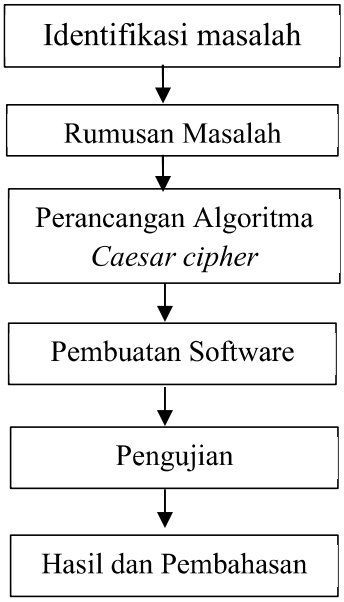
BAB III

METODE PENELITIAN

3.1 Desain Penelitian

Berikut tahapan-tahapan desain penelitian untuk merancang aplikasi penyandian pesan.



Gambar 3. 1 Desain Penelitian

Peracangan sistem kriptografi ini dilakukan dengan beberapa tahap yang saling berhubungan antara satu dengan yang lain. Pada pembuatan program pengiriman pesan tersandi yang berbasis desktop, pengirim pesan akan menentukan dengan siapa pesan akan dikirim dengan cara memasukkan nomor tujuan, menginput plain teks yang menjadi cipherteks. Pada proses pengiriman, user akan melalukan log in terlebih dahulu dengan melakukan scan qrcode ke aplikasi desktop yang telah di instal.

1. Identifikasi masalah

   Dalam identifikasi masalah sudah dijelaskan dari atas yaitu memahami cara pengamanan isi pesan sehingga tidak ada perubahan selama proses pengiriman. Dalam komunikasi yang dilakukan banyak pihak diluar sana yang sengaja mencari tahu isi pesan yang akan disampaikan. Selama proses pengiriman pesan banyak kejahatan *cyber* yang bisa terjadi seperti mengubah isi pesan dan mencuri informasi yang ada pada pesan.

2. Rumusan masalah

   Pada bagian ini, penulis akan menggambarkan proses mengamankan isi pesan dengan cara menggunakan teknik kriptografi algoritma caesar cipher. Dengan menggunakan caesar cipher isi pesan tidak mudah dimengerti oleh orang yang bukan penerima sebenarnya. Sebelum pesan dikirimkan teks asli dari pesan akan disandikan terlebih dahulu, mengubah bentuk teks asli menjadi pesan yang tidak bisa dimengerti maknanya.

3. Perancagan algoritma caesar cipher

   Pada perancangan algoritma caesar cipher, penulis akan menjabarkan cara-cara yang harus dilakukan. Tujuan caesar cipher mengubah atau menyamarkan isi pesan dengan cara subtitusi tiap karakter dari teks asli menjadi teks tersandi.

4. Pembuatan software

   Aplikasi penyandian pesan dirancang dan didesain dengan sederhana sehingga mudah dimengerti oleh pengguna. Aplikasi ini berbasis desktop yang dirancang

menggunakan bahasa pemrograman bvb.net. Tampilan utama dari aplikasi penyandian pesan berisikan *log in, log out*, enkripsi (kirim) dan deskripsi.

5. Pengujian

   Pengujian yang dilakukan hanya berfokus pada fungsional dari aplikasi, hasil *input* dan *output.* Pengujian dilakukan dengan metode *blackbox testing* fungsional.

6. Hasil dan pembahasan

   Hasil dan pembahasan merupakan hasil akhir dari pembuatan aplikasi, tampilan dan cara kerja serta menampilkan hasil-hasil dari pengujian yang dilakukan.

3.2 Teknik Pengumpulan Data

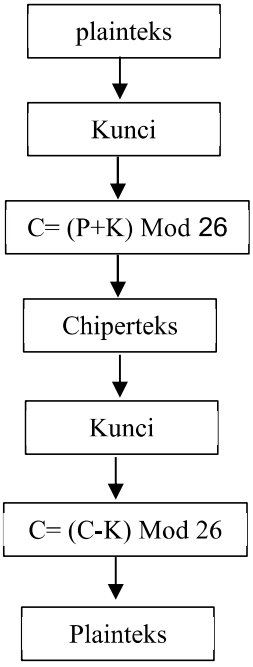
Dalam penelitian ini penulis melakukan pengumpulan data untuk menambah referensi dengan metode studi pustaka. Dalam studi pustaka mencari yang bahan pendukung seperti teori para ahli baik dari buku maupun dari jurnal yang sesuai dengan pembahasan atau topik yang diteliti.

