BAB II
TINJAUAN PUSTAKA

II.1. Penelitian Terkait

Penelitian terkait dilakukan oleh Irfan Anas, Putra Arya Nanda, Abdul Hidayat (2018) yang berjudul ***"IMPLEMENTASI ALGORITMA VIGENERE CIPHER DAN GOST DALAM KEAMANAN DATA"*** yang berkesimpulan bahwa pengkombinasian dua algoritma ini dalam mengamankan data berjenis teks yang sifatnya rahasia atau penting. Pengamanan data berjenis teks berdasarkan kombinasi dua metode ini dilakukan dengan mengenkripsi data terlebih dahulu berdasarkan algoritma *vigeneere cipher*, kemudian *cipher vigeneere* dienkripsi kembali berdasarkan algoritma *GOST*, sehingga dihasilkan *cipher* akhir yang benar-benar acak. Kombinasi dua metode ini diharapkan dapat dijadikan sebagai salah satu solusi dalam pengoptimalan pengaman data khususnya data yang sifatnya rahasia.

Penelitian terkait dilakukan oleh Akim Manaor Hara Pardede, Hotler Manurung, Dina Filina (2017) yang berjudul ***"ALGORITMA VIGENERE CIPHER DAN HILL CIPHER DALAMA APLIKASI KEAMANAN DATA PADA FILE DOKUMEN"*** yang berkesimpulan bahwa solusi untuk memperkuat algoritma menjadi lebih sulit untuk dapat dipecahkan dan untuk mengecoh kriptanalisis. File teks yang telah diamankan menggunakan Algoritma Vigenere Cipher akan diamankan lagi menggunakan Algoritma Hill Cipher. Implementasi sistem menggunakan perangkat lunak Visual Basic.Net 2010. Hasil dari sistem ini

berupa file yang ter-enkripsi (cipherfile) yang tidak bisa dimengerti. Kemudian fileteks kembali normal setelah di-dekripsi.

Penelitian terkait dilakukan oleh Victor Saputra Ginting (2020) yang berjudul ***"PENERAPAN ALGORITMA VIGENERE CIPHER DAN HILL CIPHER MENGGUNAKAN SATUAN MASSA"*** yang berkesimpulan bahwa 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.

Penelitian terkait dilakukan oleh Celine Aloyshima Haris, Dony Ariyus (2020) yang berjudul ***"KOMBINASI DAN MODIFIKASI VIGENERE CIPHER DAN HILL CIPHER MENGGUNAKAN METODE HYBRID KODE POS, TRIGONOMETRI, DAN KONVERSI SUHU SEBAGAI PENGAMANAN PESAN "*** yang berkesimpulan bahwa menyulitkan kriptanalis untuk memecahkan pesan asli. Semakin banyak proses yang diperlukan dan semakin panjang waktu yang dibutuhkan untuk memecahkan pesan yang telah di enkripsi tersebut artinya semakin aman digunakan untuk merahasiakan pesan. Agar semakin sulit memecahkannya maka menggunakan metode hybrid antara kode pos, trigonometri, dan konversi suhu yang diimplementasikan dalam bahasa pemrograman Java.

II.2. Landasan Teoritis

II.2.1. Rancang Bangun

Rancang Bangun adalah penggambaran, perencanaan, dan pembuatan sketsa atau pengaturan dari beberapa elemen yang terpisah kedalam suatu kesatuan yang utuh dan berfungsi. Dengan demikian pengertian rancang bangun merupakan kegiatan menerjemahkan hasil analisa ke dalam bentuk paket perangkat lunak kemudian menciptakan sistem tersebut atau memperbaiki sistem yang sudah ada (Abdur Rauf JH, Agung Tri Prastowo: 2021).

