PENERAPAN ALGORITMA *VIGENERE CIPHER* UNTUK MENINGKATKAN KEAMANAN PADA *DASHBOARD*

SKRIPSI

Diajukan sebagai Salah Satu Syarat untuk Mendapatkan Gelar Sarjana Komputer (S.Kom) Program Studi Informatika

TRI TIARA PENINA DEBY

105841101618

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MAKASSAR

2023

FAKULTAS TEKNIK

GEDUNG MENARA IQRA LT. 3

Jl. Sultan Alauddin No. 259 Telp. (0411) 866 972 Fax (0411) 865 588 Makassar 90221
Website: www.unismuh.ac.id, e_mail: unismuh@gmail.com
Website: http://teknik.unismuh.makassar.ac.id

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

HALAMAN PENGESAHAN

Tugas Akhir ini diajukan untuk memenuhi syarat ujian guna memperoleh gelar Sarjana Komputer (S.Kom) Program Studi Informatika Fakultas Teknik Universitas Muhammadiyah Makassar.

Judul Skripsi : **PENERAPAN ALGORITMA VIGENERE CIPHER UNTUK MENINGKATKAN KEAMANAN PADA DASHBOARD**

Nama : TRI TIARA PENINA DEBY
Stambuk : 105841101618

Makassar, 31 Agustus 2023

Telah Diperiksa dan Disetujui
Oleh Dosen Pembimbing;

Pembimbing I	Pembimbing II
Rizki Yusliana Bakti, ST., MT.	**Muhyiddin A.M Hayat, S.Kom, M.T**

Mengetahui,
Ketua Program Studi Informatika

Muhyiddin A.M Hayat,S.Kom,M.T
NBM : -

FAKULTAS TEKNIK

GEDUNG MENARA IQRA LT. 3

Jl. Sultan Alauddin No. 259 Telp. (0411) 866 972 Fax (0411) 865 588 Makassar 90221
Website: www.unismuh.ac.id, e_mail: unismuh@gmail.com
Website: http://teknik.unismuh.makassar.ac.id

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

PENGESAHAN

Skripsi atas nama **Tri Tiara Penina Deby** dengan nomor induk Mahasiswa **105 84 11016 18**, dinyatakan diterima dan disahkan oleh Panitia Ujian Tugas Akhir/Skripsi sesuai dengan Surat Keputusan Dekan Fakultas Teknik Universitas Muhammadiyah Makassar Nomor : 405/05/A.5-II/VIII/45/2023, sebagai salah satu syarat guna memperoleh gelar Sarjana Komputer pada Program Studi Informatika Fakultas Teknik Universitas Muhammadiyah Makassar pada hari Sabtu tanggal 31 Agustus 2023.

Makassar, 02 Safar 1444 H / 31 Agustus 2023 M

Panitia Ujian :

1. Pengawas Umum
   a. Rektor Universitas Muhammadiyah Makassar
      Prof. Dr. H. AMBO ASSE, M.Ag : .....
   b. Dekan Fakultas Teknik Universitas Hasanuddin
      Prof. Dr. Eng. MUHAMMAD ISRAN RAMLI, ST., MT : .....
2. Penguji
   a. Ketua : Dr. Ir. Zahir Zainuddin, M.Sc. : .....
   b. Sekertaris : Fahrim Irhamna Rahman, S.Kom.,MT. : .....
3. Anggota : 1. Titin Wahyuni , S.Pd., MT. : .....
   2. Lukman Anas, S.Kom., MT. : .....
   3. Lukman, S.Kom., MT. : .....

Mengetahui :

Pembimbing I

Rizki Yusliana Bakti, ST., MT.

Pembimbing II

Muhyiddin A.M Hayat,S.Kom,M.T

Dekan Fakultas Teknik

Dr. Ir. Hj. Nurnawaty, ST., MT., IPM
NBM : 795 108

ABSTRACT

The importance of maintaining information confidentiality in the face of data security threats has brought a focus on the field of cryptography. In this context, this research aims to enhance security on the University of Muhammadiyah Makassar Dashboard platform using the Vigenere Cipher encryption technique. This method has dual objectives: first, to integrate the Vigenere Cipher into messages transmitted through the platform, and second, to compare the level of data security before and after the implementation of this algorithm. Testing was conducted by applying the Vigenere Cipher encryption technique to data and conducting Time-based One-Time Password (TOTP) tests. The test results indicate that the implementation of the Vigenere Cipher successfully enhances data security on the University of Muhammadiyah Makassar Dashboard platform. Key advantages include the convenient online access capability through various devices and safeguarding against unauthorized access through message validation between clients and servers. However, the study also reveals that cipher algorithms, including the Vigenere Cipher, have vulnerability ranges, particularly against brute force attacks. Therefore, additional efforts are required to strengthen security layers. In conclusion, this research effectively implements the Vigenere Cipher on the University of Muhammadiyah Makassar Dashboard platform. This technique has diminished the risk of unauthorized access and demonstrated its positive impact on preserving data confidentiality and integrity. Nonetheless, it is important to remember that cryptographic algorithms are not ultimate solutions but rather components of a broader strategy in maintaining data security.

Keywords: *Data Security, Vigenere Cipher, Dashboard.*

ABSTRAK

Pentingnya menjaga kerahasiaan informasi dalam menghadapi ancaman keamanan data telah membawa fokus pada bidang kriptografi. Dalam konteks ini, penelitian ini bertujuan untuk meningkatkan keamanan pada platform Dashboard Unversitas Muhammadiyah Makassar menggunakan teknik enkripsi Vigenere Cipher. Metode ini memiliki tujuan ganda: pertama, untuk mengintegrasikan Vigenere Cipher ke dalam pesan yang dikirim melalui platform, dan kedua, untuk membandingkan tingkat keamanan data sebelum dan setelah penerapan algoritma ini. Pengujian dilakukan dengan menerapkan teknik enkripsi Vigenere pada data dan pengujian Time-based One-Time Password (TOTP). Hasil pengujian menunjukkan bahwa implementasi Vigenere Cipher berhasil meningkatkan keamanan data pada platform Dashboard Unismuh Makassar. Kelebihan utamanya termasuk kemampuan akses online yang nyaman melalui berbagai perangkat, serta perlindungan terhadap akses tidak sah melalui validasi pesan antara klien dan server. Namun demikian, penelitian ini juga mengungkapkan bahwa algoritma cipher, termasuk Vigenere Cipher, memiliki rentang kerentanannya, khususnya terhadap serangan brute force. Oleh karena itu, upaya tambahan perlu dilakukan untuk memperkuat lapisan keamanan. Dalam kesimpulannya, penelitian ini berhasil mengimplementasikan Vigenere Cipher pada platform Dashboard Unismuh Makassar dengan efektif. Teknik ini telah mengurangi risiko akses ilegal dan telah membuktikan dampak positifnya dalam menjaga kerahasiaan dan integritas data. Meskipun demikian, perlu diingat bahwa algoritma kriptografi bukan solusi akhir, melainkan bagian dari strategi yang lebih luas dalam menjaga keamanan data.

***Kata kunci**: Kemanan Data, Vigenere Cipher, Dashboard.*

KATA PENGANTAR

Syukur Alhamdulillah penulis panjatkan atas kehadirat Allah Subhanahu Wa Ta'ala, karena rahmat dan hidayah-Nya yang iada henti diberikan kepada hamba-Nya. Shalawat serta salam tak lupa penulis kirimkan kepada Rasulullah Muhammad Shalallahu 'Alaihi Wasallam. Beserta keluarga, sahabat dan para pengikutnya hingga akhir zaman. Adapun judul tugas akhir kami adalah "PENERAPAN ALGORITMA *VIGENERE CIPHER* UNTUK MENINGKATKAN KEAMANAN PADA *DASHBOARD*".

Tugas Proposal ini merupakan salah satu persyaratan akademik yang harus ditempuh dalam rangka menyelesaikan Studi di Fakultas Teknik Program Studi Informatika Universitas Muhammadiyah Makassar. Penulis menyadari sepenuhnya bahwa didalam penulisan tugas proposal ini masih terdapat banyak kekurangan, karena penulis sebagai manusia biasa tidak lepas dari kesalahan dan kekurangan baik itu ditinjau dari segi teknis penulisan. Oleh karena itu penulis menerima dengan sangat ikhlas dan senang hati segala koreksi serta perbaikan guna menyempurnakan tulisan ini agar kelak dapat bermanfaat.

Tugas akhir ini tidak akan terwujud tanpa adanya bantuan, arahan, bimbingan dan dorongan dari berbagai pihak. Maka dari itu penghargaan yang setinggi-tingginya dan terimakasih banyak kami haturkan dengan hormat kepada:

1. Kedua orangtua kami tercinta, penulis mengucapkan terima kasih yang sebesar-besarnya atas segala limpahan kasih saying. Doa dan dukungan baik secara moral maupun materi.
2. Bapak Prof. Dr. H. Ambo Asse, M.ag. Sebagai Rektor Universitas Muhammadiyah Makassar.
3. Ibu Dr. Ir. Hj. Nurnawaty, ST., MT., IPM. Sebagai Dekan Fakultas Teknik Universitas Muhammadiyah Makassar.
4. Bapak Muhyiddin AM Hayat, S.Kom.,M.T. Sebagai Ketua Prodi Informatika, Fakultas Teknik Universitas Muhammadiyah Makassar.

5. Ibu Rizki Yusliana Bakti, S.T., M.T. selaku Pembimbing I dan Bapak Muhyiddin AM Hayat, S.Kom., M.T. selaku Pembimbing II yang senantiasa meluangkan waktunya membimbing dan mengarahkan penulis dalam penyusunan tugas Proposal ini.
6. Bapak/Ibu Dosen dan Staff Administrasi Prodi Informatika Fakultas Teknik Universitas Muhammadiyah Makassar.
7. Seluruh dosen pengajar di Jurusan Informatika Fakultas Teknik Universitas Muhammadiyah Makassar
8. Saudara/saudari kami di Fakultas Teknik, Mekanika 2018, dan Sahabat terbaik saya Reski Abbas, S.Kom., yang selalu berjuang bersama dengan rasa persaudaraan yang tinggi banyak membantu serta memberi dukungan dalam menyelesaikan tugas akhir ini.

Akhir kata, penulis mengharapkan tugas akhir ini dapat bermanfaat bagi pengembangan ilmu pengetahuan khususnya dibidang Keinformatikaan. Aamiin.

"Billahi Fii Sabilil Haq Fastabiqul Khaerat"

Makassar, 29 Agustus 2023

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR ISTILAH

Jaringan computer	Infrastruktur yang terdiri dari perangkat keras, perangkat lunak, dan protokol yang memungkinkan komunikasi dan pertukaran data antara komputer dan perangkat lainnya.
Teknologi informasi dan komunikasi	Sektor yang melibatkan penggunaan teknologi untuk mengumpulkan, menyimpan, mengirim, dan memproses informasi.
Informasi digital	Data yang dikodekan dalam bentuk digital, dapat dengan mudah dibagikan dan diakses melalui jaringan komputer.
Peretasan	Upaya yang tidak sah untuk mengakses, mengubah, atau mencuri data atau informasi melalui jaringan komputer.
Keamanan data	Praktik dan teknologi yang digunakan untuk melindungi data dari akses yang tidak sah, kerusakan, atau kebocoran.
Ilmu pendidikan	Bidang studi yang berkaitan dengan teori dan praktik pendidikan.
Kriptografi	Bidang studi yang berfokus pada teknik enkripsi dan dekripsi untuk menjaga keamanan data.

Enkripsi	Proses mengubah teks biasa (plaintext) menjadi bentuk yang tidak dapat dibaca (ciphertext) agar tidak dapat dimengerti oleh pihak yang tidak berwenang.
Firewall	Sistem keamanan yang digunakan untuk memantau dan mengendalikan lalu lintas data yang masuk dan keluar dari jaringan komputer.
Secure Socket Layer (SSL)	Protokol keamanan yang mengamankan komunikasi online dengan mengenkripsi data yang dikirim antara server dan klien.
Pretty Good Privacy (PGP)	Program yang digunakan untuk mengenkripsi dan mendekripsi pesan elektronik dengan menggunakan kunci publik dan kunci privat.
Vigenere Cipher	Metode enkripsi sederhana yang menggunakan pola pergeseran dalam alfabet untuk mengubah teks biasa menjadi ciphertext menggunakan kunci yang terdiri dari huruf-huruf.
Dashboard Layanan Pendidikan Tinggi (LLDIKTI)	Platform yang digunakan untuk mengelola data dan informasi terkait pendidikan tinggi di Indonesia.

Time Based One Time Password (TOTP)	Metode keamanan yang menghasilkan password sekali pakai berdasarkan waktu saat ini.
Plaintext	Teks biasa atau pesan sebelum dienkripsi.
Ciphertext	Teks yang telah dienkripsi dan tidak dapat dimengerti oleh pihak yang tidak berwenang.
OTO	One Time Password, password yang hanya berlaku untuk satu kali penggunaan.
REST (Representational State Transfer)	Arsitektur dan pendekatan pengembangan layanan web yang berfokus pada penggunaan protokol HTTP dan URL untuk berinteraksi dengan sumber daya online.
Otentikasi (Authentication)	Otentikasi adalah proses untuk mengonfirmasi identitas atau keaslian dari dua titik akhir koneksi. Dalam konteks keamanan sistem, otentikasi dilakukan dengan membandingkan password yang diberikan oleh klien dengan password yang tersimpan di server untuk memastikan kecocokan.
Token	Token adalah suatu kode yang digunakan dalam proses otentikasi. Token ini berfungsi sebagai bukti atau kredensial yang memverifikasi identitas pengguna atau klien saat mengakses sistem.

JSON (JavaScript Object Notation)	JSON adalah format ringkas yang digunakan untuk pertukaran data antara server dan klien. Format ini mudah dipahami oleh manusia dan mesin, dan sering digunakan dalam pesan-balik yang dikirim melalui REST API. JSON terdiri dari objek (nama/value pairs) dan array (daftar nilai).
HTTP (Hypertext Transfer Protocol)	HTTP adalah protokol jaringan lapisan aplikasi yang digunakan dalam sistem informasi terdistribusi, kolaboratif, dan hypermedia. Protokol ini memungkinkan klien dan server berkomunikasi melalui pola permintaan-respons, di mana berbagai metode seperti POST, GET, PUT, dan DELETE digunakan untuk operasi yang berbeda.
Algoritma Vigenere Cipher	Algoritma Vigenere Cipher adalah teknik enkripsi klasik yang digunakan untuk mengamankan pesan. Metode ini menggunakan substitusi karakter berdasarkan pada kunci yang terdiri dari beberapa huruf, yang menghasilkan ciphertext dari plaintext.
Enkripsi dan Deskripsi	Enkripsi adalah proses mengubah plaintext menjadi ciphertext menggunakan algoritma tertentu dan kunci. Dekripsi adalah proses sebaliknya, yaitu mengubah ciphertext kembali menjadi plaintext menggunakan

	algoritma yang sama dengan kunci yang sesuai.
Middleware	Middleware adalah perangkat lunak atau komponen yang berfungsi sebagai perantara antara aplikasi dan sistem lainnya. Dalam konteks REST API, middleware dapat digunakan untuk menambahkan lapisan keamanan, pengolahan data, atau fungsi lainnya sebelum permintaan mencapai server.
Dasa teori keamanan data	Konsep-konsep dasar yang digunakan untuk menjaga keamanan data, termasuk enkripsi, dekripsi, dan teknik keamanan lainnya.
Perangkat keras	Komponen fisik yang digunakan dalam sistem, seperti laptop Hp Pavillion dengan RAM 4GB dan smartphone iPhone 6s.
Sistem Operasi	Perangkat lunak yang mengendalikan operasi perangkat keras, misalnya Windows 11, macOS, dan Linux.
Jaringan Wifi	Jaringan nirkabel yang digunakan untuk menghubungkan perangkat dengan internet, dengan kecepatan minimal 20 Mbps atau 5 Mbps tergantung pada konteks.
Aplikasi	Perangkat lunak yang diinstal pada perangkat, seperti WhatsApp dan Gmail,

	yang digunakan sebagai media pengiriman TOTP (Time-Based One Time Password).
Software Visual Studio Code	Perangkat lunak yang digunakan untuk menulis kode program dan mengembangkan website.
Software Navicat Premium	Perangkat lunak yang digunakan untuk mengelola database.
Software Postman	Perangkat lunak yang digunakan sebagai REST CLIENT untuk menguji coba REST API.
Perancangan system	Proses merancang dan merencanakan sistem, termasuk perangkat keras dan perangkat lunak yang akan digunakan, serta proses enkripsi dan deskripsi yang akan diterapkan.
Flowchart	Diagram yang menunjukkan alur proses dalam sistem, seperti flowchart akses data penerapan TOTP.
ASCII (American Standard Code for Information Interchange)	Kode karakter yang digunakan dalam komputer untuk merepresentasikan karakter, seperti huruf, angka, dan simbol.
Tabel Vigenere	Tabel yang digunakan dalam metode Vigenere Cipher untuk menggabungkan alfabet dengan menggunakan kunci yang diulang.