3.3 Pemodelan Fungsional

Dalam perancangan sistem penulis akan menggambarkan tahapan-tahapan yang akan dilakukan dalam merancang desain dan juga intruksi yang digunakan dalam melaksanakan penelitian ini.

3.3.1 Flowchart caesar cipher

Flowchart caesar cipher merupakan diagaram yang menampilkan langklah-langkah atau instruksi untuk melakukan penyandian pesan dengan cara mengganti atau mengubah posisi setiap karakter pada plainteks menjadi cipherteks.



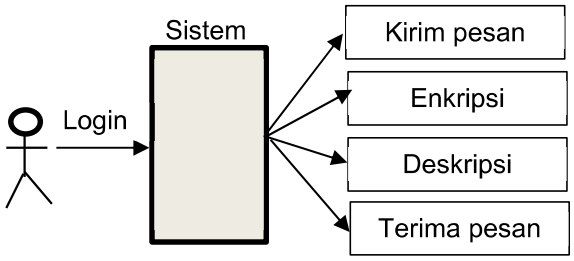
Gambar 3. 2 *Flowchart Caesar Cipher*

Pada *flowchart* ini menggmbarkan proses penyandian pesan dengan algoritma caesar cipher. Algoritma caesar cipher yaitu urutan logis yang sistematis untuk mengamankan pesan dengan teknik subtitusi untuk mengganti setiap urutan huruf yang ada diplainteks dengan huruf-huruf yanga ada diabjad sesuai dengan nilai angka yang dipilih. Urutan instruksi yang dilakukan yaitu dengan menyiapkan teks asli yang akan dikirimkan kepada penerima pesan. Setelah itu menyiapkan kunci yang digunakan dalam pergeseran karakter. Besaran pergeseran karakter tergantung

nilai kunci yang digunakan. Cara penyandiannya urutan plainteks yaitu dengan menambahkan posisi karakter pada plainteks dengan kunci, setelah dapat jumlahnya akan digantikan karakter plainteks sesuai dengan urutan yang didapat dari penjumlahan sehingga karakter plainteks akan menjadi cipherteks. Kegiatan pergeseran karakter akan dilakukan sampai semua isi pesan berubah bentukanya. Pada proses deskripsi pesan tersandi untuk mengubah kebentuk aslinya harus menggunakan kunci yang sama ketika seorang pengguna melakukan enkripsi. Caranya mengurangi setiap karakter pada cipherteks dengan nilai kunci yang ada dan hasil dari pengurangan akan dijadikan patokan untuk melakukan pergeseran sehingga menghasilkan teks asli. Proses ini dilakukan pada setiap karakter cipherteks sampai membentuk plainteks.

3.3.2 Diagram Use Case

Diagram uses case pada aplikasi penyadian pesan ini merupakan urutan interaksi seorang pengguna dengan sistem yang telah dirancang.



Gambar 3. 3 Diagram *Usecase*

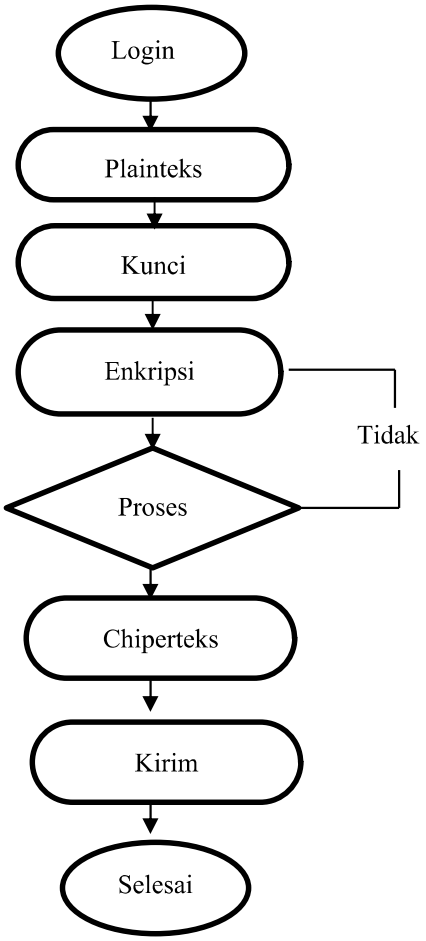
Gambar diatas menjelaskan uraian tentang tahapan urutan yang bisa dilakukan oleh pengguna yaitu memiliki dengan melakukan login terlebih dahulu, dengan bisa masuk ke sistem seorang user bisa mengirimkan pesan tersandi. Melakukan login

