

**A. Judul: Penerapan Algoritma Vigenere Cipher Untuk Enkripsi Dokumen Dalam Mengamankan Informasi Yang Dikecualikan Di Badan Perencanaan Pembangunan, Riset dan Inovasi Daerah (BAPPERIDA) Kabupaten Malaka**

**B. Latar Belakang**

Kerahasiaan dari data atau informasi merupakan suatu kelengkapan pelayanan yang dibuat untuk menjaga agar informasi yang tersimpan tidak dapat dibaca atau dibuka oleh pihak yang tidak berhak. Upaya dalam menjaga kerahasiaan dari data informasi tersebut sudah tercetus sejak zaman dahulu tepatnya pada zaman romawi dengan metode pergeseran huruf atau karakter dengan dasar nilai tertentu (Prameshwari & Sastra, 2018).

Perkembangan teknologi dalam sistem pengaman untuk menjamin kerahasiaan informasi data sudah berkembang dengan pesat. Dalam menjaga kerahasiaan dalam informasi data terdapat ilmu dalam pengembangan seperti steganografi dan kriptografi. Penerapan yang dilakukan tidak hanya pada satu teknik pengamanan data, melainkan bisa juga dengan melakukan kombinasi atau modifikasi algoritma (Ginting, 2020).

Keamanan data dan informasi merupakan hal yang sangat penting di era reformasi saat ini. Umumnya, setiap institusi memiliki dokumen-dokumen penting dan bersifat rahasia yang hanya boleh diakses oleh orang tertentu. Sistem informasi yang dikembangkan harus menjamin keamanan dan kerahasiaan dokumen-dokumen tersebut. Namun kendalanya bahwa media-media yang digunakan seringkali dapat disadap oleh pihak lain (Handoko & Kom, 2015).

Laporan *National Cyber Security Index* (NCSI) mencatat, skor indeks keamanan data di Indonesia sebesar 38,96 poin dari 100 pada 2022. Angka ini menempatkan Indonesia berada di peringkat ke-3 terendah di antara negara-negara G20. Sementara secara global, Indonesia menduduki peringkat ke-83 dari 160 negara dalam daftar di laporan tersebut (*Indeks Keamanan Siber Indonesia Peringkat Ke-3 Terendah Di Antara Negara G20*, 2023).

Badan Perencanaan Pembangunan, Riset dan Inovasi Daerah (BAPPERIDA) adalah lembaga teknis daerah dibidang penelitian dan perencanaan pembangunan daerah yang dipimpin oleh seorang kepala badan yang berada dibawah dan bertanggung jawab kepada Gubernur/Bupati/Wali kota melalui Sekretaris Daerah. Badan ini mempunyai tugas pokok membantu Gubernur/Bupati/Wali kota dalam penyelenggaraan pemerintahan daerah dibidang penelitian dan perencanaan pembangunan daerah (*Badan Perencanaan Pembangunan Daerah - Wikipedia Bahasa Indonesia, Ensiklopedia Bebas*).

Badan Perencanaan Pembangunan, Riset dan Inovasi Daerah (BAPPERIDA) Kabupaten Malaka melakukan sinkronisasi dengan beberapa dinas lainnya dalam pelaksanaan program, diantaranya Dinkes BKKBN(sinkronisasi data stanting), Dinas PMD dan Statistik (Sinkronisasi data kemiskinan extrim). Selain itu Badan Perencanaan Pembangunan, Riset dan Inovasi Daerah (BAPPERIDA) Kabupaten Malaka masih melakukan kerja sama dengan dinas terkait lainnya dalam pelaksanaan program kegiatan, adapun data-data yang rentan terjadinya penyalagunaan seperti data penerima bantuan perumahan ataupun data-data terkait lainnya.

Terkait sistem keamanan data pada Badan Perencanaan Pembangunan, Riset dan Inovasi Daerah (BAPPERIDA) Kabupaten Malaka sampai dengan saat ini belum memiliki sebuah sistem untuk mengamankan data-data yang diproses oleh Badan Perencanaan Pembangunan, Riset dan Inovasi Daerah (BAPPERIDA) sehingga memungkinkan terjadinya penyalagunaan data contohnya penyalahgunaan data dari Badan Perencanaan Pembangunan, Riset dan Inovasi Daerah (BAPPERIDA) Kabupaten Malaka oleh pihak Desa Umalor, dimana Badan Perencanaan Pembangunan, Riset dan Inovasi Daerah (BAPPERIDA) Kabupaten Malaka mengeluarkan data penerima bantuan pangan sebanyak 207 kk. Namun, karena belum adanya pengaman data di Badan Perencanaan Pembangunan, Riset dan Inovasi Daerah (BAPPERIDA) Kabupaten Malaka, maka pihak Desa Umalor dapat mengakses dan menyalahgunakan data dengan cara mengganti atau mengubah penerima bantuan pangan yang dimaksud ("22 KPM Di Desa Umalor Dicoret Dari Penerima

Beras Bantuan Pangan, Kades Bilang....,” 2024). Oleh karena itu sebuah sistem keamanan data sangat diperlukan dalam mengamankan data-data penting pada Badan Perencanaan Pembangunan, Riset dan Inovasi Daerah (BAPPERIDA) Kabupaten Malaka.

