PENERAPAN METODE VIGENERE PADA PERANCANGAN APLIKASI PENGAMANAN PESAN TEKS

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	:	**FACHRI SYAUKANI**
NPM	:	**1524370671**
PROGRAM STUDI	:	**SISTEM KOMPUTER**

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2019

LEMBAR PENGESAHAN

PENERAPAN METODE VIGENERE PADA PERANCANGAN APLIKASI PENGAMANAN PESAN TEKS

Disusun Oleh:

NAMA	**: FACHRI SYAUKANI**
NPM	**: 1524370671**
PROGRAM STUDI	**: SISTEM KOMPUTER**

Skripsi Telah Disetujui oleh Dosen Pembimbing Skripsi
Pada Tanggal : 12 Juli 2020

Dosen Pembimbing I	Dosen Pembimbing II
Andysah P. U. Siahaan, S.Kom., M.Kom., Ph.D.	Dedi Purwanto, S.Kom., M.Kom.

Mengetahui:

Dekan Fakultas Sains dan Teknologi	Ketua Program Studi Sistem Komputer
Hamdani, S.T., M.T.	Eko Hariyanto, S.Kom., M.Kom.

SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama	: Fachri Syaukani
NPM	: 1524370671
Prodi	: Sistem Komputer
Konsentrasi	: Keamanan Jaringan Komputer
Judul Skripsi	: Penerapan Metode Vigenere pada Perancangan Aplikasi Pengamanan Pesan Teks

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 pihak lembaga,dan saya tidak akan menuntut akibat publikasi tersebut

Demikian pernyataan ini saya perbuat dengan sebenar-benarnya, terima kasih

Medan, 1 Juli 2020

Yang membuat pernyataan

FACHRI SYAUKANI

PERNYATAAN ORISINALITAS

Dengan ini saya menyatakan bahwa dalam skripsi ini tidak terdapat karya yang di ajukan untuk memperoleh gelar kesarjanaan di suatu perguruan tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah di tulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis di acu dalam skripsi ini dan di sebutkan dalam dalam daftar pustaka.

Medan, 1 Juli 2020

FACHRI SYAUKANI

NPM.1524370671

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*

bertanda tangan di bawah ini :

gkap	: FACHRI SYAUKANI
Tgl. Lahir	: MEDAN / 15 Mei 1994
ok Mahasiswa	: 1524370671
tudi	: Sistem Komputer
si	: Keamanan Jaringan Komputer
edit yang telah dicapai	: 143 SKS, IPK 3.17
	: 081363363491

i mengajukan judul sesuai bidang ilmu sebagai :

Judul
erapan Metode Vigenere Pada Perancangan Aplikasi Pengamanan Pesan Teks0

si Oleh Dosen Jika Ada Perubahan Judul

g Tidak Perlu

Medan, ~~26 Februari 2020~~ 19 September 2020
Pemohon,

(Fachri Syaukani)

Rektor

(Ir. Bhakti Alamsyah, M.T., Ph.D.)

Tanggal : 28/9/2020
Disahkan oleh :
Dekan

(Hamdani, ST., MT)

Tanggal : 26-02-2020
Disetujui oleh :
Dosen Pembimbing I :

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

Tanggal : .....
Disetujui oleh:
Ka. Prodi Sistem Komputer

(Eko Hariyanto, S.Kom., M.Kom)

Tanggal : 26-02-2020
Disetujui oleh:
Dosen Pembimbing II:

(Dedi Purwanto, S.Kom., M.Kom)

Telah Diperiksa oleh LPMU
dengan Plagiarisme 19 %
Medan 05 MARET 2020
An Ka. LPMU
Cahyo Pramono, SE, MM

FM-BPAA-2012-041

Hal : Permohonan Meja Hijau

Medan, 02 Maret 2020
Kepada Yth : Bapak/Ibu Dekan
Fakultas SAINS & TEKNOLOGI
UNPAB Medan
Di -
Tempat

Telah di terima
berkas persyaratan
dapat di proses
Medan 09/03/2020
Ka. BPAA
An.
TEGUH WAHYONO, SE., MM.

