

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dengan berkembangnya teknologi informasi saat ini, media komunikasi mengalami kemajuan yang sangat pesat, mengakses suatu data atau informasi melalui bermacam-macam media salah satunya melalui media website dalam internet. Seseorang dengan mudah menyimpan, mengunduh, dan mengakses suatu data atau informasi. Keamanan dalam menyimpan data atau informasi sangat penting dan tidak bisa diabaikan. Salah satu pengaruh negative perkembangan teknologi adalah pencurian data. Pencurian data ini tentunya merugikan bagi pemilik data, untuk mencegah kejahatan tersebut maka dibutuhkan pengamanan dalam penyimpanan data yang dianggap penting untuk mencegah kejahatan teknologi informasi.[1]

Semua perusahaan didirikan dengan tujuan menghasilkan keuntungan dalam jangka panjang. Namun, perusahaan cenderung mengabaikan pentingnya keamanan data untuk mencapai tujuan mereka, itu sebabnya banyak perusahaan tidak terlalu memperhatikan keamanan data. Perusahaan harus memperhatikan apa yang dianggap penting oleh penggunanya, karena memperhatikan keamanan data adalah faktor penting dan sangat besar bagi kelangsungan hidup suatu perusahaan dalam persaingan. [2]

Saat ini masih banyak pelaku bisnis atau pengusaha yang belum menerapkan sistem informasi untuk bisnisnya, akibatnya seringkali terjadi tindak kecurangan yang dapat merugikan perusahaan maupun pelanggan seperti manipulasi harga, nota kosong, *lapping* dan *mark up* harga. Hal tersebut terjadi karena proses bisnis seperti transaksi, pembukuan, dan nota masih dilakukan secara manual. Sehingga memungkinkan terjadinya kesalahan penulisan dalam transaksi yang dapat mengakibatkan kerugian.

[3]

Hal tersebut selaras dengan yang terjadi pada Toko MMC CCTV, MMC CCTV adalah sebuah toko yang menjual berbagai perangkat CCTV yang beralamat di Jl. Raya susukan ciawigebang, Susukan, Cipicung, Kuningan, Jawa Barat. Berdasarkan hasil wawancara kepada pemilik Toko, Bapak Arief Budiman yang mengungkapkan bahwa pada bulan Juni 2023 terjadi keluhan dari *customer* yang disebabkan oleh harga pemasangan dan harga barang yang terlalu mahal berdasarkan brosur di Toko MMC CCTV, setelah diusut ternyata terjadi manipulasi nota dan *mark up* harga yang dilakukan oleh karyawan, sehingga merugikan *customer* karena harus membayar mahal dan juga merugikan perusahaan karena merusak citra perusahaan.

Salah satu solusi agar dapat mencegah hal tersebut terjadi yaitu dengan membangun sebuah sistem untuk mengelola transaksi. Dengan memanfaatkan enkripsi dan dekripsi data nota transaksi sehingga dapat meningkatkan keamanan dan menjaga kepercayaan *customer*.

Enkripsi dan deskripsi adalah teknik dalam keamanan komputer yang digunakan untuk melindungi kerahasiaan dan integritas data. Enkripsi adalah proses mengubah data asli menjadi bentuk yang tidak terbaca atau sulit dimengerti oleh pihak yang tidak berwenang. Hal ini dilakukan dengan menerapkan algoritma enkripsi tertentu menggunakan kunci enkrip. Deskripsi (dekripsi) adalah proses mengembalikan data yang telah dienkripsi ke bentuk aslinya agar dapat dibaca dan dimengerti kembali. Hal ini dilakukan menggunakan kunci dekripsi yang sesuai. [1]

Enkripsi juga dapat digunakan untuk memastikan integritas data. Dengan menggunakan tanda tangan digital, enkripsi dapat membantu memastikan bahwa data tidak diubah atau dimanipulasi selama proses pengiriman atau penyimpanan. Dengan menerapkan enkripsi dan deskripsi yang tepat, informasi sensitif dan data pribadi dapat terlindungi dari ancaman keamanan dan risiko penyalahgunaan. [1]

Algoritma *Caesar Cipher* merupakan 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 tertentu dalam alphabet. Caranya adalah dengan mengganti setiap karakter dengan karakter lain dalam susunan abjad (alphabet). Misalnya tiap huruf disubstitusikan dengan huruf yang ketiga berikutnya dari susunan abjad. Misalnya A akan digantikan oleh D dan B akan digantikan oleh E, dan seterusnya. Dalam hal ini kuncinya adalah jumlah pergeseran huruf (yaitu $k = 3$). [1]