Vigenere Cipher merupakan bentuk pola alphabetic substitution seperti yang diungkapkan Caesar Cipher, namun menambahkan kunci lebih aman. Ide ini sudah diterapkan berkali-kali, namun pada tahun 1553 metode ini baru dikemukakan oleh Giovan Battista Bellaso di bukunya *La cifra del. Sig. Giovan Battista Bellaso* (Ramli, 2017). Algoritma ini, dengan kemampuannya dalam menghasilkan enkripsi yang sederhana namun sulit dibobol, dapat menjadi benteng pertahanan terhadap upaya tidak sah yang dapat merugikan kepentingan dan keamanan daerah.

Berdasarkan latar belakang di atas maka penulis memilih judul: **Penerapan Algoritma Vigenere Cipher Untuk Enkripsi Dokumen Dalam Mengamankan Informasi Yang Dikecualikan Di Badan Perencanaan Pembangunan, Riset dan Inovasi Daerah (BAPPERIDA) Kabupaten Malaka.**

### **C. Rumusan Masalah**

Berdasarkan latar belakang di atas, maka yang menjadi rumusan masalah adalah proses bagaimana tahapan merancang aplikasi yang dapat menerapkan algoritma Vigenere Cipher untuk enkripsi dokumen dalam mengamankan informasi yang dikecualikan di Badan Perencanaan Pembangunan, Riset Dan Inovasi Daerah (BAPPERIDA) Kabupaten Malaka.

### **D. Batasan Masalah**

Agar tidak keluar dari maksud dan tujuan yang ada, maka batasan masalahnya adalah:

1. Penelitian ini berfokus pada pengembangan aplikasi enkripsi dokumen yang menerapkan algoritma Vigenere Cipher, menggunakan bahasa pemrograman PHP (*Hypertext Preprocessor*) dan Database MySQL.
2. Sistem ini diuji pada jenis file dokumen

3. Algoritma yang digunakan adalah algoritma Vigenere Cipher.

#### **E. Tujuan Penelitian**

Tujuan utama penelitian ini adalah memastikan bahwa data dan informasi yang disimpan oleh lembaga seperti BAPPERIDA tetap rahasia dan tidak dapat diakses atau dimanipulasi oleh pihak yang tidak berwenang.

#### **F. Manfaat Penelitian**

1. Mengembangkan pengetahuan yang dimiliki oleh peneliti sehingga bisa bermanfaat bagi orang lain.
2. Dengan adanya penelitian ini, lembaga seperti BAPPERIDA dapat mengimplementasikan sistem keamanan data yang lebih canggih. Ini akan mengurangi risiko penyalahgunaan data, seperti yang terjadi pada kasus Desa Umalor, di mana data penerima bantuan pangan disalahgunakan karena kurangnya sistem pengaman data.
3. Penelitian ini dapat membantu dalam melindungi informasi sensitif dari akses yang tidak sah. Dengan menggunakan algoritma seperti Vigenere Cipher, data dapat dienkripsi sehingga hanya pihak yang berwenang yang dapat mengaksesnya. Ini penting bagi institusi yang menangani dokumen rahasia.

#### **G. Tinjauan Pustaka**

##### **1. Penelitian Terdahulu**

“Implementasi Kriptografi Vigenere Cipher Dengan PHP”, penelitian ini dilakukan untuk membuat implementasi kriptografi Vigenere Cipher. Sistem ini dirancang dengan melakukan analisa dengan metode deskriptif, dan metode komparatif. Setelah dilakukan analisa, maka dilakukan pemodelan dengan UML (*Unified Modelling Language*) dan dilakukan perancangan sistem kriptografi Vigenere Cipher dengan bentuk enkripsi dan dekripsi text yang dapat diprogram dengan menggunakan *software* PHP. Hasil penelitian ini adalah sebuah implementasi sistem kriptografi Vigenere Cipher dengan PHP (Irawan, 2017).

“Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher”,

penelitian ini dilakukan untuk menerapkan algoritma Vigenere Cipher untuk mengamankan pesan text. Keamanan informasi pada sebuah aplikasi sangatlah penting, sistem keamanan sangat diperlukan pada sebuah aplikasi karena di sebagian perusahaan atau bahkan di suatu negara membutuhkan keamanan informasi, dan informasi penting yang tidak boleh diakses oleh sembarangan penerima pesan harus diamankan. Untuk mengamankan informasi tersebut dibutuhkan suatu algoritma yang dapat menyamarkan pesan penting agar tidak bisa dibaca oleh pihak yang tidak memiliki hak untuk menerima informasi tersebut. Kriptografi merupakan salah satu cara yang bisa digunakan untuk memproteksi pengiriman data, data yang dikirim akan diubah menjadi kode tertentu dan hanya bisa dibuka oleh penerima yang memiliki kunci untuk merubah kode itu kembali sehingga kerahasiaan pesan atau informasi tetap dapat dijaga, dan untuk mempermudah pemrosesan data diperlukan sebuah aplikasi, aplikasi kriptografi berbasis web bisa dibangun dan digunakan untuk mempermudah pemrosesan data, selain itu aplikasi berbasis web dapat di akses dari mana saja (Amrulloh & Ujianto, 2019).