II.2.2. Pengertian Aplikasi

Aplikasi merupakan program yang dikembangkan untuk memenuhi kebutuhan pengguna dalam menjalankan pekerjaan tertentu. Perangkat lunak aplikasi dibedakan menjadi beberapa macam berdasarkan kegunaannya. (Abdur Rauf JH, Agung Tri Prastowo: 2021).

II.2.3. Pengertian Website

Website adalah kumpulan dari halaman-halaman situs, yang terangkum dalam sebuah domain atau subdomain, yang tempatnya berada di dalam *World Wide Web (WWW)* di dalam internet, *website* juga dapat diartikan sebagai sebuah halaman yang berisi data, baik data text, gambar, suara dan lainya yang dapat diakses secara online. ada banyak model pengembangan sistem yang bisa dimanfaatkan untuk membangun *website* salah satunya model *Prototyping.* (Ahmad Josi, 2017: 50)

II.2.4. Pengertian Kriptografi

Secara etimologi, kriptografi berasal dari bahasa Yunani yaitu kryptos yang bermakna tersembunyi dan graphein yang bermakna tulisan. Kriptografi adalah ilmu menulis pesan rahasia dengan tujuan menyembunyikan makna pesan tersebut (Muhammad Khoiruddin Harahap, 2016 : 62).

Berikut ini adalah lima istilah kriptografi secara umum yaitu:

1. Plaintext: Pesan asli sebelum diubah menjadi pesan rahasia.
2. Key: Kunci rahasia yang akan digunakan untuk mengubah pesan asli menjadi pesan rahasia.
3. Ciphertext: Pesan rahasia yang sudah berbentuk kode-kode yang sulit untuk diterjemahkan.
4. Enkripsi: Proses mengubah Plaintext menjadi Ciphertext.
5 Dekripsi: Proses mengubah Ciphertext menjadi Plaintext.

II.2.5. Pengertian Algoritma Vigenere Cipher

Metode Vigenere Cipher adalah suatu metode penyandian teks alfabet menggunakan deretan sandi Caesar berdasarkan huruf pada kunci. Sandi Vigenere merupakan bentuk sederhana dari substitusi. Kelebihan sandi dibanding sandi Caesar dan sandi monoalfabetik lain adalah sandi yang tidak rentan terhadap metode pemecahan sandi. (Victor Saputra Ginting, 2020: 242)

Setiap huruf teks terang digantikan dengan huruf lain yang memiliki perbedaan tertentu pada urutan alfabet. Misalnya pada sandi Caesar dengan geseran 3, A menjadi D, B menjadi E and dan seterusnya.

Enkripsi (penyandian) dengan sandi Vigenère juga dapat dituliskan secara matematis, dengan menggunakan penjumlahan dan operasi modulus, yaitu:

$Ci = (Pi + Ki) \bmod 26$……(1)

Ci = nilai ascii dari karakter *ciphertext* ke-*i*

Pi = nilai ascii dari karakter *plaintext* ke-*i*

Ki = nilai ascii dari karakter kunci ke-i

Sedangkan proses dekripsi dengan sandi Vigenere dituliskan secara matematis sebagai berikut,

$Pi = (Ci – Ki) \bmod 26$……(2)

Ci = nilai ascii dari karakter *ciphertext* ke-*i*

Pi = nilai ascii dari karakter *plaintext* ke-*i*

Ki = nilai ascii dari karakter kunci ke-i

Angka modulo 26 di atas, digunakan apabila jumlah karakter yang ingin diproses hanya berjumlah 26 karakter. Apabila karakter yang ingin diproses adalah semua karakter ASCII yang berjumlah 256 karakter, maka rumus yang digunakan adalah modulo 256 (Niria Laila, Anita Sindar RMS, 2018: 50).