Kode QR adalah suatu jenis kode matriks atau kode batang dua dimensi yang dikembangkan oleh Denso Wave, sebuah divisi Denso Corporation yang merupakan sebuah perusahaan Jepang dan dipublikasikan pada tahun 1994. Agar dapat membaca *QR Code* diperlukan sebuah pembaca atau pemindai berupa software yaitu *QR Code Reader* atau *QR Code Scanner* yang harus diinstal pada perangkat telepon mobile. QR merupakan singkatan dari quick response atau respons cepat, yang sesuai dengan tujuannya adalah untuk menyampaikan informasi dengan cepat dan mendapatkan respons yang cepat pula. Berbeda dengan kode batang, yang hanya menyimpan informasi secara horizontal, kode QR mampu menyimpan informasi secara horizontal dan vertical. [1]

Berdasarkan latar belakang diatas, maka peneliti tertarik melakukan penelitian dengan judul “Rancang Bangun Aplikasi Pengelolaan Transaksi di Toko MMC CCTV Menggunakan Algoritma *Caesar Cipher* Untuk Enkripsi dan Deskripsi Kode Transaksi Berbasis *QR Code*”

1.2 Identifikasi Masalah

Dari latar belakang yang telah diuraikan, maka dapat diidentifikasi permasalahan pada penelitian, yaitu sebagai berikut.

1. Terjadinya manipulasi nota dan *mark up* harga, dimana harga yang tertera pada nota tidak sama dengan harga yang tertera pada brosur baik itu harga barang maupun pemasangan. Sehingga dapat merugikan *customer* karena harus membayar lebih besar dari harga di brosur.

2. Adanya keluhan dari *customer* terkait *mark up* harga sehingga dapat merusak citra perusahaan.

1.3 Rumusan Masalah

Berdasarkan latar belakang dan identifikasi masalah di atas maka dapat disusun rumusan masalah dari penelitian ini yaitu sebagai berikut:

1. Bagaimana merancang dan membangun aplikasi untuk mengelola transaksi di toko MMC CCTV?
2. Bagaimana mengimplementasikan algoritma Caesar Cipher pada QR-Code untuk proses enkripsi dan deskripsi pada aplikasi pengelola transaksi?

1.4 Batasan Masalah

Agar penelitian ini lebih terarah, maka diperlukan batasan masalah pada penelitian ini. Berikut ini adalah batasan masalah dari penelitian yang akan dilakukan:

1. Penelitian dilakukan di Toko MMC CCTV yaitu Perusahaan CCTV yang bertempat di desa Susukan kecamatan Cipicung kabupaten Kuningan dan Bapak Arief Budiman sebagai pemilik.
2. Aplikasi yang dibuat memiliki fungsi melakukan enkripsi dan deskripsi data pada Kode Transaksi.
3. Algoritma yang digunakan untuk mengenkripsi dan mendeskripsikan adalah algoritma Caesar Cipher.

4. Data yang akan diamankan adalah nomor nota transaksi yang berisi semua informasi mengenai transaksi, baik itu data *customer* maupun produk yang dibeli.
5. Informasi yang akan dimunculkan adalah informasi pembeli dan informasi transaksi (produk).
6. QR-Code dibuat berdasarkan nota transaksi.
7. QR-Code akan ditempatkan pada bagian bawah nota transaksi.
8. Metodologi pengembangan sistem yang digunakan adalah metode Rational Unified Process (RUP).
9. User dapat mengakses aplikasi melalui website.
10. Hak akses masing-masing aktor yaitu:
 - a. Konsumen dapat melihat katalog produk dan juga bisa melakukan transaksi pembelian maupun pemasangan perangkat CCTV, serta melakukan scan pada kode QR yang terdapat di nota transaksi .
 - b. Manager dapat mengelola data pesanan, produk, paket, dan transaksi menggunakan aplikasi.
11. Aplikasi yang dibuat berbasis client server dengan menggunakan Bahasa pemrograman PHP dan *DBMS* menggunakan MySQL.
12. Tools Pemrograman PHP yang digunakan adalah visual studio code untuk pembuatan aplikasi Scan QR-Code dengan memanfaatkan teknologi PWA.

1.5 Tujuan Penelitian

Adapun tujuan penelitian dari permasalahan yang dipaparkan adalah sebagai berikut :

1. Merancang dan Membangun Aplikasi Pengelola Transaksi di Toko MMC CCTV yang efisien untuk mempermudah pengelolaan transaksi di toko.
2. Mengimplementasikan algoritma Caesar Cipher pada QR-Code sebagai metode enkripsi.