Tabel ASCII	Tabel yang memetakan karakter-karakter ASCII dengan kode numerik yang sesuai.
Tabel Alfabet	Tabel yang memetakan huruf-huruf alfabet dengan nilai numerik yang sesuai.
Running-key Vigenere Cipher	Variasi dari Vigenere Cipher di mana kunci yang digunakan terdiri dari teks yang berulang, seperti cipherteks sebelumnya.
Tes Pengujian Sistem	Proses pengujian yang dilakukan untuk memastikan sistem memenuhi persyaratan dan berfungsi dengan baik.

BAB I
PENDAHULUAN

A. Latar Belakang

Dengan meningkatnya penggunaan jaringan komputer, kemajuan teknologi informasi dan komunikasi membawa perubahan yang signifikan. Keuntungannya adalah bahwa informasi dapat dibagikan sebagai informasi digital di seluruh jaringan komputer. Pada saat yang sama, keuntungan ini digunakan untuk melakukan tindakan ilegal misal peretasan username, kata kunci, dan informasi transaksi bank (Prabowo, 2015).

Menjaga kerahasiaan informasi perlu memperhatikan keamanan data, khususnya yang berisi informasi yang isinya hanya boleh diketahui oleh pihak yang berwenang. Menurut ilmu pendidikan, kriptografi adalah bidang studi yang berfokus pada keamanan data. Masalah keamanan data merupakan salah satu aspek penting dari sebuah sistem informasi. Sehingga masalah keamanan ini harus diperhatikan oleh para pemilik dan pengelola sistem informasi sebagai salah satu masalah yang dianggap penting dan harus dicari pemecahan masalahnya. Salah satu masalah keamanan data yang kurang mendapat perhatian adalah keamanan data pada aplikasi.

Keamanan data ada beberapa macam, diantaranya Enkripsi, Firewall, Secure SocketLayer, Kriptografi, Pretty Good Privacy. Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca).

Teknik enkripsi Vigenere dapat digunakan untuk menjaga keamanan dan privasi data. Menurut metode kriptografi terkenal yang dikenal sebagai enkripsi vigenere, cipher tidak dapat dipecahkan. Pendekatan ini telah ditentang sejak Kasiski dapat membacanya pada abad ke-19. Perbedaan utama antara *Vigenere Cipher* dan Caesar Cipher adalah yang pertama menggeser setiap huruf dari pesan asli dengan satu huruf

kunci, sedangkan yang kedua juga mengganti setiap huruf dengan huruf yang identik (Alam, Habibi, & Widya, 2022). Setiap baris dalam kotak mewakili huruf ciphertext yang diperoleh dengan sandi Caesar.

Dashboard Layanan Pendidikan Tinggi (LLDIKTI) adalah platform yang digunakan untuk mengelola data dan informasi terkait pendidikan tinggi di Indonesia. Platform ini digunakan untuk menghubungkan berbagai pihak yang terkait dengan pendidikan tinggi, seperti perguruan tinggi, mahasiswa, dan lembaga pemerintah terkait. Namun, seperti halnya platform digital lainnya, *Dashboard* LLDIKTI juga memiliki risiko keamanan. Tanpa adanya sistem keamanan yang memadai, data dan informasi yang disimpan pada *Dashboard* tersebut dapat dengan mudah diakses dan dimanipulasi oleh orang yang tidak berhak. Oleh karena itu, diperlukan langkah-langkah untuk meningkatkan keamanan pada platform tersebut.

Salah satu teknik yang dapat digunakan untuk meningkatkan keamanan pada *Dashboard* LLDIKTI adalah dengan menerapkan *Vigenere Cipher* pada pesan yang dikirimkan melalui platform tersebut. *Vigenere Cipher* adalah sebuah teknik enkripsi sederhana yang dapat mengubah pesan asli menjadi sebuah pesan yang sulit dipahami oleh orang yang tidak memiliki kunci enkripsi yang benar.

Dengan menerapkan *Vigenere Cipher* pada pesan yang dikirimkan melalui *Dashboard* LLDIKTI, keamanan data dapat ditingkatkan. Orang yang tidak berhak tidak dapat membaca atau memanipulasi data yang dikirimkan melalui platform tersebut tanpa memiliki kunci enkripsi yang benar. Hal ini akan menjaga kerahasiaan dan mencegah terjadinya pencurian data atau informasi yang sensitif.

Dalam konteks ini, perbedaan antara sebelum dan sesudah menerapkan *Vigenere Cipher* pada *Dashboard* LLDIKTI adalah pada tingkat keamanan data dan informasi yang disimpan pada platform tersebut. Sebelum diterapkan *Vigenere Cipher*, data dan informasi yang disimpan pada *Dashboard* LLDIKTI rentan terhadap pencurian atau manipulasi oleh

orang yang tidak berhak. Setelah diterapkan *Vigenere Cipher*, data dan informasi tersebut akan lebih terlindungi dari ancaman keamanan dan kerahasiaannya lebih terjaga.

Informasi kemahasiswaan Universitas Muhammadiyah Makassar dapat diakses secara online melalui *Dashboard*. Klien harus memasukkan kode TOTP yang dihasilkan oleh algoritma *Vigenere Cipher* untuk mengakses data ini. Karena web saat ini tidak memiliki lapisan perlindungan tambahan, informasi tersebut rentan untuk diubah atau digunakan secara tidak tepat oleh individu yang ceroboh (peretas). Berdasarkan hal tersebut maka kami tertarik untuk melakukan penelitian dengan judul Penerapan Algoritma *Vigenere Cipher* Untuk Meningkatkan Keamanan Pada *Dashboard*, mengingat maraknya kejahatan pencurian data dengan media internet.

B. Rumusan Masalah

Berdasarkan uraian diatas maka penulis dapat merumuskan masalah sebagai berikut:

1. Bagaimana penerapan Algoritma *Vigenere Cipher* untuk meningkatkan keamanan data pada pada *Dashboard*?
2. Apa saja perbedaan yang terjadi pada keamanan data *Dashboard* setelah diterapkannya algoritma *Vigenere Cipher*?

C. Tujuan Penelitian

Adapun yang menjadi tujuan penelitian adalah :

1. Algoritma *Vigenere Cipher* bertujuan untuk meningkatkan keamanan data pada *Dashboard*
2. Mengetahui perbedaan yang terjadi pada keamanan data *Dashboard* sebelum dan sesudah diterapkannya algoritma *Vigenere Cipher*.

D. Manfaat Penelitian

1. Meningkatkan keamanan data pada *Dashboard*
2. Sebagai penambahan wawasan melindungi data informasi pada sistem dengan implementasi *Time Based One Time Password (TOTP).*

E. Ruang Lingkup Penelitian

1. Mengimplementasikan TOTP untuk keamanan data pada *Dashboard*
2. Algoritma enkripsi yang digunakan adalah *Vigenere Cipher*

F. Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini mencakup konteks, masalah utama, tujuan penulisan, deskripsi masalah, metode penelitian, dan proses penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan dasar-dasar teoritis yang dikembangkan dari tinjauan literatur program yang dibuat dengan menggunakan metode kata sandi satu kali berbasis waktu yang dinyatakan, serta buku, jurnal, makalah, internet, atau referensi lain yang digunakan sebagai referensi untuk aplikasi yang dibuat.

BAB III METODE PENELITIAN

Kesulitan yang dihadapi, teknik untuk mengatasinya, desain layar, diagram alir, algoritme program, dan struktur data semuanya tercakup dalam bab ini.

BAB IV HASIL DAN PEMBAHASAN

Berdasarkan rancangan yang telah dibuat, bab ini membahas implementasi program, tampilan layar, dan pengujian program.

BAB V KESIMPULAN DAN SARAN

Untuk memastikan bahwa program bekerja dengan baik sekali lagi, bab ini menyajikan saran untuk menciptakan hasil yang tidak dihasilkan dalam proyek sebelumnya dan merangkum temuan dari hasil tersebut.

BAB II
TINJAUAN PUSTAKA

A. Landasan Teori

1. Keamanan Komputer

Di era informasi saat ini, keamanan dan kerahasiaan data sangat penting dan sekarang diperlukan karena arus informasi global semakin tidak aman. Jika informasi yang dikirimkan diretas atau disadap oleh pihak yang tidak bertanggung jawab, akan ada kerugian yang signifikan. Ada kemungkinan bahwa beberapa pengguna sistem akan dengan sengaja mengubah data dan informasi yang mereka miliki (Bagas Wahyu Utomo, 2018).

Keamanan data pada komputer tidak hanya dipengaruhi oleh teknologi tetapi juga oleh kebijakan dan proses keamanan operasional, serta tingkat manajemen sumber daya manusia. Untuk mencegah data atau informasi terbaca jika firewall dan sistem keamanan lainnya dicegat oleh orang yang tidak berwenang, tujuan utama kriptografi adalah untuk mengamankan mekanisme enkripsi (Bagas Wahyu Utomo 2018).

2. *Vigenere Cipher*

Metode enkripsi yang mudah namun lebih aman adalah *Vigenere Cipher*. Metode turunan Caesar Cipher ini menggunakan karakter huruf sebagai kunci enkripsi. Sandi substasiun polialfabet lainnya adalah Sandi Vigenere (Bagas Wahyu Utomo, 2018). *Vigenere Cipher* menggunakan huruf huruf A, B, C,..., Z, yang setara dengan angka 0, 1, 2,..., 25. Kunci ditulis berulang kali selama prosedur enkripsi. Penulisan kunci diulangi sampai setiap karakter dalam pesan memuat sepasang karakter dari kunci tersebut.

Model matematis algoritma *Vigenere Cipher* untuk enkripsi adalah sebagai berikut:

$C_i = Ek(M_i) = (M_i + K_i) \bmod 26$ ……(1)

Dan model matematika untuk deskripsinya adalah :

M*i* = Dk (C*i*) = (C*i* - K*i*) mod 26 (2)

Dengan C memodelkan ciphertext, M memodelkan plaintext, dan K pemodelan kunci. Dalam kriptografi Vigenere, kuncinya adalah kata, bukan huruf. Plaintext akan berisi pengulangan kata kunci ini sehingga kunci dan plaintext keduanya memiliki jumlah huruf yang sama. Ilustrasi penggunaan algoritma *Vigenere Cipher* dengan plain text yang akan dienkripsi adalah sebagai berikut:

Plaintext : PENELITIAN KOMPUTER

Kunci : JOKOIRFAN

Plaintext kemudian akan dienkripsi dengan cara yang dijelaskan di bawah ini:

Plaintext : PENELITIAN KOMPUTER

Kunci : JOKOIRFANJ OKOIRFAN

Ciphertext : YSXSTZYINW YYAXLYEE

Huruf kunci akan diubah menjadi angka, dengan nilai mulai dari A = 0, B = 1, hingga Z = 25, misalnya. Selanjutnya, prosedurnya sama dengan algoritma caesar cipher, dimana setiap huruf dalam plaintext dipindahkan ke lokasi yang sesuai dengan jarak yang sama dengan nilai kunci. Tabel 26x26 yang memetakan antara huruf dalam teks biasa dan huruf dalam kunci dapat digunakan untuk memetakan pergeseran dalam huruf tersebut. Gambar 1 menampilkan tabel pemetaan untuk algoritma *cipher Vigenere*.

	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 1. Tabel Pemetaan Algoritma *Vigenere Cipher (Efrandi, Asnawati, & Yupiyanti, 2014)*

Vigenere Cipher dapat dibuat tanpa teknik *Vigenere Cipher* square atau mapping table cukup dengan menyatukan plaintext dan key lalu modulo 26. Mengingat bahwa a = 0, b = 1, c = 2,..., dan z = 25.

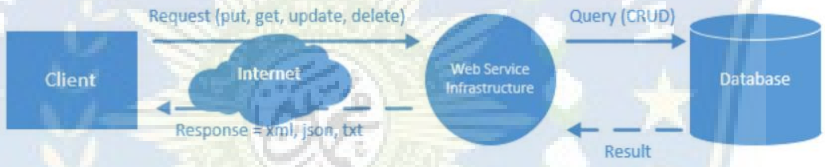
2. TOTP.

   TOTP adalah metode berbasis HMAC yang membuat OTP satu kali dengan memanfaatkan fungsi hash kriptografis untuk menggabungkan kunci rahasia dan stempel waktu saat ini. Setiap OTP yang dihasilkan memiliki batas waktu, memungkinkan pengguna untuk mengakses *password* selama 1 menit maka jika batas waktu telah habis maka *user* tidak dapat mengakses dengan menggunakan *password* sebelumnya namun *server* akan memberikan *password* baru untuk *use*.

3. REST (Representational State Transfer)

   Model arsitektur layanan web tidak benar-benar diimplementasikan oleh REST, yang merupakan semacam arsitektur layanan web dan pemutakhiran SOAP, versi awal transportasi RPC menggunakan teknologi web. REST menggunakan pengalihan status untuk mempraktikkan ide. Tujuan dari status dalam hal ini dapat dijelaskan, misalnya, dengan mengatakan bahwa jika browser meminta halaman web, server akan mengirimkan browser status halaman web saat ini.

Status halaman web dapat diubah dengan mengklik tautan yang tersedia. REST beroperasi dengan cara yang sama, menggunakan tautan HTTP untuk menavigasi dan menjalankan tugas tertentu. Intinya, URL (Uniform Resource Locators) digunakan oleh layanan web REST untuk menjelaskan sumber daya online yang Anda minta menggunakan perintah protokol HTTP (GET, POST, PUT, dan DELETE). Berbeda dengan sekelompok aktivitas yang mengolah sumber daya, orientasi pada sumber daya merupakan orientasi yang menawarkan sumber daya sebagai layanan. Selain itu, karena masih ada celah dalam standar, mereka tidak cocok untuk digunakan dalam aplikasi yang harus bekerja sama dengan aplikasi lain, di mana standar yang sangat baik akan sangat membantu karena berkomunikasi dalam bahasa yang sama. Gambar 2 Arsitektur REST.



Gambar 2. Arsitektur REST *(Chandra & Irfan, 2019)*

REST API tidak memiliki kewarganegaraan, memungkinkan panggilan dilakukan secara independen dan memberikan semua informasi yang diperlukan untuk prosedur yang berhasil di setiap panggilan. Layanan web yang berkonsentrasi pada sumber daya sistem dapat dibuat menggunakan konsep arsitektur yang ditentukan oleh arsitektur REST ini. Sumber daya yang dibuat oleh berbagai klien dalam berbagai bahasa komputer ditujukan dan dikirim melalui tautan HTTP. Dengan menggunakan metode HTTP seperti POST, GET, PUT, dan DELETE, operasi CRUD (Buat, Baca, Perbarui, dan Hapus) dapat dilakukan melalui REST. Karena REST dapat diimplementasikan di atas infrastruktur jaringan saat ini, tidak perlu mengubah protokol jaringan.