Dengan hormat, saya yang bertanda tangan di bawah ini :

Nama	: FACHRI SYAUKANI
Tempat/Tgl. Lahir	: MEDAN / 15 Mei 1994
Nama Orang Tua	: SYAFARUDDIN
N. P. M	: 1524370671
Fakultas	: SAINS & TEKNOLOGI
Program Studi	: Sistem Komputer
No. HP	: 081363363491
Alamat	: Dusun VII Jalan Bambu Gang Seroja Desa Helvetia

Datang bermohon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul **Penerapan Metode Vigenere Pada Perancangan Aplikasi Pengamanan Pesan Teks**, 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 transkipnya sebanyak 1 lembar.
7. Terlampir pelunasan kwintasi pembayaran uang kuliah berjalan dan wisuda sebanyak 1 lembar
8. Skripsi sudah dijilid lux 2 examplar (1 untuk perpustakaan, 1 untuk mahasiswa) dan jilid kertas jeruk 5 examplar untuk penguji (bentuk dan warna penjilidan 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.	600.000	
2. [170] Administrasi Wisuda	: Rp.	1,500,000	
3. [202] Bebas Pustaka	: Rp.	100,000	
4. [221] Bebas LAB	: Rp.	5,000	
Total Biaya	: Rp.	~~1,605,000~~	2.205.000 3 Rp. 5.080.000 ff 09/03-2020.
Uk. T. 50%	Rp.		2.875.000

Periode Wisuda Ke :

Ukuran Toga : M

UKM CENTER PANCA BUDI
Telah Diperiksa oleh UKM-C
Medan ...., ..., ...
Ka. UKM-C
Roro Rian Agustin

Diketahui/Disetujui oleh :

Hamdani, ST., MT
Dekan Fakultas SAINS & TEKNOLOGI

Hormat saya

FACHRI SYAUKANI
1524370671

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.

TANDA BEBAS PUSTAKA
No. 1736 / Perp / BP / 2020
Dinyatakan tidak ada sangkut paut dengan UPT. Perpustakaan
04 MAR 2020
Ka. UPT. Perpustakaan
Nanda Khairidah, S.IP

SIDANG : 2.205.000
Uk. T.50 % : 2.875.000 +
Rp. 5.080.000

Plagiarism Detector v. 1460 - Originality Report

Analyzed document: 03/05/20 08:56:49

"FACHRI SYAUKANI_1524370671_SISTEM KOMPUTER.doc"

Check Type: Internet - via Google and Bing

Licensed to: **Universitas Pembangunan Panca Budi_License03**

LEMBAGA PENJAMIN MUTU UNIVERSITAS
UNIVERSITAS PEMBANGUNAN PANCA BUDI
2/05/20

Relation chart:

Distribution graph:

Comparison Preset: Rewrite. Detected language: Indonesian

Top sources of plagiarism:

% 5	wrds: 407	https://satukan-halawa.blogspot.com/2015/03/laporan-kp-saya.html
% 4	wrds: 277	https://kuliah-kami.blogspot.com/2011/12/makalah-perbandingan-visual-basic-c-dan...
% 3	wrds: 226	https://widuri.raharja.info/index.php?title=SI1314475579

w other Sources:]

Processed resources details:

92 - Ok / 3 - Failed

ow other Sources:]

Important notes:

Wikipedia:	Google Books:	Ghostwriting services:	Anti-cheating:
[not detected]	[not detected]	[not detected]	[not detected]

Active References (Urls Extracted from the Document):

RLs detected

Excluded Urls:

RLs detected

Included Urls:

YAYASAN PROF. DR. H. KADIRUN YAHYA
UNIVERSITAS PEMBANGUNAN PANCA BUDI
LABORATORIUM KOMPUTER
Jl. Jend. Gatot Subroto Km 4,5 Sei Sikambing Telp. 061-8455571
Medan - 20122

KARTU BEBAS PRAKTIKUM

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

Nama	:	FACHRI SYAUKANI
N.P.M.	:	1524370671
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, 02 Maret 2020
a.n. Ka. Laboratorium

YAYASAN PROF. DR. H. KADIRUN YAHYA
LABORATORIUM KOMPUTER
INDONESIA
KAMPUS PANCA

Rachmi Wadly, S. Kom

No. Dokumen : FM-LAKO-06-01	Revisi : 01	Tgl. Efektif : 04 Juni 2015

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI
Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571
website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id
Medan - Indonesia

itas : Universitas Pembangunan Panca Budi
s : SAINS & TEKNOLOGI
Pembimbing I : Andysah Putera Utama Siahaan, Ph. D.
Pembimbing II : Dedi Purwanto, S.Kom., M.Kom.
Mahasiswa : FACHRI SYAUKANI
/Program Studi : Sistem Komputer
Pokok Mahasiswa : 1524370671
Pendidikan : S-1
ugas Akhir/Skripsi : Penerapan Metode Vigenere Pada Perancangan Aplikasi Pengamanan Pesan Teks

NGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
2019	ACC SEMPRO		
/2019	BAB I & BAB II Referensi agar dimurat. ~~ke~~ Referensi menggunakan Data 5 tahun terakhir		
/2020	BAB II Landasan teori belum memuat seluruhnya sesuai Rumusan masalah.		
/2020	Bahasa inggris di konsistensikan		
/2020	BAB IV Flowchart disesuaikan dengan Metodenya		
2020	Murat keterangan gambar		
	ACC Seminar Hasil		
2/2020	ACC Sidang		
17/2020	ACC judul		

Medan, 07 Oktober 2019
Diketahui/Disetujui oleh :
Dekan,

Sri Shindi Indira, S.T., M.Sc.
Hamdani, S.T., M.T

yang tidak perlu

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI
Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571
website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id
Medan - Indonesia

sitas	: Universitas Pembangunan Panca Budi
ss	: SAINS & TEKNOLOGI
Pembimbing I	: Andysah Putera Utama Siahaan, Ph.D.
Pembimbing II	: Dedi Purwanto, S.Kom, M.Kom.
Mahasiswa	: FACHRI SYAUKANI
n/Program Studi	: Sistem Komputer
Pokok Mahasiswa	: 1524370671
g Pendidikan	: S-1
Tugas Akhir/Skripsi	: Penerapan Metode Vigenere Pada Perancangan Aplikasi Pengamanan Pesan Teks

NGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
2019	Acc Seminar Judul		
0	Rev. Bab I		
11	Revisi Bab II		
11	Rev. Bab III		
4	Revisi Bab IV		
11	Revisi Bab IV, V		
12.	Acc Seminar Hasil		
2020	Acc Sidang		
12/7/2020	Acc Jilid		

Medan, 07 Oktober 2019
Diketahui/Disetujui oleh :
Dekan

Sri Shindi Indira, S.T., M.Sc.
Hamdani, S.T., M.T.

t yang tidak perlu

ABSTRAK

FACHRI SYAUKANI

Penerapan Metode Vigenere Pada Perancangan Aplikasi Pengamanan Pesan Teks

2019

Keamanan data adalah seperangkat standar dan teknologi yang melindungi data dari kehancuran, modifikasi, atau pengungkapan yang disengaja atau tidak disengaja. Keamanan data dapat diterapkan dengan menggunakan berbagai teknik dan teknologi, termasuk kontrol administratif, keamanan fisik, kontrol logis, standar organisasi, dan teknik perlindungan lainnya yang membatasi akses ke pengguna atau proses yang tidak sah atau berbahaya. Untuk meningkatkan keamanan data, diperlukan suatu teknik kriptografi. Algoritma Vigenere dapat membantu mengamankan data dari usaha pencurian dan pengambilan informasi tanpa seizin pemiliknya. Algoritma ini bekerja dengan sangat cepat karena hanya melakukan pergeseran plaintext sebesar nilai kunci yang digunakan. Vigenere akan bekerja sesuai dengan tabel ASCII sehingga ada banyak peluang dalam menempatkan kunci untuk proses enkripsi dan dekripsi. Kunci yang digunakan juga dapat bervariasi dan panjang kunci juga dapat ditentukan sesuai dengan yang diinginkan oleh pengguna. Dengan menerapkan algoritma Vigenere, keamanan data akan dapat ditingkatkan dan lebih baik.

Kata Kunci: dekripsi, enkripsi, kriptografi, Vigenere

DAFTAR GAMBAR

DAFTAR ISI

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi sangat erat dengan meningkatnya kejahatan terutama kejahatan digital. Kejahatan ini tidak melakukan tindak kekerasan fisik melainkan melakukan manipulasi, pencurian dan penyalahgunaan data yang dapat diperoleh dari jaringan global. Setiap manusia sekarang sudah pasti terkoneksi ke internet. Tanpa disadari data atau informasi miliknya memiliki kerentanan yang cukup tinggi untuk dicuri. Pada saat kita mengirimkan informasi, file atau data ke seseorang melalui jaringan komputer, maka data tersebut akan berjalan dengan leluasa tanpa memikirkan resiko yang akan dihadapi.