1.6 Manfaat Penelitian

Manfaat Teoritis

1. Bagi Peneliti

Mengimplementasikan ilmu pembuatan aplikasi menggunakan metode RUP, algoritma caesar cipher yang telah diperoleh selama menempuh pendidikan di Fakultas Ilmu Komputer Universitas Kuningan dengan membuat penelitian secara ilmiah dan sistematis.

Manfaat Praktis

1. Bagi Pihak Toko MMC CCTV

Dengan adanya aplikasi ini dapat membantu meminimalisir tingkat manipulasi nota dan peningkatan harga dari MMC CCTV dan meningkatkan kepercayaan customer.

2. Customer

Dengan adanya aplikasi ini dapat membantu customer dalam melakukan pengecekan nota transaksi.

1.7 Pertanyaan Penelitian

Berdasarkan latar belakang diatas, maka terdapat pertanyaan penelitian sebagai berikut :

1. Apakah aplikasi yang dibangun (pengelola transaksi di Toko MMC CCTV) dapat mempermudah pengelolaan transaksi di toko secara efisien?
2. Apakah algoritma Caesar Cipher dapat diimplementasikan untuk proses enkripsi dan deskripsi pada aplikasi pengelola transaksi di MMC CCTV?

1.8 Hipotesis Penelitian

Dengan adanya aplikasi pengelolaan transaksi dengan mengimplementasikan algoritma Caesar Cipher sebagai proses enkripsi dan deskripsi diharapkan dapat mempermudah pengelolaan transaksi di Toko MMC CCTV.

1.9 Metodologi Penelitian

Untuk memperoleh data penelitian, harus ditentukan metode dan teknik penelitian. Karena itu, pada bagian ini dijelaskan metode yang akan digunakan dalam penelitian yang sesuai dengan karakteristik penelitian

1.9.1 Metode Pengumpulan Data

1. Studi Pustaka

Studi pustaka dilakukan untuk menyusun laporan penelitian dengan melakukan pengumpulan data dan berupa

pengumpulan informasi yang relevan dan di peroleh dari Literatur RUP, Website, Algoritma Caesar Chiper dan literatur lainnya yang berkaitan dengan penelitian.

2. Observasi

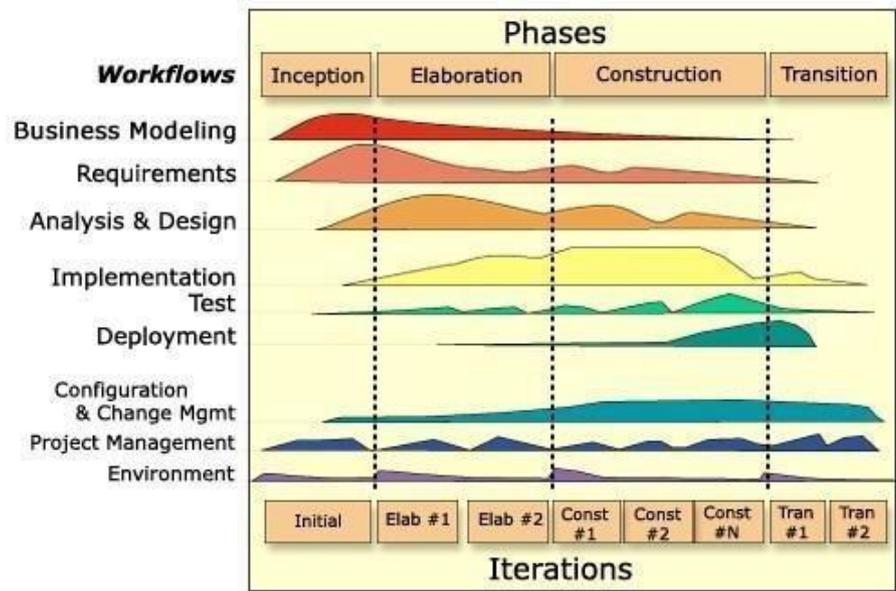
Pada metode observasi ini peneliti melakukan pengamatan langsung ke tempat Toko MMC CCTV . Hasil observasi digunakan sebagai bahan untuk penyusunan penelitian ini.

3. Wawancara

Pada metode wawancara ini, peneliti melakukan wawancara kepada Sodara Arief Budiman selaku pemilik toko MMC CCTV.