4. Otentikasi

   Teknik yang disebut Otentikasi *(Authentication)* digunakan untuk mengonfirmasi bahwa dua titik akhir koneksi akurat atau identik. Kriteria otentikasi yang berhasil, seperti halnya *password* pada umumnya, adalah *password* yang diberikan oleh klien cocok dengan *password* yang disimpan oleh *server*.

   Dalam situasi ini, kata sandi yang digunakan untuk otentikasi tidak lagi cukup aman, sehingga memerlukan penggunaan strategi otentikasi yang kuat, seperti penggunaan token (kode) dan kartu ATM. Kata sandi sebenarnya digunakan untuk meningkatkan keamanan pengguna, tetapi biaya penyedia layanan untuk menyediakan perlindungan kecil. Namun, penggunaan perangkat seluler yang digunakan sebagai token keamanan harus dihindari. Salah satunya adalah keamanan model otentikasi, yaitu penggunaan OTP untuk mengkonfirmasi pengguna (Wicaksono & Fatimah, 2018).

5. JSON (Javascript object notation)

   JSON adalah format message-back ringkas yang sederhana untuk diproduksi dan dibaca oleh manusia dan mesin. JSON adalah salah satu pesan balik yang dapat digunakan oleh REST API.

   JSON memiliki dua kategori struktur yang berbeda:

   1) Menggabungkan nama/value, juga disebut sebagai objek atau record dalam bahasa pemrograman
   2) Daftar nilai, juga disebut sebagai array dalam bahasa komputer.

6. HTTP (Hypertext Transfer Protokol)

   Protokol jaringan lapisan aplikasi yang disebut HTTP digunakan untuk sistem informasi terdistribusi, kolaboratif, dan hypermedia.

   "HTTP adalah protokol agar client dan server dapat berkomunikasi dengan gaya request-response," (Listanto & Hartanto, 2018). Format dan transmisi pesan, serta perilaku dan respons browser web terhadap berbagai permintaan, semuanya diatur oleh HTTP.

HTTP adalah protokol jaringan layer aplikasi yang digunakan untuk sistem informasi terdistribusi, kolaboratif, dan hypermedia (Handoko & Aditya, 2017).

Gagasan HTTP dapat dicirikan sebagai protokol jaringan lapisan aplikasi yang digunakan untuk sistem informasi terdistribusi, kolaboratif, dan hypermedia, di mana protokol seperti klien dan server dapat berkomunikasi dalam pola respons-permintaan. Kesimpulan ini dapat ditarik dari teori yang dikemukakan di atas.

B. Penelitian Terkait

Ada beberapa penelitian terkait dengan penerapan algoritma *Vigenere Cipher* untuk meningkatkan keamanan data pada *Dashboard*.

1. Hasil Penelitian Uung Ungkawa, Irma Amelia Dewi, Kurnia Ramadhan Putra (2017)

   Penelitian Uung Ungkawa, Irma Amelia Dewi, Kunria Ramadhan Putra yang berjudul "IMPLEMENTASI ALGORITMA TIME-BASED ONE TIME PASSWORD DALAM OTENTIKASI TOKEN INTERNET BANKING". Penerapan algoritma Time-Based One Time Password (TOTP) pada otentikasi token internet banking berbasis Android merupakan tujuan dari proyek ini (Ungkawa, Dewi, & Putra, 2015).

   Atas dasar pengecekan fakta, kesimpulan berikut dapat ditarik dari penelitian ini:

   a. Kata sandi satu kali dapat dibuat menggunakan algoritma Kata Sandi Satu Kali Berbasis Waktu.
   b. Implementasi algoritma TimeBased One Time Password (TOTP) dan Something You Know (kata sandi web internet banking) dan Something You Have (token android) teknik otentikasi dua faktor (2FA) berhasil.
   c. Pengguna wajib menginput token pada setiap transaksi di website internet banking, sehingga meningkatkan keamanan transaksi.

d. Sinkronisasi token antara internet banking online dan Android telah tercapai.
e. Di situs internet banking, pengguna hanya memiliki batas waktu 3 menit untuk setiap transaksi; jika batas waktu terlampaui, transaksi akan gagal.

2. Hasil Penelitian Muhammad Iqbal Perkasa, Eko Budi Setiawan (2018)

   Penelitian Muhammad Iqbal Perkasa, Eko Budi Setiawan yang berjudul "PEMBANGUNAN WEB SERVICE DATA MASYARAKAT MENGGUNAKAN REST API DENGAN ACCESS TOKEN". Dari hasil yang didapat dari tahap-tahap yang telah dikerjakan melalui proses perancangan, implementasi, pengujian, dan wawancara dengan administrator, didapat kesimpulan sebagai berikut (Perkasa & Setiawan, 2018):

   a. Web service ini mampu dan dapat mempercepat pendaftaran dengan keandalan server yang baik.
   b. Administrator data penduduk dapat dimudahkan dalam memonitor penggunaan data penduduk dan mengatur hak akses masing-masing access token.

3. Hasil Penelitian Bagas Wahyu Utomo, Subandi (2018)

   Penelitian Bagas Wahyu Utomo, Subandi yang berjudul "IMPLEMENTASI ALGORITMA ENKRIPSI CAESAR CIPHER DAN *VIGENERE CIPHER* PADA APLIKASI MOBILE DAN REST API DATA PERUSAHAAN PADA PT. CENTRAL CAPITAL FUTURES". Menerapkan teknik kriptografi yang menggabungkan algoritma Caesar Cipher dan *Vigenere Cipher* selama proses pertukaran data merupakan tujuan dari pekerjaan ini (Utomo & Subandi, 2018).

   Atas dasar pengecekan fakta, kesimpulan berikut dapat ditarik dari penelitian ini:

   a. Karena konversi dari plaintext ke ciphertext yang lebih panjang, ukuran data yang telah dienkripsi dan didekripsi berubah.

b. Aplikasi ini hanya dapat digunakan oleh pengguna yang telah terdaftar di database perusahaan.
c. Menurunkan kemungkinan intersepsi data oleh pihak yang ceroboh.

4. Hasil penelitian Ismail Adi Susanto, Achmad Solichin (2018)

   Penelitian Ismail Adi Susanto , Achmad Solichin yang berjudul "ENKRIPSI DATA PENGGAJIAN DENGAN ALGORITMA CAESAR CIPHER DAN *VIGENERE CIPHER* PADA PT. KEMASINDO CEPAT NUSANTARA". Kesimpulan berikut dapat ditarik dari desain, produksi, berbagai pengujian, dan analisis sistem informasi penggajian terenkripsi berbasis web ini (Susanto & Achmad, 2018):

   a. Informasi atau data gaji karyawan dapat dirahasiakan dengan penggunaan solusi penggajian enkripsi berbasis web ini.
   b. Bagi mereka yang tertarik, sistem penggajian enkripsi ini menawarkan sesuatu yang segar dan menarik untuk digunakan.
   c. Untuk administrator baru, sistem penggajian ini mudah disiapkan dan digunakan.
   d. Algoritma Caesar cipher dan Vigenere keduanya dapat diimplementasikan.

5. Hasil Penelitian Joko Christian Chandra, Irfan Irmawan (2019)

   Penelitian Joko Christian Chandra, Irfan Irmawan yang berjudul "PENERAPAN KRIPTOGRAFI PADA REST API WEB SERVICE STUDI KASUS KAFA PHOTOGRAPHY". Kesimpulan berikut dapat terbentuk setelah menyelesaikan proses pengumpulan kebutuhan, analisis, desain, pengembangan, dan sejumlah uji coba (Chandra & Irfan, 2019):

   a. Proses pengembangan sistem middleware efektif menggunakan metodologi waterfall.
   b. Hasil akhir dari pengembangan ini adalah sistem middleware yang dibangun di atas layanan web RESTful yang menggunakan kriptografi Viginere untuk menyimpan data dengan lebih aman.

c. Meskipun mereka memiliki bahasa dan platform pemrograman yang berbeda, teknologi antarmuka yang berbeda seperti android dan aplikasi web dapat mengakses layanan web yang dibuat menggunakan teknik REST.

   Berikut adalah beberapa rekomendasi yang dapat dilakukan oleh penelitian pengembangan:

   1) Penambahan layanan titik akhir layanan web diperlukan karena beberapa prosedur, seperti pembatalan pesanan, masih belum didukung.
   2) Menggunakan cipher viginere yang ditingkatkan dan metode kriptografi lain yang lebih rumit, dan melakukan studi keamanan dan kinerja untuk validasi.

6. Hasil Penelitian Bima Galih Ritwiyan, Rizky Pradana (2021)

   Penelitian Bima Galih Ritwiyan, Rizky Pradana yang berjudul "IMPLEMENTASI KRIPTOGRAFI PADA WEB SERVICE DENGAN METODE CAESAR CIPHER BERBASIS JAVA DI PT. INTEGRASI MEDIA KREASI". Tujuan laporan penelitian ini adalah untuk melindungi data yang telah disediakan melalui layanan web untuk menghentikan penggunaan data yang tidak sah dan pencurian data (Ritwiyan & Pradana, 2021).

   Kesimpulan berikut dibuat berdasarkan analisis masalah dan penyelesaiannya:

   a. Karena sudah ada enkripsi pada layanan web, penjahat tidak dapat mengakses konten data meskipun enkripsi memungkinkan tampilan antarmuka pengguna aplikasi diubah.
   b. Informasi aset perusahaan yang penting disimpan dalam data layanan web, sehingga tidak mungkin bagi penjahat untuk melihat atau mencuri konten data untuk keuntungan mereka sendiri. Ini karena layanan web dengan data terdistribusi terenkripsi tidak dapat dibaca oleh pencuri.

c. Kriptografi Caesar Cipher hanya mengenkripsi teks biasa dengan kunci satu arah (konvensional), sehingga tidak mengubah ukuran data dan tidak mengubah dekripsi.
d. Tanpa persetujuan PT. Integrasi Media Kreatif, pengembang lain dapat menggabungkan aplikasi mereka dengan manajemen aset layanan web, tetapi data yang dihasilkan dari layanan web tidak dapat dibaca karena dienkripsi.
e. Layanan web aplikasi manajemen aset memiliki keberhasilan 100% dengan mengenkripsi dan mendekripsi data dengan benar dan berhasil.

7. Hasil Penelitian Veny Cahya Hardita, Eka Wahyu Sholeha (2021)

   Penelitian Veny Cahya Hardita, Eka Wahyu Sholeha yang berjudul "PENERAPAN KOMBINASI METODE *VIGENERE CIPHER*, CAESAR CIPHER DAN SIMBOL BACA DALAM MENGAMANKAN PESAN". Tujuan dari penelitian ini agar sebuah informasi yang dikirim dapat dibuat lebih aman dan mengurangi kemungkinan terjadinya pencurian informasi dengan menggabungkan dua algoritma menggunakan kunci simetris yaitu Caesar Cipher dengan *Vigenere Cipher* (Hardita & Sholeha, 2021).

   Dalam menjaga kerahasiaan suatu pesan dapat digunakan kombinasi algoritma *Vigenere Cipher* dan Caesar Cipher agar keamanan isi pesan terproteksi lebih kuat dan aman sehingga apabila pesan yang dikirimkan dibajak ataupun disadap oleh orang yang tidak bertanggung jawab maka si pembajak kesulitan untuk mengetahui isi pesannya. Pesan yang telah di dekripsi dari kombinasi *Vigenere Cipher* dan caesar cipher dapat dibaca dan dipahami oleh penerima pesan. Hanya pengirim dan penerima pesan yang mengetahui kunci dari pesan tersebut. Sehingga kerahasiaan dan keaslian pesan terjaga sampai kepada penerima. Dari contoh proses kriptografi menggunakan kalimat "HABIS GELAP TERBITLAH TERANG" didapatkan suatu hasil yaitu >*/@!!?#>[/=*@/+#!:<(@!# sehingga orang lain yang tidak berhak

untul menerima pesan rahasia tersebut kesulitan dalam membaca pesannya. Dan hanya penerima yang bisa membaca pesan tersebut dengan melalui proses Deskripsi. Keunggulan dari penelitian ini yaitu menerapkan *Vigenere Cipher* tidak hanya menggunakan 1 kunci saja tetapi menggunakan 2 kunci dalam pengamanannya serta menggunakan hasil keluaran berupa symbol bukan huruf untuk memperkuat pengamanan isi pada suatu pesan.

8. Hasil Penelitian Tomy Satria Alasi, Pristiwati Fitriani (2022)

   Hasil Penelitian Tomy Satria Alasi, Pristiwati Fitriani yang berjudul "PENINGKATAN KEAMANAN UNTUK PASSWORD MENGGUNAKAN ALGORITMA *VIGENERE CIPHER*" (Alasi & Prastiwati, 2022). 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. Pengembangan komponen sistem yang mampu melakukan proses penyandian record dengan hanya menentukan nama database. Pelebaran jumlah karakter record dan kombinasi kunci serta faktor pengali yang acak, sangat baik dalam upaya peningkatan keamanan dan kesulitan pemecahan hasil penyandian. Implementasi algoritma *Vigenere Cipher* dapat dikembangkan pada aplikasi yang berbasis online dengan menggunakan database yang dibuat dari aplikasi yang database lainnya.

9. Hasil Penelitian Dicky Arfandy, Magdalena Simanjuntak, Tio Pasaribu (2022)

   Penelitian Dicky Arfandy, Magdalena Simanjuntak, Tio Pasaribu yang berjudul "PENERAPAN METODE *VIGENERE CIPHER* UNTUK MENGAMANKAN DATA TEXT". Penerapan metode *Vigenere Cipher* merupakan tujuan dari proyek ini untuk mengamankan data teks (Arfandy, Simanjuntak, & Pasaribu, 2022).

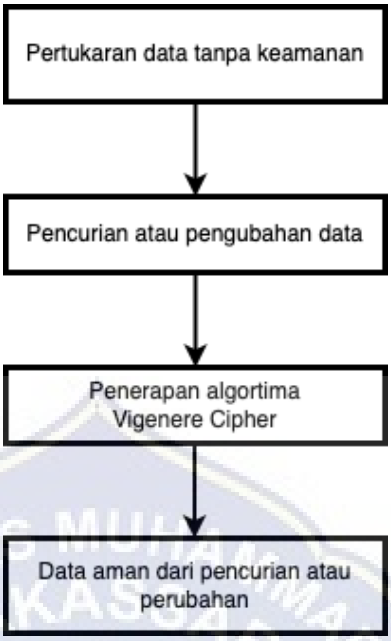
Berikut temuan yang dapat penulis ambil dari analisis, perancangan, implementasi, dan pengujian sistem pada makalah yang berjudul "Penerapan Metode *Vigenere Cipher* untuk Mengamankan Data Teks":

a. Sebuah data teks dapat diamankan secara efektif menggunakan program keamanan data teks.
b. Penggunaan metode *Vigenere Cipher* oleh sistem ini memungkinkannya mengamankan data teks secara memadai.
c. Metode *cipher Vigenere* dapat digunakan untuk mengamankan data teks dengan sistem ini.

C. Kerangka Pikir

API biasanya digunakan sebagai perantara antara server dan klien dalam sistem pertukaran data. Karena sistem tidak dapat mengidentifikasi bukti nyata bahwa data tersebut milik Anda, sistem pertukaran data memiliki keamanan yang sangat lemah. Oleh karena itu, data dapat dengan mudah dicuri, dirusak, atau dihapus oleh peretas. Data penting dengan demikian terancam dan dapat menyebabkan kerugian bagi pihak ketiga.