II.2.6. Pengertian Algoritma Hill Cipher

Algoritma Hill Cipher merupakan algoritma kriptografi kunci simetris yang mempunyai berbagai kelebihan dalam mengenkripsi data). Hill Cipher ialah penerapan aritmatika modulo pada kriptografi. Teknik kriprografi ini menggunakan matrik persegi sebagai kunci yang nantinya digunakan untuk melakukan enkripsi dan dekripsi. (Victor Saputra Ginting, 2020: 242)

Dasar dari teknik *hill cipher* adalah aritmatika modulo terhadap matriks. Dalam penerapannya, *hill cipher* menggunakan teknik perkalian matriks dan teknik invers terhadap matriks. Kunci pada *hill cipher* adalah matriks *n* x *n* dengan *n* merupakan ukuran blok. Jika matriks kunci disebut dengan *K*, maka matriks *K* adalah sebagai berikut :

$K_{2X2} = \begin{bmatrix} K11 & K12 \\ K21 & K22 \end{bmatrix}$

Matriks *K* yang menjadi kunci ini harus merupakan matriks yang *invertible*, yaitu memiliki *multiplicative inverse K*-1 sehingga :

K : Kunci Matriks

K-1 : Inverse Matriks

K . *K-1* = 1 (Ahmat Sayuti, Hamdan Habibi,Wijang Widhiarso, 2019: 5)

II.2.7. Pengertian Xampp

Menurut Heriyanto (2012:12). Xampp adalah sebuah aplikasi yang dapat menjadikan komputer kita menjadi sebuah server. Kegunaan Xampp ini untuk membuat jaringan local sendiri dalam artian kita dapat membuat website secara offline untuk masa coba-coba di komputer sendiri. Jadi fungsi dari Xampp server itu sendiri merupakan server website kita untuk cara memakainya. Disebut server karena dalam hal ini komputer yang akan kita pakai harus memberikan pelayanan untuk mengakseskan web, untuk itu komputer kita harus menjadi server. (Ahmad Josi, 2017: 52)

II.2.8. UML *(Unified Modeling Language)*

Menurut (Henry Februariyanti, 2012) *UML (Unified Modeling Langguage)* adalah bahasa untuk visualisasi, spesifikasi, membangun sistem perangkat lunak,

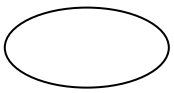
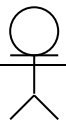
serta dokumentasi. UML menyediakan model- model yang tepat, tidak ambigu, dan lengkap. Secara khusus UML menspesifikasi langkah-langkah penting dalam pengembangan keputusan analisis, perancangan, serta implementasi dalam sistem perangkat lunak. (Asep Hardiyanto Nugroho, Toyip Rohimi, 2020: 4)

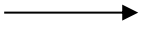
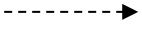
Perancangan menggunakan UML pada penelitian ini menggunakan 4 diagram yaitu: *Use Case Diagram, Class Diagram,Sequence Diagram* dan *Activity Diagram.*

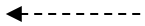
II.2.8.1. *Use Case Diagram*

Use case diagram merupakan pemodelan untuk kelakuan sistem informasi yang akan dibuat. Use case bekerja dengan mendeskripsikan tipikal interaksi antara user sebuah sistem dengan sistemnnya sendiri melalui sebuah cerita bagaimana sistem itu dipakai.

Tabel II.1. Simbol *Use Case* Diagram

Gambar	Keterangan	Deskripsi
	*Use Case*	Menggambarkan fungsionalitas yang disediakan sistem sebagai unit-unit yang bertukar pesan antar unit dengan aktor, biasanya dinyatakan dengan menggunakan kata kerja di awal nama use case.
	Aktor	Sistem yang lain yang mengaktifkan fungsi dari target

		sistem. Untuk mengidentifikasikan aktor, harus ditentukan pembagian tenaga kerja dan tugas-tugas yang berkaitan dengan peran pada konteks target sistem.
———	Asosiasi tanpa panah	Penghubung antara aktor dan use case, digambarkan dengan garis tanpa panah yang mengindikasikan siapa atau apa yang meminta interaksi secara langsung dan bukannya mengindikasikan aliran data.
	Asosiasi dengan panah	Penghubung antara aktor dan use case yang menggunakan panah terbuka untuk mengidinkasikan bila aktor berinteraksi secara pasif dengan sistem.
	*Include*	Merupakan di dalam use case lain (required) atau pemanggilan use case oleh use case lain, contohnya

