BAB 1
PENDAHULUAN

1.1 Latar Belakang

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek penting pada sebuah sistem pengiriman informasi. Dalam hal ini, sangat terkait dengan betapa pentingnya informasi tersebut dikirim dan diterima oleh orang yang berkepentingan. Informasi berguna apabila di tengah proses pengiriman, informasi itu disadap atau dibajak oleh orang yang tidak berhak [1]. Ada beberapa cara melakukan pengamanan data ataupun pesan, diantaranya adalah dengan menggunakan teknik penyamaran data yang disebut dengan kriptografi.

Kriptografi berasal dari bahasa Yunani yaitu *kryptos* yang artinya "yang tersembunyi" dan *graphein* yang artinya "tulisan", jadi kriptografi adalah seni dan ilmu untuk menjaga keamanan data [2]. Teknik kriptografi banyak diterapkan untuk pengamanan data ataupun informasi penting agar terhindar dari oknum-oknum yang tidak berhak.

Covid-19 pertama kali muncul di kota Wuhan, Cina. Penyebarannya sangat cepat dan mematikan. Penyebarannya melalui kontak langsung fisik manusia ditularkan melalui mulut, hidung dan mata. Upaya memutus mata rantai penyebaran *Covid-19* dilakukan pemerintah dan lembaga keagamaan dengan menerbitkan beberapa peraturan untuk dipatuhi oleh masyarakat [3]. Dampak wabah *Covid-19* terlihat hampir di seluruh sektor kehidupan masyarakat. Begitu pula dengan angka kematian ataupun korban yang terserang *Covid-19* di Indonesia yang semakin hari semakin bertambah. Pada Kabupaten Rokan Hulu kasus terinfeksi *Covid-19* juga

semakin meningkat. Dilansir dari laman corona.riau.go.id, *update* data per tanggal 28 Maret 2021 tercatat 10.193 kasus, 1.368 pasien yang terkonfirmasi *covid-19*, 236 pasien yang di isolasi, 43 pasien di rawat, 1.024 pasien yang telah dinyatakan sembuh dan 65 pasien yang meninggal. Jumlah tersebut diperkirakan akan semakin bertambah. Pemerintahan pusat bekerja sama dengan pemerintahan daerah untuk memutus rantai pandemi *Covid-19* tersebut. Data pasien *Covid-19* terus di*update* setiap harinya untuk melihat perkembangan kasus *Covid-19* di Kabupaten Rokan Hulu. Data yang ditampilkan hanyalah jumlah yang terserang *Covid-19*, sedangkan data pasiennya tidak ditampilkan dikarenakan merupakan data privasi yang tidak perlu disebarluaskan.

Saat ini, data pasien *Covid-19* yang ada pada Dinas Kesehatan Kabupaten Rokan Hulu hanya dilakukan pengelolaan dengan menggunakan aplikasi *Microsoft Excel* sehingga bisa saja data tersebut dicuri atau pun rusak. Data pasien *Covid-19* yang tercatat harus diamankan dan dikelola dengan baik agar data tersebut terjaga dari oknum-oknum yang tidak bertanggungjawab, untuk itu diperlukan sebuah wadah khusus untuk mengelola data serta diterapkan sistem pengamanan yang dapat melindungi data pasien *Covid-19* di Kabupaten Rokan Hulu. Kriptografi menjadi pilihan yang tepat agar data pasien *Covid-19* di Kabupaten Rokan Hulu lebih aman. Pada pemakaian teknik pengamanan kriptografi dengan menggunakan metode yaitu *Vigenere Cipher* dan *Caesar 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 [4]. Sedangkan, *Caesar Cipher* merupakan salah satu jenis *cipher* substitusi yang membentuk *cipher* dengan cara melakukan penukaran satu karakter diganti dengan karakter yang berada di sejumlah digit sebelah kanan atau kirinya, tergantung arah pergeserannya [5].

Metode *Vigenere Cipher* dan *Caesar Cipher* telah diterapkan di dalam beberapa penelitian. Pada penelitian yang dilakukan oleh Priyono (2016) dengan judul "Penerapan Algoritma *Caesar Cipher* Dan Algoritma *Vigenere Cipher* Dalam Pengamanan Pesan Teks", maka didapatkan hasil bahwa keamanan pesan teks dapat diimplementasikan dengan metode enkripsi, salah satunya adalah enkripsi *Vigenere Cipher* dan *Caesar Cipher*. Dimana proses pesan yang dikirim atau diterima dapat diubah dengan metode *Caesar* dan *Vigenere* untuk keamanan isi dari pesan. Selain itu, Metode penyandian *Caesar Cipher* dan *Vigenere Cipher* termasuk dalam kriptografi klasik dimana kedua algoritma tersebut merupakan teknik enkripsi yang paling sederhana dan banyak digunakan [6].

Berdasarkan latar belakang yang telah dipaparkan, maka penelitian ini diberi judul sebagai berikut "Implementasi *Double* Kripto dengan Metode *Vigenere Cipher* dan *Caesar Cipher* Untuk Perlindungan Data Pasien *Covid-19* (Studi Kasus : Dinas Kesehatan Kabupaten Rokan Hulu)".

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang dipaparkan, dapat dirumuskan sebagai berikut :

1. Bagaimana menerapkan metode *Vigenere Cipher* dan *Caesar Cipher* untuk perlindungan data pasien *Covid-19* pada sistem informasi *Covid-19* Kabupaten Rokan Hulu ?
2. Bagaimana membuat sistem informasi *Covid-19* Kabupaten Rokan Hulu dengan menerapkan kriptografi metode *Vigenere Cipher* dan *Caesar Cipher* untuk perlindungan data pasien *Covid-19* ?

1.3 Tujuan Penelitian

Tujuan kegiatan penelitian tugas akhir ini adalah :

1. Menerapkan *Vigenere Cipher* dan *Caesar Cipher* untuk perlindungan data pasien *Covid-19* pada sistem informasi *Covid-19* Kabupaten Rokan Hulu
2. Membuat sebuah sistem informasi *Covid-19* Kabupaten Rokan Hulu dengan menerapkan kriptografi metode *Vigenere Cipher* dan *Caesar Cipher* untuk perlindungan data pasien *Covid-19*.

1.4 Batasan Masalah

Pada pembangunan sistem ini dibuat beberapa batasan masalah agar pembahasan lebih terfokus pada masalah yang diteliti sesuai dengan tujuan yang akan dicapai. Adapun batasan masalahnya adalah sebagai berikut :

1. Aplikasi yang akan dibuat yaitu berupa sistem informasi *Covid-19* Kabupaten Rokan Hulu dengan perlindungan data pasien *Covid-19* pada database di Dinas Kesehatan Kabupaten Rokan Hulu.
2. Metode yang digunakan dalam perlindungan data pasien *Covid-19* adalah metode *Vigenere Cipher* dan *Caesar Cipher*.

