



**SIMULASI PENGAMANAN INFORMASI PADA PESAN  
RAHASIA DENGAN *CIPHER SUBSTITUSI* SATU ARAH**

Disusun dan Diajukan untuk Memenuhi Persyaratan Ujian Akhir Memperoleh  
Gelar Sarjana Komputer pada Fakultas Sains dan Teknologi  
Universitas Pembangunan Panca Budi  
Medan

**SKRIPSI**

**OLEH:**

**NAMA : ISKANDAR AJI SAPUTRA**  
**NPM : 1614370011**  
**PROGRAM STUDI : SISTEM KOMPUTER**

**FAKULTAS SAINS DAN TEKNOLOGI  
UNIVERSITAS PEMBANGUNAN PANCA BUDI  
MEDAN  
2020**

**LEMBAR PENGESAHAN**

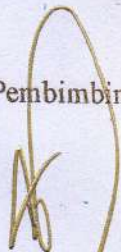
**SIMULASI PENGAMANAN INFORMASI PADA PESAN RAHASIA  
DENGAN CIPHER SUBSTITUSI SATU ARAH**

**Disusun Oleh:**

**NAMA : ISKANDAR AJI SAPUTRA**  
**NPM : 1614370011**  
**PROGRAM STUDI : SISTEM KOMPUTER**

**Skripsi Telah Disetujui oleh Dosen Pembimbing Skripsi  
Pada Tanggal :**

Dosen Pembimbing I



A. P. U. Siahaan, S.Kom., M.Kom.

Dosen Pembimbing II



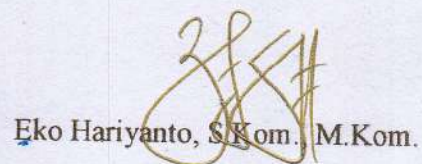
Dedi Purwanto, S.Kom., M.Kom.

**Mengetahui:**

Dekan Fakultas Sains dan Teknologi

  
  
Hamdani, S.T., M.T.

Ketua Program Studi Sistem Komputer

  
Eko Hariyanto, S.Kom., M.Kom.

## SURAT PERNYATAAN

Saya yang bertandatangan di bawah ini :

Nama : Iskandar Aji Saputra  
NPM : 1614370011  
Prodi : Sistem Komputer  
Judul Skripsi : Simulasi Pengamanan Informasi Pada Pesan Rahasia Dengan Cipher Substitusi Satu Arah

Dengan ini menyatakan bahwa :

1. Tugas Akhir/Skripsi saya bukan hasil plagiat.
2. Saya tidak akan menuntut perbaikan nilai indeks prestasi kumulatif (IPK) setelah ujian Sidang Meja Hijau
3. Skripsi saya dapat dipublikasikan oleh lembaga, dan saya tidak akan menuntut akibat publikasi tersebut.

Demikian pernyataan ini saya perbuat dengan sebenar-benarnya terimakasih.

Medan, 20 Desember 2020

Yang membuat pernyataan



ISKANDAR AJI SAPUTRA

1614370011

**SURAT PERNYATAAN**

Saya Yang Bertanda Tangan Dibawah Ini :

Nama : ISKANDAR AJI SAPUTRA  
N. P. M : 1614370011  
Tempat/Tgl. Lahir : P.BERANDAN / 24 April 1997  
Alamat : JL. SUKAMULIA GG. BINA  
No. HP : 081973418177  
Nama Orang Tua : SUTARMAN/PARIYEM  
Fakultas : SAINS & TEKNOLOGI  
Program Studi : Sistem Komputer  
Judul : Simulasi Pengamanan Informasi Pada Pesan Rahasia Dengan Cipher Substitusi Satu Arah

Bersama dengan surat ini menyatakan dengan sebenar - benarnya bahwa data yang tertera diatas adalah sudah benar sesuai dengan ijazah pada pendidikan terakhir yang saya jalani. Maka dengan ini saya tidak akan melakukan penuntutan kepada UNPAB. Apabila ada kesalahan data pada ijazah saya.

Demikianlah surat pernyataan ini saya buat dengan sebenar - benarnya, tanpa ada paksaan dari pihak manapun dan dibuat dalam keadaan sadar. Jika terjadi kesalahan, Maka saya bersedia bertanggung jawab atas kelalaian saya.

Medan, 09 Januari 2021



at Pernyataan

**ISKANDAR AJI SAPUTRA**  
1614370011



**UNIVERSITAS PEMBANGUNAN PANCA BUDI**  
**FAKULTAS SAINS & TEKNOLOGI**

Jl. Jend. Gatot Subroto Km 4,5 Medan Fax. 061-8458077 PO.BOX : 1099 MEDAN

PROGRAM STUDI TEKNIK ELEKTRO	(TERAKREDITASI)
PROGRAM STUDI ARSITEKTUR	(TERAKREDITASI)
PROGRAM STUDI SISTEM KOMPUTER	(TERAKREDITASI)
PROGRAM STUDI TEKNIK KOMPUTER	(TERAKREDITASI)
PROGRAM STUDI AGROTEKNOLOGI	(TERAKREDITASI)
PROGRAM STUDI PETERNAKAN	(TERAKREDITASI)

**PERMOHONAN JUDUL TESIS / SKRIPSI / TUGAS AKHIR\***

Saya yang bertanda tangan di bawah ini :

Nama Lengkap	: ISKANDAR AJI SAPUTRA
Tempat/Tgl. Lahir	: P. BERANDAN / 24 April 1997
Nomor Pokok Mahasiswa	: 1614370011
Program Studi	: Sistem Komputer
Konsentrasi	: Keamanan Jaringan Komputer
Jumlah Kredit yang telah dicapai	: 148 SKS, IPK 3,43
Nomor Hp	: 081973418177

Dengan ini mengajukan judul sesuai bidang ilmu sebagai berikut :

No.	Judul
1.	Simulasi Pengamanan Informasi Pada Pesan Rahasia Dengan Cipher Substitusi Satu Arah

Catatan : Diisi Oleh Dosen Jika Ada Perubahan Judul

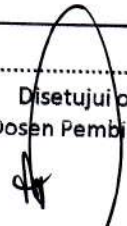
\*Coret Yang Tidak Perlu


  
**Prambono, SE., MM**


Medan, 28 Juli 2020  
 Pemohon,

  
 (Iskandar Aji Saputra)

Tanggal : .....  
 Disahkan oleh :  
 Dekan  
  
 (Haridani, ST., MT)

Tanggal : .....  
 Disetujui oleh :  
 Dosen Pembimbing I :  
  
 (Andysah Putera Utama Siahdan, S.Kom., M.Kom)

Tanggal : .....  
 Disetujui oleh :  
 Ka. Prodi Sistem Komputer  
  
 (Eko Hariyanto, S.Kom., M.Kom)


Tanggal : .....  
 Disetujui oleh :  
 Dosen Pembimbing II :  
  
 (Dedi Purwanto, S.Kom., M.Kom)

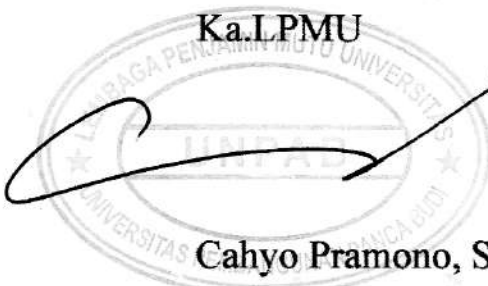
## **SURAT KETERANGAN PLAGIAT CHECKER**

Dengan ini saya Ka.LPMU UNPAB menerangkan bahwa surat ini adalah bukti pengesahan dari LPMU sebagai pengesah proses plagiat checker Tugas Akhir/ Skripsi/Tesis selama masa pandemi *Covid-19* sesuai dengan edaran rektor Nomor : 7594/13/R/2020 Tentang Pemberitahuan Perpanjangan PBM Online.

Demikian disampaikan.

NB: Segala penyalahgunaan/pelanggaran atas surat ini akan di proses sesuai ketentuan yang berlaku UNPAB.

Ka.LPMU  
  
Cahyo Pramono, SE.,MM



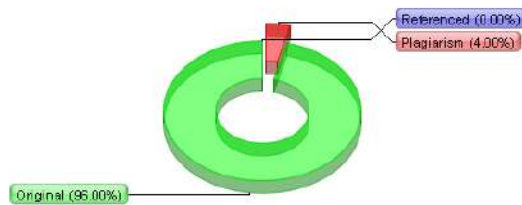
### Plagiarism Detector v. 1731 - Originality Report 29/07/2020 08.48.36

Analyzed document: ISKANDAR AJI SAPUTRA\_1614370011\_SISTEM KOMPUTER.docx Licensed to: Universitas Pembangunan Panca Budi

Comparison Preset: Rewrite. Detected language: Indonesian



Relation chart:



Distribution graph:



YAYASAN PROF. DR. H. KADIRUN YAHYA

# UNIVERSITAS PEMBANGUNAN PANCA BUDI

JL. Jend. Gatot Subroto KM 4,5 PO. BOX 1099 Telp. 061-30106057 Fax. (061) 4514808  
MEDAN - INDONESIA

Website : [www.pancabudi.ac.id](http://www.pancabudi.ac.id) - Email : [admin@pancabudi.ac.id](mailto:admin@pancabudi.ac.id)

## LEMBAR BUKTI BIMBINGAN SKRIPSI

Nama Mahasiswa : ISKANDAR AJI SAPUTRA  
NPM : 1614370011  
Program Studi : Sistem Komputer  
Jenjang Pendidikan : Strata Satu  
Dosen Pembimbing : Andysah Putera Utama Siahaan, S.Kom.,M.Kom  
Judul Skripsi : Simulasi Pengamanan Informasi Pada Pesan Rahasia Dengan Cipher Substitusi Satu Arah

Tanggal	Pembahasan Materi	Status	Keterangan
04 Mei 2020	ACC BAB 1 dan 2, Lanjut Bab 3	Disetujui	
29 Mei 2020	ACC Seminar Hasil	Disetujui	
02 Juli 2020	ACC Sidang	Disetujui	
23 Juli 2020	ACC Sidang Meja Hijau	Disetujui	
19 Agustus 2020	ACC Jilid	Disetujui	

Medan, 09 Januari 2021  
Dosen Pembimbing,



Andysah Putera Utama Siahaan, S.Kom.,M.Kom





YAYASAN PROF. DR. H. KADIRUN YAHYA

# UNIVERSITAS PEMBANGUNAN PANCA BUDI

JL. Jend. Gatot Subroto KM 4,5 PO. BOX 1099 Telp. 061-30106057 Fax. (061) 4514808

MEDAN - INDONESIA

Website : [www.pancabudi.ac.id](http://www.pancabudi.ac.id) - Email : [admin@pancabudi.ac.id](mailto:admin@pancabudi.ac.id)

## LEMBAR BUKTI BIMBINGAN SKRIPSI

Nama Mahasiswa : ISKANDAR AJI SAPUTRA  
NPM : 1614370011  
Program Studi : Sistem Komputer  
Jenjang Pendidikan : Strata Satu  
Dosen Pembimbing : Dedi Purwanto, S.Kom., M.Kom  
Judul Skripsi : Simulasi Pengamanan Informasi Pada Pesan Rahasia Dengan Cipher Substitusi Satu Arah

Tanggal	Pembahasan Materi	Status	Keterangan
07 Mei 2020	Acc Bab I dan Bab II lanjut Bab III	Disetujui	
20 Mei 2020	Acc BAB III lanjut BAB IV	Disetujui	
01 Juni 2020	Acc BAB IV	Disetujui	
01 Juni 2020	Acc BAB V	Disetujui	
01 Juni 2020	Acc seminar hasil	Disetujui	
28 Juli 2020	Acc Jilid	Disetujui	
28 Juli 2020	Acc Sidang Meja Hijau	Disetujui	

Medan, 09 Januari 2021  
Dosen Pembimbing,



Dedi Purwanto, S.Kom., M.Kom



**KARTU BEBAS PRAKTIKUM**  
**Nomor. 1307/BL/LAKO/2020**

Yang bertanda tangan dibawah ini Ka. Laboratorium Komputer dengan ini menerangkan bahwa :

Nama : ISKANDAR AJI SAPUTRA  
N.P.M. : 1614370011  
Tingkat/Semester : Akhir  
Fakultas : SAINS & TEKNOLOGI  
Jurusan/Prodi : Sistem Komputer

Benar dan telah menyelesaikan urusan administrasi di Laboratorium Komputer Universitas Pembangunan Panca Budi Medan.

Medan, 09 Januari 2021  
Ka. Laboratorium

Melva Sari Panjaitan, S. Kom., M.Kom.





**YAYASAN PROF. DR. H. KADIRUN YAHYA**  
**PERPUSTAKAAN UNIVERSITAS PEMBANGUNAN PANCA BUDI**  
Jl. Jend. Gatot Subroto KM. 4,5 Medan Sunggal, Kota Medan Kode Pos 20122

**SURAT BEBAS PUSTAKA**  
**NOMOR: 2484/PERP/BP/2020**

Kepala Perpustakaan Universitas Pembangunan Panca Budi menerangkan bahwa berdasarkan data pengguna perpustakaan atas nama saudara/i:

Nama : ISKANDAR AJI SAPUTRA  
N.P.M. : 1614370011  
Tingkat/Semester : Akhir  
Fakultas : SAINS & TEKNOLOGI  
Jurusan/Prodi : Sistem Komputer

Bahwasannya terhitung sejak tanggal 22 Juli 2020, dinyatakan tidak memiliki tanggungan dan atau pinjaman buku sekaligus tidak lagi terdaftar sebagai anggota Perpustakaan Universitas Pembangunan Panca Budi Medan.

Medan, 22 Juli 2020  
Diketahui oleh,  
Kepala Perpustakaan,



Sugiarjo, S.Sos., S.Pd.I

Hal : Permohonan Meja Hijau

Medan, 09 Januari 2021  
 Kepada Yth : Bapak/Ibu Dekan  
 Fakultas SAINS & TEKNOLOGI  
 UNPAB Medan  
 Di -  
 Tempat

Dengan hormat, saya yang bertanda tangan di bawah ini :

Nama : ISKANDAR AJI SAPUTRA  
 Tempat/Tgl. Lahir : P.BERANDAN / 24 April 1997  
 Nama Orang Tua : SUTARMAN  
 N. P. M : 1614370011  
 Fakultas : SAINS & TEKNOLOGI  
 Program Studi : Sistem Komputer  
 No. HP : 081973418177  
 Alamat : JL. SUKAMULIA GG. BINA

Datang bermohon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul **Simulasi Pengamanan Informasi Pada Pesan Rahasia Dengan Cipher Substitusi Satu Arah**, Selanjutnya saya menyatakan :

1. Melampirkan KKM yang telah disahkan oleh Ka. Prodi dan Dekan
2. Tidak akan menuntut ujian perbaikan nilai mata kuliah untuk perbaikan indek prestasi (IP), dan mohon diterbitkan ijazahnya setelah lulus ujian meja hijau.
3. Telah tercap keterangan bebas pustaka
4. Terlampir surat keterangan bebas laboratorium
5. Terlampir pas photo untuk ijazah ukuran 4x6 = 5 lembar dan 3x4 = 5 lembar Hitam Putih
6. Terlampir foto copy STTB SLTA dilegalisir 1 (satu) lembar dan bagi mahasiswa yang lanjutan D3 ke S1 lampirkan ijazah dan transkripnya sebanyak 1 lembar.
7. Terlampir pelunasan kwintasi pembayaran uang kuliah berjalan dan wisuda sebanyak 1 lembar
8. Skripsi sudah dijilid lux 2 exemplar (1 untuk perpustakaan, 1 untuk mahasiswa) dan jilid kertas jeruk 5 exemplar untuk penguji (bentuk dan warna penjiilidan diserahkan berdasarkan ketentuan fakultas yang berlaku) dan lembar persetujuan sudah di tandatangani dosen pembimbing, prodi dan dekan
9. Soft Copy Skripsi disimpan di CD sebanyak 2 disc (Sesuai dengan Judul Skripsinya)
10. Terlampir surat keterangan BKKOL (pada saat pengambilan ijazah)
11. Setelah menyelesaikan persyaratan point-point diatas berkas di masukan kedalam MAP
12. Bersedia melunaskan biaya-biaya uang dibebankan untuk memproses pelaksanaan ujian dimaksud, dengan perincian sbb :

1. [102] Ujian Meja Hijau	: Rp.	0
2. [170] Administrasi Wisuda	: Rp.	1,500,000
3. [202] Bebas Pustaka	: Rp.	100,000
4. [221] Bebas LAB	: Rp.	5,000
<b>Total Biaya</b>	<b>: Rp.</b>	<b>1,605,000</b>

Ukuran Toga :



Diketahui/Disetujui oleh :



Hamdani, ST., MT.  
 Dekan Fakultas SAINS & TEKNOLOGI

Hormat saya



ISKANDAR AJI SAPUTRA  
 1614370011

Catatan :

- 1. Surat permohonan ini sah dan berlaku bila ;
  - a. Telah dicap Bukti Pelunasan dari UPT Perpustakaan UNPAB Medan.
  - b. Melampirkan Bukti Pembayaran Uang Kuliah aktif semester berjalan
- 2. Dibuat Rangkap 3 (tiga), untuk - Fakultas - untuk BPAA (asli) - Mhs.ybs.

## ABSTRAK

ISKANDAR AJI SAPUTRA

**Simulasi Pengamanan Informasi Pada Pesan Rahasia Dengan *Cipher*  
*Substitusi Satu Arah*  
2020**

Informasi adalah berita yang memiliki makna tertentu. Informasi terkadang memiliki kandungan yang sangat tidak boleh diketahui oleh orang lain tanpa seizin pemiliknya. Orang-orang yang tidak bertanggung jawab tetap berusaha untuk mencuri informasi tersebut. Teknik kriptografi sangat disarankan dalam menjaga keamanan informasi. Penelitian ini melakukan proses enkripsi dengan *Cipher Substitusi* satu arah dimana *plaintext* akan dienkripsi dengan arah ke kanan dan *Ciphertext* akan didekripsi dengan arah ke kiri. Penggunaan kunci sangat berpengaruh dalam meningkatkan keamanan informasi tersebut. Informasi yang sudah mengalami proses enkripsi akan terhindar dari pencurian dan penyalahgunaan informasi secara paksa. Penerapan teknik ini akan sangat menghasilkan tingkat keamanan yang baik.