Oleh karena itu, sangat penting untuk menambah keamanan pada sistem pertukaran data untuk lebih meningkatkan keamanan dan menghentikan hal-hal yang tidak menyenangkan tersebut terjadi. Algoritma *Vigenere Cipher* dan TOTP, yang memiliki masa berlaku singkat dan dapat berubah seiring waktu, dapat digunakan untuk menambah keamanan tambahan. Data penting di dasbor tidak dapat dengan mudah dicuri atau diubah karena mekanisme pertukaran data menjadi lebih aman. Berdasarkan uraian di atas, kerangka konseptual penelitian dapat diringkas sebagai berikut:



Gambar 3. Kerangka Pikir

BAB III
METODE PENELITIAN

A. Tempat dan Waktu Penelitian

1. Lokasi Penelitian

Fakultas Teknik Universitas Muhammadiyah Makassar menjadi tempat pengambilan data penelitian ini.

2. Waktu Penelitian

Mulai Desember 2022, kegiatan penelitian akan dilakukan hingga seluruh prosedur pengumpulan data selesai.

Table 1. Waktu Penelitian

NO	KEGIATAN	BULAN										
		DESEMBER 2022				JANUARI 2023				FEBRUARI 2023		
		1	2	3	4	1	2	3	4	1	2	3
1	Perumusan topik penelitian											
2	Perencanaan penelitian											
3	Pelaksanaan penelitian											
	a. Pembuatan Program											
	b. Penelitian uji Program											
4	Penulisan laporan											

B. Alat dan Bahan

Dasar teori keamanan data yang digunakan dalam penelitian ini diambil dari berbagai sumber, antara lain buku, jurnal, dan artikel baik dalam format hardcopy maupun softcopy. Berikut persyaratan teknis alat yang digunakan dalam penelitian ini:

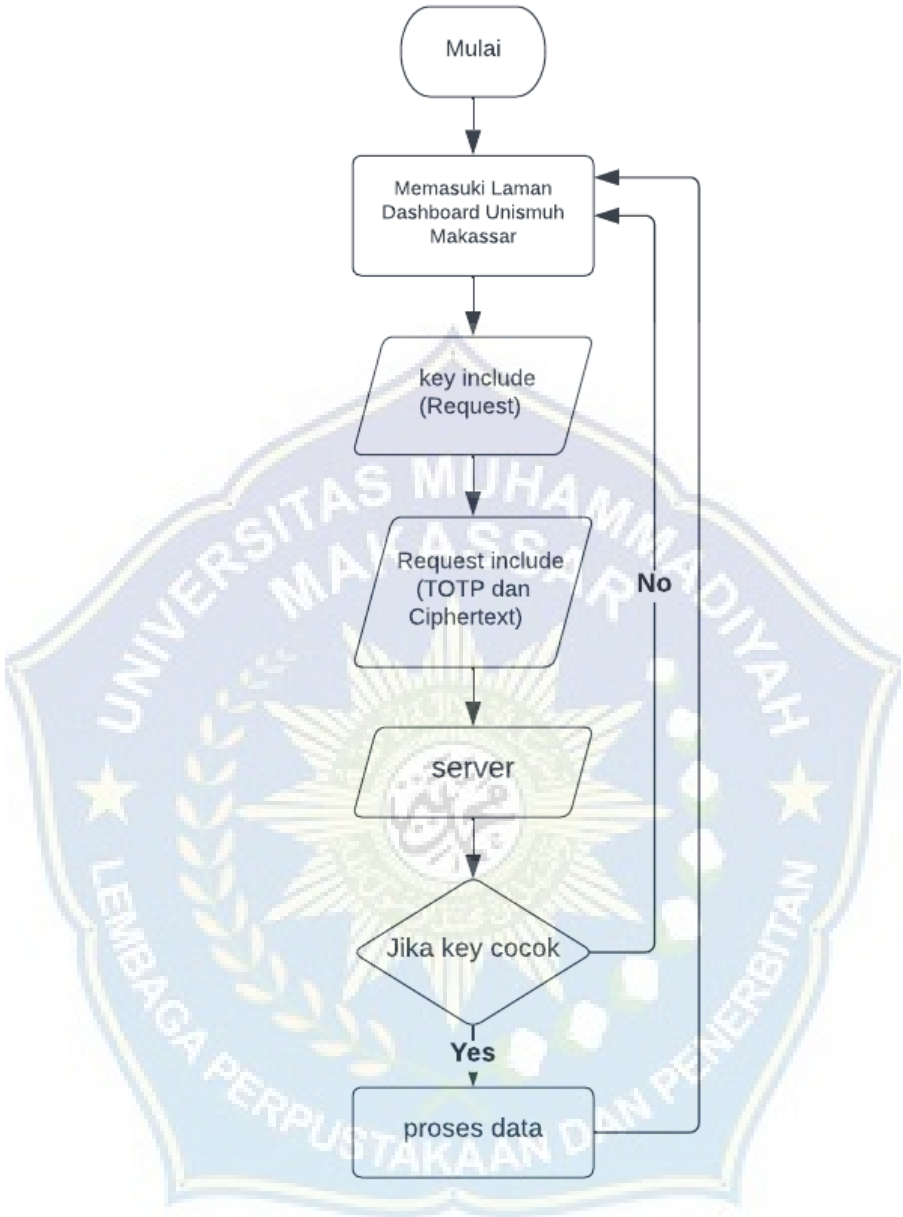
1. Perangkat keras dan sistem operasi yang digunakan.
   a. Laptop *Hp Pavillion, Memory 4Gb*
   b. Sistem Operasi *Windows 11*
   c. Jaringan *wifi* minimal 20 mbps
   d. Aplikasi *WhatsApp* dan *Gmail* sebagai media mengirimkan TOTP
   e. *Smartphone Iphone 6s* (sebagai tempat mengirimkan *TOTP*)
2. Perangkat lunak yang digunakan.
   a. *Software Visual Studio Code* untuk menulis kode program sehingga menjadi website
   b. *Software Navicat Premium,* berfungsi untuk mengelola database
   c. *Software Postman,* berfungsi sebagai *REST CLIENT* untuk uji coba *REST API*
3. Perangkat keras dan sistem operasi untuk pengimplementasian
   a. Laptop, *Personal Computer* (PC), *Tablet, Smartphone*
   b. Sistem Operasi *macOs, Windows, Linux*
   c. Jaringan *wifi* Minimal 5mbps
4. Perangkat lunak untuk pengimplementasian
   a. *Browser (Google Chrome, Safari, Mozilla firefox)*

C. Perancangan sistem

Tahapan ini meliputi metode atau metodologi yang digunakan untuk mengembangkan sistem, perangkat keras atau perangkat lunak apa saja yang digunakan, proses enkripsi, dan bagaimana metode tersebut diterapkan dalam penelitian tugas akhir.

1. *Flowchart*

   Berikut adalah desain *flowchart* dan algoritma alur penerapan algoritma *Vigenere Cipher* untuk meningkatkan keamanan pada *Dashboard*.



Gambar 4. *Flowchart* akses data penerapan TOTP

Algoritma proses dari *flowchart* diatas:

1. Client mengakses laman *Dashboard* Unismuh lalu melakukan login
2. System kemudian melakukan generate key
3. Key include sesuai request
4. Request include totp dan ciphertext

5. Server terhubung
6. Jika key cocok maka data bias di akses/terproses.
7. Jika key tidak cocok maka otomatis kembali ke laman dashboard Unismuh Makassar

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

Enkripsi : Ci = (Pi+Ki) mod 26

Deskripsi : Pi = (Ci – Ki) mod 26

Keterangan

Pi : Nilai karakter plainteks ke-i

Ci : Nilai karakter cipherteks ke-i

Ki : Nilai karakter kunci ke-i

Pada rumus diatas terdapat penggunaan mod 26 dikarenakan untuk menyandikan suatu pesan, digunakan sebuah tabel alfabet yang disebut tabel Vigenere. Tabel Vigenere berisi alfabet yang dituliskan ke dalam 26 baris, masing-masing baris digeser satu urutan ke kiri dari baris sebelumnya, setiap huruf disandingkan dengan menggunakan baris yang berbeda-beda, sesuai kata kunci yang diulang.

```
import { encrypt } from "vigenere-cipher";
import crypto from "crypto";
import Long from "long";

export const numberToAscii = (number) => {
    let _number = parseInt(number) + 65;
    return String.fromCharCode(_number);
}

export const generateTOTP = (secret, encryptionLength) => {
     let encryptedTotp = '';
    const time = Math.floor(Date.now() / 1000 / 5);
    const timeLong = Long.fromNumber(time);
    const buffer = Buffer.from(timeLong.toBytesBE());
    const hmac = crypto.createHmac('sha1', secret).update(buffer).digest();
    const offset = hmac[hmac.length - 1] & 0xf;
    let code = ((hmac[offset] & 0x7f) << 24)
        | ((hmac[offset + 1] & 0xff) << 16)
        | ((hmac[offset + 2] & 0xff) << 8)
        | (hmac[offset + 3] & 0xff);
    code = code.toString().padStart(encryptionLength, '0').slice(0, encryptionLength);
    for (let i = 0; i < code.length; i++) {
        encryptedTotp += numberToAscii(code[i]);
    }
    return encrypt(encryptedTotp, secret);
}

export const generateKey = (second) => {
    const time = Math.floor(Date.now() / 1000 / second);
    let timeToString = time.toString();
    let key = '';
    for (let i = 0; i < timeToString.length; i++) {
        key += numberToAscii(timeToString[i]);
    }
    return key;
}
```

Gambar 5. TOTP Frontend

Adapun proses Enkripsi dan Deskripsi dari program di atas, sebagai berikut:

A. Enkripsi

a. Merubah time berupa angka (pesan asli) yang dihasilkan oleh program menjadi teks (huruf) menggunakan variasi full vigenere cipher.

   Time yang dihasilkan adalah “168390073”, dimana time ini termasuk timestamp dari perubahan waktu saat ini yang dihasilkan Date.now() dari milidetik menjadi detik. Time (pesan asli) yang dihasilkan dapat berubah terus tergantung kapan client merequest data.

b. Menentukan kunci variasi full vigenere cipher

   Kunci yang digunakan adalah “qwerty”.

c. Melakukan perhitungan pada time yang akan kita rubah menjadi teks dengan cara setiap angka di jumlahkan dengan ASCII karakter A=65. Sebenarnya, pada program bebas memakai ASCII karakter huruf apa saja karna tetap memiliki fungsi dan tujuan yang sama, jadi saya hanya menggunakan ASCII A saja.

Time	1	6	8	3	9	0	0	7	3
Hasil	66	71	73	68	74	65	65	72	68

Table 2. Perhitungan Pada Time

Kemudian cek huruf sesuai kode yang di atas pada table ASCII berikut:

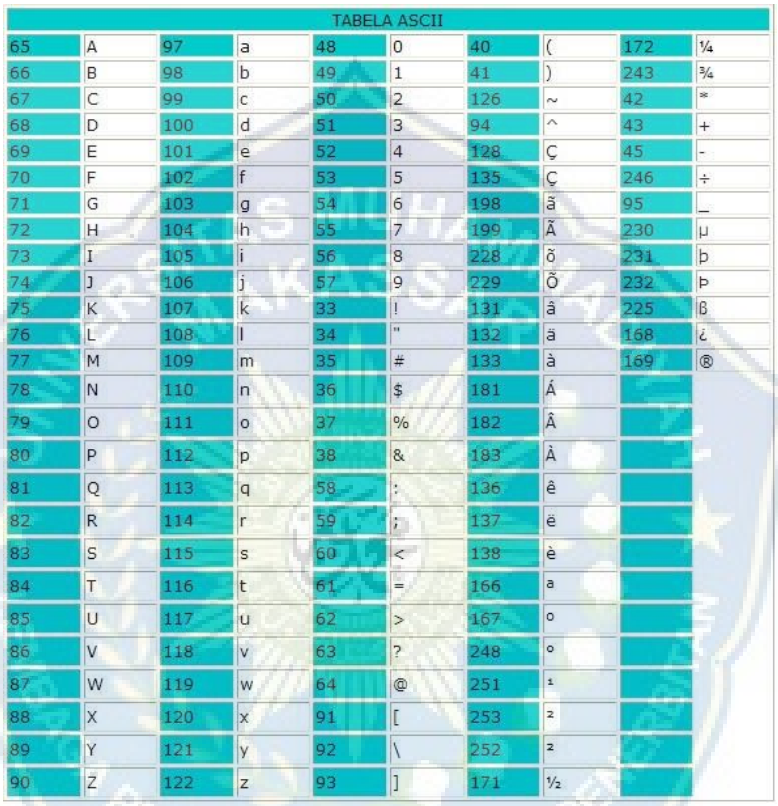


TABELA ASCII

65	A	97	a	48	0	40	(	172	¼
66	B	98	b	49	1	41	)	243	¾
67	C	99	c	50	2	126	~	42	*
68	D	100	d	51	3	94	^	43	+
69	E	101	e	52	4	128	Ç	45	-
70	F	102	f	53	5	135	Ç	246	÷
71	G	103	g	54	6	198	ã	95	_
72	H	104	h	55	7	199	Ã	230	µ
73	I	105	i	56	8	228	õ	231	þ
74	J	106	j	57	9	229	Õ	232	Þ
75	K	107	k	33	!	131	â	225	ß
76	L	108	l	34	"	132	ä	168	¿
77	M	109	m	35	#	133	à	169	®
78	N	110	n	36	$	181	Á		
79	O	111	o	37	%	182	Â		
80	P	112	p	38	&	183	À		
81	Q	113	q	58	:	136	ê		
82	R	114	r	59	;	137	ë		
83	S	115	s	60	<	138	è		
84	T	116	t	61	=	166	ª		
85	U	117	u	62	>	167	º		
86	V	118	v	63	?	248	°		
87	W	119	w	64	@	251	¹		
88	X	120	x	91	[	253	²		
89	Y	121	y	92	\	252	³		
90	Z	122	z	93	]	171	½		

Table 3. Tabel ASCII

Berdasarkan table ASCII diatas maka hasil dari perubahan time “168390073” menjadi teks yaitu: “BGIDJAAHD”

Pi	B	G	I	D	J	A	A	H	D

d. Melakukan perhitungan enkripsi vigenere cipher menggunakan rumus Ci = (Pi + Ki) mod 26

Ki	Q	W	E	R	T	Y	Q	W	E

Tabel kunci dari setiap karakter Cipherteks variasi auto key Vigenere Cipher

Table 4. Tabel Enkripsi

Proses enkripsi menggunakan tabel substitusi model matematika dari enkripsi pada algoritma vigener cipher yaitu dengan cara mengkonversi huruf alphabet dari A-Z menjadi 0-25

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Table 5. Tabel Alfabet

C1 (B,Q) = (P1 + K1) mod 26 = (1 + 16) mod 26 = 17 mod 26 = 17

C2 (G,W) = (P2 + K2) mod 26 = (6 + 22) mod 26 = 28 mod 26 = 2

C3 (I,E) = (P3 + K3) mod 26 = (8 + 4) mod 26 = 12 mod 26 = 12

C4 (D,R) = (P4 + K4) mod 26 = (3 + 17) mod 26 = 20 mod 26 = 20

C5 (J,T) = (P5 + K5) mod 26 = (9 + 19) mod 26 = 28 mod 26 = 2

C6 (A,Y) = (P6 + K6) mod 26 = (0 + 24) mod 26 = 24 mod 26 = 24

C7 (A,Q) = (P7 + K7) mod 26 = (0 + 16) mod 26 = 16 mod 26 = 16

C8 (H,W) = (P8 + K8) mod 26 = (7 + 22) mod 26 = 29 mod 26 = 3

C9 (D,E) = (P9 + K9) mod 26 = (3 + 4) mod 26 = 7 mod 26 = 7

e. Mendapatkan hasil enkripsi variasi auto-key vigenere cipher “RCMUCYQDH”

B. Deskripsi

a. Melakukan perhitungan vigenere cipher menggunakan rumus Pi = (Ci – Ki) mod 26

Tabel kunci dari setiap karakter cipherteks variasi Running-key Vigenere cipher

Ci	R	C	M	U	C	Y	Q	D	H
Ki	Q	W	E	R	T	Y	Q	W	E

Table 6. Tabel Kunci

P1 (R,Q) = (P1 - K1) mod 26 = (17 - 16) mod 26 = 1 mod 26 = 1

P2 (C,W) = (P2 - K2) mod 26 = (2– 22) mod 26 = -20 mod 26 = 6

P3 (M,E) = (P3 – K3) mod 26 = (12 – 4) mod 26 = 8 mod 26 = 8

P4 (U,R) = (P4 - K4) mod 26 = (20 – 17) mod 26 = 3 mod 26 = 3

P5 (C,T) = (P5 – K5) mod 26 = (2 – 19) mod 26 = -17 mod 26 = 9

P6 (Y,Y) = (P6 – K6) mod 26 = (24 – 24) mod 26 = 0 mod 26 = 0

P7 (Q,Q) = (P7 – K7) mod 26 = (16 – 16) mod 26 = 0 mod 26 = 0

P8 (D,W) = (P8 – K8) mod 26 = (3 – 22) mod 26 = -19 mod 26 = 7

b. Mendapatkan hasil deskripsi metode vigenere cipher variasi full vigenere cipher “BGIDJAAHD”.