1.9.2 Metode Pengembangan Sistem

Metode pengembangan yang digunakan dalam penelitian ini adalah menggunakan metode RUP (Rational Unified Process). RUP adalah pendekatan pengembangan perangkat lunak yang dilakukan berulang-ulang (iterative). Fokus pada arsitektur (architecture-centric), lebih diarahkan berdasarkan penggunaan proses rekayasa perangkat lunak dengan pendefinisian yang baik (well defined) dan penstrukturan yang baik (well structured). RUP adalah sebuah produk proses perangkat lunak yang dikembangkan oleh Rational Software Corporation yang diakuisisi oleh IBM dibulan Februari 2003. Berikut gambar Arsitektur dari Metode Rational Unified Process.[4]



Gambar 1. 1 Metode RUP [4]

Berikut ini penjelasan pada setiap fase RUP :

1. *Inception* (pemulaan)

Pada tahapan ini, melakukan studi pustaka dengan mencari jurnal-jurnal mengenai enkripsi dan dekripsi dengan algoritma *Caesar Chiper*, membua website pengelolaan transaksi, serta *QR Code* yang dapat membantu dalam proses pembuatan aplikasi. Serta melakukan observasi langsung di lokasi penelitian dan melakukan wawancara dengan pemilik yaiu Bapak Arief Budiman MMC CCTV untuk mendapatkan data-data yang dibutuhkan.

2. *Elaboration* (perencanaan)

Tahap ini melakukan desain secara lengkap berdasarkan hasil

analisis pada tahap inception. Aktivitas yang dilakukan pada tahap ini antara lain mencakup pembuatan desain arsitektur subsistem (architecture pattern), desain komponen sistem, desain format data (protokol komunikasi), desain database, desain user interface, desain sistem menggunakan UML dan pembuatan dokumentasi.

3. *Construction* (kontruksi)

Tahap ini melakukan implementasi hasil dan melakukan pengujian hasil implementasi. Implementasi dengan menggunakan bahasa pemrograman PHP, dan algoritma yang digunakan untuk enkripsi dan dekripsi kode transaksi adalah algoritma *Caesar Chiper*.

4. *Transition* (transisi)

Tahap ini menyerahkan sistem aplikasi kepada user (roll-out), yang umumnya mencakup pelaksanaan kegunaan aplikasi kepada pengguna. Pada instalasi sistem agar dapat dimengerti oleh user, pemeliharaan, pengujian dan pengimplementasikan sistem. Pada tahap ini peneliti melakukan pengujian *white box*, *black box*, dan UAT.

1.9.3 Metode Penyelesaian Masalah

Dalam kriptografi, sandi Caesar, atau sandi geser, kode Caesar atau Geseran Caesar adalah salah satu teknik enkripsi paling terkenal. Sandi ini termasuk sandi substitusi dimana setiap huruf

pada teks terang (plaintext) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet. Ini adalah algoritma kriptografi yang mula-mula digunakan oleh kaisar Romawi, Julius Caesar (sehingga dinamakan juga caesar chiper), untuk menyandikan pesan yang ia kirim kepada para gubernurnya. Caranya adalah dengan mengganti (menyulih atau mensubstitusi) setiap karakter dengan karakter lain dalam susunan abjad (alfabet). Misalnya, tiap huruf disubstitusi dengan huruf ketiga berikutnya dari susunan abjad. Dalam hal ini kuncinya adalah jumlah pergeseran huruf (yaitu $k = 3$). Dengan mengkodekan setiap huruf abjad dengan integer sebagai berikut: $A = 0, B = 1, \dots, Z = 25$, maka secara matematis caesar chiper menyandikan plaintexts p_i menjadi c_i dengan aturan.[1]

Tabel 1. 1 Tabel Deret Alfabet

A	B	C	D	E	F
0	1	2	3	4	5
G	H	I	J	K	L
6	7	8	9	10	11
M	N	O	P	Q	R
12	13	14	15	16	17
S	T	U	V	W	X
18	19	20	21	22	23
Y	Z	0	1	2	3
24	25	26	27	28	29
4	5	6	7	8	9
30	31	32	33	34	35

Pada Tabel 1 merupakan table susunan alfabet untuk aturan perubahan karakter menjadi angka. Berikut ini tahapan enkripsi dan dekripsi Caesar Cipher :

1. Enkripsi Algoritma *Caesar Cipher*

Enkripsi data menggunakan rumus sebagai berikut :

$$c_i = E(p_i) = (p_i + k) \bmod 36$$

Keterangan :