Data adalah aset penting bagi seseorang atau perusahaan. Oleh karenanya, penting untuk melindungi data tersebut dari serangan penjahat online. Organisasi di seluruh dunia banyak melakukan penelitian dalam teknologi informasi untuk meningkatkan dan kemampuan pertahanan dari serangan dunia maya. Pada dasarnya, ada yang saling terkait dalam melindungi data yaitu orang, proses, dan teknologi. Keamanan data tidak hanya penting bagi seseorang melainkan untuk menjaga keamanan dunia. Perlindungan data mulai berlaku di komputer pribadi, tablet, dan perangkat seluler yang bisa menjadi target penjahat siber berikutnya.

Melindungi data butuh teknik yang dapat menghindari dari pencurian dan pembacaan data. Teknik ini dapat dilakukan dengan kriptografi. Ada banyak metode yang dapat diterapkan untuk melindungi data dari pencurian. Algoritma

Vigenere adalah salah satu teknik kriptografi yang cukup mudah untuk dilakukan. Algoritma ini akan melakukan pergeseran plaintext dengan kunci yang sudah ditentukan. Hasil ciphertext akan memiliki kekuatan yang baik untuk menghindari pencurian informasi. Dengan menerapkan algoritma ini, diharapkan keamanan informasi dapat terjaga dengan baik. Algoritma ini dibuat dengan menggunakan program aplikasi Microsoft Visual Basic.NET 2010. Hasil aplikasi adalah pembuktian bahwa algoritma ini dapat bekerja dengan baik dan sesuai dengan harapan yang sebelumnya ingin dicapai. Algoritma ini cukup sederhana dan dapat diaplikasikan ke proses pengiriman data untuk menghindari pencurian data. Berdasarkan latar belakang di atas maka penulis tertarik untuk mengambil judul "**PENERAPAN METODE VIGENERE PADA PERANCANGAN APLIKASI PENGAMANAN PESAN TEKS**".

1.2 Rumusan Masalah

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

1. Bagaimana mengetahui cara kerja algoritma Vigenere Cipher?
2. Bagaimana menentukan pergeseran kunci pada saat proses enkripsi dan dekripsi?
3. Bagaimana melakukan ekspansi kunci sehingga sesuai dengan panjang plaintext?

1.3 Batasan Masalah

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

1. Data yang diamankan adalah berupa pesan teks.
2. Jumlah pergeseran yang digunakan akan dilakukan modulo 256.
3. Aplikasi yang digunakan adalah Microsoft Visual Basic.NET 2010.

1.4 Tujuan Penelitian

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

1. Untuk mengetahui cara kerja algoritma Vigenere Cipher.
2. Untuk menentukan pergeseran kunci pada saat proses enkripsi dan dekripsi.
3. Untuk melakukan ekspansi kunci sehingga sesuai dengan panjang plaintext.

1.5 Manfaat Penelitian

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

1. Memberikan keamanan pada seseorang yang akan mengirimkan data.
2. Proses enkripsi dan dekripsi dengan algoritma Vigenere bekerja dengan sangat cepat.
3. Menghindari pencurian data dan penyalahgunaan data.

BAB II

LANDASAN TEORI

2.1 Sistem Informasi

Sistem informasi, seperangkat komponen terintegrasi untuk mengumpulkan, menyimpan, dan memproses data dan untuk menyediakan informasi, pengetahuan, dan produk digital. Perusahaan bisnis dan organisasi lain bergantung pada sistem informasi untuk melaksanakan dan mengelola operasi mereka, berinteraksi dengan pelanggan dan pemasok mereka, dan bersaing di pasar. Sistem informasi digunakan untuk menjalankan rantai pasokan antar organisasi dan pasar elektronik. Misalnya, perusahaan menggunakan sistem informasi untuk memproses akun keuangan, untuk mengelola sumber daya manusia mereka, dan untuk menjangkau pelanggan potensial mereka dengan promosi online. Banyak perusahaan besar dibangun sepenuhnya di sekitar sistem informasi. Ini termasuk eBay, pasar lelang sebagian besar; Amazon, mal elektronik yang berkembang dan penyedia layanan cloud computing; Alibaba, e-marketplace bisnis-ke-bisnis; dan Google, perusahaan mesin pencari yang memperoleh sebagian besar pendapatannya dari iklan kata kunci di pencarian Internet. Pemerintah menggunakan sistem informasi untuk menyediakan layanan yang hemat biaya bagi warga negara. Barang digital — seperti buku elektronik, produk video, dan perangkat lunak — dan layanan online, seperti game dan jejaring sosial, dikirimkan dengan sistem informasi. Individu mengandalkan sistem informasi, umumnya berbasis Internet,

untuk melakukan banyak kehidupan pribadi mereka: untuk bersosialisasi, belajar, berbelanja, perbankan, dan hiburan.