3. Data yang diinputkan ke dalam sistem berupa data pasien, kemudian dilakukan proses enkripsi untuk menghasilkan data berupa plainteks pada database sistem.
4. Aplikasi yang dibuat berfungsi untuk menggantikan pengelolaan data menggunakan *Microsoft Excel* dan menerapkan perlindungan data.
5. Aplikasi ini dibuat berbasis *web* dengan menggunakan bahasa pemrograman PHP dan database MySQL.

1.5 Manfaat Penelitian

Manfaat yang ingin dicapai dalam implementasi tugas akhir ini adalah :

1. Manfaat bagi Dinas Kesehatan Kabupaten Rokan Hulu melindungi data pasien *Covid-19* agar tidak dapat disadap oleh pihak yang tidak berhak.
2. Manfaat bagi peneliti selanjutnya dapat dijadikan sebagai bahan informasi untuk penelitian selanjutnya.

1.6 Sistematika Penulisan

Sistematika penulisan dari tugas akhir ini terdiri dari pokok-pokok permasalahan yang dibahas pada masing-masing yang diuraikan menjadi beberapa bagian :

BAB 1 PENDAHULUAN

Berisi latar belakang, rumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian, dan sistematika penulisan.

BAB 2 LANDASAN TEORI

Bab ini berisi teori-teori yang digunakan pada penelitian ini. Teori-teori yang berhubungan dengan keamanan data, kriptografi, *Vigenere Cipher*,

Caesar Cipher, pasien, *Covid-19,* alat bantu perancangan program dan alat bantu perancangan aplikasi.

BAB 3 METODOLOGI PENELITIAN

Bab ini berisi kerangka penelitian yang diusulkan dalam pengembangan sistem dengan tujuan mampu menjadi pemandu didalam pengembangan proyek, dan menyediakan solusi kepada *statement* masalah.

BAB 4 ANALISA DAN PERANCANGAN

Bab ini berisi analisa dan perancangan sistem informasi *Covid-19* Kabupaten Rokan Hulu dengan menerapkan kriptografi metode *Vigenere Cipher* dan *Caesar Cipher* untuk perlindungan data pasien *Covid-19* pada database di Dinas Kesehatan Kabupaten Rokan Hulu.

BAB 5 IMPLEMENTASI DAN PENGUJIAN

Bab ini berisi implementasi hasil rancangan kode program dan hasil pengujian perangkat lunak, serta analisa terhadap hasil pengujian.

BAB 6 PENUTUP

Bab ini berisi rangkuman dari hasil penelitian yang telah dilakukan dan saran-saran untuk pengembangan aplikasi atau penelitian selanjutnya.

BAB 2

LANDASAN TEORI

Bab ini berisi landasan teori sebagai parameter rujukan untuk dilaksanakannya penelitian ini. Adapun landasan teori tersebut adalah tentang implementasi, perlindungan, perlindungan data, keamanan data, kriptografi, *Vigenere Cipher*, *Caesar Cipher*, pasien, *Covid-19*, alat bantu perancangan program dan alat bantu perancangan aplikasi.

2.1 Implementasi

Kata implementasi berasal dari bahasa Inggris yaitu *to implement* yang berarti mengimplementasikan. Implementasi adalah penyediaan sarana untuk melaksanakan sesuatu yang menimbulkan dampak/akibat terhadap sesuatu [7].

Implementasi merupakan suatu proses mendapatkan suatu hasil yang sesuai dengan tujuan atau sasaran kebijakan itu sendiri. Dimana pelaksana kebijakan melakukan suatu aktivitas atau kegiatan [8].

2.2 Perlindungan Data

Perlindungan data pada dasarnya dapat berhubungan secara khusus dengan privasi seperti yang dikemukakan oleh Allan Westin yang untuk pertama kali mendefinisikan privasi sebagai hak individu, grup atau lembaga untuk menentukan apakah informasi tentang mereka akan dikomunikasikan atau tidak kepada pihak lain sehingga definisi yang dikemukakan oleh Westin disebut dengan information privacy karena menyangkut informasi pribadi. Perlindungan data juga merupakan hak asasi manusia yang fundamental, sejumlah negara telah mengakui perlindungan data sebagai hak konstitusional atau dalam

bentuk ‘habeas data’ yakni hak seseorang untuk mendapatkan pengamanan terhadap datanya dan untuk pembenaran ketika ditemukan kesalahan terhadap datanya [9].

2.3 Keamanan Data

Keamanan data merupakan salah satu hal yang selayaknya diberikan perhatian yang lebih, khususnya bagi pemakai yang senantiasa melakukan proses *sharing* data yang bersifat rahasia, sehingga perlu dilakukan penyadian data agar beberapa pihak yang tidak memiliki kewenangan tidak akan dapat membuka informasi yang dikirim. Banyak cara telah dilakukan untuk meningkatkan keamanan data, salah satunya dengan menggunakan teknik kriptografi. Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Salah satu cara untuk mengamankan pesan dalam bentuk *text* agar tidak diketahui oleh pihak-pihak yang tidak diinginkan, dilakukan dengan cara mengenkripsi (*encrypt*) pesan (*plaintext*) tersebut menjadi karakter-karakter acak yang tidak dimengerti (*chipertext*) dan untuk memperoleh kembali pesan yang asli, dilakukan dengan cara mendeskripsi (*decrypt*) sehingga hanya bagi seseorang yang memiliki kunci (*key*) yang dapat mengembalikan pesan kebentuk semula [10].

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek penting dari suatu informasi. Secara umum keamanan komputer mencakup beberapa aspek, yaitu [11] :

a. *Privacy / Confidentiality*

Privacy lebih kearah data-data yang sifatnya rahasia, sedangkan *confidentiality* berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu.

b. *Integrity*

Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seizin pemilik informasi. Informasi yang diterima harus sesuai dan sama persis seperti saat informasi dikirimkan. Jika terdapat perbedaan antara informasi atau data yang dikirim dengan yang diterima maka aspek *integrity* tidak tercapai.

c. *Authenticity*

Aspek ini berhubungan dengan metode atau cara untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud.

d. *Availability*

Aspek ini behubungan dengan ketersediaan data dan informasi. Data dan informasi yang berbeda dalam suatu sistem komputer tersedia dan dapat dimanfaatkan oleh orang yang berhak.

e. *Access Control*

Aspek ini berhubungan dengan cara pengaturan akses kepada informasi. Hal ini biasanya berhubungan dengan klasifikasi data, mekanisme *authentication* dan juga *privacy*. *Access control* seringkali dilakukan dengan menggunakan kombinasi *user id/password* atau dengan menggunakan mekanisme lain.