“ *Vigenere cipher algorithm modification by adopting RC6 key expansion and double encryption process* ”, penelitian ini dilakukan untuk melakukan enkripsi citra digital dengan melakukan dua kali proses enkripsi menggunakan Vigenere Cipher dan mengadopsi *expansion key* menggunakan algoritma RC6 pada media teks. Penelitian ini memiliki tujuan untuk mengetahui perbandingan perbedaan ukuran suatu data sebelum dan sesudah dienkripsi (*avalanche effect*) pada beberapa skenario seperti penggunaan Vigenere Cipher secara standar, penggabungan dengan *expansion key RC6*, dan lain-lain (Subandi et al., 2018).

“Penerapan Algoritma Vigenere Cipher Dan Hill Cipher”, Menggunakan Satuan Massa Penelitian ini dilakukan untuk menerapkan algoritma Vigenere Cipher untuk satuan massa, sistem ini dirancang untuk pengamanan data dalam menjamin kerahasiaan informasi data yang sudah berkembang dengan pesat. Dalam menjaga kerahasiaan dalam informasi data terdapat ilmu dalam pengembangan seperti steganografi

dan kriptografi. Penerapan yang dilakukan tidak hanya pada satu teknik pengamanan data, melainkan bisa juga dengan melakukan kombinasi atau modifikasi algoritma. Penelitian ini bertujuan untuk membuat sistem keamanan data dengan melakukan penerapan modifikasi algoritma Vigenere Cipher dan Hill Cipher. Hasil dari penelitian ini sendiri berupa proses enkripsi dengan menggunakan metode gabungan seperti algoritma Vigenere Cipher dan algoritma Hill Cipher dapat dilakukan dan menggabungkan dua metode atau lebih dapat membuat pesan semakin sulit dimengerti bagi orang lain. hal ini dapat memudahkan bagi pengirim pesan untuk menyampaikan pesan yang bersifat rahasia ke penerima (Ginting, 2020).

“ Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher ” , tujuan dari penelitian ini dilakukan agar bisa melakukan enkripsi dan dekripsi pada media citra digital menggunakan Vigenere Cipher. Proses enkripsi dilakukan dengan terlebih dahulu mengubah suatu citra digital menjadi format *encoding* base64, sehingga bisa dilakukan proses enkripsi dengan memakai tabula recta yang berisi susunan huruf radix-64 yang digunakan untuk proses *encoding* base64. Sebaliknya, proses dekripsi dilakukan dengan mengembalikan file yang sudah dienkripsi menggunakan susunan huruf radix-64, sehingga didapatkan file citra dalam format *encoding* base64. Lalu, citra berformat encoding base64 ini di-decode menjadi file asli. Proses enkripsi membutuhkan waktu kurang dari 0,2 detik dan 0,19 detik untuk proses dekripsi serta mengalami penambahan ukuran rata-rata sebesar 33,34% pada file hasil enkripsi dari ukuran file semula. Pengujian pada sepuluh citra digital dengan ukuran dan dimensi berbeda-beda menunjukkan tingkat keberhasilan sebesar 100%, hal ini berarti bahwa penelitian berhasil dilakukan (Imam Riadi et al., 2022).

Tabel 1. Perbandingan Terhadap Peneliti Terdahulu

| No | Peneliti                   | Judul  | Hasil   |
|----|----------------------------|--|---|
| 1  | (Irawan, 2017)             | Implementasi Kriptografi Vigenere Cipher Dengan PHP        | Hasil penelitian ini adalah sebuah implementasi sistem kriptografi Vigenere Cipher dengan PHP, dengan melakukan analisa metode deskriptif dan metode komparatif.  |
| 2  | (Amrulloh & Ujianto, 2019) | Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher | Hasil dari penelitian ini adalah sebuah aplikasi kriptografi simetris berbasis web yang bisa diakses dimana saja dengan menerapkan algoritma Vigenere Cipher untuk mengamankan pesan text.  |
| 3  | (Ginting, 2020)            | Penerapan Algoritma Vigenere Cipher Dan Hill Cipher        | Hasil dari penelitian ini sendiri berupa proses enkripsi dengan menggunakan metode gabungan seperti algoritma Vigenere Cipher dan algoritma Hill Cipher yang dapat dilakukan dan Menggabungkan dua metode atau lebih, dapat membuat pesan semakin sulit |

|   |   |   |   |
|---|---|---|---|
|   |   |   | dimengerti bagi orang lain  |
| 4 | (Imam Riadi, Abdul Fadlil dan Fahmi Auliya Tsani, 2022) | Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher                       | Penelitian ini menghasilkan output berupa aplikasi berbasis konsol dengan kata lain dijalankan melalui terminal / command prompt dan dibangun menggunakan bahasa pemrograman PHP versi 7.2.19 di atas platform Windows 10 Pro 64-bit. |
| 5 | Subandi et al. (2018)                                   | <i>Vigenere cipher algorithm modification by adopting RC6 key expansion and double encryption process</i> | Hasil dari penelitian ini adalah melakukan enkripsi citra digital dengan melakukan dua kali proses enkripsi menggunakan Vigenere Cipher dan mengadopsi <i>expansion key</i> menggunakan algoritma RC6 pada media teks.                |