Ketika teknologi baru utama untuk merekam dan memproses informasi ditemukan selama ribuan tahun, kemampuan baru muncul, dan orang-orang menjadi diberdayakan. Penemuan mesin cetak oleh Johannes Gutenberg pada pertengahan abad ke-15 dan penemuan kalkulator mekanik oleh Blaise Pascal pada abad ke-17 hanyalah dua contoh. Penemuan ini menghasilkan revolusi besar dalam kemampuan untuk merekam, memproses, menyebarluaskan, dan menjangkau informasi dan pengetahuan. Hal ini pada gilirannya, mengarah pada perubahan yang lebih dalam kehidupan individu, organisasi bisnis, dan tata kelola manusia.

Sistem informasi mekanis skala besar pertama adalah tabulator sensus Herman Hollerith. Diciptakan pada waktunya untuk memproses sensus 1890 AS, mesin Hollerith mewakili langkah besar dalam otomatisasi, serta inspirasi untuk mengembangkan sistem informasi yang terkomputerisasi.

2.2 Keamanan Informasi

Keamanan informasi adalah serangkaian strategi untuk mengelola proses, alat, dan kebijakan yang diperlukan untuk mencegah, mendeteksi, mendokumentasikan, dan melawan ancaman terhadap informasi digital dan non-digital. Tanggung jawab Infosec termasuk membangun serangkaian proses bisnis yang akan melindungi aset informasi terlepas dari bagaimana informasi itu diformat atau apakah sedang transit, sedang diproses atau sedang dalam penyimpanan (W. Stallings, 2013).

Banyak perusahaan besar mempekerjakan grup keamanan khusus untuk mengimplementasikan dan memelihara program infosec organisasi. Biasanya, grup ini dipimpin oleh seorang kepala petugas keamanan informasi. Grup keamanan umumnya bertanggung jawab untuk melakukan manajemen risiko, suatu proses di mana kerentanan dan ancaman terhadap aset informasi terus menerus dinilai, dan kontrol perlindungan yang sesuai diputuskan dan diterapkan. Nilai organisasi terletak pada informasinya - keamanannya sangat penting untuk operasi bisnis, serta mempertahankan kredibilitas dan mendapatkan kepercayaan dari klien.

2.2.1 Prinsip Keamanan Informasi

Keamanan informasi dibangun bertujuan menjaga kerahasiaan, integritas, dan ketersediaan sistem TI dan data bisnis. Tujuan ini memastikan bahwa informasi sensitif hanya diungkapkan kepada pihak yang berwenang (kerahasiaan), mencegah modifikasi data yang tidak sah (integritas) dan menjamin data dapat diakses oleh pihak yang berwenang ketika diminta (ketersediaan).

Pertimbangan keamanan pertama, kerahasiaan, biasanya memerlukan penggunaan enkripsi dan kunci enkripsi. Pertimbangan kedua, integritas, menyiratkan bahwa ketika data dibaca kembali, itu akan persis sama seperti ketika itu ditulis. Dalam beberapa kasus, mungkin perlu mengirim data yang sama ke dua lokasi yang berbeda untuk melindungi terhadap korupsi data di satu tempat. Bagian ketiga adalah ketersediaan. Bagian dari triad ini berupaya memastikan bahwa data baru dapat digunakan tepat waktu dan data cadangan dapat dipulihkan dalam waktu pemulihan yang dapat diterima (William Stallings, 2005).

2.2.2 Respon ancaman dan ancaman

Ancaman terhadap informasi sensitif dan pribadi datang dalam berbagai bentuk, seperti malware dan serangan phishing, pencurian identitas, dan ransomware. Untuk mencegah penyerang dan mengurangi kerentanan di berbagai titik, berbagai kontrol keamanan diterapkan dan dikoordinasikan sebagai bagian dari pertahanan berlapis dalam strategi mendalam. Ini harus meminimalkan dampak serangan. Agar siap untuk pelanggaran keamanan, kelompok keamanan harus memiliki rencana respons insiden di tempat. Ini harus memungkinkan mereka untuk menahan dan membatasi kerusakan, menghilangkan penyebabnya dan menerapkan kontrol pertahanan yang diperbarui.