**Kata Kunci:** algoritma, keamanan, satu, arah, enkripsi, dekripsi

## KATA PENGANTAR

Puji syukur penulis ucapkan ke hadirat Allah SWT karena berkat rahmat kesehatan dan hidayah-Nya, sehingga penulis dapat menyelesaikan penulisan skripsi tepat pada waktunya. Dalam penulisan skripsi ini, penulis memilih judul **“SIMULASI PENGAMANAN INFORMASI PADA PESAN RAHASIA DENGAN CIPHER SUBSTITUSI SATU ARAH”**.

Penulisan skripsi ini adalah Salah satu syarat untuk memperoleh gelar sarjana komputer, selama proses penulisan skripsi ini, penulis telah banyak mendapatkan bimbingan dan bantuan baik moral maupun materi dari berbagai pihak. Pada kesempatan ini penulis mengucapkan terima kasih kepada:

1. Bapak Dr. H. Muhammad Isa Indrawan, S.E., M.M., selaku Rektor Universitas Pembangunan Panca Budi Medan.
2. Hamdani, S.T., M.T., selaku Dekan Fakultas Sains dan Teknologi Universitas Pembangunan Panca Budi Medan.
3. Bapak Eko Hariyanto, S.Kom., M.Kom., selaku Ketua Program Studi Sistem Komputer Fakultas Sains dan Teknologi Universitas Pembangunan Panca Budi Medan.
4. Bapak Andysah Putera Utama Siahaan, S.Kom., M.Kom., selaku dosen pembimbing I yang telah meluangkan waktunya untuk membimbing dan memberikan arahan kepada penulis sehingga penulisan skripsi ini dapat diselesaikan.
5. Bapak Dedi Purwanto, S.Kom., M.Kom., selaku dosen pembimbing II yang telah meluangkan waktunya untuk membimbing dan memberikan arahan kepada penulis sehingga penulisan skripsi ini dapat diselesaikan.
6. Kedua orang tua penulis yang telah banyak memberikan dukungan kepada penulis, memberikan motivasi dan doa sehingga penulis dapat menyelesaikan skripsi ini.
7. Bapak dan Ibu Dosen selaku Pengajar pada Fakultas Sains dan Teknologi Universitas Pembangunan Panca Budi Medan.

Penulis menyadari bahwa dalam penulisan skripsi ini masih banyak terdapat kesalahan dan kekurangan. Untuk itu saran dan kritik yang sehat dari semua pihak sangat penulis harap demi pengembangan isi skripsi ini. Akhirnya penulis berharap skripsi ini dapat berguna bagi para pembaca dan bagi penulis khususnya.

Medan, 25 Mei 2020  
Penulis

Iskandar Aji Saputra  
1614370011

## DAFTAR ISI

<b>KATA PENGANTAR</b> .....	<b>i</b>
<b>DAFTAR ISI</b> .....	<b>ii</b>
<b>DAFTAR GAMBAR</b> .....	<b>iv</b>
<b>DAFTAR TABEL</b> .....	<b>v</b>
<b>BAB I PENDAHULUAN</b> .....	<b>1</b>
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	2
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian .....	3
1.5 Manfaat Penelitian .....	4
<b>BAB II LANDASAN TEORI</b> .....	<b>5</b>
2.1 Pengertian Aplikasi .....	5
2.2 Data .....	5
2.2.1 Bagaimana Data Disimpan .....	6
2.2.2 Jenis data .....	7
2.2.3 Pengelolaan dan Penggunaan Data.....	7
2.3 Logika dan Algoritma .....	8
2.4 Kriptografi.....	10
2.4.1 Sejarah Kriptografi .....	11
2.4.2 Tujuan Kriptografi.....	12
2.4.3 Kriptografi Simetris.....	12
2.4.4 Kriptografi Asimetris .....	14
2.5 Enkripsi .....	16
2.6 Dekripsi .....	18
2.7 Kriptografi Substitusi .....	19
2.7.1 Proses Enkripsi .....	22
2.7.2 Proses Dekripsi .....	23
2.8 <i>Unified Modeling Language (UML)</i> .....	24
2.8.1 <i>Use Case Diagram</i> .....	25
2.8.2 <i>Activity Diagram</i> .....	27
2.9 Visual Basic.Net 2010.....	28
2.9.1 Lingkungan kerja Visual Basic.Net 2010.....	29
2.9.2 Komponen Visual Basic.Net 2010 .....	30
<b>BAB III METODE PENELITIAN</b> .....	<b>34</b>
3.1 Tahapan Penelitian .....	34
3.2 Metode Pengumpulan Data .....	36
3.3 Analisa Sistem.....	36
3.1.1 Analisa Sistem Yang Berjalan.....	37
3.1.2 Analisa Sistem Yang Diusulkan.....	37
3.2 Rancangan UML .....	38

3.2.1	<i>Use Case Diagram</i> Enkripsi.....	38
3.2.2	<i>Use Case Diagram</i> Dekripsi.....	39
3.2.3	<i>Activity Diagram</i> Enkripsi.....	40
3.2.4	<i>Activity Diagram</i> Dekripsi.....	41
3.2.5	<i>Sequence Diagram</i> Enkripsi.....	42
3.2.6	<i>Sequence Diagram</i> Dekripsi.....	43
3.3	Analisis <i>Cipher Substitusi</i> .....	44
3.4	Perancangan Antarmuka .....	45
3.4.1	Desain Antarmuka Judul .....	45
3.4.2	Desain Antarmuka Menu Utama .....	46
3.4.3	Desain Antarmuka <i>Cipher Substitusi</i> .....	47
3.4.4	Desain Antarmuka Materi .....	48
3.4.5	Desain Antarmuka Tentang.....	48
<b>BAB IV HASIL DAN PEMBAHASAN .....</b>		<b>50</b>
4.1	Kebutuhan Perangkat Keras dan Lunak.....	50
4.2	Implementasi Program Aplikasi.....	51
4.2.1	Tampilan Halaman Judul.....	51
4.2.2	Tampilan Halaman Menu Utama .....	52
4.2.3	Tampilan Halaman Enkripsi.....	52
4.2.4	Tampilan Halaman Dekripsi .....	53
4.2.5	Halaman Materi .....	54
4.2.6	Halaman Tentang .....	55
4.3	Perhitungan Manual .....	55
<b>BAB V PENUTUP.....</b>		<b>59</b>
5.1	Kesimpulan .....	59
5.2	Saran.....	59

## DAFTAR PUSTAKA



## DAFTAR GAMBAR

Gambar 2.1 Skema kriptografi simetris .....	13
Gambar 2.2 Skema kriptografi asimetris .....	15
Gambar 2.3 Tampilan Microsoft Visual Studio 2010 .....	30
Gambar 2.4 Tampilan Menu Bar .....	30
Gambar 2.5 Tampilan Toolbar .....	31
Gambar 2.6 Tampilan Toolbox .....	31
Gambar 2.7 Tampilan Properties .....	32
Gambar 2.8 Tampilan Form .....	33
Gambar 2.9 Tampilan Code Editor .....	33
Gambar 3.1 Tahapan Penelitian .....	34
Gambar 3.2 <i>Use Case Diagram</i> Enkripsi .....	38
Gambar 3.3 <i>Use Case Diagram</i> Dekripsi .....	39
Gambar 3.4 <i>Activity Diagram</i> Enkripsi .....	40
Gambar 3.5 <i>Activity Diagram</i> Dekripsi .....	41
Gambar 3.6 <i>Sequence Diagram</i> Enkripsi .....	42
Gambar 3.7 <i>Sequence Diagram</i> Dekripsi .....	43
Gambar 3.8 Desain Antarmuka Judul .....	45
Gambar 3.9 Desain Antarmuka Menu Utama .....	46
Gambar 3.10 Desain Antarmuka <i>Cipher Substitusi</i> .....	47
Gambar 3.11 Desain Antarmuka Materi .....	48
Gambar 3.12 Desain Antarmuka Tentang .....	49
Gambar 4.1 Halaman Judul .....	51
Gambar 4.2 Halaman Menu Utama .....	52
Gambar 4.3 Halaman Enkripsi .....	53
Gambar 4.4 Halaman Dekripsi .....	54
Gambar 4.5 Halaman Materi .....	54
Gambar 4.6 Halaman Tentang .....	55

## DAFTAR TABEL

Tabel 2.1 Simbol <i>Use Case Diagram</i> .....	26
Tabel 2.2 Simbol <i>Activity Diagram</i> .....	28

# **BAB I**

## **PENDAHULUAN**

### **1.1 Latar Belakang**

Dalam melakukan proses peningkatan keamanan informasi, ada banyak hal yang dapat dilakukan. Salah satu cara adalah dengan cara mengamankan informasi tersebut dan menjauhkan informasi tersebut dari jangkauan orang-orang yang tidak bertanggung jawab. Informasi yang memiliki kandungan sensitif atau rahasia harus dijaga dengan baik agar tidak terjadi hal-hal yang tidak diinginkan. Salah satu hal negatif yang paling sering terjadi adalah pencurian data. Pencurian data ini dilakukan karena informasi ini dikirimkan melalui jaringan terbuka. Ada banyak proses-proses percobaan peretasan pada informasi yang mengalir di jaringan internet.

Bagi pihak yang tidak begitu memahami teknik pengiriman data secara aman, mereka dengan tidak merasa bersalah mengirimkan data atau informasi tanpa memiliki sistem keamanan yang baik. Pihak pengirim tidak sadar bahwa mereka sedang mengalami ancaman dan bahaya. Apabila data mereka merupakan data umum, mungkin tidak masalah apabila data mereka dicuri oleh orang lain. Tetapi, jika data mereka memiliki informasi yang sangat rahasia, maka ini suatu kerugian yang besar bagi mereka.

Ada beberapa cara yang dapat dilakukan dalam melindungi informasi tersebut. Salah satu caranya adalah dengan menerapkan ilmu kriptografi pada sistem aplikasi yang bertugas mengirimkan data tersebut. Teknik yang digunakan

pada penelitian ini adalah teknik yang menggunakan model *Cipher Substitusi*. Teknik kriptografi ini adalah melakukan pertukaran *plaintext* dengan karakter lain sesuai dengan kunci yang sudah ditentukan. *Plaintext* akan digeser satu arah sesuai dengan arah yang ditentukan. *Plaintext* akan digeser ke arah kanan untuk mendapatkan *Ciphertext*. Sementara pada proses dekripsi, *Ciphertext* akan digeser kembali ke arah yang berlawanan, yaitu arah kiri. Hasil penelitian ini diharapkan dapat memberikan sistem keamanan yang baik bagi suatu informasi yang akan dikirim. Penelitian ini merupakan simulasi dimana proses enkripsi dan dekripsi akan dijelaskan melalui program aplikasi.

Penelitian ini bertujuan untuk memberikan perlindungan terhadap informasi agar tidak dapat diretas oleh orang yang tidak bertanggung jawab. Keamanan data diharapkan akan lebih terjamin. Berdasarkan latar belakang yang telah disebutkan sebelumnya, penulis mengambil judul **“SIMULASI PENGAMANAN INFORMASI PADA PESAN RAHASIA DENGAN *CIPHER SUBSTITUSI SATU ARAH*”**.

## **1.2 Rumusan Masalah**

Adapun rumusan masalah yang digunakan dalam penulisan skripsi ini adalah sebagai berikut:

1. Bagaimana merancang aplikasi pengamanan pesan menggunakan *Cipher Substitusi* satu arah?
2. Bagaimana melaksanakan proses enkripsi dan dekripsi pada teknik tersebut?

3. Bagaimana menentukan kunci yang digunakan pada proses kriptografi tersebut?

### **1.3 Batasan Masalah**

Adapun batasan masalah yang digunakan dalam penulisan tugas akhir ini adalah sebagai berikut:

1. Proses enkripsi dilakukan dengan menggeser posisi *plaintext* ke arah kanan dan sebaliknya.
2. Proses dekripsi dilakukan dengan menggeser posisi *Ciphertext* ke arah kiri dan sebaliknya.
3. Batas proses enkripsi dan dekripsi adalah 1000 karakter.
4. Panjang kunci maksimal adalah 10 karakter.
5. Pesan yang digunakan adalah berbasis teks yang dimasukkan langsung pada *textbox*.
6. Bahasa pemrograman yang digunakan adalah menggunakan Microsoft Visual Basic.Net 2010.
7. Program aplikasi yang dihasilkan adalah berbasis *desktop* dan tidak *online*.

### **1.4 Tujuan Penelitian**

Adapun tujuan penelitian yang digunakan dalam penulisan tugas akhir ini adalah sebagai berikut:

1. Untuk merancang aplikasi pengamanan pesan menggunakan *Cipher Substitusi* satu arah.
2. Untuk melaksanakan proses enkripsi dan dekripsi pada teknik tersebut.

3. Untuk menentukan kunci yang digunakan pada proses kriptografi tersebut.

### **1.5 Manfaat Penelitian**

Adapun manfaat penelitian yang digunakan dalam penulisan tugas akhir ini adalah sebagai berikut:

1. Informasi setelah dilakukan proses enkripsi akan terhindar dari pencurian dan penyalahgunaan informasi.
2. Memberi kenyamanan bagi pengirim dan penerima informasi.
3. Memberikan pengetahuan tentang bagaimana melakukan proses *Cipher Substitusi* satu arah.

## **BAB II**

### **LANDASAN TEORI**

#### **2.1 Pengertian Aplikasi**

Secara istilah pengertian aplikasi adalah suatu program yang siap untuk digunakan yang dibuat untuk melaksanakan suatu fungsi bagi pengguna jasa aplikasi serta penggunaan aplikasi lain yang dapat digunakan oleh suatu sasaran yang akan dituju. Menurut kamus komputer eksekutif, aplikasi mempunyai arti yaitu pemecahan masalah yang menggunakan salah satu teknik pemrosesan data aplikasi yang biasanya berpacu pada sebuah komputasi yang diinginkan atau diharapkan maupun pemrosesan data yang di harapkan (Sopyan, Supriyadi, & Kurniadi, 2016).

Aplikasi adalah penerapan dari rancang sistem untuk mengolah data yang menggunakan aturan atau ketentuan bahasa pemrograman tertentu. Aplikasi adalah suatu program komputer yang dibuat untuk mengerjakan dan melaksanakan tugas khusus dari pengguna. Aplikasi merupakan rangkaian kegiatan atau perintah untuk dieksekusi oleh komputer.

#### **2.2 Data**

Data merupakan bentuk yang masih mentah yang belum dapat bercerita banyak, sehingga perlu diolah lebih lanjut. Data diolah melalui suatu model untuk dihasilkan informasi (Jogiyanto, 2016). Kegiatan suatu perusahaan, misalnya transaksi penjualan oleh sejumlah *salesman*, dihasilkan sejumlah faktor-faktor yang

merupakan data dari penjualan pada suatu periode tertentu. Faktor-faktor penjualan tersebut masih belum dilaporkan secara terperinci kepada manajemen. Untuk keperluan pengambilan keputusan, maka faktor-faktor tersebut perlu diolah lebih lanjut untuk menjadi suatu informasi (Sun, Zhang, Xiong, & Zhu, 2014).

### **2.2.1 Bagaimana Data Disimpan**

Komputer mewakili data, termasuk video, gambar, suara dan teks, sebagai nilai biner menggunakan pola hanya dua angka: 1 dan 0. Sedikit adalah unit data terkecil dan hanya mewakili nilai tunggal. Satu byte terdiri dari delapan digit biner. Penyimpanan dan memori diukur dalam megabit dan gigabit.

Unit-unit pengukuran data terus bertambah seiring dengan meningkatnya jumlah data yang dikumpulkan dan disimpan. Istilah "brontobyte" yang relatif baru, misalnya, adalah penyimpanan data yang setara dengan 10 hingga 27 byte. Data dapat disimpan dalam format file, seperti pada sistem mainframe menggunakan ISAM dan VSAM. Format file lain untuk penyimpanan, konversi, dan pemrosesan data termasuk nilai yang dipisah koma. Format ini terus menemukan kegunaan di berbagai jenis mesin, bahkan ketika pendekatan yang lebih berorientasi data terstruktur memperoleh pijakan dalam komputasi perusahaan. Spesialisasi yang lebih besar dikembangkan sebagai basis data, sistem manajemen basis data, dan kemudian teknologi basis data relasional muncul untuk mengatur informasi (Zhang et al., 2009).



### **2.2.2 Jenis data**

Pertumbuhan web dan telepon pintar selama dekade terakhir menyebabkan peningkatan dalam penciptaan data digital. Data sekarang termasuk informasi teks, audio dan video, serta catatan aktivitas log dan web. Banyak dari itu adalah data yang tidak terstruktur.

Istilah big data telah digunakan untuk menggambarkan data dalam kisaran petabyte atau lebih besar. Tulisan singkat menggambarkan data besar dengan 3V - volume, variasi, dan kecepatan. Ketika e-commerce berbasis web telah menyebar, model bisnis berbasis data besar telah berevolusi yang memperlakukan data sebagai aset. Tren semacam itu juga telah menimbulkan keasyikan yang lebih besar dengan penggunaan sosial data dan privasi data.

Data memiliki makna di luar penggunaannya dalam aplikasi komputasi yang berorientasi pada pemrosesan data. Misalnya, dalam interkoneksi komponen elektronik dan komunikasi jaringan, istilah data sering dibedakan dari "informasi kontrol," "bit kontrol," dan istilah serupa untuk mengidentifikasi konten utama dari unit transmisi. Selain itu, dalam sains, istilah data digunakan untuk menggambarkan kumpulan fakta. Itu juga terjadi di bidang-bidang seperti keuangan, pemasaran, demografi dan kesehatan.