2.4 Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu *kryptos* yang artinya "yang tersembunyi" dan *graphein* yang artinya "tulisan", jadi kriptografi adalah seni dan ilmu untuk menjaga keamanan data. Dan ahlinya disebut sebagai *cryptographer*. *Cryptanalst* merupakan orang yang melakukan *cryptanalysis*, yaitu seni dan ilmu untuk membuka *ciphertext* menjadi *plaintext* tanpa melalui cara yang seharusnya. Data yang dapat dibaca disebut *plaintext* dan teknik untuk membuat data tersebut menjadi tidak dapat dibaca disebut *enkripsi*. Data hasil dari enkripsi disebut *ciphertext*, dan proses untuk mengembalikan *ciphertext* menjadi *plaintext* disebut dekripsi. Cabang matematika yang mencakup kriptografi dan *cryptanalysis* disebut *cryptology* dan pelakunya disebut *cryptologist* [2].

Dalam era teknologi informasi sekarang ini, mekanisme yang sama masih digunakan tetapi tentunya implementasi sistemnya berbeda. Sebelum membahas lebih jauh mekanisme kriptografi modern, berikut ini diberikan beberapa istilah yang umum digunakan dalam pembahasan kriptografi [12] :

a. *Plaintext*

   Plaintext (*message*) merupakan pesan asli yang ingin dikirimkan dan dijaga keamanannya. Pesan ini tidak lain dari informasi tersebut.

b. *Chipertext*

   Chipertext merupakan pesan yang telah dikodekan (disandikan) sehingga siap untuk dikirimkan.

c. *Cipher*

Cipher merupakan algoritma matematis yang digunakan untuk proses penyandian *plaintext* menjadi *ciphertext*.

d. Enkripsi

Enkripsi (*encryption*) merupakan proses yang dilakukan untuk menyandikan *plaintext* sehingga menjadi *chipertext*.

e. Dekripsi

Dekripsi (*decryption*) merupakan proses yang dilakukan untuk memperoleh kembali *plaintext* dari *chipertext*.

f. Kriptosistem

Kriptosistem merupakan sistem yang dirancang untuk mengamankan suatu sistem informasi dengan memanfaatkan kriptografi.

Dalam kriptografi terdapat dua konsep utama, yaitu: enkripsi dan dekripsi. Proses kriptografi secara umum disajikan seperti gambar berikut :

Gambar 2.1 Proses Enkripsi Dekripsi

Terdapat empat tujuan yang mendasari kriptografi, yaitu [13] :

1. Kerahasiaan. Memberikan kerahasiaan pesan dan menyimpan data dengan menyembunyikan data/informasi dengan teknik enkripsi.
2. Integritas data. Memberikan jaminan bahwa dari setiap bagian dalam informasi tidak mengalami perubahan dari saat dibuat/dikirim hingga saat informasi tersebut dibuka.

3. Penyangkalan. Memberikan cara untuk membuktikan bahwa suatu dokumen datang dari seseorang mencoba menyangkal telah memiliki dokumen tersebut.
4. Autentikasi. Memberikan dua bentuk layanan, pertama adalah mengidentifikasi keaslian suatu pesan dan memberikan jaminan keotentikannya, kedua adalah untuk menguji identitas seseorang akan memasuki sebuah sistem.

2.5 *Vigenere Cipher*

Vigenère Cipher adalah salah satu algoritma kriptografi klasik yang diperkenalkan pada abad 16 atau pada tahun 1986. Algoritma kriptografi 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 [1].

Vigenere Cipher adalah metode mengenkripsi teks alfabet dengan menggunakan serangkaian *Caesar Cipher* yang berbeda berdasarkan huruf dari kata kunci dan merupakan bentuk substitusi polyalphabetic yang sederhana. Karakter yang digunakan dalam *Vigenere Cipher* yaitu A, B, C, ..., Z dan dikonversi kedalam angka 0, 1, 2, ..., 25. Proses enkripsi dilakukan dengan menulis kunci berulang kali sesuai dengan panjang karakter pada pesan. Jika pada *Caesar Cipher* kuncinya hanya satu nilai saja, maka pada *Vigenere Cipher* kunci yang digunakan berbentuk deretan huruf. Kunci yang berbetuk deretan kata tersebut akan memungkinkan setiap huruf plainteks untuk dienkripsi dengan kunci yang berbeda. Jika panjang

kunci yang digunakan lebih pendek dari panjang plainteks maka kunci akan diulang sampai panjang kunci sama dengan panjang plainteks. Algoritma ini akan meminimalkan kemungkinan dipecahkannya cipherteks jika satu huruf plainteks diketahui [14].

Model matematika dari enkripsi dan dekripsi pada algoritma *Vigenere Cipher* adalah seperti berikut [15] :

Proses Enkripsi (E) pada algoritma *Vigenere Cipher* dalam fungsi :

$$E(x) = (Pi + Ki)\ mod\ 26 \quad \text{.....(1)}$$

Keterangan : Ei = Enkripsi Karakter ke x

Pi = Karakter ke i Pada Pesan

Ki = Karakter ke i Pada Kunci

Sedangkan proses Dekripsi (D) pada algoritma *Vigenere Cipher* dalam fungsi :

$$D(x) = (Ci - Ki)\ mod\ 26 \quad \text{.....(2)}$$

Keterangan : Di = Dekripsi Karakter ke x

Ci = Karakter ke i Pada *Chipertext*

Ki = Karakter ke i Pada Kunci

Teknik subtitusi *Vigenere* dengan huruf dilakukan menggunakan tabel *Vigenere Cipher* seperti pada gambar 2.2 :

	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 2.2 Tabel *Vigenere Cipher*

Salah satu kelebihan kode *Vigenere* adalah sulitnya melakukan kapitanalisis dengan metode analisis frekuensi karena dua huruf yang sama dalam teks-kode belum tentu bisa dideskripsikan menjadi dua huruf yang sama dalam teks asli. Kelemahan utama kode *Vigenere* adalah kuncinya yang pendek dan penggunaannya yang berulang-ulang. Jika kriptanalis dapat menentukan panjang kunci saja maka teks kode dapat diperlakukan seperti rangkaian beberapa kode Kaisar [16].