bertujuan untuk memperkenalkan diri sebagai pengguna, sehingga teman yang berkomunikasi lainnya mengenal dengan siapa dia mengirim dan menerima pesan. Kegiatan lainnya yang bisa dilakukan adalah melakukan pengiriman pesan, melakukan enkripsi, menerima pesan, melakukan deskripsi.

3.3.3 Diagram Activity

Pada diagram *aktivity* penulis membagi dua kegiatan yang akan dilakukan yaitu proses kirim pesan dan terima pesan.

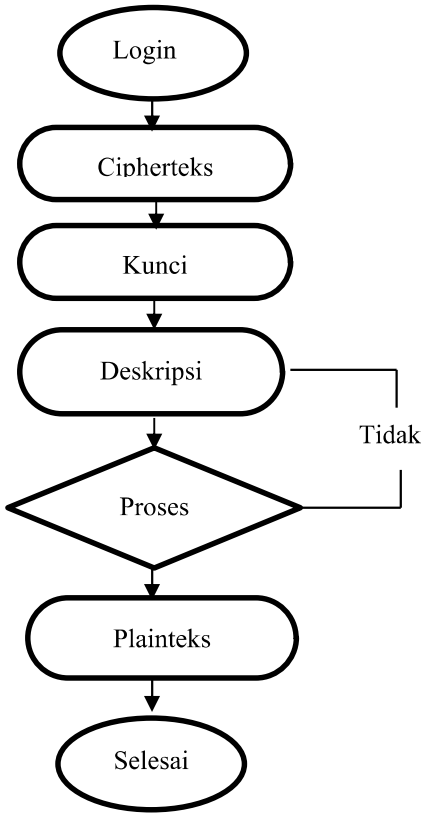
a. Enkripsi Pesan



Gambar 3. 4 *Diagaram aktivity Enkripsi* pesan

Gambar diatas menjelaskan proses pada saat kirim pesan, pengirim akan melakukan log in terlebih dahulu keaplikasi penyandian pesan. Menentukan siapa penerima dengan cara memasukkan nomor whatsapp, membuat plainteks dan menyiapkan kunci. Proses berikutnya yaitu mengubah plainteks menjadi cipherteks. Seteleh mendapatkan cipherteks pengirim melakukan pengiriman pesan kepenerima. Isi pesan yang akan dikirimkan berupa cipherteks hasil enkripsi dengan kunci yang disiapkan pengirim.

b. Deskripsi pesan



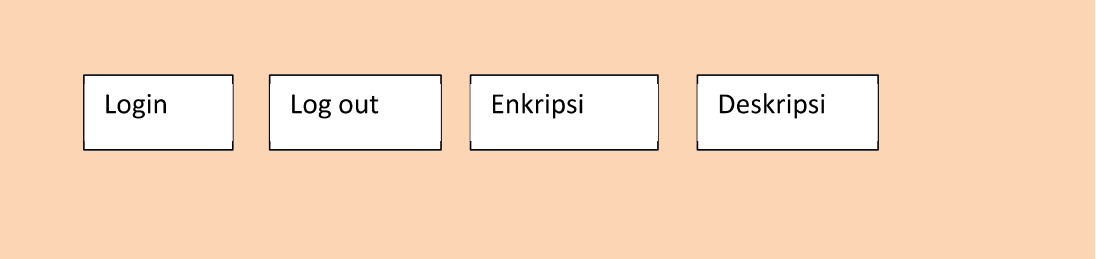
Gambar 3. 5 *Diagram Activity* Enkripsi Pesan