### **2.2.3 Pengelolaan dan Penggunaan Data**

Dengan semakin banyaknya data dalam organisasi, penekanan tambahan telah ditempatkan pada memastikan kualitas data dengan mengurangi duplikasi dan menjamin yang paling akurat, catatan saat ini digunakan. Banyak langkah yang

terlibat dengan manajemen data modern termasuk pembersihan data, serta mengekstrak, mengubah dan memuat (ETL) proses untuk mengintegrasikan data. Data untuk diproses telah dilengkapi dengan metadata, kadang-kadang disebut sebagai "data tentang data," yang membantu administrator dan pengguna memahami database dan data lainnya.

Analisis yang menggabungkan data terstruktur dan tidak terstruktur menjadi bermanfaat, karena organisasi berupaya memanfaatkan informasi tersebut. Sistem untuk analitik semacam itu semakin berupaya untuk kinerja waktu-nyata, sehingga mereka dibangun untuk menangani data yang masuk yang dikonsumsi dengan tingkat konsumsi tinggi, dan untuk memproses aliran data untuk penggunaan langsung dalam operasi.

Seiring waktu, gagasan basis data untuk operasi dan transaksi telah diperluas ke basis data untuk pelaporan dan analitik data prediktif. Contoh utama adalah gudang data, yang dioptimalkan untuk memproses pertanyaan tentang operasi untuk analisis bisnis dan pemimpin bisnis. Meningkatnya penekanan pada menemukan pola dan memprediksi hasil bisnis telah mengarah pada pengembangan teknik penambangan data (Barone, Williams, & Micklos, 2017).

### **2.3 Logika dan Algoritma**

Pengertian algoritma sangat lekat dengan kata logika, yaitu kemampuan seorang manusia untuk berfikir dengan akal tentang suatu permasalahan menghasilkan sebuah kebenaran, dibuktikan dan dapat diterima akal, logika

seringkali dihubungkan dengan kecerdasan, seseorang yang mampu berlogika dengan baik sering orang menyebutnya sebagai pribadi yang cerdas.

Logika identik dengan masuk akal dan penalaran. Penalaran adalah salah satu bentuk pemikiran. Pemikiran adalah pengetahuan tak langsung yang didasarkan pada pernyataan langsung pemikiran mungkin benar dan mungkin juga tak benar. Definisi logika sangat sederhana yaitu ilmu yang memberikan prinsip-prinsip yang harus diikuti agar dapat berfikir valid menurut aturan yang berlaku. Pelajaran logika menimbulkan kesadaran untuk menggunakan prinsip-prinsip untuk berfikir secara sistematis. Logika berasal dari bahasa Yunani yaitu LOGOS yang berarti ilmu. Logika dapat diartikan ilmu yang mengajarkan cara berpikir untuk melakukan kegiatan dengan tujuan tertentu. Algoritma berasal dari nama seorang Ilmuwan Arab yang bernama Abu Jafar Muhammad Ibnu Musa Al Khuwarizmi penulis buku berjudul Al Jabar Wal Muqabala. Kata Al Khuwarizmi dibaca orang barat menjadi Algorism yang kemudian lambat laun menjadi Algorithm diserap dalam bahasa Indonesia menjadi Algoritma.

Logika identik dengan masuk akal dan penalaran. Penalaran adalah salah satu bentuk pemikiran. Pemikiran adalah pengetahuan tak langsung yang didasarkan pada pernyataan langsung pemikiran mungkin benar dan mungkin juga tak benar. Definisi logika sangat sederhana yaitu ilmu yang memberikan prinsip-prinsip yang harus diikuti.

## 2.4 Kriptografi

Menurut M. Miftakhul Amin, kriptografi (*Cryptography*) berasal dari bahasa Yunani terdiri dari dua suku kata yaitu kriptos dan graphia. Kriptos artinya menyembunyikan sedangkan graphia artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi (Amin, 2016). Adapun istilah-istilah yang sering digunakan dalam ilmu kriptografi di antara sebagai berikut:

1. *Plaintext*

*Plaintext* merupakan pesan asli yang belum disandikan atau informasi yang ingin dikirimkan atau dijaga keamanannya.

2. *Ciphertext*

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

3. Enkripsi

Enkripsi merupakan proses yang dilakukan untuk menyandikan *plaintext* menjadi *Ciphertext* dengan tujuan pesan tersebut tidak dapat dibaca oleh pihak yang tidak berwenang.

4. Deskripsi

Deskripsi merupakan proses yang dilakukan untuk memperoleh kembali *plaintext* dari *Ciphertext*.

## 5. Kunci

Kunci yang dimaksud disini adalah kunci yang dipakai untuk melakukan dekripsi dan enkripsi. Kunci terbagi menjadi dua bagian, diantaranya yaitu kunci pribadi (*private key*) dan kunci umum (*public key*).

## 6. Kriptosistem

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

## 7. Kriptanalisis

Kriptanalisis merupakan suatu ilmu untuk mendapatkan *plaintext* tanpa harus mengetahui kunci secara wajar.

Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan. Ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan tersebut. Untuk menjaga pesan maka pesan tersebut dapat diubah menjadi sebuah kode yang tidak dapat dimengerti pihak lain.

### 2.4.1 Sejarah Kriptografi

Sejarah kriptografi sebagian besar merupakan sejarah kriptografi klasik, yaitu metode enkripsi yang menggunakan kertas dan pensil atau mungkin dengan bantuan alat mekanik sederhana. Secara umum algoritma kriptografi klasik dikelompokkan menjadi dua kategori, yaitu algoritma transposisi (*transposition Cipher*) dan algoritma substitusi (*substitution Cipher*). *Cipher* transposisi

mengubah susunan huruf-huruf di dalam pesan, sedangkan *Cipher Substitusi* mengganti setiap huruf atau kelompok huruf dengan sebuah huruf atau kelompok huruf lain (Pabokory, Astuti, & Kridalaksana, 2015).

#### **2.4.2 Tujuan Kriptografi**

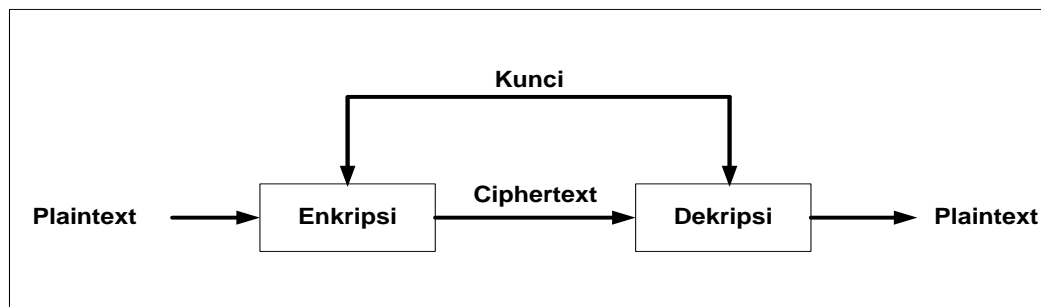
Dari paparan awal dapat dirangkumkan bahwa kriptografi bertujuan untuk member layanan keamanan. Yang dinamakan aspek-aspek keamanan:

1. Kerahasiaan (*confidentiality*) adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak.
2. Integritas data (*data integrity*) adalah layanan yang menjamin bahwa pesan masih asli atau belum pernah dimanipulasi selama pengiriman.
3. Otentikasi (*authentication*) adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication*).
4. *Non-repudiation* adalah layanan untuk menjaga entitas yang berkomunikasi melakukan penyangkalan.

#### **2.4.3 Kriptografi Simetris**

Kriptografi simetris adalah teknik kriptografi dimana kunci yang digunakan pada proses enkripsi dan dekripsi adalah kunci yang sama. Dalam kriptografi kunci simetris dapat diasumsikan bahwa si penerima dan pengirim pesan telah terlebih dahulu berbagi kunci sebelum pesan dikirimkan. Keamanan dari sistem ini terletak pada kerahasiaan kuncinya.

Pada umumnya yang termasuk ke dalam kriptografi simetris ini beroperasi dalam mode blok (*block Cipher*), yaitu setiap kali proses enkripsi atau dekripsi dilakukan terhadap satu blok data (yang berukuran tertentu), atau beroperasi dalam mode aliran (*stream Cipher*), yaitu setiap kali enkripsi atau dekripsi dilakukan terhadap satu bit atau satu byte data. Contoh algoritma simetris, yaitu: Trithemius, Double Transposition *Cipher*, DES (Data Encryption Standard), AES (Advanced Encryption Standard). Gambar 2.1 adalah skema algoritma simetris.



**Gambar 2.1 Skema kriptografi simetris**

Sumber: (Putri, Setyorini, & Rahayani, 2018)

Kelebihan kriptografi simetris adalah:

1. Proses enkripsi atau dekripsi kriptografi simetris membutuhkan waktu yang singkat.
2. Ukuran kunci simetris *relative* lebih pendek.
3. Otentikasi pengiriman pesan langsung dari *Ciphertext* yang diterima, karena kunci hanya diketahui oleh penerima dan pengirim saja.

Kelemahan kriptografi simetris antara lain:

1. Kunci simetris harus dikirim melalui saluran komunikasi yang aman, dan kedua entitas yang berkomunikasi harus menjaga kerahasiaan kunci.
2. Kunci harus sering diubah, setiap kali melaksanakan komunikasi. Apabila kunci tersebut hilang atau lupa, maka pesan tersebut tidak dapat dibuka.

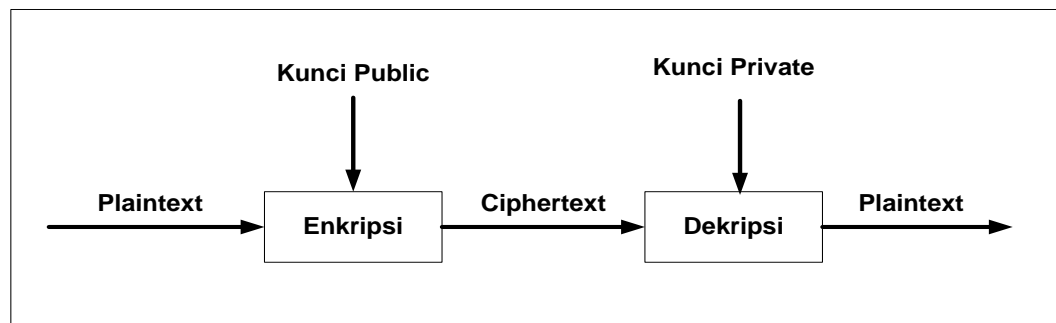
#### **2.4.4 Kriptografi Asimetris**

Berbeda dengan kriptografi kunci simetris, kriptografi kunci public memiliki dua buah kunci yang berbeda pada proses enkripsi dan dekripsinya. Dimana kunci yang digunakan untuk proses enkripsi atau sering disebut *public key* dan dekripsi atau sering disebut *private key* menggunakan kunci yang berbeda. Entitas pengirim akan mengenkripsi dengan menggunakan kunci *public*, sedangkan entitas penerima mendekripsi menggunakan kunci *private* (Kamil, 2016).

Contoh algoritma asimetris, yaitu RSA (*Riverst Shamir Adleman*), Knapsack, Rabin, ElGamal (Ayushi, 2010) (S., L. Ribeiro, & David, 2012). Pada algoritma tak simetri kunci terbagi menjadi dua bagian:

1. Kunci umum (*public key*) adalah kunci yang dapat dan boleh diketahui oleh semua orang.
2. Kunci pribadi (*private key*) adalah kunci yang hanya dapat diketahui penerima dan bersifat rahasia.





**Gambar 2.2 Skema kriptografi asimetris**

Sumber: (Putri et al., 2018)

Kelebihan kriptografi asimetris adalah:

1. Hanya kunci *private* yang perlu dijaga kerahasiaannya oleh setiap entitas yang berkomunikasi. Tidak ada kebutuhan mengirim kunci *private* sebagaimana kunci simetri.
2. Pasangan kunci *private* dan kunci *public* tidak perlu diubah dalam jangka waktu yang sangat lama.
3. Dapat digunakan dalam pengamanan pengiriman kunci simetri.

Kelemahan kriptografi asimetris adalah:

1. Proses enkripsi dan dekripsi umumnya lebih lambat dari algoritma simetri, karena menggunakan bilangan yang besar dan operasi bilangan yang besar.
2. Ukuran *Ciphertext* lebih besar dari *plaintext*.
3. Ukuran kunci relatif lebih besar daripada ukuran kunci simetri.

## 2.5 Enkripsi

*Enkripsi* adalah proses penyandian *plaintext* menjadi *Ciphertext*, atau pengubahan data menjadi bentuk rahasia. Proses *enkripsi algoritma AES* terdiri dari 4 jenis *transformasi bytes*, yaitu *SubBytes*, *ShiftRows*, *Mixcolumns*, dan *AddRoundKey*. Pada awal proses *enkripsi*, input yang telah dicopykan ke dalam *state* akan mengalami *transformasi byte AddRoundKey*. Setelah itu, *state* akan mengalami *transformasi SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* secara berulang-ulang sebanyak *Nr*. Proses ini dalam *algoritma AES* disebut sebagai *round function*. *Round* yang terakhir agak berbeda dengan *round-round* sebelumnya dimana pada *round* terakhir, *state* tidak mengalami transformasi *MixColumns* (Amin, 2016).

Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang lain. Dengan enkripsi, data kita disandikan (Encrypted) dengan menggunakan sebuah kunci (key). Untuk membuka (mendecrypt) data tersebut, digunakan kunci yang sama ketika mengenkrip. Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Dikarenakan enkripsi telah digunakan untuk mengamankan komunikasi di berbagai negara, hanya organisasi-organisasi tertentu dan individu yang memiliki kepentingan yang sangat mendesak akan kerahasiaan yang menggunakan enkripsi. Di pertengahan tahun 1970-an, enkripsi kuat dimanfaatkan untuk pengamanan oleh sekretariat agen pemerintah Amerika Serikat pada domain publik, dan saat ini enkripsi telah

digunakan pada sistem secara luas, seperti Internet e-commerce, jaringan Telepon bergerak dan ATM pada bank.

Keamanan dari enkripsi tergantung beberapa faktor salah satunya yaitu menjaga kerahasiaan kuncinya bukan algoritmanya. Proses enkripsi dapat diterangkan sebagai berikut:

1. Masukkan file dan key
2. Baca isi file
3. Lakukan perhitungan untuk melakukan enkripsi
4. Outputnya adalah *Ciphertext*
5. Pilih Folder Penyimpanan
6. Selesai

Langkah-langkah pada proses enkripsi adalah sebagai berikut:

1. *Plaintext* diubah ke dalam bentuk bilangan. Untuk mengubah *plaintext* yang berupa huruf menjadi bilangan dapat digunakan kode *ASCII* dalam sistem bilangan desimal.
2. *Plaintext*  $m$  dinyatakan menjadi blok-blok  $m_1, m_2, m_3, \dots$ , sedemikian sehingga setiap blok merepresentasikan nilai di dalam selang  $[0, n-1]$ , sehingga transformasinya menjadi satu ke satu.
3. Setiap blok  $m_i$  dienkripsi menjadi blok  $c_i$  dengan rumus  $m_i = c_i e \pmod n$

## 2.6 Dekripsi

Dekripsi digunakan untuk mengembalikan data-data atau informasi yang sudah dienkripsi ke bentuk awal sehingga dapat dibaca kembali dengan baik. Satu kaidah upaya pengolahan data menjadi sesuatu yang dapat diutarakan secara jelas dan tepat dengan tujuan agar dapat dimengerti oleh orang yang tidak langsung mengalaminya sendiri dalam keilmuan, deskripsi diperlukan agar peneliti tidak melupakan pengalamannya dan agar pengalaman tersebut dapat dibandingkan dengan pengalaman peneliti lain, sehingga mudah untuk dilakukan pemeriksaan dan kontrol terhadap deskripsi tersebut. Pada umumnya deskripsi menegaskan sesuatu, seperti apa sesuatu itu kelihatannya, bagaimana bunyinya, bagaimana rasanya, dan sebagainya (Amin, 2016).

Deskripsi yang detail diciptakan dan dipakai dalam disiplin ilmu sebagai istilah teknik. Saat data yang dikumpulkan, deskripsi, analisis dan kesimpulannya lebih disajikan dalam angka-angka maka hal ini dinamakan penelitian kuantitatif. Sebaliknya, apabila data, deskripsi, dan analisis kesimpulannya disajikan dalam uraian kata-kata maka dinamakan penelitian kualitatif. Proses deskripsi dapat diterangkan sebagai berikut:

1. Pilih folder penyimpanan
2. Masukkan file *Cipher* & key
3. Baca isi file
4. Lakukan perhitungan untuk dekripsi
5. Outputnya adalah *plaintext*

*Dekripsi* adalah proses memperoleh kembali *plaintext* menjadi *Ciphertext*, atau proses pengubahan kembali data yang berbentuk rahasia menjadi semula. *Transformasi byte* yang digunakan pada invers *Cipher* adalah *InvShiftRows*, *InvSubBytes*, *InvMixColumns*, dan *AddRoundKey*. Langkah-langkah pada proses *dekripsi* adalah sebagai berikut:

1. Setiap blok *Ciphertext*  $c_i$  *didekripsi* kembali menjadi blok  $m_i$  dengan rumus
 
$$m_i = c_i \cdot d \pmod{n}$$
2. Kemudian blok-blok  $m_1, m_2, m_3, \dots$ , diubah kembali ke bentuk huruf dengan melihat kode *ASCII* hasil *dekripsi*. (Yuza, dkk, 2018)

## 2.7 Kriptografi Substitusi

Dalam kriptografi, subtitle *Cipher* adalah metode enkripsi yang dengannya unit *plaintext* diganti dengan *Ciphertext*, sesuai dengan sistem tetap; "unit" dapat berupa huruf tunggal (paling umum), pasangan huruf, kembar tiga huruf, campuran di atas, dan sebagainya. Penerima menafsirkan teks dengan melakukan substitusi terbalik.