2.6 *Caesar Cipher*

Dalam kriptografi terdapat beberapa algoritma, salah satunya yaitu algoritma *Caesar Cipher*. Sandi *Caesar* atau sandi geser, kode *Caesar* atau geseran *Caesar* adalah sandi substitusi dimana setiap huruf pada teks terang (plainteks) digantikan oleh huruf lain yang memiliki selisih posisi tertetu dalam alphabet. Caranya adalah dengan mengganti setiap karakter dengan karakter lain dalam susunan abjad (alphabet) [17].

Adapun langkah-langkah yang dilakukan untuk membentuk chiperteks dengan *Caesar Cipher* adalah [18] :

a. Menentukan besarnya pergeseran karakter yang digunakan dalam membentuk cipherteks ke plainteks.
b. Menukarkan karakter pada plainteks menjadi cipherteks dengan berdasarkan pada pergeseran yang telah ditentukan sebelumnya.

Model matematika dari enkripsi dan dekripsi pada algoritma *Caesar Cipher* adalah seperti berikut :

Proses Enkripsi (E) pada algoritma *Caesar Cipher* dalam fungsi :

$$C = E(P) = (P + K)\ mod\ 26 \quad \text{..... (1)}$$

Keterangan : E = Enkripsi Karakter

C = *Ciphertext*

P = *Plaintext*

K = *Key*

Sedangkan proses Dekripsi (D) pada algoritma *Caesar Cipher* dalam fungsi:

$$P = D(C) = (C - K)\ mod\ 26 \quad \text{..... (2)}$$

Keterangan : D = Dekripsi Karakter

C = *Ciphertext*

P = *Plaintext*

K = *Key*

2.7 Pasien

Pasien adalah seseorang yang menerima perawatan medis. Kata pasien dari bahasa Indonesia analog dengan kata *patient* dari bahasa Inggris. *Patient* diturunkan dari bahasa Latin yaitu patiens yang memiliki kesamaan arti dengan kata kerja pati yang artinya "menderita". Sedangkan menurut Kamus Besar Bahasa Indonesia, pasien adalah orang sakit (yang dirawat dokter), penderita (sakit). Dalam Undang-Undang Republik Indonesia Nomor 29 Tahun 2004 tentang Praktik Kedokteran menyebutkan bahwa pasien adalah setiap orang yang melakukan konsultasi masalah kesehatannya untuk memperoleh pelayanan kesehatan yang diperlukan baik secara langsung maupun tidak langsung kepada dokter. Pasien adalah penerima jasa pelayanan kesehatan di rumah sakit baik dalam keadaan sakit maupun sehat [19].

2.8 *Coronavirus Disesase* (*Covid-19*)

Coronavirus adalah virus dengan ukuran partikel 120-160 nm. Virus ini utamanya menginfeksi hewan, termasuk di antaranya adalah kelelawar dan unta. Sebelum terjadinya wabah *Covid-19*, ada 6 jenis *coronavirus* yang dapat menginfeksi manusia, yaitu *alphacoronavirus* 229E, *alphacoronavirus* NL63, *betacoronavirus* OC43, *betacoronavirus* HKU1, *Severe Acute Respiratory Illness*

*C*oronavirus (SARS-CoV), dan *Middle East Respiratory Syndrome Coronavirus* (MERS-CoV) [20].

Coronavirus merupakan virus RNA strain tunggal positif, berkapsul dan tidak bersegmen. Coronavirus tergolong ordo *Nidovirales*, keluarga *Coronaviridae*. Struktur coronavirus membentuk struktur seperti kubus dengan protein S berlokasi dipermukaan virus. Protein S atau spike protein merupakan salah satu protein antigen utama virus dan merupakan struktur utama untuk penulisan gen[21].

Berikut klasifikasi menurut buku Pedoman Pencegahan dan Pengendalian *Coronavirus Disesase* (*Covid-19*) per 27 Maret 2020 [22] :

1. Pasien dalam Pengawasan (PdP)
    a. Orang dengan Infeksi Saluran Pernapasan Akut (ISPA) yaitu demam (≥38ºC) atau riwayat demam; disertai salah satu gejala / tanda penyakit pernapasan seperti: batuk / sesak nafas / sakit tenggorokan / pilek / pneumonia ringan hingga berat dan tidak ada penyebab lain berdasarkan gambaran klinis yang meyakinkan dan pada 14 hari terakhir sebelum timbul gejala memiliki riwayat perjalanan atau tinggal di negara/wilayah yang melaporkan transmisi lokal.
    b. Orang dengan demam (≥38ºC) atau riwayat demam atau ISPA dan pada 14 hari terakhir sebelum timbul gejala memiliki riwayat kontak dengan kasus konfirmasi *Covid-19*.
    c. Orang dengan ISPA berat/pneumonia berat yang membutuhkan perawatan di rumah sakit dan tidak ada penyebab lain berdasarkan gambaran klinis yang meyakinkan.

2. Orang dalam Pemantauan (OdP)
    a. Orang yang mengalami demam (≥38ºC) ; atau gejala gangguan sistem pernapasan seperti pilek/sakit tenggorokan/batuk dan tidak ada penyebab lain berdasarkan gambaran klinis yang meyakinkan dan pada 14 hari terakhir sebelum timbul gejala memiliki riwayat perjalanan atau tinggal di negara / wilayah yang melaporkan transmisi lokal.
    b. Orang yang mengalami gejala gangguan sistem pernapasan seperti pilek / sakit tenggorokan / batuk dan pada 14 hari terakhir sebelum timbul gejala memiliki riwayat kontak dengan kasus konfirmasi *Covid-19*.
3. Orang Tanpa Gejala (OTG)

Seseorang yang tidak bergejala dan memiliki risiko tertular dari orang konfirmasi *Covid-19*. Orang tanpa gejala merupakan seseorang dengan riwayat kontak erat dengan kasus konfirmasi *Covid-19*.

2.9 Alat Bantu Perancangan Aplikasi

2.9.1 *Flowchart*

Flowchart adalah bagan-bagan yang mempunyai arus yang menggambarkan langkah-langkah penyelesaian suatu masalah. Penggambaran secara grafik dari langkah-langkah dan urut-urutan prosedur dari suatu program. *Flowchart* menolong analis dan *programmer* untuk memecahkan masalah kedalam segmen-segmen yang lebih kecil dan menolong dalam menganalisis alternatif-alternatif lain dalam pengoperasian [23].

2.9.2 *Context Diagram*

Diagram konteks adalah diagram yang terdiri dari suatu proses dan menggambarkan ruang lingkup suatu sistem. Diagram Konteks merupakan level tertinggi dari DFD yang menggambarkan seluruh input ke sistem atau *output* dari sistem [24].