Pada proses penerima pesan, penerima atau seorang pengguna harus melakukan login keaplikasi terlebih dahulu. Setelah menerima pesan, isi pesan harus dideskripsi terlebih dahulu untuk mengetahui arti dari pesan. Kegiatan deskripsi harus menggunakan kunci yang sama sehingga bisa mengembalikkan

3.4 Perancangan Interface

Perancangan *form* antarmuka pada halaman utama terbagi menjadi 4 bagian utama:

3.4.1 Halaman Utama



Gambar 3. 6 Halaman Utama

Gambar diatas yaitu halaman utama dari aplikasi penyandian pesan. Pada tampilan halaman utama ada beberapa pilihan menu antara lain log in, log out, enkripsi dan deskripsi. Pada menu login untuk bisa masuk ke sistem, log out untuk mengakhiri sesi atau keluar dari aplikasi, enkripsi untuk menyandikan pesandan deskripsi untuk mengembalikan kembali makna dari pesan.

3.4.2 Menu *Login*

Gambar 3. 7 *Menu Login*

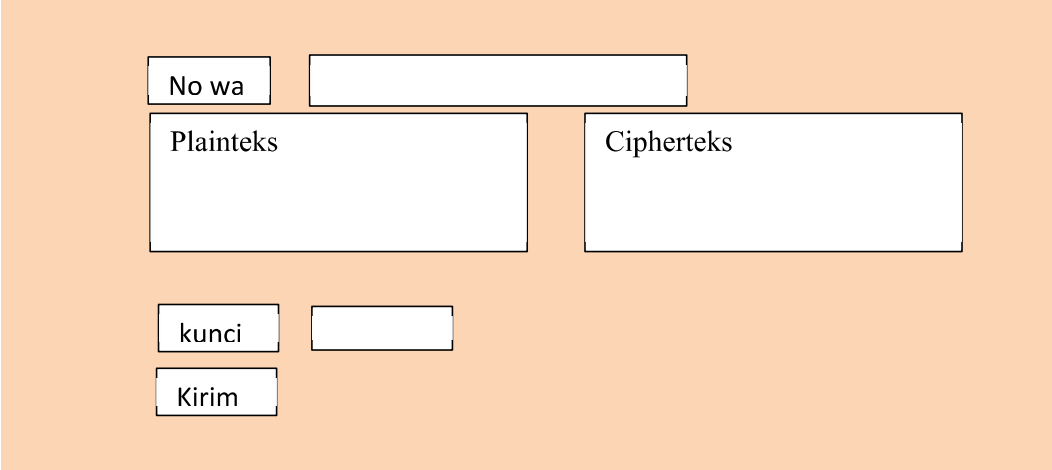
Gambar diatas merupakan desain halaman menu login, seorang pengguna akan diarahkan untuk melakukan scan *qrcode*. Hal ini bertujuan untuk memperkenalkan diri pada sistem sehingga bisa melakukan pengiriman dan penerimaan pesan.

3.4.3 Menu log out

Gambar 3. 8 *Menu Logout*

Desain antar muka menu log out. Untuk mengakhiri sebuah sesi dalam aplikasi, seorang pengguna diarahkan untuk memilih menu log out.