*Cipher* pergantian dapat dibandingkan dengan *Cipher* transposisi. Dalam sandi transposisi, satuan *plaintext* disusun ulang dalam urutan yang berbeda dan biasanya cukup kompleks, tetapi satuan itu sendiri tidak berubah. Sebaliknya, dalam *Cipher* substitusi, unit *plaintext* dipertahankan dalam urutan yang sama dalam *Ciphertext*, tetapi unit itu sendiri diubah.

Ada sejumlah jenis *Cipher Substitusi* yang berbeda. Jika sandi beroperasi pada huruf tunggal, itu disebut sandi substitusi sederhana; sandi yang beroperasi pada kelompok huruf yang lebih besar disebut poligrafi. *Cipher* monoalphabetic menggunakan substitusi tetap atas seluruh pesan, sedangkan *Cipher* polyalphabetic menggunakan sejumlah substitusi pada posisi yang berbeda dalam pesan, di mana unit dari *plaintext* dipetakan ke salah satu dari beberapa kemungkinan dalam *Ciphertext* dan sebaliknya.. (Azanuddin, 2015).

Substitusi huruf tunggal secara terpisah — substitusi sederhana — dapat diperlihatkan dengan menuliskan alfabet untuk mewakili substitusi. Ini disebut abjad substitusi. Alfabet sandi dapat digeser atau dibalik (masing-masing menciptakan sandi Caesar dan Atbash) atau diacak dengan cara yang lebih kompleks, dalam hal ini disebut alfabet campuran atau alfabet gila. Secara tradisional, huruf campuran dapat dibuat dengan terlebih dahulu menuliskan kata kunci, menghapus huruf berulang di dalamnya, kemudian menulis semua huruf yang tersisa dalam alfabet dalam urutan yang biasa.

Menggunakan sistem ini, kata kunci "zebra" memberi kita alfabet berikut:

Alfabet *Plaintext*: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Alfabet teks sandi: ZEBRASCDFGHIJKLMNOPQTVWXY

Meskipun metode kata kunci tradisional untuk membuat alfabet substitusi campuran adalah sederhana, kerugian yang serius adalah bahwa huruf terakhir dari

alfabet (yang sebagian besar frekuensinya rendah) cenderung tetap pada akhirnya. Cara yang lebih kuat untuk membangun alfabet campuran adalah dengan melakukan transposisi kolom pada alfabet biasa menggunakan kata kunci, tetapi ini tidak sering dilakukan.

Meskipun jumlah kunci yang mungkin sangat besar ( $26! \approx 288,4$ , atau sekitar 88 bit), sandi ini tidak terlalu kuat, dan mudah patah. Asalkan pesan tersebut memiliki panjang yang masuk akal (lihat di bawah), cryptanalyst dapat menyimpulkan kemungkinan makna dari simbol yang paling umum dengan menganalisis distribusi frekuensi *Ciphertext*. Ini memungkinkan pembentukan kata-kata parsial, yang dapat diisi sementara, memperluas solusi (parsial) secara progresif (lihat analisis frekuensi untuk peragaan ini). Dalam beberapa kasus, kata-kata yang mendasarinya juga dapat ditentukan dari pola huruf mereka; misalnya, menarik, osseous, dan kata-kata dengan keduanya sebagai root adalah satu-satunya kata bahasa Inggris yang umum dengan pola ABBCADB. Banyak orang memecahkan sandi semacam itu untuk rekreasi, seperti dengan teka-teki kriptogram di koran.

Menurut jarak keutuhan bahasa Inggris, 27,6 huruf *Ciphertext* diperlukan untuk memecahkan substitusi alfabet campuran sederhana. Dalam praktiknya, biasanya dibutuhkan sekitar 50 huruf, meskipun beberapa pesan dapat dipecah dengan lebih sedikit jika ditemukan pola yang tidak biasa. Dalam kasus lain, *plaintext* dapat dibuat untuk memiliki distribusi frekuensi yang hampir datar, dan *plaintext* yang lebih lama akan dibutuhkan oleh cryptanalyst.

### 2.7.1 Proses Enkripsi

Proses enkripsi dilakukan dengan cara melakukan penambahan *plaintext* dengan kunci atau menggeser *plaintext* ke arah kanan. *Plaintext* terlebih dahulu pesan tersebut diubah ke kode nilai desimal, plaintexts yang dihasilkan akan menjadi *chiperteks*. Langkah-langkah proses enkripsi adalah sebagai berikut:

1. Tentukan *plaintexts* yang akan dienkrpsi beserta kunci.
2. Jika panjang kunci tidak sama dengan panjang plaintexts maka kunci yang ada diulang secara priodik sehingga jumlah karakter kuncinya sama dengan jumlah plaintexts nya.
3. Selanjutnya ubah plaintexts ke bentuk nilai desimal kemudian ditambahkan dengan kunci. Jika penambahan lebih besar dari jumlah *mod*, maka diambil nilai sisa hasil bagi nya.
4. Setelah dijumlahkan dengan kunci maka langkah berikutnya adalah mengubah kembali ke bentuk karakter.

Algoritma enkripsi:  $C_i = (P_i + K_i) \bmod 256$

Contoh Proses Enkripsi :

*Plaintext* : GRO

Kunci : 734

G = 71

R = 82

O = 79



Key : 7,3,4

$$C1 = (G + k1) \text{ mod } 256$$

$$= (71 + 7) \text{ mod } 256$$

$$= 78 \text{ mod } 256$$

$$= 78 = N$$

$$C2 = (R + k2) \text{ mod } 256$$

$$= (82 + 3) \text{ mod } 256$$

$$= 85 \text{ mod } 256$$

$$= 85 = U$$

$$C3 = (O + k3) \text{ mod } 256$$

$$= (79 + 4) \text{ mod } 256$$

$$= 83 \text{ mod } 256$$

$$= 83 = S$$

Chipertext : NUS

### 2.7.2 Proses Dekripsi

Dekripsi adalah proses sebaliknya, dimana *chiperteks* nya diubah menjadi nilai *decimal* dan dikurangi atau digeser ke kiri dengan jumlah kunci kemudian dikembalikan ke karakter. Langkah-langkah proses dekripsi adalah sebagai berikut:

1. Terlebih dahulu mengubah *chiperteks* ke nilai desimal.
2. Kemudian nilai desimal *chiperteks* nya dikurangi sesuai dengan kunci

3. Setelah dikurangi dengan kunci maka langkah berikutnya adalah mengubah kembali kebentuk karakter

Contoh Proses Dekripsi :

$$C1 = (N - k1) \text{ mod } 256$$

$$= (78 - 7) \text{ mod } 256$$

$$= 71 \text{ mod } 256$$

$$= 71 = G$$

$$C2 = (U - k2) \text{ mod } 256$$

$$= (85 - 3) \text{ mod } 256$$

$$= 83 \text{ mod } 256$$

$$= 83 = R$$

$$C3 = (S - k3) \text{ mod } 256$$

$$= (83 - 4) \text{ mod } 256$$

$$= 79 \text{ mod } 256$$

$$= 79 = O$$

*Plaintext* : GRO

## 2.8 *Unified Modeling Language (UML)*

*Unified Modeling Language (UML)* adalah sebuah “bahasa” yg telah menjadi standar dalam industri untuk visualisasi, merancang dan mendokumentasikan sistem piranti lunak (Mallu, 2015). *UML* menawarkan sebuah standar untuk merancang model sebuah system. Notasi *UML* merupakan

sekumpulan bentuk khusus untuk menggambarkan berbagai diagram piranti lunak. Notasi *UML* terutama diturunkan dari 3 notasi yang telah ada sebelumnya: Grady Booch OOD (*Object-Oriented Design*), Jim Rumbaugh OMT (*Object Modeling Technique*), dan Ivar Jacobson OOSE (*Object-Oriented Software Engineering*) (Isa & Hartawan, 2017).

*Unified Modeling Language* (UML) adalah keluarga notasi grafis yang didukung oleh meta-model tunggal, yang membantu pendeskripsian dan desain sistem perangkat lunak, khususnya sistem yang dibangun menggunakan pemrograman berorientasi objek (Wasserkrug et al., 2019).

Penggunaan model ini bertujuan untuk mengidentifikasi bagian-bagian yang termasuk dalam lingkup sistem yang dibahas dan bagaimana hubungan antara sistem dengan subsistem maupun sistem lain diluarnya (Sukmawati & Priyadi, 2019).

### **2.8.1 Use Case Diagram**

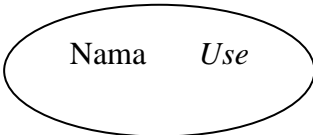
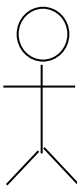

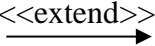
*Use Case Diagram* digunakan untuk menggambarkan sistem dari sudut pandang pengguna sistem tersebut (*user*). sehingga pembuatan *Use Case Diagram* lebih dititik beratkan pada fungsionalitas yang ada pada sistem, bukan berdasarkan alur atau urutan kejadian. Sebuah *Use Case Diagram* mempresentasikan sebuah interaksi antara aktor dengan sistem (Isa & Hartawan, 2017).

*Use Case Diagram* adalah deskripsi fungsi dari sebuah sistem dari perspektif pengguna. *Use Case Diagram* bekerja dengan cara mendeskripsikan tipikal interaksi antara *user* (pengguna) sebuah sistem dengan sistemnya sendiri

melalui sebuah cerita bagaimana sebuah sistem dipakai. Urutan langkah-langkah yang menerangkan antara pengguna dan sistem disebut skenario. Setiap skenario mendeskripsikan urutan kejadian. Setiap urutan diinisialisasi oleh orang, sistem yang lain, perangkat keras atau urutan waktu.

Sedangkan menurut Ade Hendini, *Use Case Diagram* merupakan pemodelan untuk kelakuan (*behavior*) sistem informasi yang akan dibuat. *Use case* digunakan untuk mengetahui fungsi apa saja yang ada di dalam sistem informasi dan siapa saja yang berhak menggunakan fungsi-fungsi tersebut (Hendini, 2016). Simbol-simbol yang digunakan dalam *Use Case Diagram* yaitu:

**Tabel 2.1 Simbol Use Case Diagram**

No	Simbol	Deskripsi
1	<p><i>Use case</i></p> 	Gambaran unit yang saling berkaitan antara aktor dengan sistem yang berjalan
2	<p>Aktor</p>  <p>Nama aktor</p>	Orang, proses atau sistem yang lain yang berinteraksi dengan sistem informasi yang akan dibuat.
3	<p>Asosiasi / <i>Association</i></p> 	Komunikasi antara aktor dan <i>use case</i> .
4	<p>Ekstensi / <i>Extend</i></p> 	Kelakuan yang hanya berjalan di bawah kondisi tertentu. Seperti jika akun sesuai, atau jika <i>session</i> sesuai.

5	Generalisasi →	Elemen yang menjadi spesialisasi elemen lain.
6	<i>Include</i> <<include>> →	Kelakuan yang harus terpenuhi agar suatu <i>event</i> dapat terjadi.


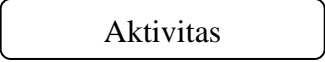
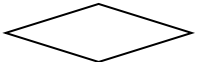

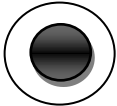
Sumber: (Hendini, 2016)

### 2.8.2 *Activity Diagram*

Menurut Indra Griha Tofik Isa dan George Pri Hartawan, *Activity Diagram* menggambarkan rangkaian aliran dari aktivitas, digunakan untuk mendeskripsikan aktivitas yang dibentuk dalam suatu operasi sehingga dapat juga digunakan untuk aktivitas lainnya. Diagram ini sangat mirip dengan flowchart karena memodelkan *workflow* dari suatu aktivitas ke aktivitas yang lainnya, atau dari aktivitas ke status. Pembuatan *Activity Diagram* pada awal pemodelan proses dapat membantu memahami keseluruhan proses. *Activity Diagram* juga digunakan untuk menggambarkan interaksi antara beberapa *use case* (Isa & Hartawan, 2017).

*Activity Diagram* adalah bagian penting dari *UML*, yang menggambarkan aspek dinamis dari sistem. logika prosedural, proses bisnis dan aliran kerja suatu bisnis bisa dengan mudah dideskripsikan dalam *Activity Diagram*. *Activity Diagram* mempunyai peran seperti halnya flowchart, akan tetapi perbedaannya dengan *flowchart* adalah *Activity Diagram* bisa mendukung perilaku paralel sedangkan *flowchart* tidak bisa (Kurniawan, 2018). *Activity Diagram* menggambarkan *workflow* (aliran kerja) atau aktivitas dari sebuah sistem atau proses bisnis. Simbol-simbol yang digunakan dalam *Activity Diagram* yaitu:

Tabel 2.2 Simbol *Activity Diagram*

No	Simbol	Deskripsi
1	Status awal 	Status awal aktivitas sistem, sebuah diagram aktivitas memiliki sebuah status awal.
2	Aktivitas 	Aktivitas yang dilakukan sistem, aktivitas biasanya diawali dengan kata kerja.
3	Percabangan / <i>decision</i> 	Asosiasi percabangan dimana jika ada aktivitas pilihan lebih dari satu.
4	Penggabungan / Join 	Asosiasi penggabungan dimana lebih dari satu aktivitas digabungkan menjadi satu.
5	Status Akhir 	Tahap akhir dari proses sistem.

Sumber: (Hendini, 2016)

## 2.9 Visual Basic.Net 2010

Bahasa Pemrograman *Microsoft Visual Basic .NET* adalah sebuah bahasa pemrograman tingkat tinggi untuk *Microsoft .NET Framework*. Walaupun *VB.NET* ini memang dibuat supaya mudah dipahami dan dipelajari, namun bahasa pemrograman ini juga cukup *powerful* untuk memenuhi kebutuhan dari

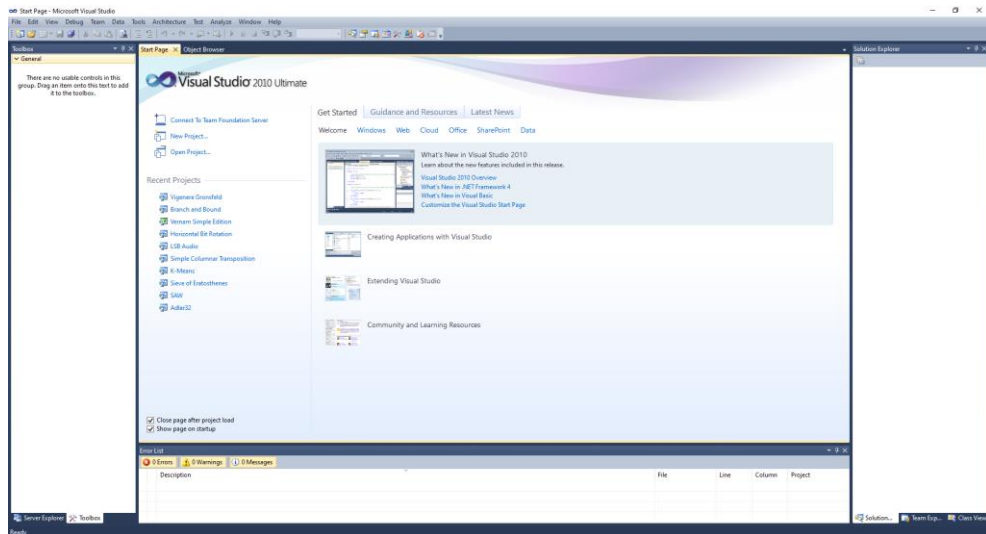
*programmer* yang berpengalaman. Bahasa pemrograman *Visual Basic .NET* mirip dengan bahasa pemrograman *Visual Basic*, namun keduanya tidak sama”.

Bahasa pemrograman *Visual Basic .NET* memiliki struktur penulisan yang mirip dengan bahasa Inggris, di mana hal ini juga menyebabkan kemudahan dalam membaca dan mengerti dari sebuah kode. Di mana dimungkinkan, kata ataupun frasa yang memiliki arti digunakan dan bukannya menggunakan singkatan, akronim ataupun *special characters*”.

Pada intinya *Visual Basic.NET* ini adalah sebuah bahasa pemrograman yang berorientasi pada *object*, yang bisa dianggap sebagai evolusi selanjutnya dari bahasa pemrograman *Visual Basic* standar (Wibowo, 2019).

### **2.9.1 Lingkungan kerja Visual Basic.Net 2010**

Pada saat pertama kali dijalankan Visual Basic 2010 Ultimate, akan menampilkan sebuah jendela Splash Visual Studio 2010 Ultimate, setelah jendela Splash Visual Studio 2010 Ultimate muncul kemudian akan keluar sebuah start page Microsoft Visual Studio seperti gambar 2.3.



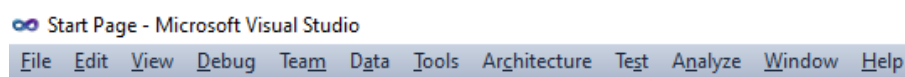
**Gambar 2.3 Tampilan Microsoft Visual Studio 2010**

## 2.9.2 Komponen Visual Basic.Net 2010

Pada saat membuka program Visual Basic.Net, ada beberapa komponen yang terlihat. Berikut ini adalah beberapa komponen dari Visual Basic.Net:

### 1. Menu Bar

*Menu Bar* adalah bagian dari *IDE* yang terdiri atas perintah-perintah untuk mengatur *IDE*, mengedit kode, dan mengeksekusi program. Menu yang terdapat pada menu bar adalah *menu file, edit, view, project, build, debug, data, tools, window* dan *help*. *Menu bar* pada *Visual Studio 2010* seperti terlihat pada gambar 2.5.