2.9.3 *Data Flow Diagram* (DFD)

Data Flow Diagram (DFD) merupakan alat yang digunakan pada metodologi pengembangan sistem yang terstruktur. *Data flow diagram* berfungsi untuk menggambarkan arus data dalam sistem dengan terstruktur dan jelas. Pembuatan *Data Flow Diagram* yang sedang berjalan ini bertujuan untuk menggambarkan sistem yang berjalan sebagai jaringan kerja antar proses yang berhubungan satu sama lain, dengan aliran data yang terdapat pada sistem [25].

2.9.4 *Entity Relationship Diagram* (ERD)

ERD (*Entity Relationship Diagram*) adalah suatu rancangan atau bentuk hubungan sesuatu kegiatan yang berkaitan langsung dan mempunyai fungsi didalam proses tersebut.

Entity Relationship Diagram (ERD) adalah suatu rancangan atau bentuk hubungan suatu kegiatan di dalam sistem yang berkaitan langsung dan mempunyai fungsi di dalam proses tersebut. Berdasarkan pengertian diatas dapat disimpulkan bahwa *Entity Relationtship Diagram* (ERD) adalah merupakan suatu model untuk menjelaskan hubungan antar data dalam basis data berdasarkan objek-objek dasar data yang mempunyai hubungan antar relasi [26].

2.10 Alat Bantu Perancangan Program

2.10.1 *Website*

Pengertian *Website* adalah ”kumpulan dari halaman *web* yang sudah dipublikasikan di jaringan internet dan memiliki domain/URL (*Uniform Resource Locator*) yang dapat diakses semua pengguna internet dengan cara mengetikan alamatnya. Hal ini dimungkinkan dengan adanya teknologi *World Wide Web* (WWW) [27].

Website adalah salah satu aplikasi yang berisikan dokumen-dokumen multimedia (teks, gambar, suara, animasi, video) didalamnya yang menggunakan protokol HTTP (*hypertext transfer protocol*) dan untuk mengaksesnya mengunakan perangkat lunak yang disebut *browser*. Beberapa jenis *browser* yang populer saat ini di antaranya : *Internet Explorer* yang diperoduksi oleh *Microsoft*, *Mozila Firefox*, Opera dan Safari yang diperoduksi oleh Apple. *Browser* (perambah) adalah aplikasi yang mampu menjalankan dokumen-dokumen *web* dengan cara diterjemahkan. Prosesnya dilakukan oleh komponen yang terdapat didalam aplikasi *browser* yang biasa disebut *web engine*. Semua dokumen *web* ditampilkan dengan cara diterjemahkan [28]

Jenis kategori *website* [29] :

a) *Web* Statis

   Merupakan *website* yang mempunyai halaman yang tidak berubah.

b) *Web* Dinamis

   Merupakan *website* yang secara terstruktur diperuntukan untuk diupdate sesering mungkin.

c) *Web* Interaktif

Merupakan *website* yang berinteraksi antara penggunanya. Biasanya berupa forum diskusi maupun blog. Dimana adanya moderator sebagai pengatur alur diskusi.

2.10.2 Basis Data (*Database*)

Beberapa defenisi tentang *database* dari beberapa orang ahli, *database* adalah sebagai berikut [30] :

a. *Database* adalah sekumpulan data store yang tersimpan dalam magnetic disck, optical disck, magnetic drum atau media penyimpanan sekunder lainnya.
b. *Database* adalah sekumpulan program-program aplikasi umum yang mengeksekusi dam memproses data secara umum seperti pencarian data, peremajaan data, penambahan dan penghapusan data.

Komponen-komponen DBMS (*Database Management System*) terdiri dari, yaitu [31] :

a) *Interface*, yang didalamnya terdapat bahasa manipulasi data (*data manipulation language*).
b) Bahasa definisi data (*data definition language*) untuk skema eksternal, skema konsepsual dan skema internal.
c) Sistem kontrol basis data (*Database Control System*) yang mengakses basis data karena adanya perintah dari bahasa manipulasi data.

Database juga memiliki tujuan-tujuan lain seperti berikut ini [32] :

1. Kecepatan dan kemudahan (*speed*)

Pemanfaat database memungkinkan kita untuk dapat menyimpan data atau melakukan perubahan terhadap data atau menampilkan kembali data tersebut dengan lebih cepat dan mudah.

2. Efesiensi ruang penyimpanan (*space*)

   Dapat melakukan penekanan jumlah pengulangan data, baik dengan menerapkan sejumlah pengkodean atau dengan membuat relasi-relasi dalam bentuk file antar kelompok data yang salin berhubungan.

3. Keakuratan (*accuracy*)

   Pemanfaatan pengkodean atau pembentukan relasi antar data bersama dengan penerapan aturan atau batasan tipe data, domain data, keunikan data, dan sebagainya, yang secara ketat dapat diterapkan dalam sebuah basis data, sangat berguna untuk menekan ketidak akuratan pemasukan atau penyimpanan data.

4. Ketersediaan (*availability*)

   Pertumbuhan data baik dari sisi jumlah, maupun jenisnya sejalan dengan waktu akan semakin membutuhkan ruang penyimpanan yang besar. Padahal tidak semua data itu selalu di butuhkan, karena itu kita dapat memilih-milih adanya data utama atau master, data transaksi, data historis, hingga data kadarluasa.

5. Kelengkapan (*completeness*)

   Untuk mengakomodasikan kebutuhan kelengkapan data yang semakin berkembang, yaitu dengan menambah *record-record* data dan melakukan

perubahan struktur dalam basis data, baik dalam bentuk penambahan objek baru tabel atau dengan penambahan file-file baru pada suatu tabel.

6. Keamanan (*security*)

   Mencegah pengaksesan data oleh orang yang tidak berwenang. Kebersamaan pemakaian database dikelola oleh sistem aplikasi yang mendukung lingkungan *multiuser*.

2.10.3 MySQL (*My Structure Query Language*)

MySQL merupakan *server* yang melayani *database*. Untuk membuat dan mengolah *database*, kita dapat mempelajari pemrograman khusus yang disebut *query* (perintah) SQL. *Database* sendiri dibutuhkan jika kita ingin menginput data dari *user* menggunakan *form* HTML untuk kemudian diolah PHP agar bisa disimpan ke dalam *database* MySQL [33].