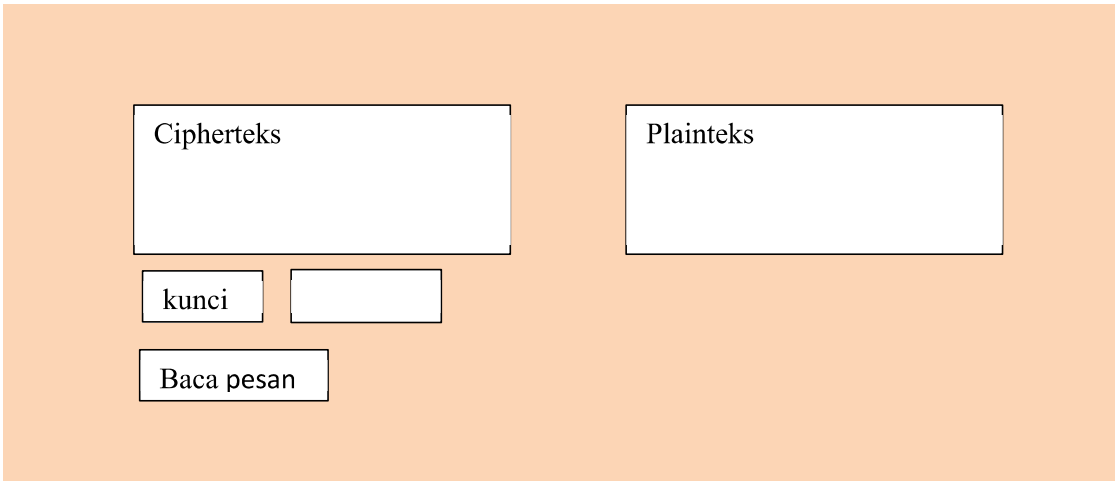
3.4.4 Menu Enkripsi



Gambar 3. 9 Menu Enkripsi

Desain menu enkripsi menampilkan beberapa form, pada menu enkripsi terdapat beberapa tampilan yang bisa dilihat oleh seorang pengguna yaitu, kolom No wa merupakan nomor yang menjadi tujuan dalam pengiriman pesan. Tempat menuliskan plainteks, tempat hasil enkripsi, kunci dan tombol kirim.

3.4.5 Menu Deskripsi



Gambar 3. 10 Menu Deskripsi

Pada menu deskripsi kegiatan pengubahan pesan dari pesan tersandi menjadi teks asli dilakukan. Dengan cara, pesan yang telah dikirm yang masih berbentuk cipherteks akan dikopi dan ditempel dikolom cipherteks pada menu deskripsi.

3.5 Perancangan algoritma *caesar cipher*

Pada perancangan algoritma *caesar cipher* menggunakan teknik penyandian dengan cara substitusi atau pergeseran posisi plainteks berdasarkan kata kunci yang gunakan. Kata kunci yang digunakan merupakan urutan alfabet dalam plainteks. Untuk melakukan pengamanan pesan seorang user akan menggunakan kata kunci yang sama untuk melakukan eskripsi dan deskripsi dengan kunci yang sama. Langkah-langkah yang harus dilakukan untuk membuat teks tersandi dengan teknik *caesar cipher*:

1. Menentukan kata kunci yang digunakan dalam pergeseran karakter
2. Menukarkan karakter pada pesan asli menjadi pesan tersandi yang telah di tentukan sebelumnya.

Sebagai contoh, melakukan pergeseran dengan kata kunci =3, untuk plain teks ABC akan melakukan pergeseran karakter berdasarkan kata kunci yang telah ditentukan sehingga ABC menjadi DEF, yang mana huruf A pada plainteks menjadi huruf D, B menjadi huruf E dan C menjadi huruf F.

Rumus enkripsi caesar cipher

C = E (P) = (P+K) Mod 26

C = Cipher teks

E = Enkripsi

P = Plainteks

K = Kunci

Mod 26 = Total jumlah huruf pada abjad

Rumus deskripsi caesar cipher

P = D (P) = (C-K) Mod 26

P = Plainteks

D = Deskripsi

C = Cipherteks

Mod 26 = Total jumlah huruf dalam karakter

Secara detail berikut tabel pergeseran plain teks menjadi cipher teks dengan kata kunci= 3,

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Tabel 3. 1 Plainteks

Menjadi

D	E	F	G	H	I	J	K	L	M	N	O	P
1	2	3	4	5	6	7	8	9	10	11	12	13
Q	R	S	T	U	V	W	X	Y	Z	A	B	C
14	15	16	17	18	19	20	21	22	23	24	25	26

Tabel 3. 2 Cipherteks

Contoh lain dalam melakukan penyandian pesan menggunakan algoritma *caesar cipher*;