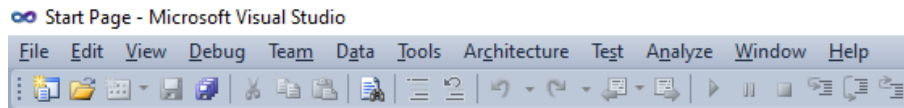


**Gambar 2.4 Tampilan Menu Bar**



## 2. *Toolbar*

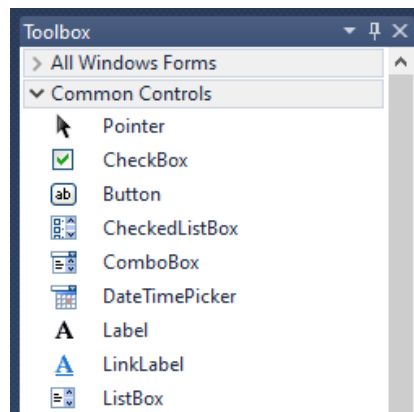
Fasilitas ini dapat mempercepat pengaksesan perintah-perintah yang ada dalam pemrograman seperti terlihat pada gambar 2.6.



**Gambar 2.5 Tampilan Toolbar**

## 3. *Toolbox*

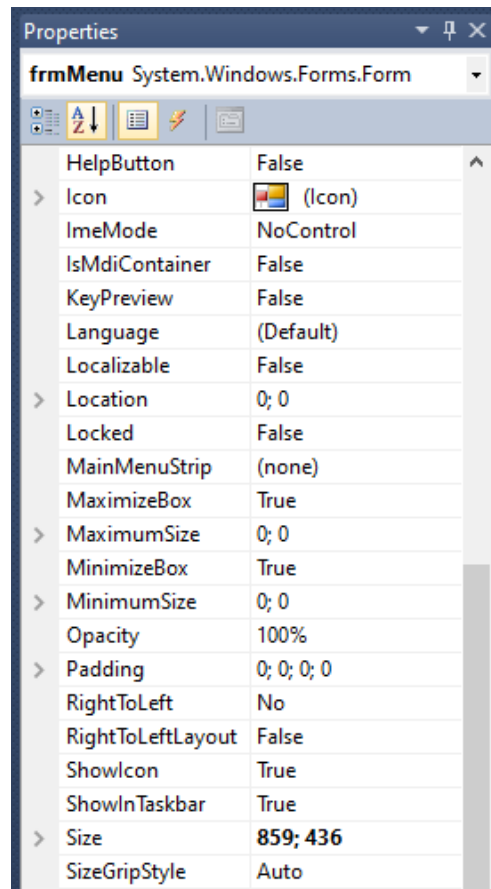
Sebuah *window* yang berisi tombol-tombol kontrol yang akan Anda gunakan untuk mendesain atau membangun sebuah *Form* atau *report* seperti terlihat pada gambar 2.7.



**Gambar 2.6 Tampilan Toolbox**

## 4. *Properties Window*

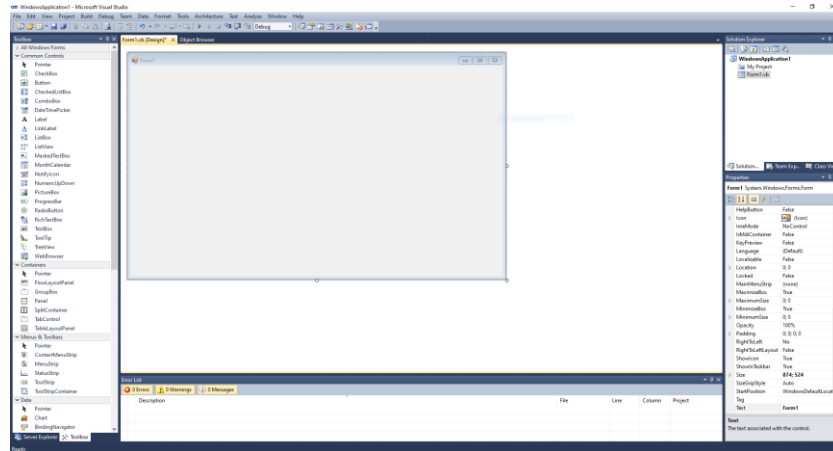
*Properties window* adalah tempat menyimpan *property* dari setiap objek control dan komponen.



**Gambar 2.7 Tampilan Properties**

## 5. *Form*

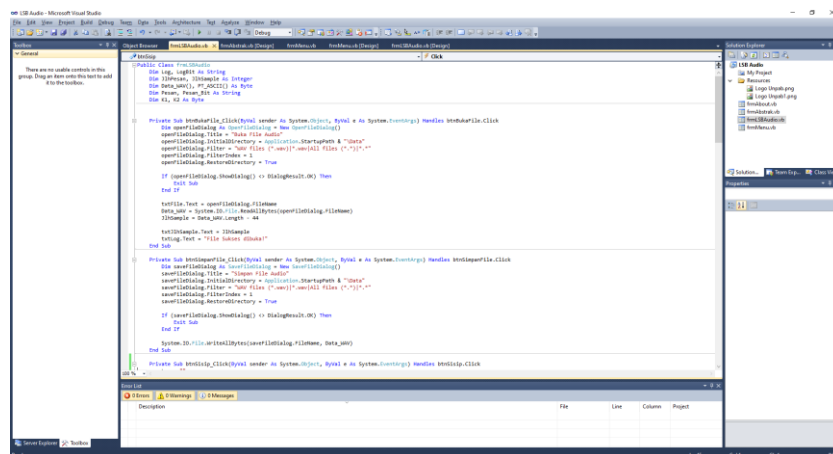
*Form* merupakan tempat di mana kontrol-kontrol diletakkan. *Form* juga berfungsi sebagai tempat pembuatan tampilan atau antarmuka (*user interface*) dari sebuah aplikasi *windows*.



**Gambar 2.8 Tampilan Form**

## 6. Code Editor

*Code Editor* adalah tempat di mana kita meletakkan atau menuliskan kode program dari program aplikasi kita.



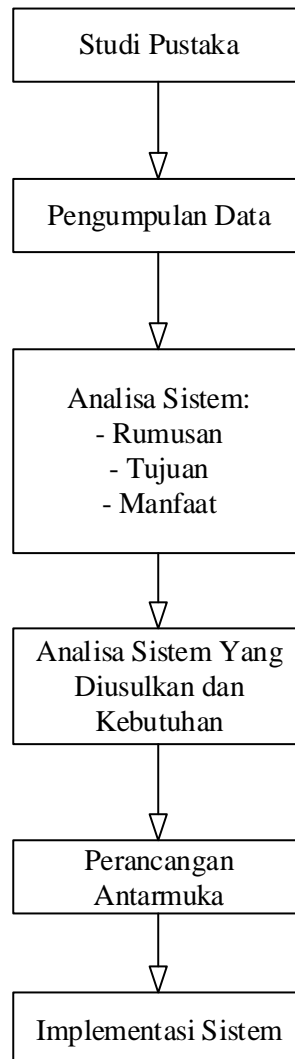
**Gambar 2.9 Tampilan Code Editor**

## **BAB III**

### **METODE PENELITIAN**

#### **1.1 Tahapan Penelitian**

Dalam melaksanakan penelitian, perlu diketahui bahwa tahapan penelitian adalah bersifat mutlak. Gambar 3.1 adalah tahapan penelitian pada tugas akhir ini.



**Gambar 3.1 Tahapan Penelitian**

Berikut merupakan penjelasan dari gambar tahapan penelitian yang ada di atas:

1. Studi pustaka, dalam skripsi ini penulis ambil dari beberapa sumber seperti jurnal, prosiding dan buku.
2. Pengumpulan data, dalam skripsi ini penulis mengumpulkan data dengan menggunakan beberapa teks untuk dijadikan input pada proses enkripsi.
3. Analisa sistem, masalah yang diangkat dalam skripsi adalah bagaimana cara kerja proses kriptografi satu arah.
4. Analisa sistem usulan, penulis akan membuat suatu sistem yang dapat digunakan dalam mengenkripsi dan mendekripsi pesan agar dapat terhindar dari pencurian data.
5. Analisa kebutuhan, untuk membuat sistem ini penulis membutuhkan beberapa perangkat keras dan perangkat lunak dalam mendukung proses pembuatan aplikasi.
6. Metode, metode algoritma yang penulis gunakan dalam penulisan skripsi ini adalah dengan teknik *Cipher Substitusi*.
7. Desain sistem, penulis memulai proses mendesain sistem dengan menggunakan *UML* agar terlihat alur proses enkripsi dan dekripsi.
8. Pembuatan sistem, penulis membuat sistem dengan menggunakan bahasa pemrograman Microsoft Visual Basic.NET 2010.
9. Implementasi dilakukan untuk menguji kebenaran program aplikasi yang telah dibuat.

## 1.2 Metode Pengumpulan Data

Metode pengumpulan data dilakukan untuk mendapatkan informasi tentang kebutuhan sistem. Metode ini dilakukan dengan beberapa cara antara lain:

1. Studi Pustaka

Pengumpulan data-data berupa teori mencari dan mengumpulkan bahan yang berhubungan dengan masalah yang sedang diteliti.

2. Studi Lapangan

Studi lapangan yaitu kegiatan terjun secara langsung ke lapangan dengan menggunakan teknik pengumpulan data.

3. Observasi

Observasi merupakan teknik yang digunakan untuk mengumpulkan data dengan cara melakukan pengamatan secara langsung terhadap cara kerja dari enkripsi dan dekripsi pada pengiriman pesan.

## 1.3 Analisa Sistem

Sitem yang dirancang diharapkan dapat memenuhi kebutuhan yang akan dicapai. Penelitian ini menggunakan teknik pergeseran karakter atau dapat disebut juga dengan kriptografi substitusi. Karakter yang akan dienkrip akan ditukan dengan karakter hasil enkripsi sehingga menghasilkan *Ciphertext*. Informasi ini diharapkan sudah aman dari penyalahgunaan yang dilakukan oleh pihak ketiga yang tidak bertanggung jawab. Penulis akan menciptakan program aplikasi yang dapat memenuhi tujuan dari penelitian ini.

### 3.1.1 Analisa Sistem Yang Berjalan

Proses pengiriman informasi tidak menggunakan teknik keamanan tertentu sehingga dapat dengan mudah diretas oleh orang yang ingin mencuri data tersebut untuk tujuan finansial atau tujuan lainnya. Informasi tersebut dengan bebas dapat diperoleh dengan menggunakan teknik-teknik tertentu sehingga pemilik data akan merasa dirugikan. Hal ini membuat informasi yang terkandung pada file yang dikirim dapat dengan mudah diambil oleh siapapun karena tidak memiliki sistem pengaman. Proses enkripsi sangat diperlukan dengan tujuan melindungi data tersebut.

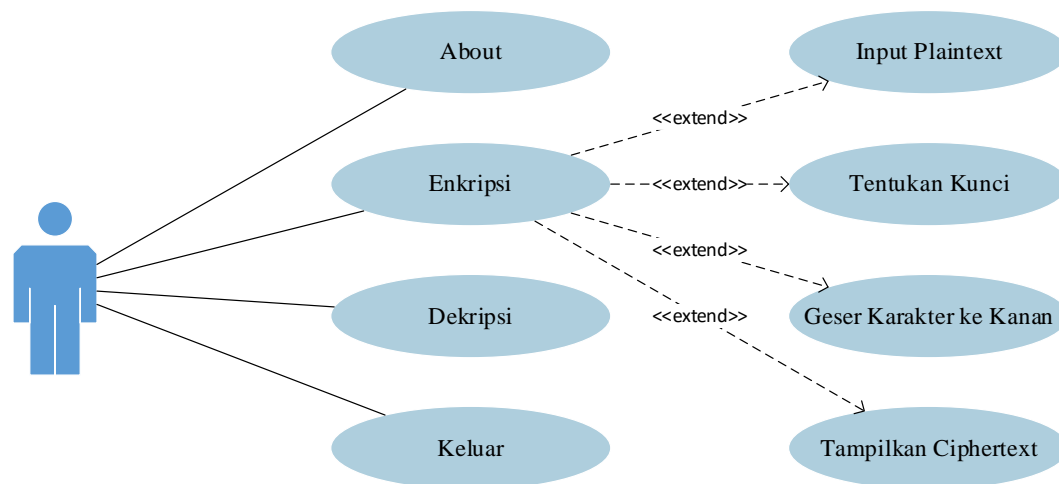
### 3.1.2 Analisa Sistem Yang Diusulkan

Penulis mengusulkan suatu sistem yang dapat menjaga kerahasiaan informasi. Sistem ini menggunakan teknik kriptografi substitusi dengan menggunakan teknik *Cipher Substitusi*. Program aplikasi akan melakukan enkripsi dan dekripsi untuk informasi tersebut melalui perantara *textbox* yang berisi *plaintext* yang akan diproses. Teknik *Cipher Substitusi* akan mengenkripsi karakter demi karakter dari informasi yang telah dimasukkan pada *textbox* sehingga pesan tersebut berubah menjadi pesan terenkripsi atau *Ciphertext*. Pengguna juga dapat melihat hasil enkripsi yang sudah dilakukan pada *textbox Ciphertext* sehingga pengguna juga dapat mengetahui hasil dan cara kerja dari teknik *Cipher Substitusi* tersebut.

## 3.2 Rancangan UML

### 3.2.1 Use Case Diagram Enkripsi

Berikut ini adalah *Use Case Diagram* yang digunakan dalam melakukan proses enkripsi pesan.



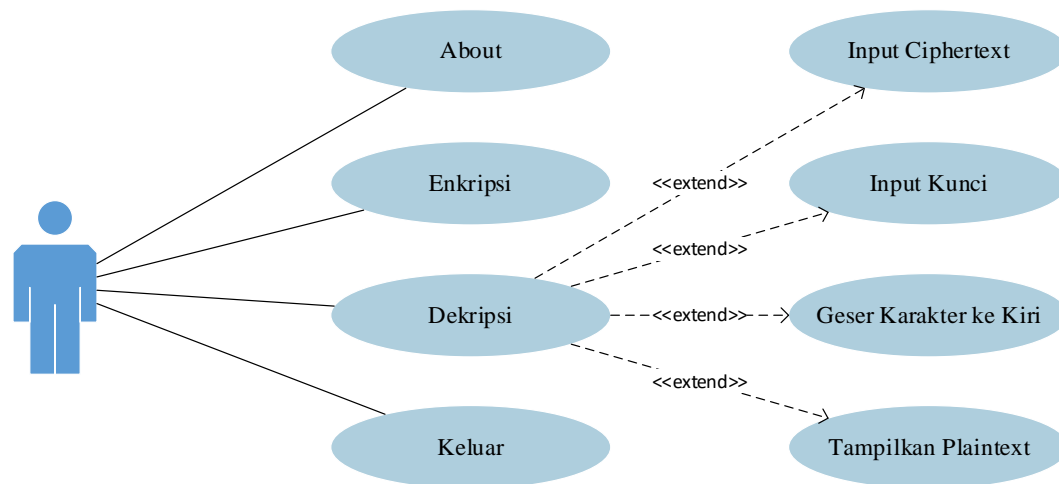
**Gambar 3.2 Use Case Diagram Enkripsi**

Gambar 3.2 menunjukkan *Use Case Diagram* enkripsi. Pada diagram ini, hal yang utama dilakukan oleh pengguna adalah pengguna dapat memasukkan pesan pada *textbox* yang sudah tersedia. Selanjutnya pengguna menentukan kunci pergeseran pada *textbox* kunci. Program aplikasi akan melakukan enkripsi pesan tersebut dengan menggunakan teknik *Cipher Substitusi* ketika tombol enkripsi ditekan. Setelah proses enkripsi dilakukan, *Ciphertext* hasil enkripsi akan ditampilkan pada *textbox* yang sudah ditentukan sebelumnya.



### 3.2.2 Use Case Diagram Dekripsi

Berikut ini adalah *Use Case Diagram* yang digunakan dalam melakukan proses dekripsi pesan.

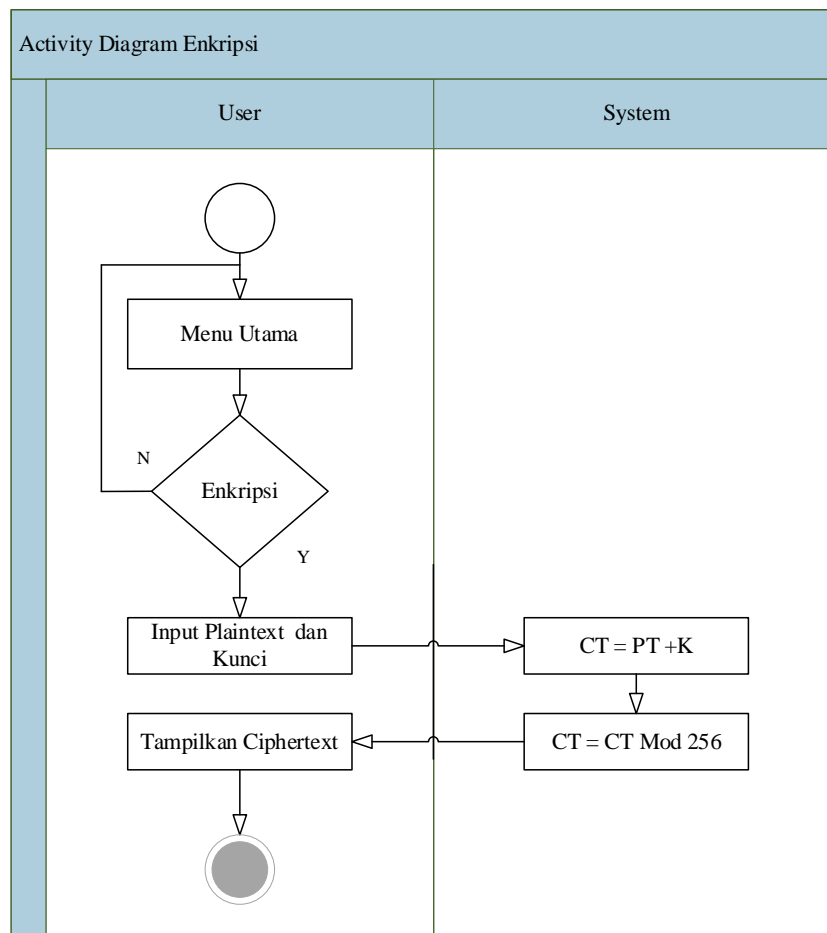


**Gambar 3.3 Use Case Diagram Dekripsi**

Gambar 3.3 menunjukkan *Use Case Diagram* dekripsi. Pada *Use Case Diagram* dekripsi tersebut, tahap awal yang harus dilakukan oleh pengguna adalah memasukkan *Ciphertext* yang sudah diperoleh sebelumnya pada proses enkripsi. Pengguna juga memasukkan kunci untuk menentukan seberapa besar karakter akan digeser. Proses dekripsi dilakukan dengan cara menekan tombol dekripsi pada tombol yang sudah tersedia. Dekripsi dilakukan dengan menggeser *Ciphertext* ke arah kiri sehingga menghasilkan *plaintext*. Hasil dekripsi merupakan *plaintext* yang akan diletakkan pada *textbox* yang tersedia. Hasil *plaintext* harus sesuai dengan pesan yang sebelumnya akan dienkripsi.