Beberapa keunggulan dari MySQL yaitu [34] :

a. Cepat, handal dan mudah dalam penggunaannya. MySQL lebih epat tiga sampai empat kali dari pada *database server* komersial yang beredar saat ini, mudah diatur dan tidak memerlukan seseorang yang ahli untuk mengatur administrasi pemasangan MySQL.
b. Didukung oleh berbagai bahasa *database server* MySQL dapat memberikan pesan *error* dalam berbagai bahasa seperti Belanda, Portugis, Spanyol, Inggris, Perancis, Jerman, dan Italia.
c. Mampu membuat tabel berukuran sangat besar. Ukuran maksimal dari setiap tabel yang dapat dibuat dengan MySQL adalah 4 GB sampai dengan ukuran file yang dapat ditangani oleh sistem operasi yang dipakai.

d. Lebih murah MySQL bersifat *open source* dan didistribusikan dengan gratis tanpa biaya untuk UNIX *platform*, OS/2 dan Windows *platform*.

2.10.4 *Hypertext Markup Language* (HTML)

HTML adalah kependekan dari (*HyperText Markup Language*), merupakan sebuah bahasa *scripting* yang berguna untuk menuliskan halaman *web*. Pada halaman *web*, HTML dijadikan sebagai bahasa *script* dasar yang berjalan bersama berbagai bahasa *scripting* pemrograman lainnya [35].

HTML adalah Bahasa pemrograman yang fleksibel di mana kita bisa meletakkan *script* dari bahasa pemrograman lain seperti JAVA, Visual Basic, C dan lain-lain. Jika HTML tersebut tidak dapat mendukung suatu perintah pemrograman tertentu. *Browser* tidak akan menampilkan kotak dialog "*Syntax Error*" jika terdapat penulisan kode yang keliru pada *script* HTML sepanjang kode-kode yang kita tuliskan merupakan kode-kode HTML tanpa penambahan kode-kode dari luar seperti java. Oleh karena itu, jika terjadi *syntax error* pada skrip HTML, efek yang paling jelas adalah HTML tersebut tak akan ditampilkan pada halaman jendela *browser* [36].

Beberapa tugas utama HTML dalam membangun website diantaranya sebagai berikut [37] :

a. Menentukan *layout website*.
b. Memformat *text* dasar seperti pengaturan paragraf, dan format font.
c. Membuat *list*.
d. Membuat tabel.
e. Menyisipkan gambar, video, dan audio.

f. Membuat *link*.

g. Membuat formulir.

2.10.5 *Hypertext Preprocessor* (PHP)

PHP adalah bahasa pemrograman yang digunakan secara luas untuk penanganan pembuatan dan pengembangan sebuah *web* dan bisa digunakan pada HTML. PHP merupakan singkatan dari " PHP : *Hypertext Preprocessor*", dan merupakan bahasa yang disertakan dalam dokumen HTML, sekaligus bekerja di sisi *server* (*server-side HTML-embedded scripting*). Artinya sintaks dan perintah yang diberikan akan sepenuhnya dijalankan di *server* tetapi disertakan pada halaman HTML biasa, sehingga *script*-nya tak tampak disisi *client* [38]

Berikut beberapa karakteristik di dalam PHP [39] :

a. *Extension* harus .php. Setiap sintak / skrip PHP harus disimpan dengan *extention*.php, misal test.php. Jika di dalam file .php tidak ada skrip PHP tidak menjadi masalah akan tetap diproses misal didalam file.php isinya hanya skrip html saja maka akan tetap diproses.

b. Sintax harus ditulis dalam dilementer atau sering disebut dengan tag PHP.

c. Sintak PHP mengikuti bahasa induknya bahasa C. Seperti pada artikel sejarah, php awalnya PHP merupakan sebuah program yang dibuat mengguna-kan bahasa C untuk menangani sebuh form untuk koneksi ke database, sehingga sintak PHP hampir sama dengan bahasa C, seperti *case sensitive* dan diakhiri tanda ; di setiap akhir dari sintak.

d. PHP dapat digunakan bersamaan dengan HTML. PHP merupakan bahasa pemograman khusus untuk web maka sangat dengan mudah digunakan bersamaan dengan html, baik tag html di dalam PHP atau sebaliknya.

e. PHP merupakan bahasa *server side scripting*. Artinya perlu penerjemah atau kompilasi dari sisi *server*. Salah satu software yang mendukung PHP adalah apache.

f. PHP *Open Source*

g. PHP Multi *Platform*. Dapat dijalankan di berbagai platfrom OS seperti linux, windows, dan mac yang membuat bahasa pemograman ini banyak diminati.

Beberapa kelebihan bahasa pemrograman PHP sebagai berikut [40]:

1. Keamanan

   Keamanan sebuah program selain sistem operasi menjadi sangat penting. PHP menyediakan 3 jenis authentikasi *user*, yaitu http authentikasi, penggunaan *cookies* dan penggunaan *session*. Selain itu ada beberapa fungsi disediakan seperti crc32, crypt, md5, base64-decode, base64- encode dan lain-lain.

2. Integritas dengan Database

   PHP mendukung integritas, kecepatan dan efisiensi akses ke database yang kebanyakan menggunakan database berjenis relational seperti MySQL, PostgreSQL, Oracle, SQLite dan lain-lain.

3. *Cross-platform*

PHP mendukung berbagai jenis sistem operasi seperti semua varian Linux, Microsoft Windows, Mac OS dan lain-lain.

4. Reliabilitas

   PHP merupakan salah satu bahasa pemrograman yang bebasis *web.* Alasan utama adalah dukungan dokumentasi yang lengkap, aman dan banyak komunitas *helpdesk* untuk membantu para pengembang web sistem yang menggunakan PHP.

5. Harga

   PHP berada dalam lisensi GPL (*GNU Public Lisence*). Hal ini berarti bahwa PHP bebas digunakan dan didistribusikan serta gratis. Saat ini juga banyak *hosting* gratis dan *unlimited* mensupport PHP.

6. Kemudahan Bermigrasi

   Tujuannya adalah memperbaiki kinerja dan menambah fitur-fitur baru. Kelebihan ini karena banyaknya dukungan terhadap PHP sehingga berdampak PHP terus menerus dikembangkan.

2.10.6 *JavaScript*

JavaScript adalah bahasa pemrograman *web* yang bersifat *Client Side Programming Language*. *Client Side Programming Language* adalah tipe bahasa pemrograman yang pemrosesannya dilakukan oleh *client*. Aplikasi *client* yang dimaksud merujuk kepada *web browser* seperti Google Chrome, Mozilla Firefox, Opera Mini dan sebagainya.