Hasil penelitian yang dipakai adalah “Implementasi Kriptografi Vigenere Cipher Dengan PHP” (Irawan, 2017). Perbedaan antara penelitian tersebut dan penelitian yang saya lakukan terletak pada aplikasi yang dihasilkan serta jenis file yang dienkripsi dan deskripsi. Penelitian ini dilakukan untuk membuat implementasi kriptografi Vigenere Cipher. Sistem ini dirancang dengan melakukan analisa dengan metode deskriptif dan metode komparatif. Setelah dilakukan analisa,



maka dilakukan pemodelan dengan UML (*Unified Modelling Language*) dan dilakukan perancangan sistem kriptografi vigenere cipher dengan bentuk enkripsi dan dekripsi text yang dapat diprogram dengan menggunakan *software* PHP. Hasil penelitian ini adalah sebuah implementasi sistem kriptografi Vigenere Cipher dengan PHP. Sedangkan penelitian yang saya lakukan yaitu Penerapan Algoritma Vigenere Cipher Untuk Enkripsi Dokumen Dalam Mengamankan Informasi Yang Dikecualikan Di Badan Perencanaan Pembangunan, Riset Dan Inovasi Daerah (BAPPERIDA) Kabupaten Malaka. Aplikasi yang dihasilkan berupa website yang dibangun menggunakan bahasa pemrograman PHP dengan bantuan *Visual Studio Code* (VSC) yang dapat melakukan enkripsi dan dekripsi pada text dan media citra digital.

## **H. Landasan Teori**

### **1. Keamanan**

Keamanan adalah keadaan bebas dari bahaya. Istilah ini dapat digunakan dengan hubungan kepada kejahatan, dan segala bentuk kecelakaan. Keamanan merupakan topik yang luas termasuk keamanan nasional terhadap seorang teroris, keamanan komputer terhadap *hacker*, keamanan rumah terhadap maling dan penyusup lainnya, keamanan finansial terhadap kehancuran ekonomi dan banyak situasi berhubungan lainnya. *Host* Komputer yang terhubung ke *network*, mempunyai ancaman keamanan lebih besar dari pada *host* yang tidak berhubungan kemana-mana. Dengan mengendalikan *network security* resiko tersebut dapat dikurangi (Santoso & Fakhriza, 2018).

### **2. Keamanan Data**

Keamanan data adalah proses melindungi data dari kehilangan, perubahan, atau akses tidak sah selama seluruh siklus hidupnya. Ini mencakup segala sesuatu mulai dari kebijakan dan praktik perusahaan hingga perangkat keras, perangkat lunak, penyimpanan, dan perangkat pengguna yang digunakan oleh perusahaan tersebut (D.M , J.Dhiipan,

2022).

### **3. Kriptografi**

Kriptografi adalah praktik mengamankan informasi melalui penggunaan kode, sandi, dan metode enkripsi lainnya. Ini adalah aspek penting dari komunikasi modern, memungkinkan transmisi data yang aman melalui jaringan dan melindungi informasi sensitif dari akses yang tidak sah. Kriptografi telah digunakan sepanjang sejarah untuk melindungi pesan dari intersepsi dan penguraian. Pada zaman kuno, kriptografi digunakan oleh para pemimpin militer dan diplomat untuk mengkomunikasikan informasi rahasia. Seiring berjalannya waktu, teknik kriptografi menjadi lebih canggih, dan kriptografi modern kini menggunakan algoritma dan prinsip matematika yang kompleks. Saat ini, kriptografi digunakan dalam berbagai aplikasi, termasuk perbankan online, e-commerce, pesan aman, dan komunikasi pemerintah (Ruma Yadav, 2023)

### **4. Enkripsi dan Dekripsi**

Enkripsi adalah proses mengubah teks biasa menjadi teks tersandi, yang tidak dapat dipahami atau diubah dengan mudah oleh orang yang tidak diinginkan, sedangkan Dekripsi adalah proses mengubah teks tersandi menjadi teks biasa. Ini juga dapat didefinisikan sebagai ilmu yang menggunakan matematika dalam operasi enkripsi dan dekripsi data (Omar G.Abood & S.Guirguis, 2018).

### **5. Algoritma Vigenere Cipher**

Vigenère Cipher adalah salah satu algoritma kriptografi klasik yang diperkenalkan pada abad 16 atau kira-kira pada tahun 1586. Algoritma kriptografi ini dipublikasikan oleh seorang diplomat dan juga kriptologis yang berasal dari Prancis, yaitu Blaise de Vigenère, namun sebenarnya algoritma ini telah digambarkan sebelumnya pada buku *La Cifra del Sig. Giovan Batista Belaso*, sebuah buku yang ditulis oleh Giovan Batista Belaso, pada tahun 1553 (Hallim & Nadhori, 2010).