### 3.2.3 Activity Diagram Enkripsi

Berikut ini adalah *Activity Diagram* proses enkripsi.

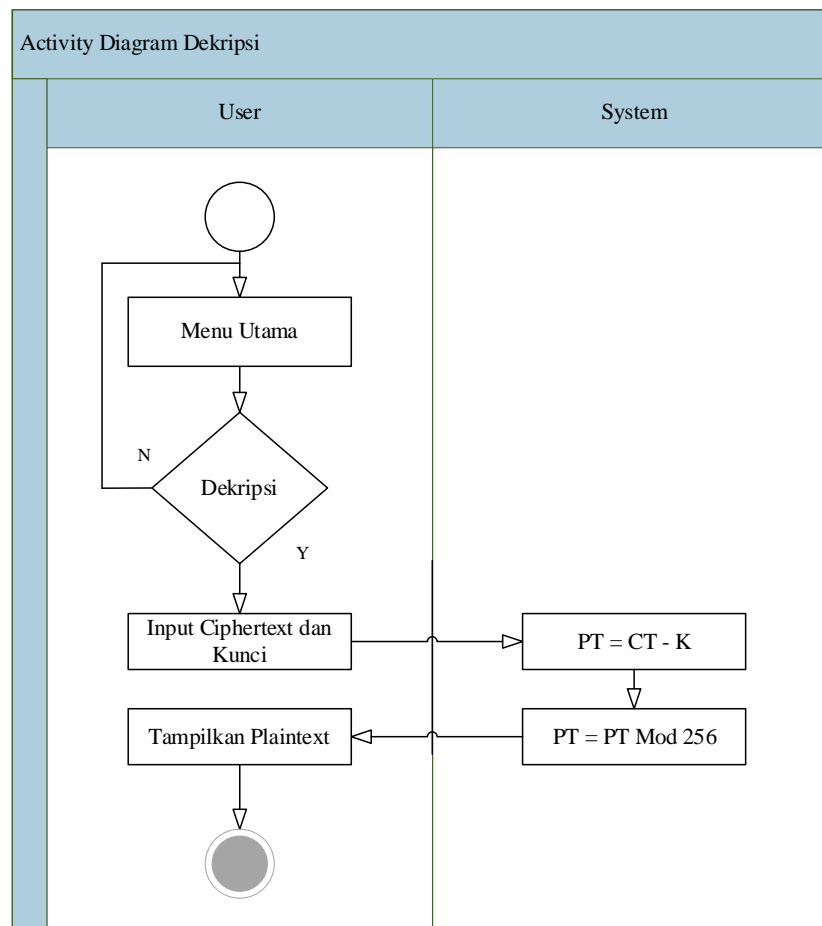


**Gambar 3.4 Activity Diagram Enkripsi**

Gambar 3.4 merupakan rancangan *Activity Diagram* enkripsi pesan dengan menggunakan teknik pergeseran ke kanan. Pada *Activity Diagram* enkripsi, pengguna akan menginputkan pesan dan kunci yang digunakan untuk proses enkripsi. Sistem akan memproses *plaintext* hingga menghasilkan *Ciphertext*.

### 3.2.4 Activity Diagram Dekripsi

Berikut ini adalah *Activity Diagram* proses dekripsi.

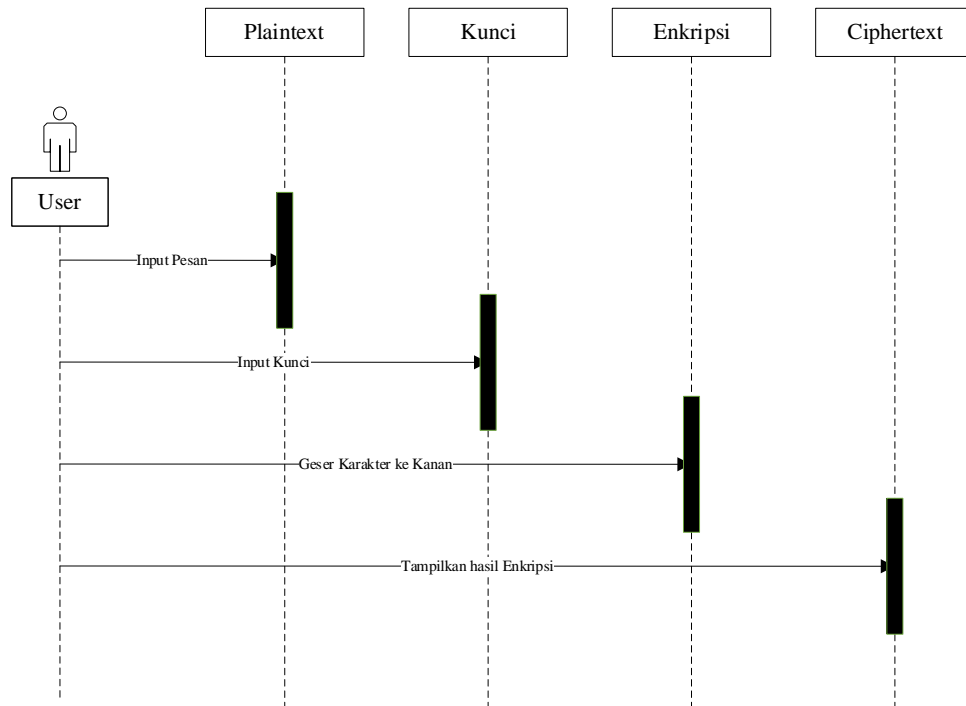


**Gambar 3.5 Activity Diagram Dekripsi**

Gambar 3.5 ini merupakan rancangan *Activity Diagram* dekripsi video dengan menggunakan teknik pergeseran ke kiri. Pada *Activity Diagram* dekripsi, pengguna memasukkan *Ciphertext* dan kunci. Sistem akan memproses dekripsi dan akan menghasilkan *plaintext*.

### 3.2.5 *Sequence Diagram* Enkripsi

Berikut ini adalah *Sequence Diagram* proses enkripsi yang menjelaskan alur dari proses enkripsi menggunakan teknik pergeseran ke kanan.

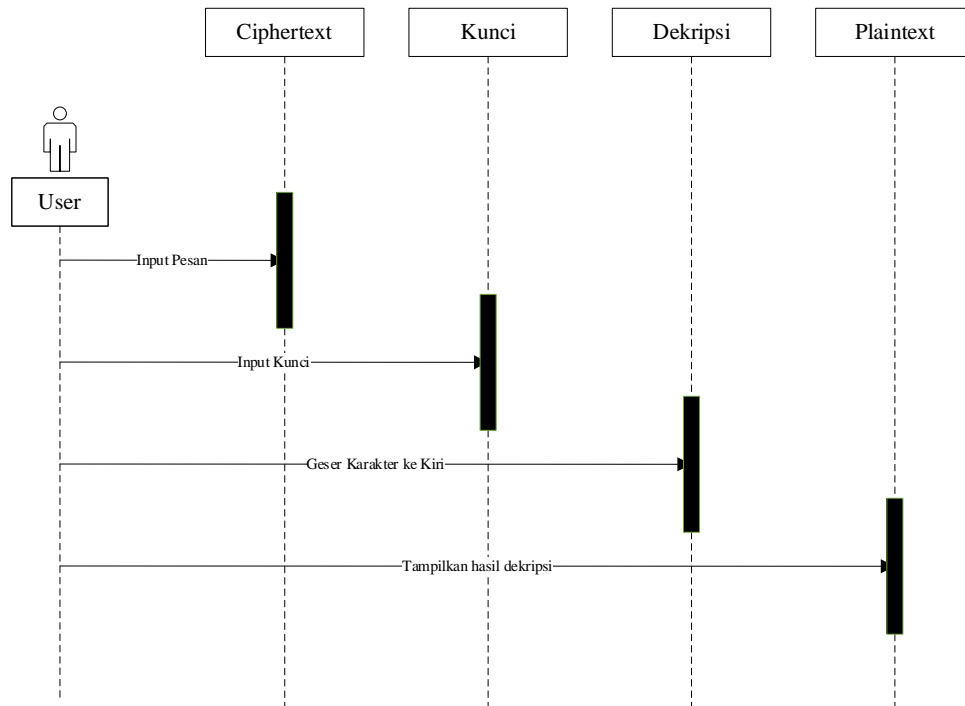


**Gambar 3.6** *Sequence Diagram* Enkripsi

Gambar 3.6 merupakan rancangan *Sequence Diagram* enkripsi. Pada *Sequence Diagram* enkripsi, terdapat empat tahap yang akan dilalui oleh pengguna yaitu memasukkan *plaintext*, memasukkan kunci, melakukan proses enkripsi, dan menampilkan hasil enkripsi. Setelah melakukan proses enkripsi, pengguna akan menunggu beberapa hingga hasil enkripsi dapat dilihat hasil pada *textbox* yang telah ditentukan.

### 3.2.6 *Sequence Diagram* Dekripsi

Berikut ini adalah *Sequence Diagram* proses dekripsi yang menjelaskan alur dari proses dekripsi menggunakan pergeseran karakter ke kiri.



**Gambar 3.7** *Sequence Diagram* Dekripsi

Gambar 3.7 merupakan rancangan *Sequence Diagram* dari proses dekripsi pesan menggunakan pergeseran karakter ke kiri. Pada *Sequence Diagram* tersebut, pengguna akan memasukkan *Ciphertext* hasil enkripsi sebelumnya dan kunci pergeseran. Proses dekripsi akan dilakukan dengan menekan tombol dekripsi. Hasil dekripsi yaitu *plaintext* yang sama persis dengan pesan sebelumnya.

### 3.3 Analisis Cipher Substitusi

Teknik *Cipher Substitusi* adalah teknik kriptografi yang bekerja dengan cara menggeser atau menukar posisi karakter dengan kunci yang berbentuk pergeseran posisi. Semua karakter yang diproses adalah berdasarkan karakter yang terdaftar pada tabel *ASCII*. Jumlah pergeseran dapat dilakukan dengan angka berapa saja. Apabila hasil perhitungan enkripsi lebih besar dari 256 atau perhitungan dekripsi lebih kecil dari 0, karakter tersebut harus dilakukan proses modulo agar karakter tetap berada pada rentang 0 – 255 sesuai dengan tabel *ASCII*.

Contoh:

$$\begin{aligned} \text{PT} &= \text{B} \\ \text{ASCII} &= 66 \\ \text{Kunci} &= 7 \\ \text{CT} &= 66 + 7 \\ &= 73 \\ &= \text{I} \end{aligned}$$

$$\begin{aligned} \text{PT} &= \text{A} \\ \text{ASCII} &= 65 \\ \text{Kunci} &= 6 \\ \text{CT} &= 65 + 6 \\ &= 71 \\ &= \text{G} \end{aligned}$$

$$\begin{aligned} \text{PT} &= \text{N} \\ \text{ASCII} &= 78 \\ \text{Kunci} &= 1 \\ \text{CT} &= 78 + 1 \\ &= 79 \\ &= \text{O} \end{aligned}$$

### 3.4 Perancangan Antarmuka

Perancangan antar muka merupakan sketsa dari tampilan aplikasi yang akan dibuat pada program aplikasi.

#### 3.4.1 Desain Antarmuka Judul

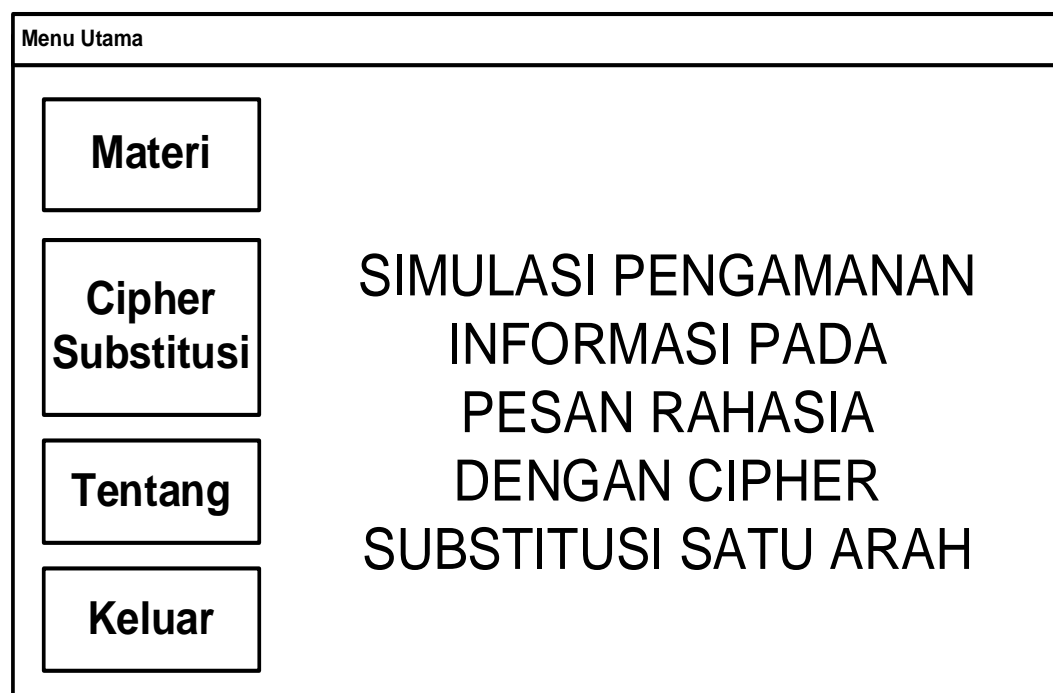
Desain antarmuka judul adalah tampilan yang digunakan pada saat program aplikasi dieksekusi. Gambar. 3.8 adalah hasil perancangan judul.



**Gambar 3.8 Desain Antarmuka Judul**

### 3.4.2 Desain Antarmuka Menu Utama

Desain antarmuka menu utama adalah tampilan yang menentukan pengguna akan menuju ke menu selanjutnya. Menu ini terdiri dari beberapa pilihan tombol eksekusi. Gambar 3.8 adalah hasil perancangan menu utama.



**Gambar 3.9** Desain Antarmuka Menu Utama

Tampilan ini memiliki berapa sub-menu antara lain:

- Materi
- *Cipher Substitusi*
- Tentang
- Keluar



### 3.4.3 Desain Antarmuka *Cipher Substitusi*

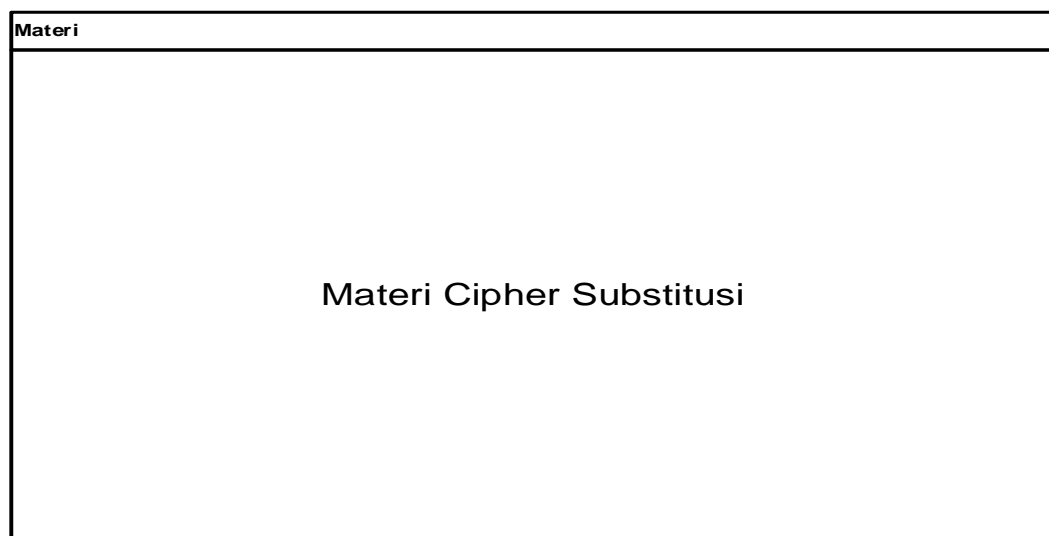
Desain antarmuka *Cipher Substitusi* dapat dilihat pada Gambar 3.10. Tampilan ini menyediakan tombol-tombol yang berfungsi untuk memproses perhitungan enkripsi dan dekripsi. Bagian ini bertujuan untuk mengkonversi informasi menjadi pesan tidak terpahami. Pada tampilan ini disediakan juga log sebagai perhitungan manual untuk mengetahui proses transformasi *plaintext* menjadi *ciphertext*.