D. Teknik Pengujian Sistem

Pengujian sistem adalah pengujian yang dilakukan sesuai dengan persyaratan atau standar perangkat lunak. Tes ini biasanya dilakukan dengan menggunakan persyaratan yang dianalisis secara manual dan dadakan.

Black Box Testing (Pengujian kotak hitam) bertujuan untuk menunjukkan bagaimana perangkat lunak menjalankan perannya, menentukan apakah data input dan output telah beroperasi sesuai dengan rencana, dan menentukan apakah data yang disimpan secara eksternal selalu diperbarui. (Nurajizah & Aziz, 2018).

Sedangkan pengertian lain tentang *Black-Box Testing* merupakan Teknik pengujian perangkat lunak yang berfokus pada spesifikasi fungsional dari perangkat lunak (Jaya, 2018). Menurut Pressman dalam (Khasanah, Kesuma, & Wijianto, 2018) “*black box testing* merupakan pengujian yang memungkinkan

software engineer mendapatkan serangkaian kondisi input yang sepenuhnya menggunakan semua persyaratan fungsional untuk suatu program"

Pengujian sistem yang akan dilakukan pada penelitian ini terdapat beberapa poin antara lain:

1. Pengujian enkripsi data

   Secara khusus mengevaluasi kelayakan pembuatan TOTP berikut enkripsi data menggunakan teknik *Vigenere Cipher*.

2. Pengujian TOTP

   Hal ini dilakukan untuk memverifikasi keefektifan pertukaran data menggunakan kode TOTP dengan memasukkan sejumlah kode TOTP pada waktu yang berbeda, serta memasukkan kode TOTP yang salah.

E. Teknik Analisis Data

Data dapat dikumpulkan untuk penelitian kualitatif dari berbagai sumber dan kumpulan data yang berbeda hingga titik maksimum, yang sering dikenal sebagai titik jenuh.

Dalam analisis data, ada tiga model yang saling berinteraksi: pengumpulan data, reduksi data, penyajian data, dan penarikan kesimpulan.

1. Pengumpulan Data

Peneliti menggunakan peralatan yang disebut instrumen pengumpul data untuk mengumpulkan data secara terorganisir dan efektif. Dalam semua upaya penelitian, penelitian instrumental memainkan peran penting dan cukup vital. Instrumen akan digunakan untuk mengumpulkan informasi yang akan digunakan untuk mengatasi masalah, mengidentifikasi sumber daya yang akan membantu mencapai tujuan, dan memvalidasi hipotesis. Variabel dalam hipotesis ditentukan oleh data yang dikumpulkan.

2. Reduksi Data

Reduksi data merupakan langkah dalam proses pengolahan data yang dilakukan setelah penelitian selesai. Setelah mengumpulkan data dari hasil penelitian dan sebelum reduksi data, berbagai alat membantu pekerjaan peneliti dalam mencapai tujuan penelitian (Salmaa, 2022).

Setiap peneliti akan diarahkan oleh tujuan dengan mempersempit ruang lingkup data yang dapat diakses. Fokus utama penelitian kualitatif adalah hasil. Oleh karena itu, peneliti harus berkonsentrasi padanya saat menurunkan data jika peneliti menemukan sesuatu yang dianggap outlier, tidak diketahui, atau tidak berpola. Reduksi data adalah aktivitas mental yang sulit yang membutuhkan kecerdasan tinggi dan banyak pengetahuan (Dqlab, 2020).

3. Display Data.

Salah satu tingkatan pendekatan analisis data kualitatif adalah penyajian data. Penyajian data adalah kegiatan di mana kumpulan data diatur dalam cara yang logis dan dapat dipahami, memungkinkan penarikan kesimpulan. Data kualitatif dapat disajikan dalam berbagai cara, termasuk teks naratif (dalam bentuk catatan lapangan), matriks, grafik, jaringan, dan bagan. Data akan disusun dan disajikan dalam pola relasional melalui tampilan data, sehingga lebih mudah dipahami (Dqlab, 2020).

4. Penarikan Kesimpulan

Menarik kesimpulan dan memvalidasi data untuk mengamati dampak reduksi data sambil tetap mengacu pada tujuan analisis yang ingin dicapai merupakan tahap terakhir dalam pendekatan analisis data kualitatif. Fase ini berusaha menjelaskan pentingnya data yang dikumpulkan dengan mengidentifikasi koneksi, kesejajaran, dan perbedaan untuk menarik temuan yang dapat digunakan untuk mengatasi masalah saat ini (Dqlab, 2020).

Penilaian awal hanyalah bersifat sementara dan dapat direvisi jika tidak ada bukti tambahan yang ditemukan saat mengumpulkan data. Namun, kesimpulan yang diambil dapat dipercaya asalkan evaluasi awal didukung oleh fakta yang dapat dipercaya. Verifikasi berfungsi untuk meningkatkan akurasi dan objektivitas evaluasi kesesuaian data dengan tujuan yang digariskan dalam tesis sentral analisis. Pembekalan rekan adalah salah satu metode untuk mencapai hal ini.

BAB IV
HASIL DAN PEMBAHASAN

A. Penanganan Masalah

Pada riset kali ini, analisis masalah yang didapatkan oleh penulis, berdasarkan rumusan masalah yang ada, bahwa permasalahan yang terjadi adalah pada system pertukaran atau sharing data masih memiliki kelemahan, yaitu tidak adanya keamanan yang memadai dalam system pertukuran data tersebut. Tujuan dari penelitian ini adalah untuk mengimplementasikan algoritma Vigenere Chiper yang diterapkan pada mekanisme otentikasi TOTP. Berdasarkan tujuan penelitian tersebut, maka dapat disimpulkan bahwa metode yang akan digunakan dalam penelitian ini ialah metode penelitian terapan. Yang dimana hasil dari penelitian tersebut dapat langsung diterapkan untuk memecahkan permasalahan yang ada. Dari tahapan awal aplikasi yaitu client menggenerate pesan yang telah di enkripsi menggunakan Vigenere Chiper. Kemudian pesan tersebut dikirim ke server, Langkah selanjutnya yaitu server melakukan validasi pesan dari client. Jika pesan yang dikirimkan client sama dengan yang telah degenerate oleh server. Maka proses pertukaran data dianggap aman dan akan diizinkan secara otomatis.

B. Tabel Pengujian

Tabel berikut adalah hasil uji coba yang telah dilakukan beberapa kali untuk mengakses data pada dashboard unismuh.

No	Time Frontend (Client)	Time Backend (Server)	Hasil
1.	5 detik	6 detik	Gagal

2	3 detik	3 detik	Berhasil
3	5 detik	5 detik	Berhasil
4	8 detik	7 detik	Gagal
5	6 detik	6 detik	Berhasil
6	9 detik	13 detik	Gagal
7	12 detik	22 detik	Gagal
8	3 detik	7 detik	Gagal
9	4 detik	4 detik	Berhasil
10	11 detik	10 detik	Gagal
11	11 detik	11 detik	Berhasil
12	9 detik	9 detik	Berhasil
13	8 detik	8 detik	Berhasil
14	20 detik	20 detik	Berhasil
15	17 detik	17 detik	Berhasil
16	32 detik	32 detik	Berhasil
17	10 detik	1 detik	Gagal
18	8 detik	3 detik	Gagal
19	4 detik	10 detik	Gagal
20	17 detik	17 detik	Berhasil
21	17 detik	1 detik	Gagal
22	18 detik	18 detik	Berhasil
23	27 detik	27 detik	Berhasil
24	23 detik	20 detik	Gagal
25	22 detik	12 detik	Gagal
26	43 detik	40 detik	Gagal
27	30 detik	31 detik	Gagal
28	14 detik	14 detik	Berhasil
29	15 detik	15 detik	Berhasil
30	19 detik	15 detik	Gagal
31	25 detik	24 detik	Gagal

32	25 detik	31 detik	Gagal
33	16 detik	16 detik	Berhasil
34	16 detik	11 detik	Gagal
35	42 detik	42 detik	Berhasil
36	52 detik	52 detik	Berhasil
37	38 detik	38 detik	Berhasil
38	29 detik	29 detik	Berhasil
39	26 detik	14 detik	Gagal
40	51 detik	51 detik	Berhasil
41	33 detik	15 detik	Gagal
42	34 detik	34 detik	Berhasil
43	25 detik	25 detik	Berhasil
44	21 detik	8 detik	Gagal
45	9 detik	17 detik	Gagal
46	16 detik	10 detik	Gagal
47	20 detik	20 detik	Berhasil
48	24 detik	24 detik	Berhasil
49	57 detik	57 detik	Berhasil
50	58 detik	58 detik	Berhasil
51	59 detik	59 detik	Berhasil
52	42 detik	42 detik	Berhasil
53	40 detik	40 detik	Berhasil
54	33 detik	33 detik	Berhasil
55	30 detik	14 detik	Gagal
56	63 detik	63 detik	Berhasil
57	50 detik	66 detik	Gagal
58	47 detik	57 detik	Gagal
59	38 detik	33 detik	Gagal
60	49 detik	49 detik	Berhasil
61	50 detik	50 detik	Berhasil

62	50 detik	51 detik	Gagal
63	77 detik	77 detik	Berhasil
64	19 detik	18 detik	Gagal
65	29 detik	29 detik	Berhasil
66	66 detik	66 detik	Berhasil
67	79 detik	79 detik	Berhasil
68	20 detik	36 detik	Gagal
69	21 detik	37 detik	Gagal
70	44 detik	44 detik	Berhasil
71	66 detik	44 detik	Gagal
72	27 detik	27 detik	Berhasil
73	22 detik	22 detik	Berhasil
74	21 detik	25 detik	Gagal
75	35 detik	34 detik	Gagal
76	26 detik	29 detik	Gagal
77	45 detik	45 detik	Berhasil
78	40 detik	20 detik	Gagal
79	77 detik	77 detik	Berhasil
80	48 detik	48 detik	Berhasil
81	49 detik	49 detik	Berhasil
82	35 detik	49 detik	Gagal
83	30 detik	30 detik	Berhasil
84	31 detik	31 detik	Berhasil
85	23 detik	23 detik	Berhasil
86	27 detik	26 detik	Gagal
87	65 detik	60 detik	Gagal
88	71 detik	44 detik	Gagal
89	27 detik	27 detik	Berhasil
90	13 detik	15 detik	Gagal
91	13 detik	13 detik	Berhasil

Table 7. Tabel Pengujian

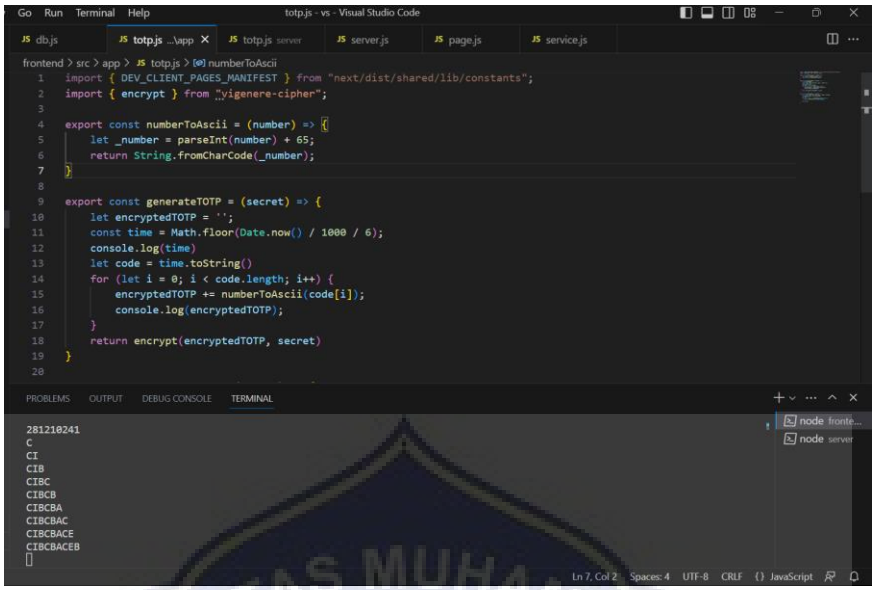
92	88 detik	88 detik	Berhasil
93	89 detik	70 detik	Gagal
94	60 detik	51 detik	Gagal
95	42 detik	42 detik	Berhasil
96	67 detik	66 detik	Gagal
97	66 detik	66 detik	Berhasil
98	77 detik	77 detik	Berhasil
99	24 detik	24 detik	Berhasil
100	24 detik	29 detik	Gagal

Dari tabel penelitian diatas dapat disimpulkan bahwa:

1. Jika waktu pada frontend dengan waktu (server), maka di akses. yang dihasilkan (client) berbeda pada backend data tidak dapat
2. Data hanya dapat diakses apabila waktu dari frontend dan backend sama.

C. Hasil Perbandingan

1. Perbandingan Hitungan Manual dan Sistem.



Gambar 6. TOTP Frontend

Adapun proses Enkripsi dari program di atas, sebagai berikut:

a. Merubah time (pesan asli) yang dihasilkan menjadi teks (huruf) menggunakan variasi full vigenere cipher. Adapun time yang dihasilkan yaitu “281210241”.
b. Kunci yang digunakan adalah “qwerty”
c. Merubah time (bentuk angka) menjadi huruf dengan cara menjumlahkan time dengan ASCII karakter A=65.