JavaScript pertama kali dikembangkan pada pertengahan dekade 90'an. Meskipun memiliki nama yang hampir serupa, *JavaScript* berbeda dengan bahasa

pemrograman Java. Untuk penulisannya, *JavaScript* dapat disisipkan di dalam dokumen HTML ataupun dijadikan dokumen tersendiri yang kemudian diasosiasikan dengan dokumen lain yang dituju. *JavaScript* mengimplementasikan fitur yang dirancang untuk mengendalikan bagaimana sebuah halaman *web* berinteraksi dengan penggunanya [41].

2.10.7 *Cascading Style Sheets* (CSS)

CSS adalah kependekan dari *Cascading Style Sheet*. CSS merupakan salah satu kode pemrograman yang bertujuan untuk menghias dan mengatur gaya tampilan/*layout* halaman *web* upaya lebih elegan dan menarik. CSS adalah sebuah teknologi internet yang direkomendasikan oleh *World Wide Web Consortium* atau W3C pada tahun 1996.

Awalnya, CSS dikembangkan di SGML pada tahun 1970 dan terus dikembangkan hingga saat ini. CSS telah mendukung banyak bahasa *markup* seperti HTML, XHTML, XML, SVG (*Scalable Vector Graphics*) dan Mozilla XUL (*XML User Interface Language*) [42].

2.10.8 XAMPP

Pengertian XAMPP adalah perangkat lunak bebas, yang mendukung banyak sistem operasi, dan merupakan kompilasi dari beberapa program. Fungsi XAMPP adalah sebagai *server* yang berdiri sendiri (*localhost*), terdiri atas program Apache HTTP *Server*, MySQL *database*, dan penerjemah bahasa yang ditulis dengan bahasa pemrograman PHP dan Perl. Nama XAMPP merupakan singkatan dari X (empat sistem operasi apapun), Apache, MySQL, PHP dan Perl. Program ini tersedia dalam GNU (*General Public License*) dan bebas, merupakan web server

yang mudah digunakan yang dapat melayani tampilan halaman web yang dinamis. XAMPP dikembangkan dari sebuah tim proyek bernama Apache *Friends*, yang terdiri dari Tim Inti (*Core Team*), Tim Pengembang (*Development Team*) & Tim Dukungan (*Support Team*) [43]

Kepanjangan dari XAMPP yaitu [32] :

X : Program ini dapat dijalankan dibanyak sistem operasi, seperti Windows, Linux, Mac OS dan juga Solaris.

A : Apache merupakan aplikasi *web server*. Tugas utama dari Apache. Adalah menghasilkan halaman web yang benar kepada *user* berdasarkan kode PHP yang dituliskan oleh pembuat web atau user.

M : MySql, merupakan aplikasi data server. Perkembangannya disebut juga Sql yang merupakan kepanjangan dari *Structured Query Language*. Sql merupakan bahasa terstruktur yang digunakan untuk mengolah database.

P : PHP, merupakan bahasa pemrograman web, dimana *user* dapat menggunakan bahasa pemrograman ini untuk membuat web yang bersifat *server-side scripting*.

P : Perl, yaitu merupakan bahasa pemrograman untuk segala keperluan, dan dikembangkan pertama kali oleh Larry Wall di mesin Unix**.**

2.11 Penelitian Terdahulu

Berikut ini merupakan penelitian terdahulu yang dapat dijadi acuan pada tugas akhir :

Tabel 2.1 Penelitian Terdahulu

No	Penulis dan Tahun	Judul	Metode	Hasil

1.	Erwin Gunadhi dan Agung Sudrajat (2016)	Pengamanan Data Rekam Medis Pasien Menggunakan Kriptografi *Vigenere Cipher*	*Vigenere Cipher*	1. Kriptografi *Vigenere Cipher* ini dapat diterapkan untuk pengamanan aplikasi rekam medis pasien. 2. Data yang ada pada rekam medis pasien menjadi lebih aman dari serangan para kriptanalis dengan algoritma *Vigenere Cipher* yang dikustomisasi.
2.	Abduh Riski, Ahmad Kamsyakawuni dan M. Ziaul Arif (2018)	Implementasi *Vigenere Cipher* Pada Pengamanan Data Medis	*Vigenere Cipher*	Hasil penelitian ini, metode *Vigenere Cipher* yang diusulkan dapat digunakan untuk pengamanan data medis berupa citra. Berdasarkan pada Tabel 4, metode *Vigenere Cipher* yang diusulkan lebih baik dari metode *Vigenere Cipher* lainnya dalam pengamanan citra. Selanjutnya metode *Vigenere Cipher* yang diusulkan dapat digunakan

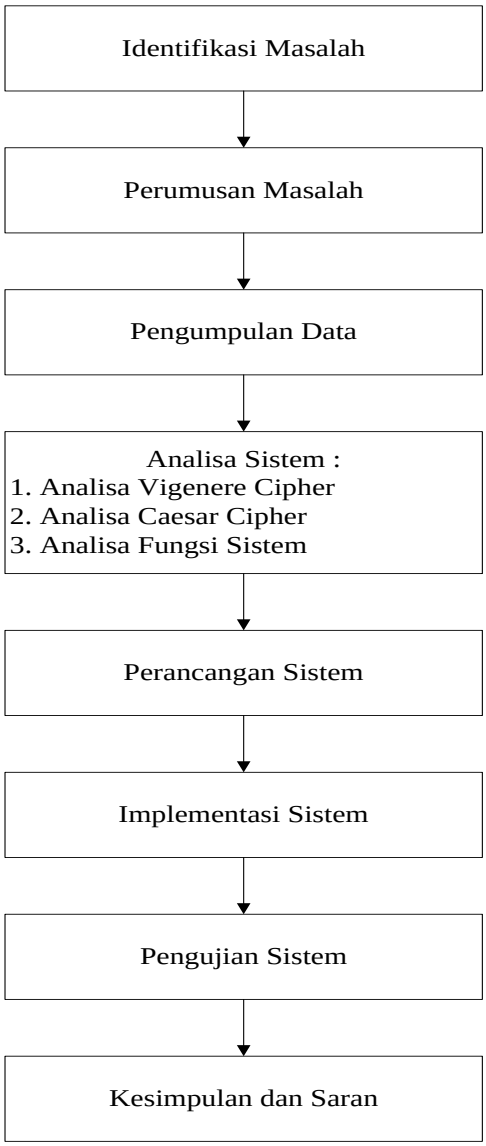
				oleh siapa saja untuk pengaman data medis berupa citra. Pada penelitian selanjutnya akan dilakukan peningkatan keamanan data yang dienkripsi dengan menggunakan metode lain dalam mengekstraksi ciri citra kunci sedemikian hingga menghasilkan nilai UACI yang lebih baik dan kunci menjadi non-simetris.
3.	Agustin Siburian dan Andy Paul Harianja (2017)	Perancangan Aplikasi Pengamanan Basis Data Menggunakan Algoritma *Caesar Cipher*	*Caesar Cipher*	1. Sistem yang dibangun mampu meningkatkan keamanan basis data dan memberikan kemudahan bagi pengguna dengan menggunakan Algoritma *Caesar Cipher*.
4.	Husni Angriani dan Yeni Saharaeni (2019)	Implementasi Algoritma *Caesar Cipher* Pada Keamanan	*Caesar Cipher*	Penerapan algoritma *Caesar Cipher* pada sistem *e-voting* pemilihan ketua UKM pada STMIK KHARISMA