The wireframe for the *Cipher Substitusi* interface is enclosed in a rectangular border. At the top left, the title "Cipher Substitusi" is displayed. The interface is divided into two main vertical sections. The left section contains four input fields: "Plaintext" (a large rectangular box), "Kunci" (a smaller rectangular box), "Hasil Enkripsi" (a large rectangular box), and "Hasil Dekripsi" (a large rectangular box). Between the "Kunci" and "Hasil Enkripsi" fields is a button labeled "Enkrip". Between the "Hasil Enkripsi" and "Hasil Dekripsi" fields is a button labeled "Dekrip". The right section is a large, empty rectangular area labeled "Riwayat Perhitungan" at the top, intended for displaying calculation logs.

Gambar 3.10 Desain Antarmuka *Cipher Substitusi*

#### 3.4.4 Desain Antarmuka Materi

Gambar 3.11 merupakan rancangan tampilan materi yang akan menjelaskan pengertian dari *cipher* substitusi dan bagaimana cipher tersebut menggunakan teknik *Cipher Substitusi* untuk mengolah plaintext menjadi ciphertext.



**Gambar 3.11 Desain Antarmuka Materi**

#### 3.4.5 Desain Antarmuka Tentang

Gambar 3.12 merupakan rancangan tampilan tentang penulis. Tampilan ini menunjukkan biodata penulis, antara lain:

1. Nama
2. NPM
3. Fakultas
4. Universitas



**Gambar 3.12 Desain Antarmuka Tentang**

## **BAB IV**

### **HASIL DAN PEMBAHASAN**

#### **1.1 Kebutuhan Perangkat Keras dan Lunak**

Kebutuhan perangkat keras dan lunak sangat mendukung dalam menjalankan program aplikasi yang telah diciptakan sebelumnya. Berikut ini adalah kebutuhan perangkat-perangkat tersebut:

##### *1. Hardware (Perangkat Keras)*

Untuk menjalankan sistem ini, penulis menggunakan laptop dengan spesifikasi RAM 4GB, Processor Intel Core i3, Hard drive 500GB dan Display 14”.

##### *2. Software (Perangkat Lunak)*

Sedangkan pada sisi *software*, penulis menggunakan beberapa perangkat lunak yaitu:

- a. Windows 7
- b. Microsoft Visual Studio 2010
- c. Microsoft Word 2019
- d. Microsoft Excel 2019
- e. Microsoft Visio 2019
- f. Snipping Tool

## 1.2 Implementasi Program Aplikasi

Implementasi program aplikasi akan melihat bagaimana hasil perancangan sistem diterapkan pada pembuatan program aplikasi. Program aplikasi terdiri dari beberapa menu yang dapat diakses satu-persatu sesuai dengan keinginan pengguna. Berikut merupakan hasil tampilan dari program aplikasi yang telah dibuat oleh penulis tentang teknik *Cipher Substitusi*.

### 1.2.1 Tampilan Halaman Judul

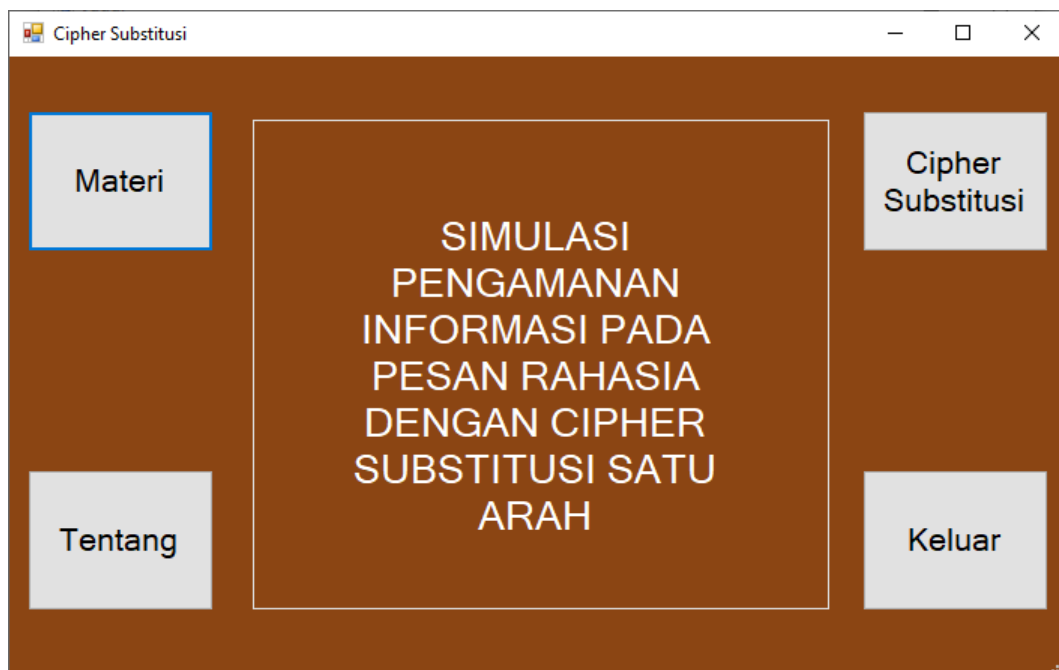
Halaman judul adalah halaman yang pertama sekali muncul ketika program aplikasi dijalankan. Gambar 4.1 adalah hasil tampilan halaman judul.



Gambar 4.1 Halaman Judul

### 1.2.2 Tampilan Halaman Menu Utama

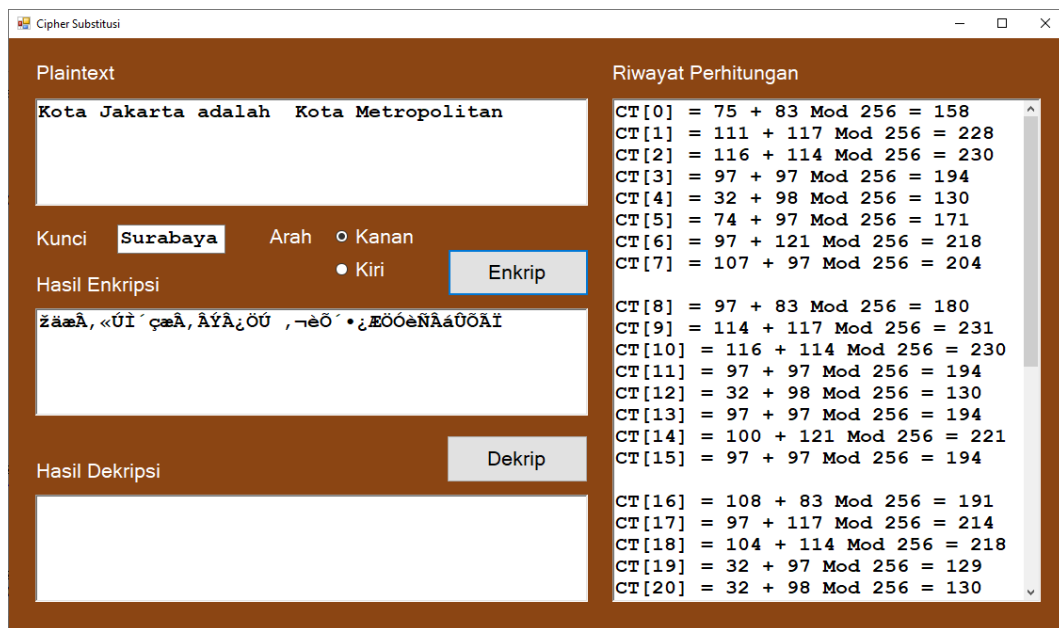
Halaman menu utama merupakan halaman utama sebuah program aplikasi dimana pengguna dapat melakukan mengakses menu-menu yang ada di dalamnya. Gambar 4.2 adalah hasil tampilan menu utama.



**Gambar 4.2 Halaman Menu Utama**

### 1.2.3 Tampilan Halaman Enkripsi

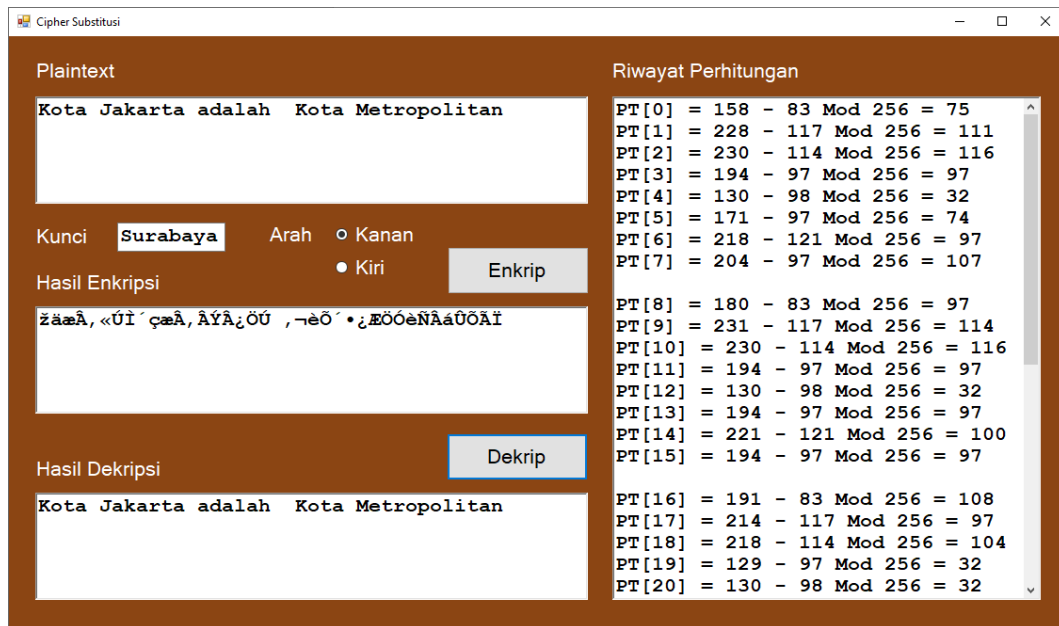
Gambar 4.3 merupakan tampilan dari halaman enkripsi pesan dengan teknik *Cipher Substitusi*. Pengguna dapat memasukkan langsung pesan pada *textbox* yang *plaintext*. Pengguna menentukan kunci dengan mengetikkan pada *textbox* kunci dan menentukan arah enkripsi apakah ke kanan atau ke kiri. Hasil *Ciphertext* dapat dilihat pada *textbox Ciphertext*.



**Gambar 4.3 Halaman Enkripsi**

#### 1.2.4 Tampilan Halaman Dekripsi

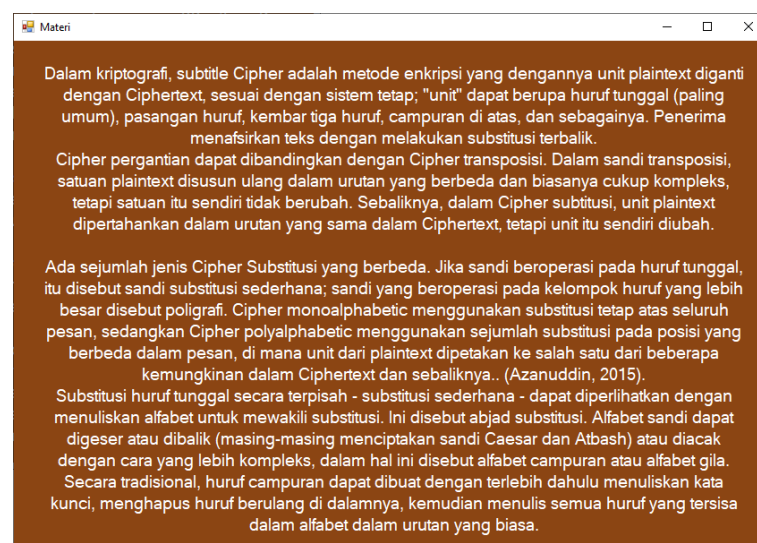
Hasil dekripsi dapat dilihat pada gambar 4.4. Gambar ini menjelaskan proses pengembalian *ciphertext* menjadi *plaintext*. Pada proses ini, pengguna menginputkan kembali *Ciphertext* pada hasil enkripsi atau dapat menggunakan dengan karakter yang telah dihasilkan pada proses enkripsi sebelumnya. Kunci dan arah dekripsi yang digunakan harus sesuai dengan yang digunakan pada proses enkripsi. Hasil *plaintext* dapat dilihat ketika tombol dekrip ditekan. Hasil dekripsi akan tampil pada *textbox* dekripsi. Riwayat perhitungan juga dapat dilihat pada *textbox* log untuk mengetahui proses dekripsi tersebut.



**Gambar 4.4 Halaman Dekripsi**

### 1.2.5 Halaman Materi

Gambar 4.5 adalah tampilan dari halaman materi yang menjelaskan secara singkat tentang teknik *Cipher Substitusi*.

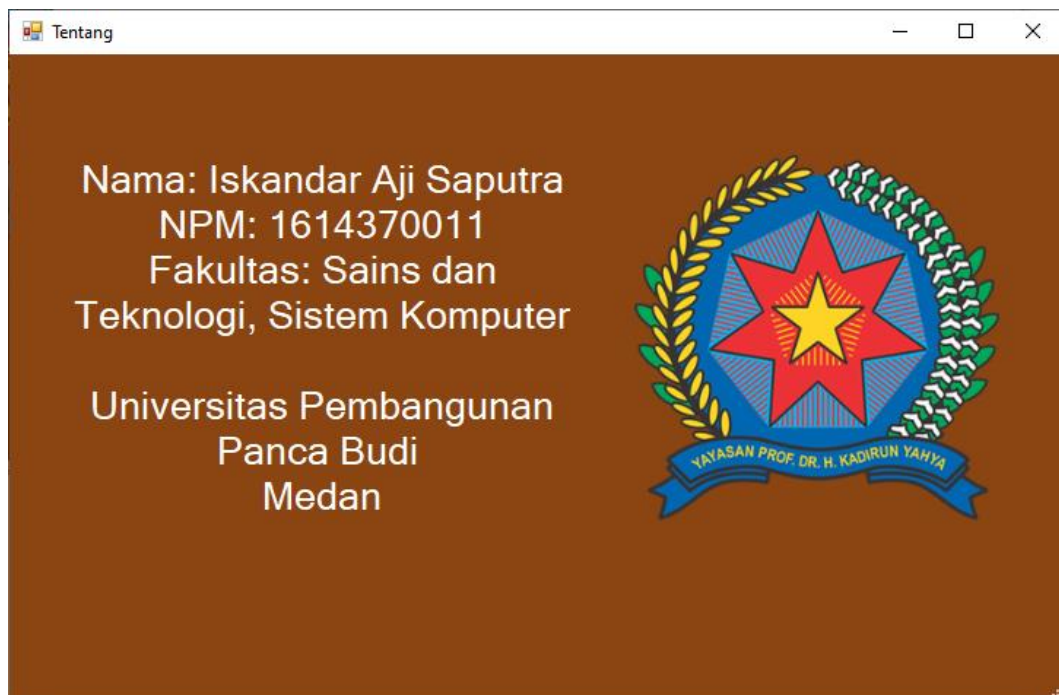


**Gambar 4.5 Halaman Materi**



### 1.2.6 Halaman Tentang

Gambar 4.6 merupakan tampilan dari halaman tentang aplikasi. Pada tampilan ini nantinya pengguna dapat melihat secara singkat biodata penulis.



**Gambar 4.6 Halaman Tentang**

### 1.3 Perhitungan Manual

Perhitungan manual dilakukan bertujuan untuk membuktikan hasil program aplikasi apakah telah sesuai seperti yang diinginkan sehingga menghindari kesalahan dalam melakukan proses enkripsi dan dekripsi. Perhitungan ini akan menghitung secara matematika proses enkripsi dan proses dekripsi pada teknik *Cipher Substitusi* tersebut. Perhitungan lengkap proses enkripsi dan dekripsi dengan teknik *Cipher Substitusi* dapat dilakukan perhitungan manual sebagai berikut:

Pesan (*Plaintext*) : Kota Jakarta adalah Kota Metropolitan

Kunci : Surabaya

Arah : Kanan

Hasil Enkripsi : žäæÂ,«ÚÌ'çæÂ,ÂÝÂ¿ÖÚ• , -èÕ'¿ÆÖÓèÑÂáÛÕÃĪ

### Perhitungan Manual:

$CT[0] = 75 + 83 \text{ Mod } 256 = 158$   
 $CT[1] = 111 + 117 \text{ Mod } 256 = 228$   
 $CT[2] = 116 + 114 \text{ Mod } 256 = 230$   
 $CT[3] = 97 + 97 \text{ Mod } 256 = 194$   
 $CT[4] = 32 + 98 \text{ Mod } 256 = 130$   
 $CT[5] = 74 + 97 \text{ Mod } 256 = 171$   
 $CT[6] = 97 + 121 \text{ Mod } 256 = 218$   
 $CT[7] = 107 + 97 \text{ Mod } 256 = 204$

$CT[8] = 97 + 83 \text{ Mod } 256 = 180$   
 $CT[9] = 114 + 117 \text{ Mod } 256 = 231$   
 $CT[10] = 116 + 114 \text{ Mod } 256 = 230$   
 $CT[11] = 97 + 97 \text{ Mod } 256 = 194$   
 $CT[12] = 32 + 98 \text{ Mod } 256 = 130$   
 $CT[13] = 97 + 97 \text{ Mod } 256 = 194$   
 $CT[14] = 100 + 121 \text{ Mod } 256 = 221$   
 $CT[15] = 97 + 97 \text{ Mod } 256 = 194$

$CT[16] = 108 + 83 \text{ Mod } 256 = 191$   
 $CT[17] = 97 + 117 \text{ Mod } 256 = 214$   
 $CT[18] = 104 + 114 \text{ Mod } 256 = 218$   
 $CT[19] = 32 + 97 \text{ Mod } 256 = 129$   
 $CT[20] = 32 + 98 \text{ Mod } 256 = 130$   
 $CT[21] = 75 + 97 \text{ Mod } 256 = 172$   
 $CT[22] = 111 + 121 \text{ Mod } 256 = 232$   
 $CT[23] = 116 + 97 \text{ Mod } 256 = 213$