Algoritma Vigenere Cipher ini menggunakan bujur sangkar Vigenere untuk melakukan enkripsi. Setiap baris di dalam bujur sangkar

menyatakan huruf-huruf *ciphertext* yang diperoleh dengan Caesar cipher. Pada proses enkripsi Vigenere Cipher ini selain menggunakan Tabula Recta untuk mendapatkan *ciphertext* juga dapat menggunakan rumus berikut:

$$C_i = (P_i + K_i) \bmod 26$$

Sedangkan untuk rumus dekripsi Vigenere Cipher:

$$P_i = (C_i - K_i) \bmod 26$$

Dimana :  $C_i = \text{cipherteks}$

$P_i = \text{plainteks}$

$K_i = \text{kunci}$

## 6. Base64

Base64 merupakan salah satu skema *encoding binary-to-text* yang merepresentasikan data *binary* menjadi susunan karakter berformat ASCII, dengan menerjemahkannya ke dalam susunan radix-64 (Wen & Dang, 2018). Base64 adalah jenis pengkodean umum yang digunakan dalam menyampaikan data biner di Internet. Prinsip dasarnya adalah membagi setiap tiga *byte kontinu* (24bit) menjadi empat nilai enam-bit, dan kemudian menyampaikan setiap nilai enam-bit sebagai karakter NVT ASCII (Wang, 2000).

Proses *encoding* menggunakan Base64 melibatkan beberapa langkah sebagai berikut:

Data biner dibagi menjadi blok-blok berukuran 24 bit.

1. Setiap blok 24 bit dipecah menjadi empat blok 6 bit.
2. Setiap blok 6 bit digunakan sebagai indeks untuk mencari karakter ASCII tertentu dalam tabel Base64.
3. Karakter-karakter ini digabungkan untuk membentuk teks yang dihasilkan.

## 7. Aplikasi

Aplikasi adalah satu unit perangkat lunak yang dibuat untuk melayani kebutuhan akan beberapa aktivitas seperti perniagaan, *game*, pelayanan

masyarakat, periklanan dan hampir semua proses kegiatan (Rohayah et al, 2015) .

## **8. PHP (*Hypertext Preprocessor*)**

Bahasa pemrograman PHP merupakan bahasa pemrograman untuk membuat website yang bersifat *server-side scripting*. PHP bersifat dinamis. PHP dapat dijalankan pada berbagai macam sistem operasi seperti Windows, Linux, dan Mac Os. Selain Apache, PHP juga mendukung beberapa web server lain, seperti Microsoft ISS, Caudium, dan PWS. PHP dapat memanfaatkan database untuk menghasilkan halaman web yang dinamis (Novendri et al, 2019).

## **9. MySQL**

Pada perkembangannya, MySQL disebut juga SQL yang merupakan singkatan dari *Structured Query Language*. SQL merupakan bahasa terstruktur yang khusus digunakan untuk mengolah database. SQL pertama kali didefinisikan oleh *American National Standards Institute* (ANSI) pada tahun 1986. MySQL adalah sebuah sistem manajemen database yang bersifat *open source* (Novendri et al, 2019).

## **10. XAMPP**

XAMPP adalah sebuah software yang berfungsi untuk menjalankan website berbasis PHP dan menggunakan pengolah data MySQL di komputer lokal. XAMPP berperan sebagai server web pada komputer lokal. XAMPP juga dapat disebut sebuah Cpanel server virtual, ang dapat membantu melakukan preview sehingga dapat dimodifikasi website tanpa harus online atau terakses dengan internet. Xampp merupakan pengembangan dari lamp (linuk, apache, MYSQL, PHP,dan PERL) (Trimarsiah & Arafat, 2017).

## **11. Database**

*Database* atau basis data adalah kumpulan data yang dikelola sedemikian rupa berdasarkan ketentuan tertentu yang saling berhubungan sehingga mudah dalam pengelolaannya. Melalui pengelolaan tersebut pengguna dapat memperoleh kemudahan dalam mencari informasi,

menyimpan informasi dan membuang informasi (Intern, 2020).

Adapun pengertian lain dari database adalah sistem yang berfungsi sebagai mengumpulkan *file*, tabel, atau arsip yang terhubung dan disimpan dalam berbagai media elektronik (Intern, 2020).

## 12. Website



Gambar 1. *Website*

*Sumber: <https://www.vhv.rs/file/max>*

Situs web adalah sekumpulan halaman web yang dapat diakses melalui Internet, disusun berdasarkan URL dasar, atau situs, tempat halaman utama berada, dan umumnya berada dalam direktori yang sama di server (Antônia & Orivaldo, 2023).

## 13. Badan Perencanaan Pembangunan, Riset Dan Inovasi Daerah (BAPPERIDA)

Badan Perencanaan Pembangunan, Riset Dan Inovasi Daerah (BAPPERIDA) adalah lembaga teknis daerah dibidang penelitian dan perencanaan pembangunan daerah yang dipimpin oleh seorang kepala badan yang berada dibawah dan bertanggung jawab kepada Gubernur/Bupati/Wali kota melalui Sekretaris Daerah. Badan ini mempunyai tugas pokok membantu Gubernur/Bupati/Wali kota dalam penyelenggaraan pemerintahan daerah dibidang penelitian dan perencanaan pembangunan daerah (*Badan Perencanaan Pembangunan Daerah - Wikipedia Bahasa Indonesia, Ensiklopedia Bebas*).

## 14. Informasi yang dikecualikan

Berdasarkan undang-undang nomor 14 tahun 2008 tentang keterbukaan informasi publik, terdapat kategori informasi publik mengenai informasi publik yang terbuka dan dikecualikan. Informasi

yang dikecualikan adalah informasi yang tidak dapat diakses oleh pemohon informasi publik sebagaimana dimaksud dalam undang-undang nomor 14 tahun 2008 tentang keterbukaan informasi publik (*Informasi Yang Dikecualikan – PPID*).