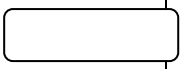
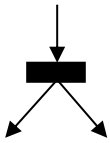
		adalah pemanggilan sebuah fungsi program.
	*Extend*	Merupakan perluasan dari use case lain jika kondisi atau syarat terpenuhi

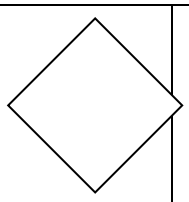
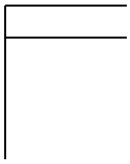
Sumber: (Dede Wira & Rahmi Andriani; 2019)

II.2.8.2. *Activity Diagram*

Activity diagram merupakan diagram yang menggambarkkan workflow atau aktivitas dari sebuah sistem yang ada pada perangkat lunak.

Tabel II.2. Simbol *Activity* Diagram

Gambar	Arti	Keterangan
	*Start Point*	Diletakkan pada pojok kiri atas dan merupakan awal aktivitas
	*End Point*	Akhir aktivitas
	*Activities*	Menggambarkan suatu proses/kegiatan bisnis
	*Fork*/percabangan	Digunakan untuk menunjukkan kegiatan yang dilakukan secara paralel atau untuk menggabung kan dua kegiatan paralel menjadi satu
	*Join* (penggabungan) atau *rake*	Digunakan untuk menunjukkan adanya dekomposisi

	*Decision* Points	Menggambar kan pilihan untuk pengambilan keputusan, tru atau false
	*Swimlane*	pembagian *activity* diagram untuk menunjukkan siapa melakukan apa

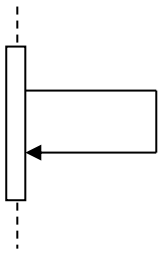
Sumber: (Dede Wira & Rahmi Andriani; 2019)

II.2.8.3 *Sequence Diagram*

Sequence diagram menggambarkan kelakuan objek pada use case dengan mendeskripsikan waktu hidup objek dan pesan yang dikirimkan dan diterima antar objek. Gambaran sequence diagram dibuat minimal sebnayak pendefinisan use case yang memiliki proses sendiri atau yang penting semua use case yang telah didefinisikan interaksi jalannya pesan sudah dicakup pada sequence diagram sehingga semakin banyak use case yang didefinisikan, maka sequence diagram yang harus dibuat juga semakin banyak.

Tabel II.3. Simbol *Sequence Diagram*

Gambar	Arti	Keterangan
	*Entity Class*	Merupakan bagian dari sistem yang berisi kumpulan kelas berupa entitas-entitas yang membentuk gambaran awal sistem dan menjadi landasan untuk menyusun basis data

	*Boundary Class*	Berisi kumpulan kelas yang menjadi *interfaces* atau interaksi antara satu atau lebih aktor dengan sistem, seperti tampilan *form entry* dan *form* cetak
	*Control class*	Suatu objek yang berisi logika aplikasi yang tidak memiliki tanggung jawab kepada entitas, contohnya adalah kalkulasi dan aturan bisnis yang melibatkan berbagai objek
	Message	Simbol mengirim pesan antar *class*
	*Recursive*	Menggambarkan pengiriman pesan yang dikirim untuk dirinya sendiri
	*Activation*	Mewakili sebuah eksekusi operasi dari objek, panjang kotak ini berbanding lurus dengan durasi aktivasi sebuah operasi

	Lifeline	Garis titik-titik yang terhubung dengan objek, sepanjang lifeline terdapat activation

Sumber: (Dede Wira & Rahmi Andriani; 2019)