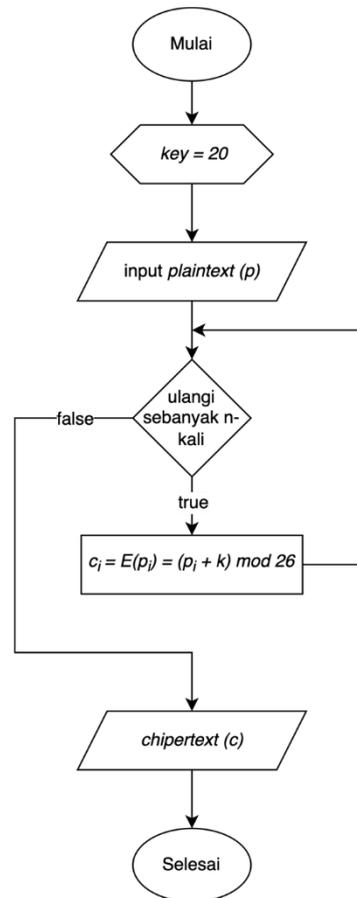
c_i : *chipertext* index ke-i

p_i : *plaintext* index ke-i

$E(p_i)$: hasil enkripsi index ke-i

k : *key*

Pada gambar dibawah ini dapat dilihat flowchart dari proses enkripsi algoritma Caesar Cipher : [5]



Gambar 1. 2 Flowchart Proses Enkripsi Algoritma Caesar

Chiper [5]

Berikut merupakan tahapan proses Enkripsi pada Algoritma Caesar Cipher: [5]

1. Memulai dengan Start.
2. Deklarasi *key*
3. Menginputkan *plaintext* atau text asli yang akan di enkripsi.
4. Di proses dengan persamaan rumus *chipertext* =

$(plaintext + key) \bmod 36$ yang dilakukan secara berulang kali sesuai jumlah karakter plaintext.

5. Setelah itu akan di dapat *chipertext*.
6. Finish.

Contoh Tahap Enkripsi

- a. Mulai
- b. Masukkan *plaintext* "CCTVMMC001"
- c. Konversi ke dalam deret huruf

<i>Plaintext</i>		
p[1]	C	2
p[2]	C	2
p[3]	T	19
p[4]	V	21
p[5]	M	12
p[6]	M	12
p[7]	C	2
p[8]	0	26

<i>Plaintext</i>		
p[9]	0	26
p[10]	1	27

- d. Hitung dengan $c_i = E(p_i) = (p_i + k) \bmod 36$ dan ulangi sampai batas ke-n

c_i	<i>Caesar Cipher</i>		Hasil
	$(p_i + k) \bmod 36$	=	
c[1]	$(2+20) \bmod 36$	22	W
c[2]	$(2+20) \bmod 36$	22	W
c[3]	$(19+20) \bmod 36$	13	N
c[4]	$(21+20) \bmod 36$	15	P
c[5]	$(12+20) \bmod 36$	6	G
c[6]	$(12+20) \bmod 36$	6	G

c[7]	$(2+20) \bmod 36$	22	W
c[8]	$(26+20) \bmod 36$	10	K
c[9]	$(26+20) \bmod 36$	10	K
c[10]	$(27+20) \bmod 36$	11	L

e. Didapatkan *chipertext* “WWDF66WKKL”

f. Selesai

2. Dekripsi Algoritma *Caesar Cipher*

Dekripsi data menggunakan rumus sebagai berikut :

$$p_i = D(c_i) = (c_i - k) \bmod 36$$

Keterangan :

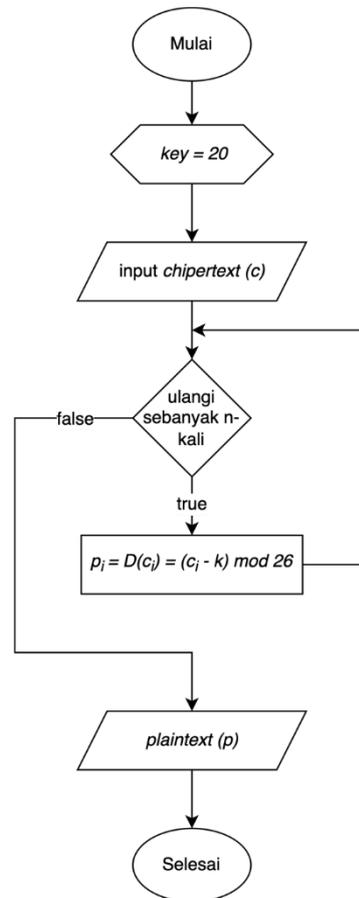
c_i : *chipertext* index ke-i

p_i : *plaintext* index ke-i

$D(p_i)$: hasil dekripsi index ke-i

k : *key*

Pada gambar dibawah ini dapat dilihat flowchart dari proses dekripsi algoritma *Caesar Cipher* :