Ciri-ciri informasi yang dikecualikan:

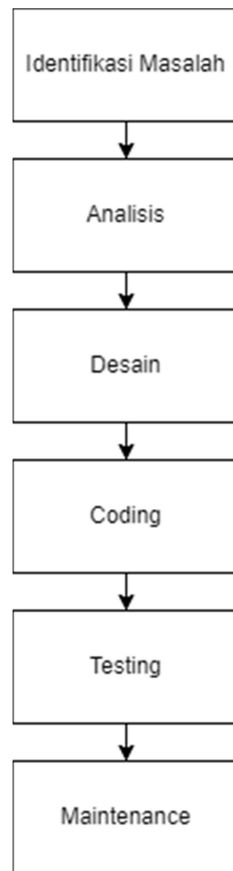
- a) Informasi yang berkaitan dengan kepentingan nasional dan keamanan negara.
- b) Informasi yang berhubungan dengan kerahasiaan negara, termasuk rahasia negara yang dilindungi oleh undang-undang.
- c) Informasi yang menyangkut kesehatan, keselamatan, dan keamanan masyarakat.
- d) Informasi yang menyangkut privasi, seperti data pribadi individu dan keluarganya.
- e) Informasi yang berkaitan dengan proses peradilan atau penegakan hukum, termasuk informasi yang terkait dengan investigasi kriminal atau keamanan nasional.
- f) Informasi yang berhubungan dengan hak kekayaan intelektual, seperti hak cipta dan paten.
- g) Informasi yang berisi rahasia dagang atau rahasia industri, serta informasi yang dapat merugikan bisnis atau usaha tertentu.
- h) Informasi yang bersifat rahasia atau dilindungi oleh undang-undang lainnya.

Contoh informasi yang dikecualikan di Badan Perencanaan Pembangunan Riset dan Inovasi Daerah seperti:

- a) Data penerima bantuan pangan
- b) Data penerima bantuan program/kegiatan perumahan

## **I. Metodologi Penelitian**

Metode yang digunakan dalam penelitian ini adalah metode *waterfall*, yang terdiri atas tahap-tahap sebagai berikut:



Gambar 2. Metodologi Penelitian

1. Identifikasi masalah merupakan tahapan awal dalam penelitian. Dalam penelitian ini, masalah yang akan diteliti adalah penerapan algoritma Vigenere Cipher untuk enkripsi dokumen dalam mengamankan informasi yang dikecualikan di Badan Perencanaan Pembangunan, Riset dan Inovasi Daerah (BAPPERIDA) Kabupaten Malaka. .
2. Analisis (*Recuirement*)

Tahap analisis merupakan langkah awal dalam model air terjun. Pengembang harus melakukan penelitian untuk mengetahui kebutuhan penggunaan sistem yang dibangunnya. Dalam tahap analisis sendiri di bagi dalam beberapa bagian yaitu:

a) Analisis kebutuhan sistem

Analisis kebutuhan sistem dilakukan untuk mengetahui data apa saja yang harus dimiliki oleh sistem agar dapat melayani kebutuhan

pengguna sistem. Adapun beberapa cara yang dapat digunakan untuk memperoleh data yaitu melalui wawancara dan studi pustaka.

- 1) Wawancara yaitu pengambilan data dengan melakukan tanya jawab secara langsung dengan pihak Badan Perencanaan Pembangunan, Riset dan Inovasi Daerah (BAPPERIDA) Kabupaten Malaka.
- 2) Studi Pustaka yaitu teknik pengumpulan data dengan mempelajari literatur yang bertujuan sebagai referensi untuk membantu dalam penelitian.

b) Analisis peran sistem

Pada tahap ini sistem yang akan dibangun mempunyai peran sebagai berikut:

1) Masukan sistem (*Input*)

Masukan (*Input*) adalah data yang diperlukan agar dimasukan ke dalam sistem untuk di olah. Data yang diperlukan dalam membangun system ini berupa data-data yang dianggap penting di Badan Perencanaan Pembangunan, Riset dan Inovasi Daerah (BAPPERIDA) Kabupaten Malaka.

2) Pengolah sistem (*Process*)

Proses merupakan serangkaian aktifitas yang dilakukan oleh system untuk mengolah input dan menghasilkan output. Dimana data atau informasi yang di ambil, di proses dan di ubah menjadi hasil yang diinginkan.

3) Keluaran sistem (*output*)

*Output* merupakan hasil atau keluaran yang dihasilkan oleh system sehingga dapat mengamankan data-data yang dianggap penting di Badan Perencanaan Pembangunan, Riset dan Inovasi Daerah (BAPPERIDA) Kabupaten Malaka .

c) Analisis Peran Pengguna.

- 1) Admin, yang berperan dalam mengelola sistem agar beroperasi dengan efisien dan aman. Pada penelitian ini yang menjadi admin adalah Kepala Badan Perencanaan Pembangunan, Riset dan Inovasi Daerah (BAPPERIDA) Kabupaten Malaka.