Time	2	8	1	2	1	0	2	4	1
Hasil	67	73	66	67	66	65	67	69	66

Table 8. Tabel Konversi

Berdasarkan table ASCII, hasil dari perubahan time “281210241” menjadi teks yaitu: “CIBCBACEB”.

d. Melakukan perhitungan enkripsi vigener cipher menggunakan rumus Ci = (Pi+Ki) mod 26

Table 9. Tabel Enkripsi

Pi	C	I	B	C	B	A	C	E	B
Ki	Q	W	E	R	T	Y	Q	W	E

C1 (C,Q) = (P1 + K1) mod 26 = (2 + 16) mod 26 = 18 mod 26 = 18

C2 (I,W) = (P2 + K2) mod 26 = (8 + 22) mod 26 = 30 mod 26 = 4

C3 (B,E) = (P3 + K3) mod 26 = (1 + 4) mod 26 = 5 mod 26 = 5

C4 (C,R) = (P4 + K4) mod 26 = (2 + 17) mod 26 = 19 mod 26 = 19

C5 (B,T) = (P5 + K5) mod 26 = (1 + 19) mod 26 = 20 mod 26 = 20

C6 (A,Y) = (P6 + K6) mod 26 = (0 + 24) mod 26 = 24 mod 26 = 24

C7 (C,Q) = (P7 + K7) mod 26 = (2 + 16) mod 26 = 18 mod 26 = 18

C8 (E,W) = (P8 + K8) mod 26 = (4 + 22) mod 26 = 26 mod 26 = 0

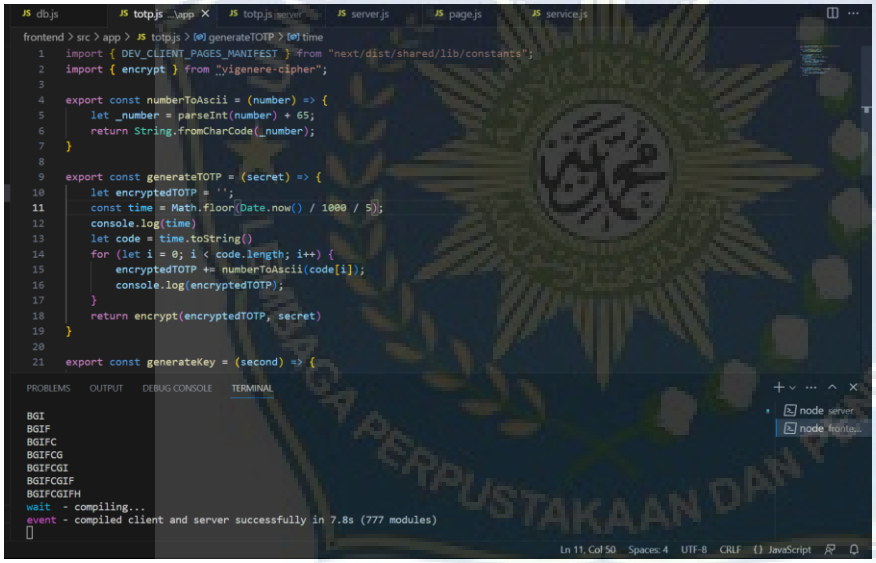
C9 (B,E) = (P9 + K9) mod 26 = (1 + 4) mod 26 = 5 mod 26 = 5

e. Mendapatkan hasil enkripsi variasi auto-key vigenere cipher “SEFTUYSAF”

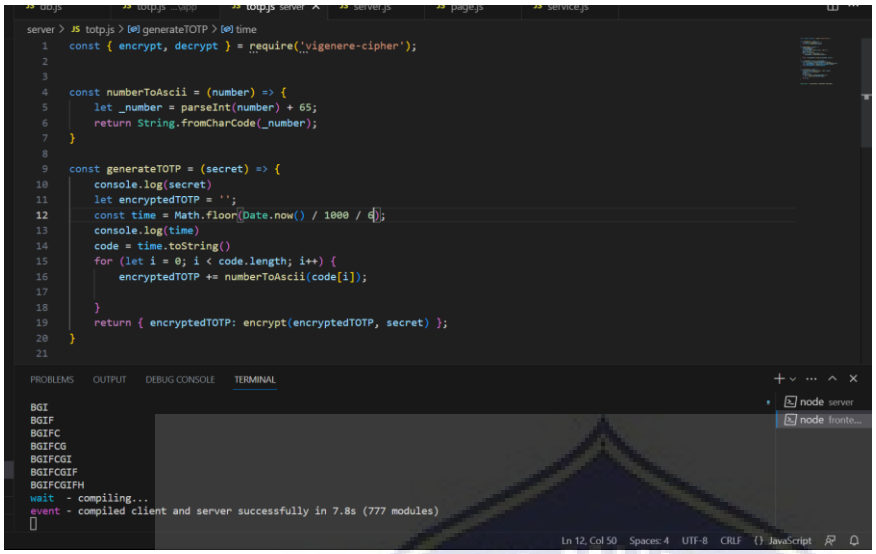
2. Perbandingan Time antara Frontend dan Backend

Uji coba perbandingan time antara frontend dan backend dalam mencocokan key yang dihasilkan antara frontend dan backend pada saat client melakukan request data.

a. Perbandingan Time Frontend: 5s,dan Backend: 6s



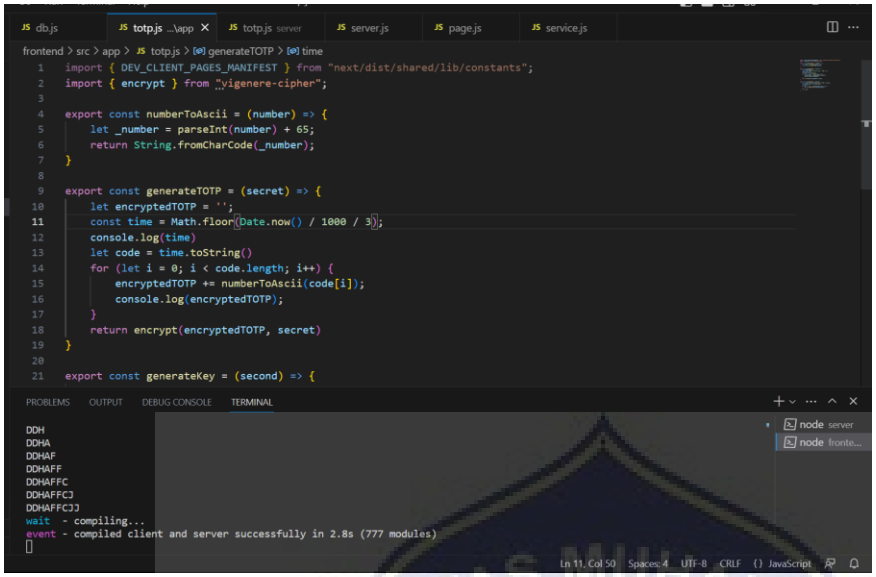
Gambar 7. TOTP Frontend



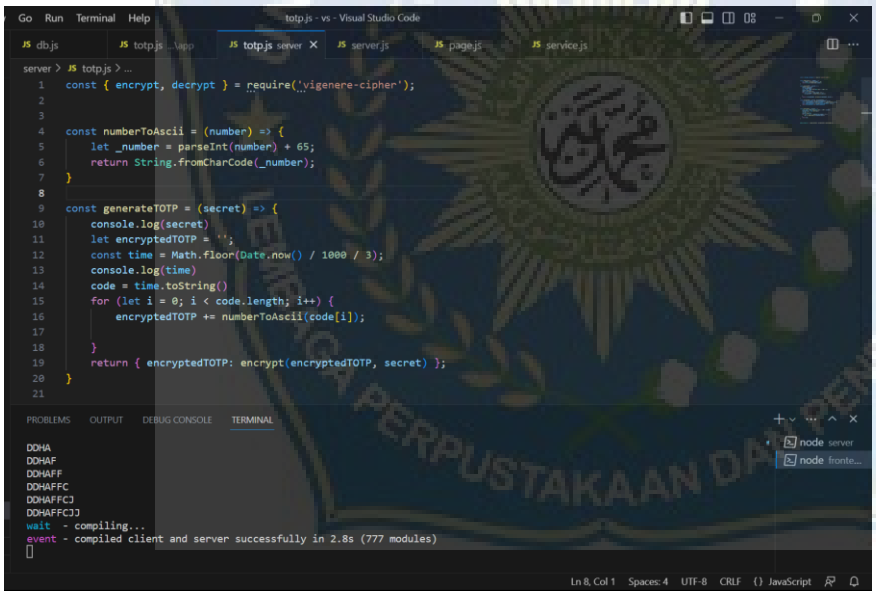
Gambar 8. TOTP Server

Gambar 9. Tampilan Dashboard

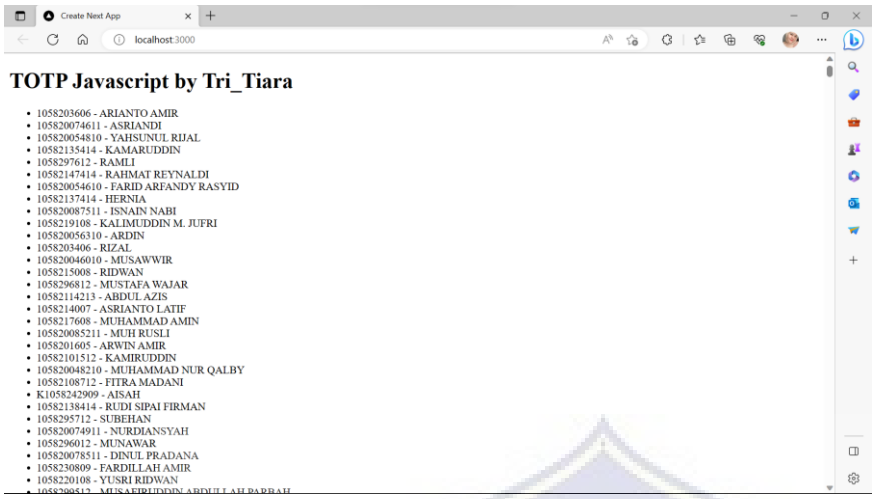
b. Perbandingan Time Frontend: 3s,dan Backend: 3s



Gambar 10. TOTP Frontend

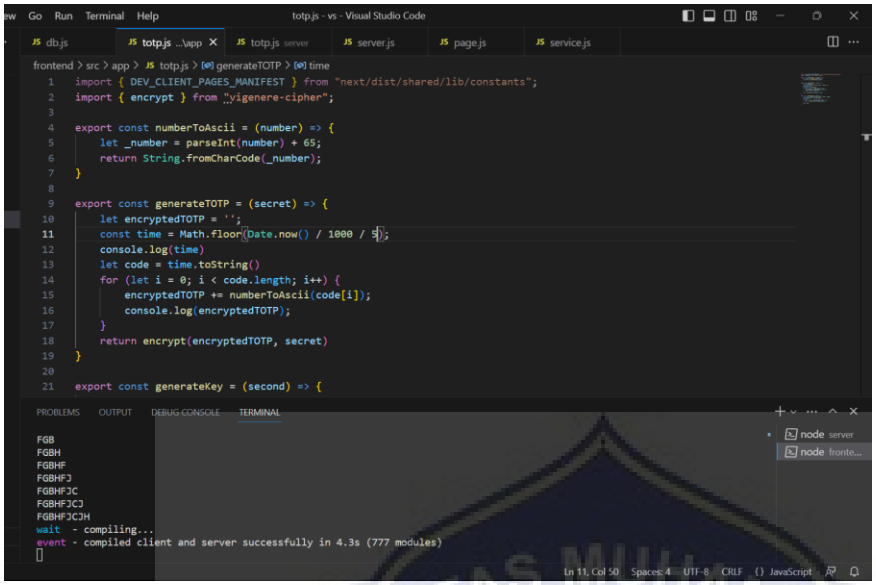


Gambar 11. TOTP Server

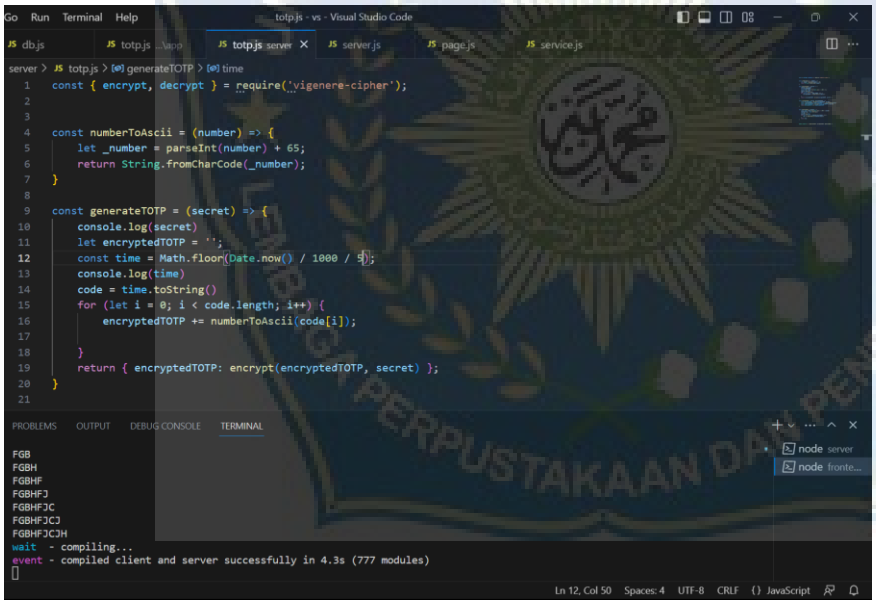


Gambar 12. Tampilan Dashboard

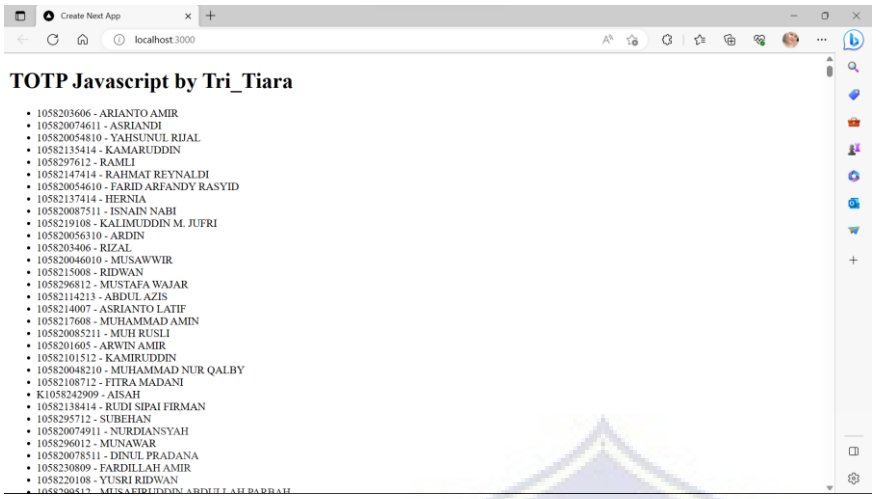
c. Perbandingan Time Frontend: 5s,dan Backend: 5s