**Gambar 1. 3 Flowchart Proses Dekripsi Algoritma Caesar
Chiper[5]**

Berikut merupakan tahapan proses Dekripsi pada Algoritma Caesar Cipher:

1. Memulai dengan Start.
2. Deklarasi *key*
3. Menginputkan *chipertext* yang akan di dekripsi.
4. Di proses dengan persamaan rumus *plaintext* = $(chipertext - key) \bmod 36$ yang dilakukan secara

berulang kali sesuai jumlah karakter *chipertext*.

5. Setelah itu akan di dapat *plaintext*.
6. Finish.

Contoh Tahap Dekripsi

- a. Mulai
- b. Masukkan *chipertext* “WWDF66WKKL”
- c. Konversi ke dalam deret huruf

<i>Chipertext</i>		
p[1]	W	22
p[2]	W	22
p[3]	D	3
p[4]	F	5
p[5]	6	32
p[6]	6	32
p[7]	W	22
p[8]	K	10

<i>Chipertext</i>		
p[9]	K	10
p[10]	L	11

- d. Hitung dengan $p_i = D(p_i) = (c_i - k) \bmod 36$ dan ulangi sampai batas ke-n

p_i	<i>Caesar Cipher</i>		Hasil
	$(c_i - k) \bmod 36$	=	
p[1]	$(22-20) \bmod 36$	2	C
p[2]	$(22-20) \bmod 36$	2	C
p[3]	$(3-20) \bmod 36$	19	T
p[4]	$(5-20) \bmod 36$	21	V
p[5]	$(32-20) \bmod 36$	12	M
p[6]	$(32-20) \bmod 36$	12	M

p[7]	$(22-20) \bmod 36$	2	C
p[8]	$(10-20) \bmod 36$	26	0
p[9]	$(10-20) \bmod 36$	26	0
p[10]	$(11-20) \bmod 36$	27	1

e. Didapatkan *plaintext* “CCTVMMC001”

7. Selesai

1.10 Jadwal Penelitian

Jadwal penelitian ini dibuat untuk menguraikan rencana pelaksanaan penelitian yang akan dilakukan dalam rangka mencapai tujuan utama penelitian. Penelitian ini merupakan bagian integral dari upaya peneliti untuk menjelajahi dan menganalisis dengan tujuan mempermudah pengelolaan transaksi. Semoga jadwal penelitian ini akan membantu peneliti untuk menjalankan penelitian dengan efisien dan mencapai hasil yang bermakna. Berikut jadwal penelitian yang diusulkan :

	Januari				Februari				Maret				April				Mei			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
<i>Inception</i>	■	■	■	■																
<i>Elaboration</i>				■	■	■	■	■												
<i>Construction</i>									■	■	■	■	■	■	■	■	■			
<i>Transition</i>																	■	■	■	■

1.11 Sistematika Penelitian

Dalam Penyusunan skripsi ini, sistematika penulisan dibagi menjadi beberapa bab sebagai berikut :

BAB I : PENDAHULUAN

Bab ini dibahas tentang latar belakang masalah, identifikasi masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, pertanyaan penelitian, metodologi penelitian, dan sistematika penulisan

BAB II : LANDASAN TEORETIS

Bagian ini menjelaskan teori-teori yang melandasi penulisan skripsi.

BAB III : ANALISIS DAN PERANCANGAN

Bab ini membahas perancangan sistem terhadap perangkat lunak yang akan dibangun, rancangan input dan output dari aplikasi.

BAB IV : PENGUJIAN DAN IMPLEMENTASI

Bab ini membahas tentang spesifikasi dari aplikasi yang dibuat, tampilan input dan output serta membahas beberapa bagian yang penting dari listing program yang berhubungan dengan materi Skripsi.

BAB V : SIMPULAN DAN SARAN

Bab ini terdiri dari kesimpulan dan saran yakni kesimpulan terhadap aplikasi yang sudah dibuat secara keseluruhan dan dikemukakan saran-saran (rekomendasi) untuk perbaikan serta pengembangan program