- 2) *User*, yang berperan sebagai pengguna dalam hal ini yang berperan sebagai *user* adalah pegawai kepercayaan Kepala Badan Perencanaan Pembangunan, Riset dan Inovasi Daerah (BAPPERIDA) Kabupaten Malaka.

### 3. Desain

Tahapan perancangan sistem ini akan didesain sesuai dengan kebutuhan sistem dari hasil analisis. Pada tahap ini akan menjelaskan bagaimana sistem ini dijalankan mulai dari rancangan sistem yang akan di bangun berupa tampilan aplikasi. Tahapan ini juga sangat penting dalam membangun suatu sistem.

### 4. Coding

Langkah ini mengikuti proses desain menggunakan implementasi yang mengarah ke pengkodean serta penerapan algoritma Vigenere Cipher dalam enkripsi dan dekripsi dokumen, dimana pada saat mengenkripsi, dokumen yang diupload dikonversi ke dalam format Base64 dan hasil dari konversi tersebut dienkripsi menggunakan algoritma Vigenere Cipher. Sedangkan pada saat mendekripsi, dokumen hasil enkripsi didekripsi menggunakan algoritma Vigenere Cipher dan hasil dekripsi tersebut dikonversi ke teks asli menggunakan Base64. Setiap unit yang dikembangkan kemudian diuji untuk melihat fungsionalitasnya yang sering disebut dengan unit *test*.

### 5. Testing

Pada tahap keempat ini akan dilakukan penggabungan modul-modul yang sudah dibuat sebelumnya. Setelah itu akan dilakukan pengujian yang bertujuan untuk mengetahui apakah *software* sudah sesuai desain yang diinginkan dan apakah masih ada kesalahan atau tidak. Pada tahap ini aplikasi sudah bisa dijalankan atau digunakan. Pengujian pada aplikasi ini bertujuan untuk mengetahui kesalahan terhadap sistem tersebut sehingga dapat diperbaiki.

### 6. Pemeliharaan Sistem (*Maintenance*)

Pada tahapan ini merupakan akhir dalam model *waterfall*. Pada tahap ini sistem dipasang dan digunakan secara nyata. *Maintenance*

melibatkan pembentukan kesalahan yang tidak ditemukan pada tahapan-tahapan sebelumnya, maka meningkatkan implementasi dari sebuah unit sistem, dan meningkatkan sebuah layanan sistem sebagai kebutuhan baru (Susilo, 2018).

#### **J. Hasil yang Diharapkan**

Hasil yang diharapkan dari penelitian ini adalah implementasi sistem keamanan data yang efektif di Badan Perencanaan Pembangunan, Riset, dan Inovasi Daerah (BAPPERIDA) Kabupaten Malaka untuk melindungi informasi sensitif, meningkatkan kesadaran dan pengetahuan staf terkait risiko keamanan data, mengurangi risiko penyalahgunaan data, memberikan kontribusi pada pengembangan metode enkripsi yang lebih kuat, serta meningkatkan kinerja dan efisiensi operasional BAPPERIDA Kabupaten Malaka dengan mengurangi risiko insiden keamanan data yang berpotensi merugikan.

#### **K. Jadwal Penelitian**

Jadwal penelitian yang dibuat bertujuan agar waktu dalam penelitian dapat diatur dengan baik sehingga pelaksanaannya dapat diselesaikan dengan tepat waktu.

Tabel 2. Jadwal Penelitian

| No | Tahapan    | I | II | III | IV | V | VI |
|----|------------|---|----|-----|----|---|----|
| 1  | Analisis   |   |    |     |    |   |    |
| 2  | Desain     |   |    |     |    |   |    |
| 3  | Pengerjaan |   |    |     |    |   |    |
| 4  | Uji Coba   |   |    |     |    |   |    |

|   |           |  |  |  |  |  |  |
|---|-----------|--|--|--|--|--|--|
| 5 | Perbaikan |  |  |  |  |  |  |
|---|-----------|--|--|--|--|--|--|

## DAFTAR PUSTAKA

- 22 KPM Di Desa Umalor Dicoret Dari Penerima Beras Bantuan Pangan, Kades Bilang.... (2024, April 7). *Sakunar*. <https://sakunar.com/2024/04/07/22-kpm-di-desa-umalor-dicoret-dari-penerima-beras-bantuan-pangan-kades-bilang/>
- Abood, O., & Guirguis, S. (2018). Survei Algoritma Kriptografi. *Jurnal Internasional Publikasi Ilmiah dan Penelitian (IJSRP)* . <https://doi.org/10.29322/IJSRP.8.7.2018.P7978> .
- Amrulloh, A., & Ujianto, E. (2019). Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher. *Jurnal CoreIT*, 5(2).
- Arafat, M. (2017). Analisis dan perancangan website sebagai sarana informasi pada lembaga bahasa kewirausahaan dan komputer Akmi Baturaja menggunakan PHP dan MySQL. *Jurnal Ilmiah MATRIK*, 19(1), 1-10.
- Badan Perencanaan Pembangunan Daerah—Wikipedia bahasa Indonesia, ensiklopedia bebas. (n.d.). Retrieved April 22, 2024, from [https://id.wikipedia.org/wiki/Badan\\_Perencanaan\\_Pembangunan\\_Daerah](https://id.wikipedia.org/wiki/Badan_Perencanaan_Pembangunan_Daerah)
- Feng, W. (2000). PENGKODEAN/DEKODE BASE64 DI VB6.0. *Teknik Komputer* .
- Ginting, Victor S. "Penerapan Algoritma Vigenere Cipher dan Hill Cipher Menggunakan Satuan Massa." *Jurnal Teknologi Informasi*, vol. 4, no. 2, 10 Dec. 2020, pp. 241-246, doi:10.36294/jurti.v4i2.1365.
- Hallim, A., Nadhori, I. U., & Setiawardhana, S. (2010). Pembuatan Perangkat Lunak Media Pembelajaran Kriptografi Klasik. *eeepis final project*.
- Imam Riadi, Abdul Fadlil, & Fahmi Auliya Tsani. (2022). Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher. *JISKA (Jurnal Informatika Sunan Kalijaga)*, 7(1), 33–45. <https://doi.org/10.14421/jiska.2022.7.1.33-45>
- Indeks Keamanan Siber Indonesia Peringkat ke-3 Terendah di Antara Negara G20. (n.d.). Retrieved April 24, 2024, from <https://databoks.katadata.co.id/datapublish/2022/09/13/indeks-keamanan-siber-indonesia-peringkat-ke-3-terendah-di-antara-negara-g20>
- Informasi yang Dikecualikan – PPID. (n.d.). Retrieved April 24, 2024, from