Gambar 13. TOTP Frontend

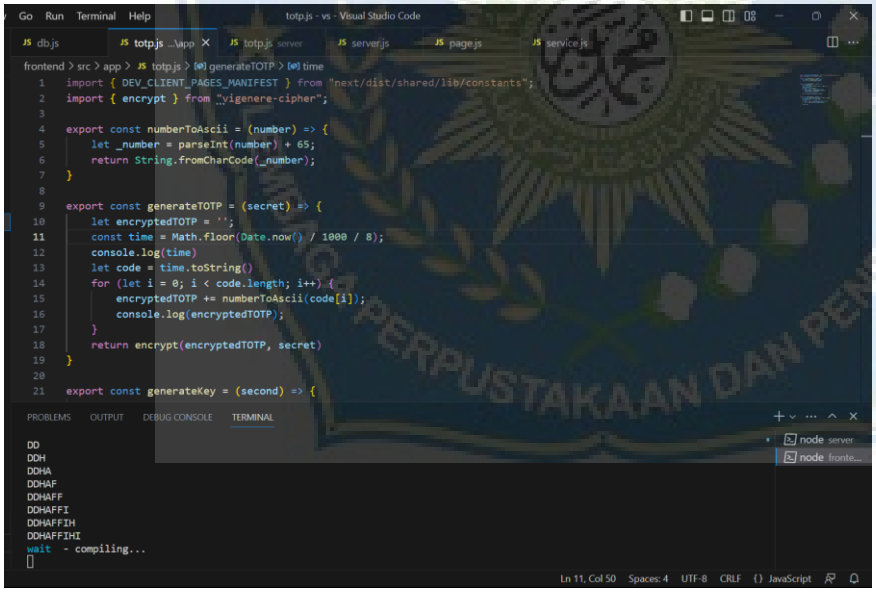


Gambar 14. TOTP Server

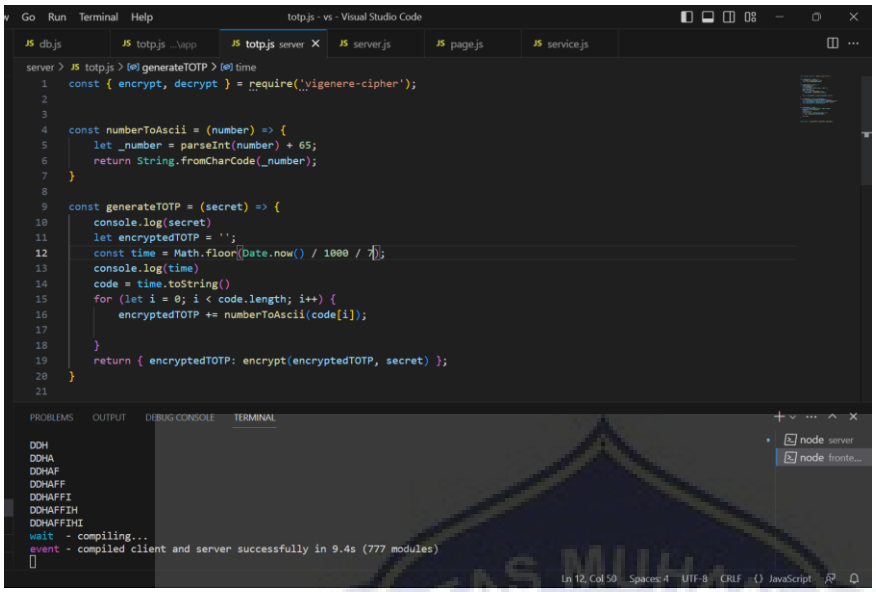


Gambar 15. Tampilan Dashboard

d. Perbandingan Time Frontend: 8s,dan Backend: 7s



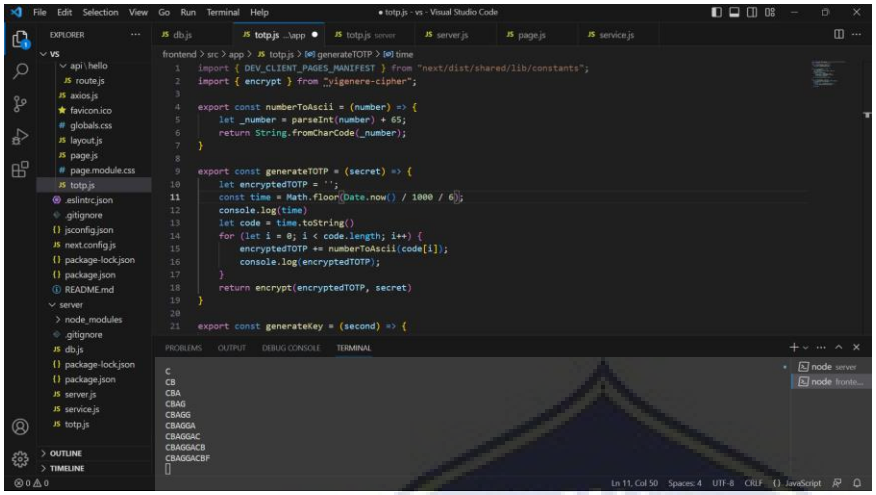
Gambar 16. TOTP Frontend



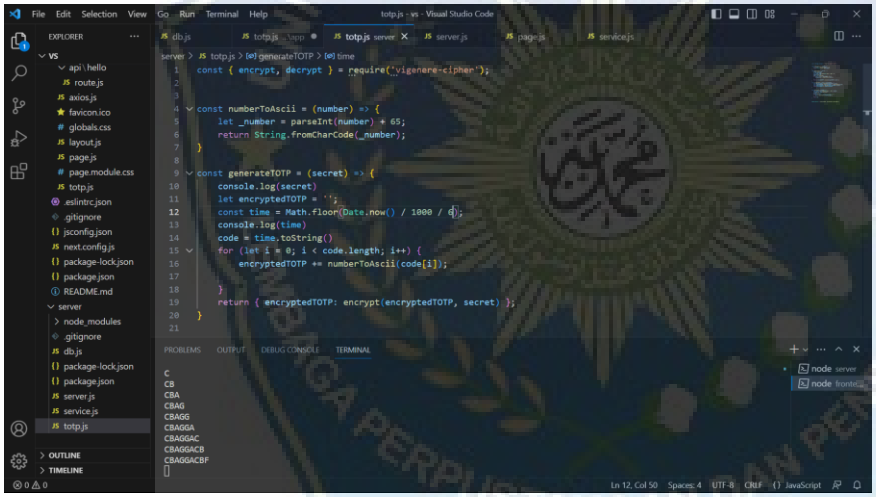
Gambar 17. TOTP Server

Gambar 18. Tampilan Dashboard

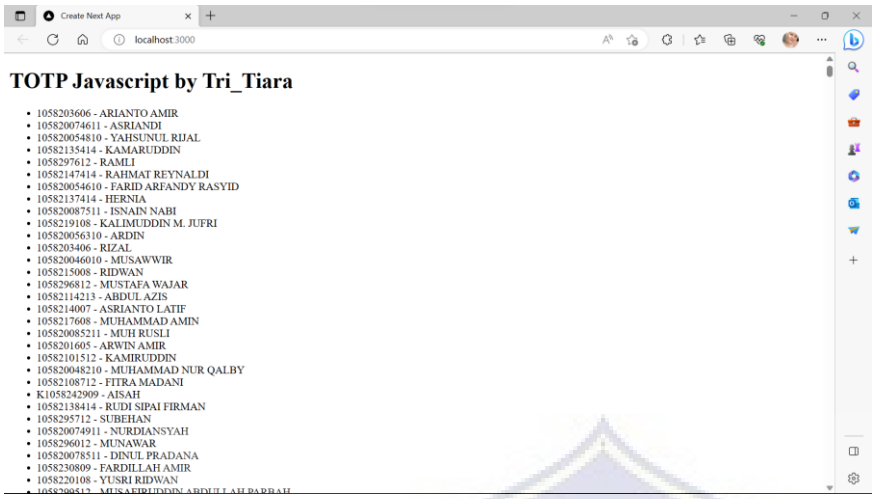
e. Frontend 6, backend 6



Gambar 19. TOTP Frontend



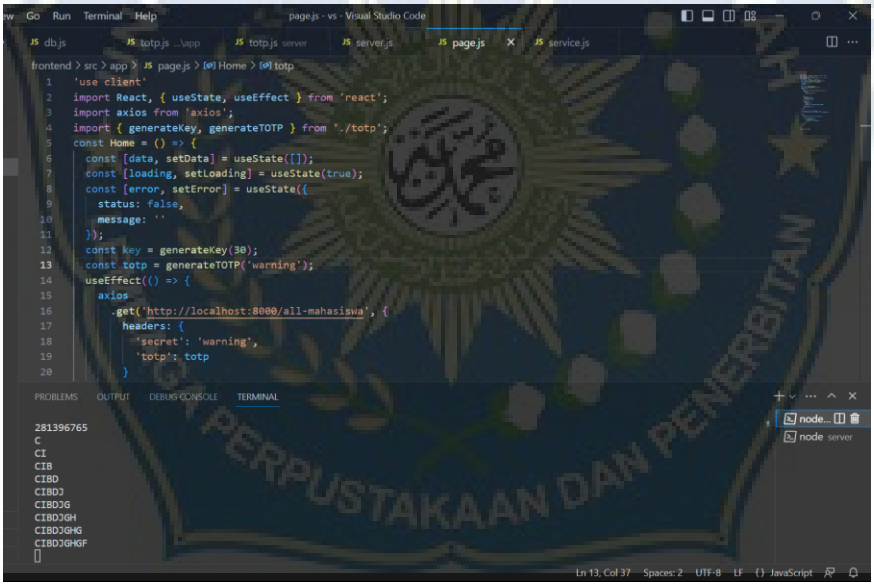
Gambar 20. TOTP Server



Gambar 21. Tampilan Dashboard

3. Perbandingan dengan menggunakan kata kunci lain

   a. Kata Kunci “warning”



Gambar 22. Page Frontend

1) Merubah time (pesan asli) yang dihasilkan menjadi teks (huruf) menggunakan variasi full vigenere cipher. Adapun time yang dihasilkan yaitu “281396765”.
2) Kunci yang digunakan adalah “warning”
3) Merubah time (bentuk angka) menjadi huruf dengan cara menjumlahkan time dengan ASCII karakter A=65.

Time	2	8	1	3	9	6	7	6	5
Hasil	67	73	66	68	74	71	72	71	70

Table 10. Tabel Konversi

Berdasarkan table ASCII, hasil dari perubahan time “281396765” menjadi teks yaitu: “CIBDJGHGF”.

4) Melakukan perhitungan enkripsi vigener cipher menggunakan rumus Ci = (Pi+Ki) mod 26

Pi	C	I	B	D	J	G	H	G	F
Ki	W	A	R	N	I	N	G	W	A

Table 11. Tabel Enkripsi

C1 (C,W) = (P1 + K1) mod 26 = (2 + 22) mod 26 = 24 mod 26 = 24

C2 (I,A) = (P2 + K2) mod 26 = (8 + 0) mod 26 = 8 mod 26 = 8

C3 (B,R) = (P3 + K3) mod 26 = (1 + 17) mod 26 = 18 mod 26 = 18

C4 (D,N) = (P4 + K4) mod 26 = (3 + 13) mod 26 = 16 mod 26 = 16

C5 (J,I) = (P5 + K5) mod 26 = (9 + 8) mod 26 = 17 mod 26 = 17

C6 (G,N) = (P6 + K6) mod 26 = (6 + 13) mod 26 = 19 mod 26 = 19

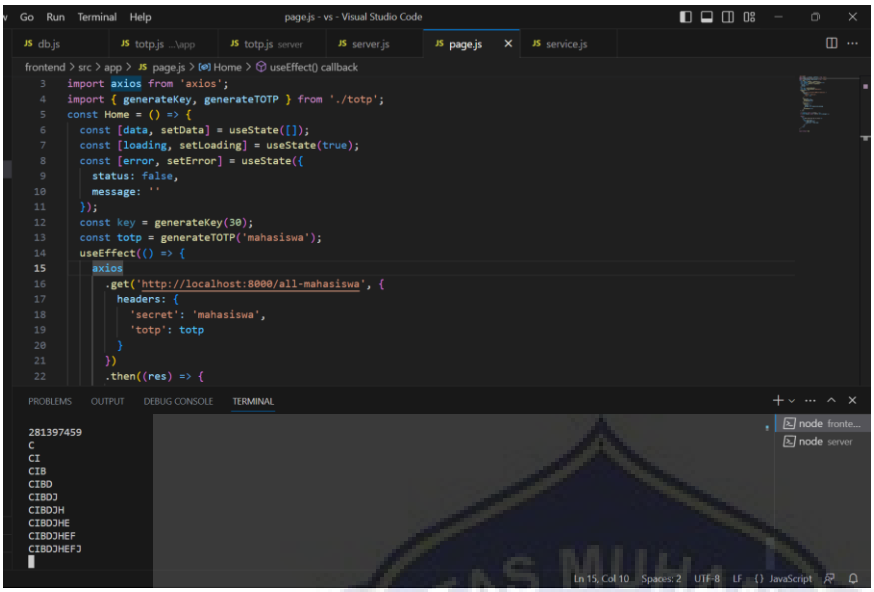
C7 (H,G) = (P7 + K7) mod 26 = (7 + 6) mod 26 = 13 mod 26 = 13

C8 (G,W) = (P8 + K8) mod 26 = (6 + 22) mod 26 = 28 mod 26 = 2

C9 (F,A) = (P9 + K9) mod 26 = (5 + 0) mod 26 = 5 mod 26 = 5

5) Mendapatkan hasil enkripsi variasi auto-key vigenere cipher “YISQRTNCF”

b. Kata Kunci “mahasiswa”



Gambar 23. Page Frontend

1) Merubah time (pesan asli) yang dihasilkan menjadi teks (huruf) menggunakan variasi full vigenere cipher. Adapun time yang dihasilkan yaitu “281397459”.
2) Kunci yang digunakan adalah “mahasiswa”
3) Merubah time (bentuk angka) menjadi huruf dengan cara menjumlahkan time dengan ASCII karakter A=65.

Time	2	8	1	3	9	7	4	5	9
Hasil	67	73	66	68	74	72	69	70	74

Table 12. Tabel Konversi

Berdasarkan table ASCII, hasil dari perubahan time “281397459” menjadi teks yaitu: “CIBDJHEFJ”.

4) Melakukan perhitungan enkripsi vigener cipher menggunakan rumus Ci = (Pi+Ki) mod 26

Pi	C	I	B	D	J	H	E	F	J
Ki	M	A	H	A	S	I	S	W	A

Table 13. Tabel Enkripsi

C1 (C,M) = (P1 + K1) mod 26 = (2 + 12) mod 26 = 14 mod 26 = 24

C2 (I,A) = (P2 + K2) mod 26 = (8 + 0) mod 26 = 8 mod 26 = 8

C3 (B,H) = (P3 + K3) mod 26 = (1 + 7) mod 26 = 8 mod 26 = 8

C4 (D,A) = (P4 + K4) mod 26 = (3 + 0) mod 26 = 3 mod 26 = 3

C5 (J,S) = (P5 + K5) mod 26 = (9 + 18) mod 26 = 27 mod 26 = 1

C6 (H,I) = (P6 + K6) mod 26 = (7 + 8) mod 26 = 15 mod 26 = 15

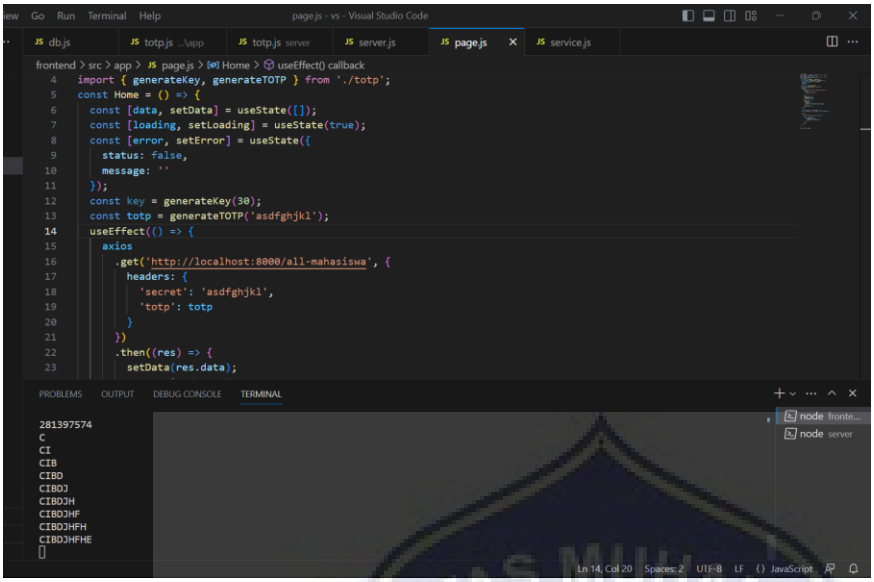
C7 (E,S) = (P7 + K7) mod 26 = (4+ 18) mod 26 = 22 mod 26 = 22

C8 (F,W) = (P8 + K8) mod 26 = (5 + 22) mod 26 = 27 mod 26 = 1

C9 (J,A) = (P9 + K9) mod 26 = (9 + 0) mod 26 = 9 mod 26 = 9

5) Mendapatkan hasil enkripsi variasi auto-key vigenere cipher “YIIDBPWBJ”

c. Kata Kunci “asdfghjkl”



Gambar 24. Page Frontend

1) Merubah time (pesan asli) yang dihasilkan menjadi teks (huruf) menggunakan variasi full vigenere cipher. Adapun time yang dihasilkan yaitu “281397574”.
2) Kunci yang digunakan adalah “mahasiswa”
3) Merubah time (bentuk angka) menjadi huruf dengan cara menjumlahkan time dengan ASCII karakter A=65.

Time	2	8	1	3	9	7	5	7	4
Hasil	67	73	66	68	74	72	70	72	69

Table 14. Tabel Konversi

Berdasarkan table ASCII, hasil dari perubahan time “281397574” menjadi teks yaitu: “CIBDJHFHE”.