		Data Sistem *E-Voting* Pemilihan Ketua Organisasi Kemahasiswaan		Makassar, cukup aman dalam menjaga kerahasiaan data.
5.	Muhammad Nurtanzis Sutoyo dan Murhaban (2016)	Kombinasi Algoritma Kriptografi *Caesar Cipher* dan *Caesar Cipher* Untuk Keamanan Data	*Caesar Cipher* dan *Vigenere Cipher*	1. Kombinasi algoritma kriptografi *Caesar Cipher* dan *Vigenere Cipher* dapat digunakan untuk mengirim pesan rahasia. 2. Dengan mengkombinasikan algoritma *Caesar Cipher* dan *Vigenere Cipher* sulit untuk dapat dipecahkan dengan cara *brute force attack*. Sandi akan dapat dipecahkan jika kunci telah ditemukan (diketahui).

BAB 3

METODOLOGI PENELITIAN

Penelitian ini dilakukan dengan melaksanakan tahapan demi tahapan yang berhubungan. Tahapan-tahapan tersebut dijabarkan dalam metode penelitian. Metode penelitian diuraikan kedalam bentuk skema yang jelas, teratur, dan sistematis. Berikut tahapan-tahapan penelitian dapat dilihat pada gambar 3.1:



Gambar 3.1 Tahapan Metodologi Penelitian

Penjelasan dari tahapan – tahapan penelitian pada gambar 3.1 dapat dilihat pada penjelasan di bawah ini :

3.1 Identifikasi Masalah

Mengidentifikasi masalah pada Dinas Kesehatan Kabupaten Rokan Hulu. Dapat diidentifikasikan perlu adanya sebuah keamanan data pasien *Covid-19* untuk melindungi data pasien *Covid-19* agar tidak dapat di sadap oleh pihak yang tidak berhak.

3.2 Perumusan Masalah

Berdasarkan permasalahan yang telah diidentifikasi, maka dapat dirumuskan bahwa bagaimana merancang dan membangun suatu membuat sistem informasi *Covid-19* Kabupaten Rokan Hulu dengan menerapkan kriptografi metode *Vigenere Cipher* dan *Caesar Cipher* untuk perlindungan data pasien *Covid-19* pada database.

3.3 Pengumpulan Data

Pada tahap ini dilakukan pengumpulan data yang berhubungan dengan penelitian dan pembuatan sistem, yaitu dengan :

1. **Observasi (Pengamatan)**

Pengamatan secara langsung di Dinas Kesehatan Kabupaten Rokan Hulu untuk mengetahui proses pengolahan data pasien *Covid-19* yang telah diambil sebelumnya.

2. Wawancara (*Interview*)

Melakukan wawancara secara langsung staff Dinas Kesehatan Kabupaten Rokan Hulu untuk mengetahui pengolahan data pasien *Covid-19* yang sedang berjalan dan diterapkan pada saat ini.

3. Studi Kepustakaan

Studi kepustakaan dilakukan dengan cara mempelajari buku-buku, jurnal-jurnal dan artikel-artikel di internet yang berhubungan dengan permasalahan yang dibahas.

3.4 Analisa Sistem

Tahapan selanjutnya adalah melakukan analisa metode sistem dari penelitian Tugas Akhir ini. Adapun tahapan analisa dalam penelitian ini adalah sebagai berikut :

3.4.1 Analisa Metode *Vigenere Cipher*

Tahap ini adalah proses dimana langkah-langkah pengolahan data dan di enkripsi dekripsi dengan menggunakan kriptografi metode *Vigenere Cipher*.

3.4.2 Analisa Metode *Caesar Cipher*

Setelah melakukan tahapan analisa dengan kriptografi metode *Vigenere Cipher*, lalu tahapan berikutnya dienkripsi kembali dengan menggunakan kriptografi metode *Caesar Cipher*.

3.4.3 Analisa Fungsi Sistem

Setelah melakukan tahapan analisa terhadap kriptografi metode *Vigenere Cipher* dan *Caesar Cipher* maka selanjutnya adalah analisa fungsional sistem yang akan dibangun. Adapun tahapan – tahapan analisa fungsional yaitu dalam

pembuatan *flowchart*, *context diagram*, *data flow diagram* (DFD), *entity relationship diagram* (ERD), dan perancangan *user interface*.

3.5 Perancangan Sistem

Setelah tahapan analisa selesai dilakukan, maka tahapan selanjutnya adalah perancangan sistem. Tahapan perancangan sistem terdiri dari :

1. Perancangan struktur menu yang akan digunakan pada sistem yang akan dibangun.
2. Tahapan rancangan database beserta atribut yang dibutuhkan.
3. Tahapan perancangan *user interface* atau antar muka pengguna terhadap sistem yang akan digunakan.

3.6 Implementasi Sistem

Implementasi sistem merupakan suatu konversi dari desain sistem yang telah dirancang kedalam sebuah program komputer dengan berbasis *web* dengan menggunakan bahasa pemrograman PHP dan database MySQL.

3.7 Pengujian Sistem

Pengujian (*testing*) yaitu uji coba yang dilakukan terhadap sistem yang dibangun apakah telah sesuai dengan yang diharapkan atau tidak. Pengujian yang dilakukan terdiri dari:

1. Pengujian *blackbox*, digunakan untuk menguji tingkat kemampuan *user interface* terhadap sistem yang dibangun.
2. Pengujian *User Acceptance Test* (UAT).

3.8 Kesimpulan dan Saran

Tahapan terakhir adalah menarik kesimpulan dari hasil penelitian yang didapatkan dalam sistem informasi *Covid-19* Kabupaten Rokan Hulu dengan menerapkan kriptografi metode *Vigenere Cipher* dan *Caesar Cipher* untuk perlindungan data pasien *Covid-19* pada database di Dinas Kesehatan Kabupaten Rokan Hulu. Pada tahapan ini juga berisikan saran penelitian bagi pembaca untuk melakukan pengembangan terhadap penelitian ini kedepannya.