$CT[24] = 97 + 83 \text{ Mod } 256 = 180$   
 $CT[25] = 32 + 117 \text{ Mod } 256 = 149$   
 $CT[26] = 77 + 114 \text{ Mod } 256 = 191$   
 $CT[27] = 101 + 97 \text{ Mod } 256 = 198$   
 $CT[28] = 116 + 98 \text{ Mod } 256 = 214$   
 $CT[29] = 114 + 97 \text{ Mod } 256 = 211$   
 $CT[30] = 111 + 121 \text{ Mod } 256 = 232$   
 $CT[31] = 112 + 97 \text{ Mod } 256 = 209$

$CT[32] = 111 + 83 \text{ Mod } 256 = 194$   
 $CT[33] = 108 + 117 \text{ Mod } 256 = 225$

$$\begin{aligned} \text{CT}[34] &= 105 + 114 \text{ Mod } 256 = 219 \\ \text{CT}[35] &= 116 + 97 \text{ Mod } 256 = 213 \\ \text{CT}[36] &= 97 + 98 \text{ Mod } 256 = 195 \\ \text{CT}[37] &= 110 + 97 \text{ Mod } 256 = 207 \end{aligned}$$

Hasil perhitungan enkripsi dengan metode *Cipher Substitusi* dapat dilakukan perhitungan manual sebagai berikut:

Pesan (*Ciphertext*) : žäæÂ,«ÚÌ'çæÂ,ÂÝÂ¿ÖÚ• , -èÕ'•¿ÆÖÓèÑÂáÛÖÃĪ

Kunci : Surabaya

Arah : Kanan

Hasil Dekripsi : Kota Jakarta adalah Kota Metropolitan

#### Perhitungan Manual:

$$\begin{aligned} \text{PT}[0] &= 158 - 83 \text{ Mod } 256 = 75 \\ \text{PT}[1] &= 228 - 117 \text{ Mod } 256 = 111 \\ \text{PT}[2] &= 230 - 114 \text{ Mod } 256 = 116 \\ \text{PT}[3] &= 194 - 97 \text{ Mod } 256 = 97 \\ \text{PT}[4] &= 130 - 98 \text{ Mod } 256 = 32 \\ \text{PT}[5] &= 171 - 97 \text{ Mod } 256 = 74 \\ \text{PT}[6] &= 218 - 121 \text{ Mod } 256 = 97 \\ \text{PT}[7] &= 204 - 97 \text{ Mod } 256 = 107 \\ \\ \text{PT}[8] &= 180 - 83 \text{ Mod } 256 = 97 \\ \text{PT}[9] &= 231 - 117 \text{ Mod } 256 = 114 \\ \text{PT}[10] &= 230 - 114 \text{ Mod } 256 = 116 \\ \text{PT}[11] &= 194 - 97 \text{ Mod } 256 = 97 \\ \text{PT}[12] &= 130 - 98 \text{ Mod } 256 = 32 \\ \text{PT}[13] &= 194 - 97 \text{ Mod } 256 = 97 \\ \text{PT}[14] &= 221 - 121 \text{ Mod } 256 = 100 \\ \text{PT}[15] &= 194 - 97 \text{ Mod } 256 = 97 \\ \\ \text{PT}[16] &= 191 - 83 \text{ Mod } 256 = 108 \\ \text{PT}[17] &= 214 - 117 \text{ Mod } 256 = 97 \\ \text{PT}[18] &= 218 - 114 \text{ Mod } 256 = 104 \\ \text{PT}[19] &= 129 - 97 \text{ Mod } 256 = 32 \end{aligned}$$

PT[20] = 130 - 98 Mod 256 = 32  
PT[21] = 172 - 97 Mod 256 = 75  
PT[22] = 232 - 121 Mod 256 = 111  
PT[23] = 213 - 97 Mod 256 = 116

PT[24] = 180 - 83 Mod 256 = 97  
PT[25] = 149 - 117 Mod 256 = 32  
PT[26] = 191 - 114 Mod 256 = 77  
PT[27] = 198 - 97 Mod 256 = 101  
PT[28] = 214 - 98 Mod 256 = 116  
PT[29] = 211 - 97 Mod 256 = 114  
PT[30] = 232 - 121 Mod 256 = 111  
PT[31] = 209 - 97 Mod 256 = 112

PT[32] = 194 - 83 Mod 256 = 111  
PT[33] = 225 - 117 Mod 256 = 108  
PT[34] = 219 - 114 Mod 256 = 105  
PT[35] = 213 - 97 Mod 256 = 116  
PT[36] = 195 - 98 Mod 256 = 97  
PT[37] = 207 - 97 Mod 256 = 110

## **BAB V**

### **PENUTUP**

#### **5.1 Kesimpulan**

Berikut merupakan kesimpulan yang penulis buat berdasarkan pembahasan pada implementasi dan penggunaan teknik *Cipher Substitusi*:

1. *Cipher Substitusi* bekerja dengan cara melakukan pertukaran karakter *plaintext* dengan hasil perhitungan proses enkripsi.
2. *Cipher Substitusi* menggunakan kunci huruf dan angka maksimal 10 karakter.
3. Sistem enkripsi ini menggunakan metode enkripsi dan dekripsi dengan teknik dapat bekerja dengan baik.
4. Arah yang dapat digunakan adalah arah kanan dan kiri dalam melakukan proses enkripsi dan dekripsi.

#### **5.2 Saran**

Berikut merupakan saran yang penulis paparkan berdasarkan pembahasan dalam implementasi dan penggunaan teknik *Cipher Substitusi*:

1. Program aplikasi masih berbasis desktop, hendaknya sistem dapat dibuat berbasis *web* dan dapat diakses secara *online*.
2. Hendaknya kunci dapat diperluas lebih dari 10 karakter.
3. Hendaknya dapat dikembangkan menjadi dua arah.

4. Hendaknya proses enkripsi dan dekripsi dapat dilakukan dengan jumlah karakter yang lebih besar dari 1000.

## DAFTAR PUSTAKA

- Amin, M. M. (2016). Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks. *Jurnal Pseudocode*, 3(2).
- Apriadi, D. (2016). Kriptografi Kunci Simetris Caesar Chiper. Retrieved October 1, 2018, from <https://dodi-apriadi.blogspot.com/2016/02/kriptografi-kunci-simetris-Caesar.html>
- Ayushi, M. (2010). A Symmetric Key Cryptographic Algorithm. *International Journal of Computer Applications*, 1(15), 1–6. <https://doi.org/10.5120/331-502>
- Barone, L., Williams, J., & Micklos, D. (2017). Unmet needs for analyzing biological big data: A survey of 704 NSF principal investigators. *PLOS Computational Biology*, 13(10), e1005755. <https://doi.org/10.1371/journal.pcbi.1005755>
- Hendini, A. (2016). Pemodelan UML Sistem Informasi Monitoring Penjualan Dan Stok Barang. *Jurnal Khatulistiwa Informatika*, 4(2), 107–116. <https://doi.org/10.31294/jki.v4i2.1262.g1027>
- Isa, I. G. T., & Hartawan, G. P. (2017). Perancangan Aplikasi Koperasi Simpan Pinjam Berbasis Web (Studi Kasus Koperasi Mitra Setia). *Jurnal Ilmiah Ilmu Ekonomi (Jurnal Akuntansi, Pajak Dan Manajemen)*, 5(10), 139–151.
- Jogiyanto, H. M. (2016). *Analisis Dan Desain Sistem Informasi, Pendekatan Terstruktur Teori Dan Praktek Aplikasi Bisnis*. Yogyakarta: Andi Offset.
- Kurniawan, T. A. (2018). Pemodelan Use Case (UML): Evaluasi Terhadap beberapa Kesalahan dalam Praktik. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, 5(1), 77. <https://doi.org/10.25126/jtiik.201851610>
- Mallu, S. (2015). Sistem Pendukung Keputusan Penentuan Karyawan Kontrak Menjadi Karyawan Teatap Menggunakan Metode TOPSIS. *Jurnal Imliah Teknologi Informasi Terapan*, 1(2), 36–42.
- Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2015). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer*, 10, 22. <https://doi.org/10.30872/jim.v10i1.23>
- Badawi, A. (2018). Evaluasi Pengaruh Modifikasi Three Pass Protocol Terhadap Transmisi Kunci Enkripsi.
- Batubara, Supina. "Analisis perbandingan metode fuzzy mamdani dan fuzzy sugeno untuk penentuan kualitas cor beton instan." *IT Journal Research and Development* 2.1 (2017): 1-11.

- Bahri, S. (2018). *Metodologi Penelitian Bisnis Lengkap Dengan Teknik Pengolahan Data SPSS*. Penerbit Andi (Anggota Ikapi). Percetakan Andi Ofset. Yogyakarta.
- Diantoro, M., Maftuha, D., Suprayogi, T., Iqbal, M. R., Mufti, N., Taufiq, A., ... & Hidayat, R. (2019). Performance of *Pterocarpus Indicus* Willd Leaf Extract as Natural Dye TiO<sub>2</sub>-Dye/ITO DSSC. *Materials Today: Proceedings*, 17, 1268-1276.
- Erika, Winda, Heni Rachmawati, and Ibnu Surya. "Enkripsi Teks Surat Elektronik (E-Mail) Berbasis Algoritma Rivest Shamir Adleman (RSA)." *Jurnal Aksara Komputer Terapan* 1.2 (2012).
- Fitriani, W., Rahim, R., Oktaviana, B., & Siahaan, A. P. U. (2017). Vernam Encrypted Text in End of File Hiding Steganography Technique. *Int. J. Recent Trends Eng. Res*, 3(7), 214-219.
- Hardinata, R. S. (2019). Audit Tata Kelola Teknologi Informasi menggunakan Cobit 5 (Studi Kasus: Universitas Pembangunan Panca Budi Medan). *Jurnal Teknik dan Informatika*, 6(1), 42-45.
- Hariyanto, E., Lubis, S. A., & Sitorus, Z. (2017). Perancangan prototipe helm pengukur kualitas udara. *KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)*, 1(1).
- Hariyanto, E., & Rahim, R. (2016). Arnold's cat map algorithm in digital image encryption. *International Journal of Science and Research (IJSR)*, 5(10), 1363-1365.
- Harumy, T. H. F., & Sulistianingsih, I. (2016). Sistem penunjang keputusan penentuan jabatan manager menggunakan metode mfep pada cv. Sapo durin. In *Seminar Nasional Teknologi Informasi dan Multimedia* (pp. 6-7).
- Iqbal, M., Siahaan, A. P. U., Purba, N. E., & Purwanto, D. (2017). Prim's Algorithm for Optimizing Fiber Optic Trajectory Planning. *Int. J. Sci. Res. Sci. Technol*, 3(6), 504-509.
- Marlina, L., Muslim, M., Siahaan, A. U., & Utama, P. (2016). Data Mining Classification Comparison (Naïve Bayes and C4. 5 Algorithms). *Int. J. Eng. Trends Technol*, 38(7), 380-383.
- Muttaqin, Muhammad. "ANALISA PEMANFAATAN SISTEM INFORMASI E-OFFICE PADA UNIVERSITAS PEMBANGUNAN PANCA BUDI MEDAN DENGAN MENGGUNAKAN METODE UTAUT." *Jurnal Teknik dan Informatika* 5.1 (2018): 40-43.
- Ramadhan, Z., Zarlis, M., Efendi, S., & Siahaan, A. P. U. (2018). Perbandingan Algoritma Prim dengan Algoritma Floyd-Warshall dalam Menentukan Rute Terpendek (Shortest Path Problem). *JURIKOM (Jurnal Riset Komputer)*, 5(2), 135-139.
- Rahim, R., Aryza, S., Wibowo, P., Harahap, A. K. Z., Suleman, A. R., Sihombing, E. E., ... & Agustina, I. (2018). Prototype file transfer protocol application for LAN and Wi-Fi communication. *Int. J. Eng. Technol.*, 7(2.13), 345-347.
- Wahyuni, Sri. "Implementasi Rapidminer Dalam Menganalisa Data Mahasiswa Drop Out." *Jurnal Abdi Ilmu* 10.2 (2018): 1899-1902.
- Putri, G. G., Setyorini, W., & Rahayani, R. D. (2018). Analisis Kriptografi Simetris AES dan Kriptografi Asimetris RSA pada Enkripsi Citra Digital. *ETHOS*





(*Jurnal Penelitian Dan Pengabdian*), 6(2), 197–207.  
<https://doi.org/10.29313/ethos.v6i2.2909>

S., G., L. Ribeiro, A. R., & David, E. (2012). Asymmetric Encryption in Wireless Sensor Networks. In *Wireless Sensor Networks - Technology and Protocols*. InTech. <https://doi.org/10.5772/48464>

Sopyan, Y., Supriyadi, S., & Kurniadi, E. (2016). Implementasi Sistem Pendukung Keputusan Penerimaan Siswa baru Menggunakan Metode Simple Additive Weighting (Studi Kasus: SMK Negeri 3 Kuningan). *Jurnal Nuansa Informatika*, 11(1).

Sukmawati, R., & Priyadi, Y. (2019). Perancangan Proses Bisnis Menggunakan UML Berdasarkan Fit/Gap Analysis Pada Modul Inventory Odoo. *INTENSIF: Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem Informasi*, 3(2), 104. <https://doi.org/10.29407/intensif.v3i2.12697>

Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data Security and Privacy in Cloud Computing. *International Journal of Distributed Sensor Networks*, 10(7), 190903. <https://doi.org/10.1155/2014/190903>

Wasserkrug, S., Dalvi, N., Munson, E. V., Gogolla, M., Sirangelo, C., Fischer-Hübner, S., ... Snodgrass, R. T. (2019). Unified Modeling Language. In *Encyclopedia of Database Systems* (pp. 3232–3239). Boston, MA: Springer US. [https://doi.org/10.1007/978-0-387-39940-9\\_440](https://doi.org/10.1007/978-0-387-39940-9_440)

Wibowo, H. R. (2019). *Visual Basic Database*. Yogyakarta: Jubilee Enterprise.

Zhang, D., Tsotras, V. J., Levialdi, S., Grinstein, G., Berry, D. A., Gouet-Brunet, V., ... Pitoura, E. (2009). Indexed Sequential Access Method. In *Encyclopedia of Database Systems* (pp. 1435–1438). Boston, MA: Springer US. [https://doi.org/10.1007/978-0-387-39940-9\\_738](https://doi.org/10.1007/978-0-387-39940-9_738)

## LISTING PROGRAM

```
Public Class frmCS
    Dim Log As String
    Dim PT() As Byte
    Dim CT() As Byte
    Dim PTS, CTS, BlokKunci, Kunci As String
    Dim Blok, Sisa As Integer

    Private Sub btnEnkrip_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles btnEnkrip.Click
        Dim vCT As Integer
        Log = ""
        PT = System.Text.ASCIIEncoding.ASCII.GetBytes(txtPT.Text)

        ReDim CT(PT.Length - 1)
        Kunci = txtKunci.Text

        If PT.Length > 1000 Then
            MessageBox.Show("Plaintext tidak boleh melebihi dari 1000 karakter!",
"Peringatan")
            Exit Sub
        End If

        If Kunci.Length > 10 Then
            MessageBox.Show("Kunci tidak boleh lebih dari 10 karakter!", "Peringatan")
            Exit Sub
        End If

        BlokKunci = ""
        Blok = Math.Floor(PT.Length / Kunci.Length)
        Sisa = PT.Length Mod Kunci.Length

        For i = 0 To Blok - 1
            BlokKunci &= Kunci
        Next

        For i = 0 To Sisa - 1
            BlokKunci &= Kunci(i)
        Next

        CTS = ""
        For i = 0 To PT.Length - 1
            If (i Mod 8) = 0 And (i > 0) Then
                Log &= vbCrLf
            End If

            If rbKanan.Checked Then
                Log &= "CT[" & i & "] = " & PT(i) & " + " & Asc(BlokKunci(i)) & " Mod 256 =
"
                CT(i) = (PT(i) + Asc(BlokKunci(i))) Mod 256
            ElseIf rbKiri.Checked Then
                Log &= "CT[" & i & "] = " & PT(i) & " - " & Asc(BlokKunci(i)) & " Mod 256 =
"

                vCT = (PT(i) - Asc(BlokKunci(i))) Mod 256
                If vCT < 0 Then
                    vCT = 256 + vCT
                End If
                CT(i) = vCT
            End If

            If (CT(i) <> 0) Then
                CTS &= Chr(CT(i))
            End If
        Next
    End Sub
End Class
```

```

        Else
            CTS &= " "
        End If
        Log &= CT(i) & vbCrLf
    Next

    txtCT.Text = CTS
    txtLog.Text = Log
End Sub

Private Sub btnDekripsi_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btnDekripsi.Click
    Dim vPT As Integer
    Log = ""
    ReDim PT(CT.Length - 1)
    Kunci = txtKunci.Text

    BlokKunci = ""
    Blok = Math.Floor(PT.Length / Kunci.Length)
    Sisa = PT.Length Mod Kunci.Length

    For i = 0 To Blok - 1
        BlokKunci &= Kunci
    Next

    For i = 0 To Sisa - 1
        BlokKunci &= Kunci(i)
    Next

    PTS = ""
    For i = 0 To CT.Length - 1
        If (i Mod 8) = 0 And (i > 0) Then
            Log &= vbCrLf
        End If

        If rbKanan.Checked Then
            Log &= "PT[" & i & "] = " & CT(i) & " - " & Asc(BlokKunci(i)) & " Mod 256 =
"

            vPT = (CT(i) - Asc(BlokKunci(i))) Mod 256
            If vPT < 0 Then
                vPT = 256 + vPT
            End If
            PT(i) = vPT
        ElseIf rbKiri.Checked Then
            Log &= "PT[" & i & "] = " & CT(i) & " + " & Asc(BlokKunci(i)) & " Mod 256 =
"

            PT(i) = (CT(i) + Asc(BlokKunci(i))) Mod 256
        End If

        PTS &= Chr(PT(i))
        Log &= PT(i) & vbCrLf
    Next

    txtPT2.Text = PTS
    txtLog.Text = Log
End Sub
End Class

```