Proses dan kebijakan keamanan informasi biasanya melibatkan langkah-langkah keamanan fisik dan digital untuk melindungi data dari akses, penggunaan, replikasi, atau perusakan yang tidak sah. Langkah-langkah ini dapat mencakup mantraps, manajemen kunci enkripsi, sistem deteksi intrusi jaringan, kebijakan kata sandi, dan kepatuhan terhadap peraturan. Audit keamanan dapat dilakukan untuk mengevaluasi kemampuan organisasi untuk memelihara sistem yang aman terhadap serangkaian kriteria yang ditetapkan.

2.2.3 Keamanan Informasi dan Keamanan Jaringan

Dalam infrastruktur komputasi perusahaan modern, data kemungkinan besar akan bergerak seperti halnya pada saat istirahat. Di sinilah keamanan jaringan masuk. Sementara secara teknis bagian dari cybersecurity, keamanan jaringan

terutama berkaitan dengan infrastruktur jaringan perusahaan. Ini berurusan dengan masalah-masalah seperti mengamankan tepi jaringan; mekanisme transportasi data, seperti sakelar dan router; dan potongan-potongan teknologi yang menyediakan perlindungan untuk data saat bergerak di antara node komputasi dimana cybersecurity dan keamanan jaringan berbeda sebagian besar dalam penerapan perencanaan keamanan. Paket keamanan siber tanpa rencana untuk keamanan jaringan tidak lengkap; namun, rencana keamanan jaringan biasanya dapat berdiri sendiri.

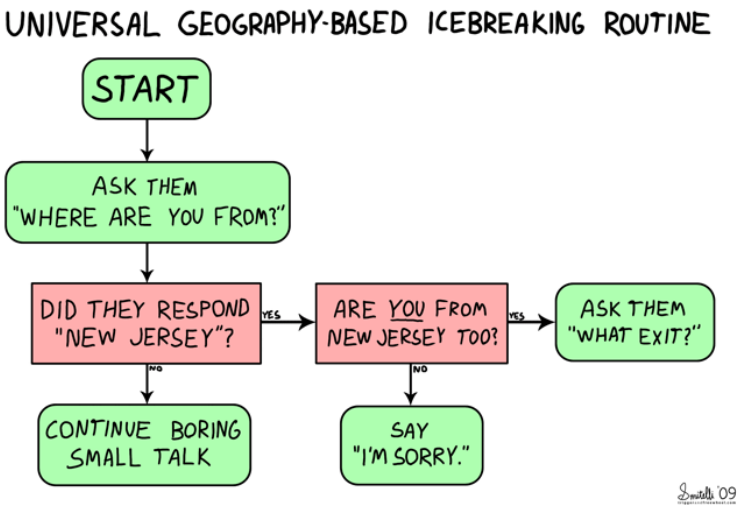
2.3 Algoritma

Kata 'algoritma' memiliki etimologi yang mirip dengan 'aljabar,' kecuali bahwa ini merujuk pada ahli matematika Arab sendiri, al-Khwarizmi (hanya berita gembira yang menarik). Algoritma, untuk yang bukan programmer di antara kita, adalah sekumpulan instruksi yang mengambil input, A, dan memberikan output, B, yang mengubah data yang terlibat dalam beberapa cara. Algoritma memiliki beragam aplikasi. Dalam matematika, mereka dapat membantu menghitung fungsi dari titik-titik dalam kumpulan data, di antara hal-hal yang jauh lebih maju. Selain penggunaannya dalam pemrograman itu sendiri, mereka memainkan peran utama dalam hal-hal seperti kompresi file dan enkripsi data.

2.3.1 Set Instruksi Dasar

Katakanlah seseorang bertemu teman di toko kelontong dan akan dibimbing ke arah yang benar. Algoritma akan mengatakan hal-hal seperti "masuk melalui pintu sisi kanan," "lewati bagian ikan di sebelah kiri," dan "jika melihat produk

susu, jalan terus." Algoritma bekerja seperti itu. Diagram alur dapat digunakan untuk menggambarkan instruksi berdasarkan kriteria yang kita ketahui sebelumnya atau mencari tahu selama proses. Gambar berikut ini adalah contoh diagram dalam penggunaan algoritma.



Gambar 2.1 Contoh alur algoritma
Sumber: (Ian Ruotsala, 2019)

Dari START, seseorang akan menuju jalan, dan tergantung pada apa yang terjadi, mengikuti "aliran" ke hasil akhir. Flowchart adalah alat visual yang dapat lebih dimengerti mewakili serangkaian instruksi yang digunakan oleh komputer. Demikian pula, algoritma membantu melakukan hal yang sama dengan model berbasis matematika lainnya.

