ce80834dec740c19b7839738bf026d0 (accessed Jun. 24, 2022).