- <https://ppid.rsud.semarangkota.go.id/informasi-dikecualikan/>
- Intern, D. (2020, September 15). *Apa itu Database? Contoh Produk dan Fungsinya*. Dicoding Blog. <https://www.dicoding.com/blog/apa-itu-database/>
- Irawan, M. D. (2017). IMPLEMENTASI KRIPTOGRAFI VIGENERE CIPHER DENGAN PHP. *JURNAL TEKNOLOGI INFORMASI*, 1(1), 11.
- M, D., & Dhiipan, J. (2022). Analisis Meta Penanggulangan Efisien untuk Keamanan Data. *Konferensi Internasional 2022 tentang Otomasi, Komputasi, dan Sistem Terbarukan (ICACRS)*, 1303-1308. <https://doi.org/10.1109/ICACRS55517.2022.10029302>.
- Novendri, M. S., Saputra, A., & Firman, C. E. (2019). Aplikasi inventaris barang pada mts nurul islam dumai menggunakan php dan mysql. *lentera dumai*, 10(2).
- Patricia, H. (2015). Teknik Keamanan Data Menggunakan Kriptografi dengan Algoritma Vigenere Cipher dan Steganografi dengan Metode End of File (EoF). *Progr. Stud. Tek. Inform. Fak. Ilmu Komput. Univ. Dian Nuswantoro*, 1-7.
- Pinho, A., & Junior, O. (2023). PENGGUNAAN WEBSITE UNTUK MEMBANTU PENGAJARAN KIMIA ANALITIK. *Jurnal Debat Interdisipliner*. <https://doi.org/10.51249/jid.v4i01.1264>.
- Prameshwari, A., & Sastra, N. P. (2018). Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen. *Eksplora Informatika*, 8(1), 52. <https://doi.org/10.30864/eksplora.v8i1.139>
- Ramli, M., Asri, R., & Zarlis, M. (2017, August). Implementasi Algoritma Vigenere Substitusi dengan Shift Indeks Prima. In *Semantika (Seminar Nasional Teknik Informatika)* (Vol. 1, No. 1, pp. 149-154).
- Rohayah, Siti, et al. "Aplikasi Steganografi Untuk Penyisipan Pesan." *Jurnal Informatika Ahmad Dahlan*, vol. 9, no. 1, 1 Jan. 2015, doi:10.26555/jifo.v9i1.a2038.
- Santoso, H., & Fakhri, M. F. M. (2018). Perancangan aplikasi keamanan file audio format wav (waveform) menggunakan algoritma RSA. *Algoritma: Jurnal Ilmu Komputer Dan Informatika*, 2(1).

- Solichin, A. (2016). *Pemrograman web dengan PHP dan MySQL*. Penerbit Budi Luhur.
- Subandi, A., Lydia, M. S., Sembiring, R. W., Zarlis, M., & Efendi, S. (2018). Vigenere cipher algorithm modification by adopting RC6 key expansion and double encryption process. *IOP Conference Series: Materials Science and Engineering*, 420, 012119. <https://doi.org/10.1088/1757-899X/420/1/012119>
- Susilo, M. (2018). RANCANG BANGUN WEBSITE TOKO ONLINE MENGGUNAKAN METODE WATERFALL. *InfoTekJar (Jurnal Nasional Informatika dan Teknologi Jaringan)*, 2(2), 98–105. <https://doi.org/10.30743/infotekjar.v2i2.171>
- Wen, S., & Dang, W. (2018). Research on Base64 Encoding Algorithm and PHP Implementation. *2018 26th International Conference on Geoinformatics*, 1–5. <https://doi.org/10.1109/GEOINFORMATICS.2018.8557068>
- Yadav, R. (2023). Analisis Kriptografi dalam Teknologi Informasi. *JURNAL INTERANTIONAL PENELITIAN ILMIAH DI BIDANG TEKNIK DAN MANAJEMEN*. <https://doi.org/10.55041/ijsrem18379>.