2.3.2 Bagaimana Algoritma Bekerja

Contoh yang sangat sederhana dari suatu algoritma adalah menemukan angka terbesar dalam daftar angka yang tidak disortir. Jika ada daftar lima nomor yang berbeda, hasil akan dapat dipecahkan dalam waktu singkat, tidak perlu

komputer. Sekarang, bagaimana dengan lima juta angka yang berbeda? Jelas, algoritma akan sangat dibutuhkan untuk melakukan ini, dan komputer membutuhkan algoritma.

Di bawah ini adalah bagaimana algoritma itu terlihat. Katakanlah input terdiri dari daftar angka, dan daftar ini disebut L. Angka L1 akan menjadi angka pertama dalam daftar, L2 angka kedua, dll. Dan kita tahu daftar tersebut tidak diurutkan - jika tidak, jawabannya akan sangat mudah. Jadi, input ke algoritma adalah daftar angka, dan output harus menjadi angka terbesar dalam daftar. Algoritma akan terlihat seperti ini:

- Langkah 1: Biarkan Terbesar = L1

  Ini berarti mulai dengan mengasumsikan bahwa angka pertama adalah angka terbesar.

- Langkah 2: Untuk setiap item dalam daftar:

  Ini berarti akan melalui daftar angka satu per satu.

- Langkah 3: Jika item> Terbesar:

  Jika menemukan angka terbesar baru, lanjutkan ke langkah empat. Jika tidak, kembali ke langkah kedua, yang berarti beralih ke nomor berikutnya dalam daftar.

- Langkah 4: Kemudian Terbesar = item

  Ini menggantikan angka terbesar lama dengan angka terbesar baru yang baru saja ditemukan. Setelah ini selesai, kembali ke langkah dua hingga tidak ada lagi angka yang tersisa dalam daftar.

- Langkah 5: Kembalikan Terbesar

  Ini menghasilkan hasil yang diinginkan.

Perhatikan bahwa algoritma dijelaskan sebagai serangkaian langkah logis dalam bahasa yang mudah dipahami. Agar komputer dapat benar-benar menggunakan instruksi ini, mereka harus ditulis dalam bahasa yang dapat dimengerti oleh komputer, yang dikenal sebagai bahasa pemrograman.

2.4 Kriptografi

Definisi: Kriptografi dikaitkan dengan proses mengubah teks biasa menjadi teks yang tidak dapat dipahami dan sebaliknya. Ini adalah metode menyimpan dan mengirimkan data dalam bentuk tertentu sehingga hanya mereka yang dimaksudkan dapat membaca dan memprosesnya. Kriptografi tidak hanya melindungi data dari pencurian atau perubahan tetapi juga dapat digunakan untuk otentikasi pengguna.

Deskripsi: Kriptografi sebelumnya secara efektif identik dengan enkripsi tetapi saat ini kriptografi terutama didasarkan pada teori matematika dan praktik ilmu komputer. Kriptografi modern berkaitan dengan:

- Kerahasiaan - Informasi tidak dapat dipahami oleh siapa pun
- Integritas - Informasi tidak dapat diubah.
- Non-repudiation - Pengirim tidak dapat menyangkal niatnya dalam transmisi informasi di tahap selanjutnya
- Otentikasi - Pengirim dan penerima dapat mengkonfirmasi masing-masing

Kriptografi digunakan dalam banyak aplikasi seperti kartu transaksi perbankan, kata sandi komputer, dan transaksi e-commerce. Tiga jenis teknik kriptografi digunakan secara umum antara lain:

- Kriptografi kunci-simetris
- Fungsi hash.
- Kriptografi kunci publik

2.5 Kunci Simtris, Asimetris dan Fungsi Hash

2.5.1 Kunci Simetris

Symmetric-key Cryptography: Baik pengirim dan penerima berbagi satu kunci. Pengirim menggunakan kunci ini untuk mengenkripsi plaintext dan mengirim ciphertext ke penerima. Di sisi lain, penerima menerapkan kunci yang sama untuk mendekripsi pesan dan memulihkan teks biasa.

Cipher simetris, juga disebut sebagai enkripsi kunci rahasia, menggunakan kunci tunggal. Kunci kadang-kadang disebut sebagai rahasia bersama karena pengirim atau sistem komputasi yang melakukan enkripsi harus berbagi kunci rahasia dengan semua entitas yang berwenang untuk mendekripsi pesan. Enkripsi kunci simetris biasanya jauh lebih cepat daripada enkripsi asimetris. Cipher kunci simetris yang paling banyak digunakan adalah Advanced Encryption Standard (AES), yang dirancang untuk melindungi informasi rahasia pemerintah.