Plainteks : informatika

Kunci : 3

Cipherteks : lqirupdwlnd

Baris plainteks

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

Tabel 3. 3 Baris plainteks

Baris Cipherteks

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

Tabel 3. 4 Baris Cipherteks

Cara merancang algoritma caesar cipher dengan menggunakan formulasi matematika. Pertama-tama harus mengkodekan setiap karakter dalam alfabet dengan sebuah angka. Pengkodean dilakukan sesuai dengan urutan setiap huruf dari 1-26. Angka 1 mewakili huruf a dan selanjutnya sampai 26. Pada pengkodean ini tidak mempermasalahkan tentang huruf besar dan huruf kecil semuanya dianggap sama. Perhitungan caesar cipher untuk enkripsi dikenal dengan persamaan C = E(p) = (P+3)

Mod 26 sedangkan pada deskripsi P = D(p) = (C- 3) Mod 26. Huruf C kepanjangan dari cipherteks, D kepanjangan dari deskripsi, E kepanjangan dari Enkripsi, P kepanjangan dari plainteks, angka 3 merupakan kunci dan mod 26 yang merupakan jumlah keseluruhan huruf dalam alfabet. Berikut cara pengerjaan plainteks menjadi cipher teks menggunakan persamaan matematika.

Plainteks : informatika

Kunci : 3

C = E(p) = (P+3) Mod 26

P1 = i = 9 ⟶ c1 = E (9) = (9+3) Mod 26 = 12 = l

P2 = n = 9 ⟶ c2 = E (14) = (14+3) Mod 26 = 17 = q

P3 = f = 9 ⟶ c3 = E (6) = (6+3) Mod 26 = 9 = i

P4 = o = 9 ⟶ c4 = E (15) = (15+3) Mod 26 = 18 = r

P5 = r = 9 ⟶ c5 = E (18) = (18+3) Mod 26 = 21 = u

P6 = m = 9 ⟶ c6 = E (13) = (13+3) Mod 26 = 16 = p

P7 = a = 9 ⟶ c7 = E (1) = (0+3) Mod 26 = 4 = c

P8 = t = 9 ⟶ c8 = E (20) = (20+3) Mod 26 = 23 = w

P9 = i = 9 ⟶ c9 = E (9) = (9+3) Mod 26 = 12 = l

P10 = k = 9⟶ c10 = E (9) = (11+3) Mod 26 = 14 = n

P11 = a = 9 ⟶ c11 = E (1) = (0+3) Mod 26 = 4 = d

Dalam perhitungan diatas maka menghasilkan cipherteks yaitu “lqirupdwlnd”

Untuk mengembalikan isi pesan sehingga bisa dimengerti maka dilakukan kegiatan deskripsi. Deskripsi melakukan pergeseran tiap karakter pada cipherteks dengan cara mengurangi urutan karakter pada pesan tersandi dengan angka kunci yang sesuai saat enkripsi. Persamaan matematika dalam melakukan kegiatan deskripsi yaitu dengan menggunakan rumus P = D(p) = (C- 3) Mod 26. Pada contoh deskripsi ini menggunakan pesan hasil enkripsi dari atas dengan kunci yang sama yaitu:

Cipherteks : lqirupdwlnd

Kunci : 3

C1 = l = 12 ⟶ P1 = D (12-3) mod 26 = 9 = i

C2 = q = 17 ⟶ P1 = D (17-3) mod 26 = 14 = n

C3 = i = 9 ⟶P1 = D (9-3) mod 26 = 6 = f

C4 = r = 18 ⟶ P1 = D (18-3) mod 26 = 15 = o

C5 = u = 21 ⟶ P1 = D (21-3) mod 26 = 28 = r

C6 = p = 16 ⟶ P1 = D (16-3) mod 26 = 13 = m

C7 = d = 4 ⟶P1 = D (4-3) mod 26 = 1 = a

C8 = w = 23 ⟶ P1 = D (23-3) mod 26 = 20 = t

C9 = l = 12 ⟶ P1 = D (12-3) mod 26 = 9 = i

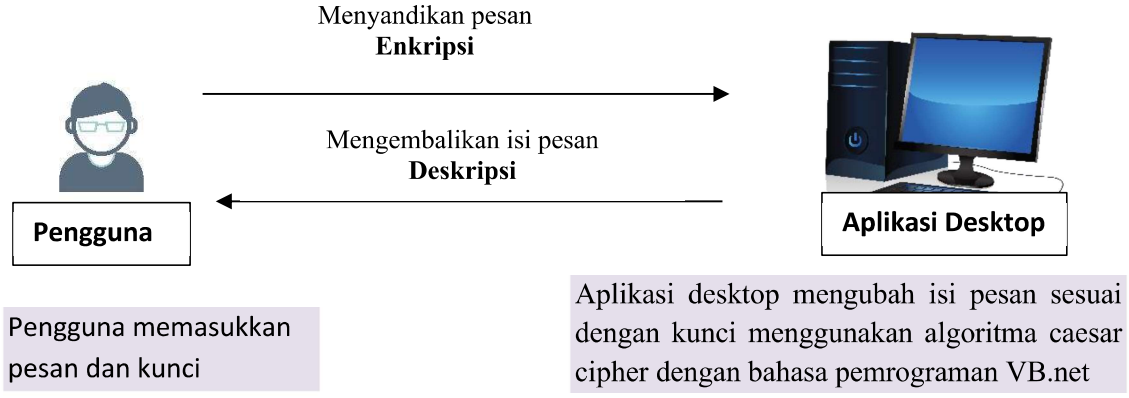
C10 = n = 14 ⟶ P1 = D (14-3) mod 26 = 11 = k

C11 = d = 4 ⟶ P1 = D (4-3) mod 26 = 1 = a

Dari operasi deskripsi diatas menghasil plainteks yaitu “informatika”.

3.6 Implementasi

Pada bagian implementasi menjadi langkah pertama untuk pembangunan sistem yang akan digunakan berdasarkan pada pendekatan dan solusi yang telah dianalisa. Pada tahap implementasi peneliti mengembangkan desain program dengan menggunakan bahasa pemgrograman vb .net 2015 untuk merancang tampilan aplikasi. Bahasa pemrograman vb. net digunakan karena mudah dimengerti dalam mengimplementasikan penyandian pesan menggunakan algoritma caesar cipher. Sedangakan untuk perangkat keras yang digunakan memiliki spesifikasi dengan processor core i5, windows 10 dan ram 8. Tampilan yang dirancang menggrunakan versi desktop untuk dapat digunakan di komputer.



Gambar 3. 11 Arsitektur Aplikasi

Gambar diatas merupakan arsitektur aplikasi penyandian pesan. Pengguna memasukkan pesan dan kunci untuk melakukan pengamanan isi pesan. Hasil enkripsi dan deskripsi akan ditampilkan pada ditampilan aplikasi penyandian pesan berbasis desktop. Teknik pengubahan isi pesan menggunakan algoritma *caesar cipher.*

3.7 Pengujian

Pada bagian pengujian peneliti melakukan pengujian terhadap sistem yang telah dibangun dengan indikator-indikator tertentu. Hal ini dilakukan untuk membuktikan bahwa sistem yang telah dibangun dapat memenuhi kebutuhan dalam penyandian pesan. Fokus pada pengujian yang akan dilakukan yaitu pengujian sistem dan pengujian algoritma caesar cipher. Pengujian sistem mencakup pada pengujian fungsional sebuah sistem sedangkan pengujian algoritma caesar cipher mencakup pada keakuratan penyandian pesan baik dihitung secara manual berdasarkan rumus matematikanya maupun dengan aplikasi yang telah dibuat.

3.8 Jadwal Penelitian

Jadwal penelitian dilakukan pada tahun 2022.

No	Kegiatan	Maret	April	Mei	Juni	Juli
1	Penginputan Judul					
2	Mengumpulkan Data					
3	Merancang Desain					
4	Implementasi					
5	Pengujian Aplikasi					
6	Membuat Laporan					

Tabel 3. 5 Jadwal Penelitian

Berdasarkan pada tabel diatas jadwal penelitian dihitung menggunakan bulan. Dimulai dari menginput judul, mengumpulkan data, merancang desain, mengimplementasikan aplikasi yang ada. Untuk memastikan aplikasi berjalan sesuai dengan tujuan dilakukan pengujian dan langkah terakhir membuat laporan.