4) Melakukan perhitungan enkripsi vigener cipher menggunakan rumus Ci = (Pi+Ki) mod 26

Pi	C	I	B	D	J	H	F	H	E
Ki	A	S	D	F	G	H	J	K	L

Table 15. Tabel Enkripsi

C1 (C,A) = (P1 + K1) mod 26 = (2 + 0) mod 26 = 2 mod 26 = 2

C2 (I,S) = (P2 + K2) mod 26 = (8 + 18) mod 26 = 26 mod 26 = 0

C3 (B,D) = (P3 + K3) mod 26 = (1 + 3) mod 26 = 4 mod 26 = 4

C4 (D,F) = (P4 + K4) mod 26 = (3 + 5) mod 26 = 8 mod 26 = 8

C5 (J,G) = (P5 + K5) mod 26 = (9 + 6) mod 26 = 15 mod 26 = 15

C6 (H,H) = (P6 + K6) mod 26 = (7 + 7) mod 26 = 14 mod 26 = 14

C7 (F,J) = (P7 + K7) mod 26 = (5 + 9) mod 26 = 14 mod 26 = 14

C8 (H,K) = (P8 + K8) mod 26 = (7 + 10) mod 26 = 17 mod 26 = 17

C9 (E,L) = (P9 + K9) mod 26 = (4 + 11) mod 26 = 15 mod 26 = 15

5) Mendapatkan hasil enkripsi variasi auto-key vigenere cipher "CAEIPOORP"

D. Analisa Hasil Uji Coba Program

Dalam *Penerapan Algorima Vigenere Cipher untuk Meningkatkan keamanan pada Dashboard* memiliki beberapa kelebihan dan kekurangan pada system tersebut, berikut adalah kekurangan dan kelebihan aplikasi :

1. Kelebihan Aplikasi
   a. Bersifat online dan dapat diakses dimana saja dan bisa melalui handphone.
   b. Berbasis web sehingga mudah untuk diakses.
   c. Pengguna lain tidak dapat mengakses data apabila pesan yang dikirimkan oleh client tidak sesuai dengan server atau tidak valid.
2. Kekurangan Aplikasi

   Terlepas dari tingkat keamanan algoritma cipher yang digunakan, algoritma cipher selalu rentan terhadap serangan brute force. Jika pihak yang tidak berwenang memiliki akses ke data yang dienkripsi dan memiliki kemampuan untuk melakukan serangan brute force, maka data tersebut bisa dipecahkan.

BAB V
PENUTUP

A. Kesimpulan

Berdasarkan penelitian yang telah dilakukan, maka dapat ditarik kesimpulan mengenai proses penerapan Algoritma Vigenere Cipher dalam masalah keamanan pada dashboard unismuh makassar tersebut, antara lain:

1. Untuk meningkatkan tingkat keamanan data yang ditampilkan, penelitian ini berhasil mengintegrasikan algoritma Vigenere Cipher pada dashboard. Efektivitas teknik ini dalam mengenkripsi dan mendekripsi data telah terbukti, mengurangi kemungkinan akses ilegal.

2. Penerapan Algoritma Vigenere Cipher pada kode TOTP dapat menjaga data dari akses yang tidak diinginkan karena data tidak dapat diakses tanpa kunci enkripsi yang benar.
3. Vigenere Cipher merupakan algoritma yang mudah dilaksanakan dan dapat dihitung secara manual atau dengan menggunakan komputer. Algoritma ini juga membutuhkan waktu yang relatif cepat untuk mengenkripsi dan mendekripsi data.

B. Saran

Berikut adalah beberapa saran yang dapat diambil dari hasil penelitian ini:

1. Keamanan kunci enkripsi memainkan peran penting dalam keamanan algoritma kriptografi seperti Vigenere Cipher. Penting untuk mengikuti praktik terbaik untuk manajemen kunci, termasuk penggunaan kunci yang berbeda, penggantian rutin, dan penyimpanan yang aman.
2. Jika dasbor digunakan oleh banyak orang, penting untuk memberikan instruksi kepada mereka tentang cara menggunakan teknologi enkripsi dan betapa pentingnya menjaga kerahasiaan kunci.
3. Studi ini dapat berfungsi sebagai batu loncatan untuk penyelidikan lebih lanjut mengenai penciptaan teknik enkripsi yang lebih efektif dan kuat, serta kemungkinan menyelidiki integrasinya dengan alat keamanan lain seperti enkripsi ujung ke ujung atau otentikasi dua faktor (2FA).).

DAFTAR PUSTAKA

Alam, H., Habibi, A. K., & Widya, H. (2022). PENGGUNAAN ALGORITMA *VIGENERE CIPHER* DAN ONE TIME PAD UNTUK KEAMANAN PESAN TEKS. *Seminar Nasional Teknik (SEMNASTEK) UISU*, 160-166.

Alasi, T. S., & P. F. (2022). Peningkatan Keamanan untuk Password menggunakan Algoritma *Vigenere Cipher*. *Jurnal Mantik Penusa*, 1-10.

Arfandy, D., Simanjuntak, M., & Pasaribu, T. (2022). Penerapan Metode *Vigenere Cipher* Untuk Mengamankan Data Text. *JUKI: Jurnal Komputer dan Informatika*, 48-54.

Chandra, J. C., & I. I. (2019). Penerapan Kriptografi Pada Rest Api Web Service Studi Kasus Kafa Photography. *Jurnal Komputasi*.

Dqlab. (2020, September 11). *Langkah-Langkah Menggunakan Teknik Analisis Data Kualitatif*. Retrieved from dqlab: https://www.dqlab.id/data-analisis-pahami-teknik-pengumpulan-data#:~:text=Display%20data%20atau%20penyajian%20data,sehingga%20memberikan%20kemungkinan%20menghasilkan%20kesimpulan.

Efrandi, Asnawati, & Yupiyanti. (2014). Aplikasi Kriptografi Pesan Menggunakan Algoritma *Vigenere Cipher*. *Jurnal Media Infotama*.

Handoko, & Aditya, I. (2017). Prototipe Pengendalian Lampu Panggung Menggunakan Web Browser Melalui Jaringan Lokal Berbasis Arduino . *Diss. STMIK AKAKOM YOGYAKARTA*.

Hardita, V. C., & Sholeha, E. W. (2021). Penerapan Kombinasi Metode *Vigenere Cipher*, Caesar Cipher dan Simbol Baca Dalam Mengamankan Pesan. *Jurnal SAINTEKOM*, 34-43.

Jaya, T. S. (2018). Pengujian aplikasi dengan metode blackbox testing boundary value analysis (studi kasus: kantor digital Politeknik Negeri Lampung). *Jurnal Informatika: Jurnal Pengembangan IT*, 45-48.

Khasanah, R. L., Kesuma, C., & Wijianto, R. (2018). Sistem Informasi Pelayanan Kesehatan Online Berbasis Web Pada PMI Kabupaten Purbalingga.

Listanto, A., & Hartanto, P. (2018). Sistem Informasi Manajemen Persediaan Barang Berbasis Web Menggunakan Metode Economic Order Quantity (EOQ) Studi Pada Toko Kudus Jaya. *JURNAL ILMIAH EKONOMI DAN BISNIS*.

Nurajizah, S., & Aziz, E. (2018). Pembelajaran Pengenalan Lafadz Tajwid Untuk Siswa Madrasah Berbasis Multimedia Pada MTsN 1 Kota BEKASI. *Jurnal Mantik Penusa*.

Perkasa, M. I., & Setiawan, E. B. (2018). Pembangunan Web Service Data Masyarakat Menggunakan Rest Api dengan Access Token. *Ultima Computing: Jurnal Sistem Komputer*, 19-26.

Prabowo, H. E. (2015). ENKRIPSI TEKS MENGGUNAKAN METODE *VIGENERE CIPHER* DENGAN PEMBENTUKAN KUNCI TIGA TAHAP. *Skripsi. Jurusan Teknik Elektro, Fakultas Teknik, Universitas Negeri Semaranf*.

Ritwiyan, B. G., & Pradana, R. (2021). Implementasi Kriptografi Pada Web Service Dengan Metode Caesar Cipher Berbasis Java Di PT.Integrasi Media Kreasi. *SKANIKA*, 38-44.

Salmaa. (2022, Maret 5). *Reduksi Data: Pengertian, Tujuan, Langkah-Langkah, dan Contohnya*. Retrieved from Penerbit dee publish: https://penerbitdeepublish.com/reduksi-data-adalah/

Susanto, I. A., & A. S. (2018). Enkripsi Data Penggajian Dengan Algoritma Caesar Cipher dan *Vigenere Cipher* Pada PT. Kemasindo Cepat Nusantara. *SKANIKA*, 399-404.

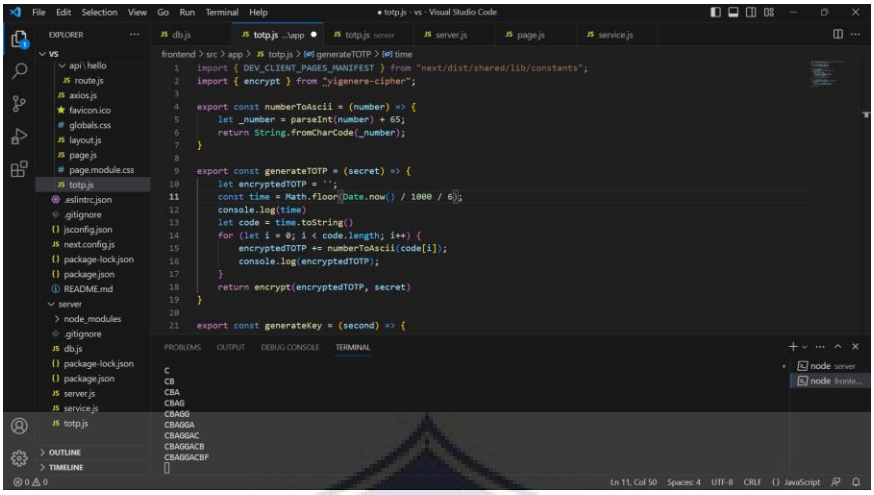
Ungkawa, U., Dewi, I. A., & Putra, K. R. (2015). Implementasi Algoritma Time Based One Time Password Dalam Otentikasi Token Internet Banking. *Library Itenas, Bandung*, 2-11.

Utomo, B. W., & Subandi. (2018). Implementasi Algoritma Enkripsi Caesar Cipher dan *Vigenere Cipher* pada Aplikasi Mobile dan Rest Api Data Perusahaan pada PT. Central Capital Futures. *SKANIKA*, 624-629.

Wicaksono, A., & Fatimah, T. (2018, Juli 3). SISTEM PENILAIAN ONLINE MENGGUNAKAN KEAMANAN ONE TIME PASSWORD DENGAN ALGORITMA SHA 512 BERBASIS WEB. *1*, 938-942.

LAMPIRAN

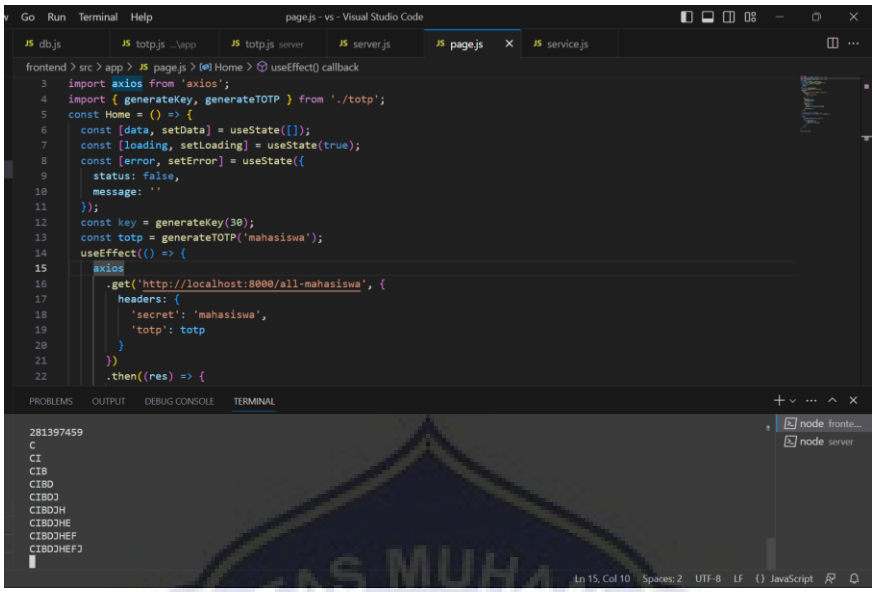
1. Tampilan Aplikasi



Gambar 1. TOTP Frontend

Gambar 2. TOTP Server

Gambar 3. Tampilan Dashboard



Gambar 4. Page Frontend

2. Source Code

```
const { encrypt, decrypt } = require('vigenere-cipher');
const crypto = require('crypto')

const numberToAscii = (number) => {
  let _number = parseInt(number) + 65;
  return String.fromCharCode(_number);
}

const generateTOTP = (secret, encryptionLength) => {
  let encryptedTotp = ''
  const time = Math.floor(Date.now() / 1000 / 5)
  const buffer = Buffer.alloc(8)
  buffer.writeBigInt64BE(BigInt(time))
  const hmac = crypto.createHmac('sha1', secret).update(buffer).digest()
  const offset = hmac[hmac.length - 1] & 0xf
  let code = ((hmac[offset] & 0x7f) << 24)
    | ((hmac[offset + 1] & 0xff) << 16)
    | ((hmac[offset + 2] & 0xff) << 8)
```

```
        | (hmac[offset + 3] & 0xff)

    code = code.toString().padStart(encryptionLength, '0').slice(0, encryptionLength)
    for (let i = 0; i < code.length; i++) {
        encryptedTotp += numberToAscii(code[i]);
    }
    return { encryptedTOTP: encrypt(encryptedTotp, secret) };
}

const validateTOTP = (secret, encryptedTOTP , encryptionLength) => {
    const decryptedTOTP = decrypt(encryptedTOTP, secret);
    const { encryptedTOTP: newEncryptedTOTP } = generateTOTP(secret , encryptionLength);
    const newDecryptedTOTP = decrypt(newEncryptedTOTP, secret);
    return decryptedTOTP === newDecryptedTOTP;
}



const generateKey = (second) => {
    const time = Math.floor(Date.now() / 1000 / second);
    timeToString = time.toString();
    let key = '';
    console.log(time)
    for (let i = 0; i < timeToString.length; i++) {
        key += numberToAscii(timeToString[i]);
    }
    return key;
}



module.exports = { generateTOTP, validateTOTP, generateKey };
```

```
import { encrypt } from "vigenere-cipher";
import crypto from "crypto";
import Long from "long";

export const numberToAscii = (number) => {
   let _number = parseInt(number) + 65;
   return String.fromCharCode(_number);
}

export const generateTOTP = (secret, encryptionLength) => {
    let encryptedTotp = '';
   const time = Math.floor(Date.now() / 1000 / 5);
   const timeLong = Long.fromNumber(time);
   const buffer = Buffer.from(timeLong.toBytesBE());
   const hmac = crypto.createHmac('sha1', secret).update(buffer).digest();
   const offset = hmac[hmac.length - 1] & 0xf;
   let code = ((hmac[offset] & 0x7f) << 24)
      | ((hmac[offset + 1] & 0xff) << 16)
      | ((hmac[offset + 2] & 0xff) << 8)
      | (hmac[offset + 3] & 0xff);
   code = code.toString().padStart(encryptionLength, '0').slice(0, encryptionLength);
   for (let i = 0; i < code.length; i++) {
      encryptedTotp += numberToAscii(code[i]);
   }
   return encrypt(encryptedTotp, secret);
}

export const generateKey = (second) => {
   const time = Math.floor(Date.now() / 1000 / second);
   let timeToString = time.toString();
```

```
    let key = '';
    for (let i = 0; i < timeToString.length; i++) {
        key += numberToAscii(timeToString[i]);
    }
    return key;
}
```