2.5.2 Kunci Asimetris

Public-Key Cryptography: Ini adalah konsep paling revolusioner dalam 300-400 tahun terakhir. Dalam Public-Key Cryptography, dua kunci terkait (kunci publik dan pribadi) digunakan. Kunci publik dapat didistribusikan secara bebas, sementara kunci privat yang dipasangkan, tetap menjadi rahasia. Kunci publik digunakan untuk enkripsi dan untuk dekripsi kunci pribadi digunakan.

Cipher asimetris, juga dikenal sebagai enkripsi kunci publik, menggunakan dua kunci yang berbeda - tetapi terhubung secara logis. Jenis kriptografi ini sering menggunakan bilangan prima untuk membuat kunci karena secara komputasional sulit untuk memperhitungkan bilangan prima yang besar dan merekayasa balik enkripsi. Algoritma enkripsi Rivest-Shamir-Adleman (RSA) saat ini merupakan algoritma kunci publik yang paling banyak digunakan. Dengan RSA, kunci publik atau pribadi dapat digunakan untuk mengenkripsi pesan; kunci mana pun yang tidak digunakan untuk enkripsi menjadi kunci dekripsi.

2.5.3 Fungsi Hash

Fungsi Hash: Tidak ada kunci yang digunakan dalam algoritma ini. Nilai hash panjang tetap dihitung sesuai teks biasa yang membuatnya tidak mungkin untuk memulihkan teks biasa. Fungsi hash juga digunakan oleh banyak sistem operasi untuk mengenkripsi kata sandi.

2.6 Enkripsi dan Dekripsi

2.6.1 Enkripsi

Enkripsi adalah metode yang digunakan untuk mengubah informasi menjadi kode rahasia yang menyembunyikan makna sebenarnya dari informasi tersebut.

Ilmu mengenkripsi dan mendekripsi informasi disebut kriptografi. Dalam komputasi, data yang tidak terenkripsi juga dikenal sebagai plaintext, dan data terenkripsi disebut ciphertext. Rumus yang digunakan untuk menyandikan dan mendekode pesan disebut algoritma enkripsi atau sandi.

Agar efektif, sandi menyertakan variabel sebagai bagian dari algoritma. Variabel, yang disebut kunci, adalah apa yang membuat output cipher unik. Ketika pesan terenkripsi dicegat oleh entitas yang tidak sah, penyusup harus menebak cipher pengirim mana yang digunakan untuk mengenkripsi pesan, serta kunci apa yang digunakan sebagai variabel. Waktu yang diperlukan untuk menebak informasi ini adalah yang menjadikan enkripsi sebagai alat keamanan yang sangat berharga.

Pada awal proses enkripsi, pengirim harus memutuskan cipher apa yang paling baik menyamarkan makna pesan dan variabel apa yang digunakan sebagai kunci untuk membuat pesan yang dikodekan menjadi unik. Jenis cipher yang paling banyak digunakan terbagi dalam dua kategori: simetris dan asimetris.

Enkripsi adalah proses mengubah data menjadi bentuk yang tidak dapat dikenali atau "dienkripsi". Ini biasanya digunakan untuk melindungi informasi sensitif sehingga hanya pihak yang berwenang yang dapat melihatnya. Ini termasuk file dan perangkat penyimpanan, serta data yang ditransfer melalui jaringan nirkabel dan Internet.

File terenkripsi akan tampak diacak oleh siapa saja yang mencoba melihatnya. Itu harus didekripsi agar dapat dikenali. Beberapa file terenkripsi memerlukan kata sandi untuk dibuka, sementara yang lain memerlukan kunci

pribadi, yang dapat digunakan untuk membuka kunci file yang terkait dengan kunci tersebut.

Enkripsi juga digunakan untuk mengamankan data yang dikirim melalui jaringan nirkabel dan Internet. Misalnya, banyak jaringan Wi-Fi diamankan menggunakan WEP atau enkripsi WPA yang jauh lebih kuat. Seseorang harus memasukkan kata sandi (dan kadang-kadang nama pengguna) terhubung ke jaringan Wi-Fi yang aman, tetapi begitu terhubung, semua data yang dikirim antara perangkat dan router nirkabel akan dienkripsi.

Banyak situs web dan layanan online lainnya mengenkripsi transmisi data menggunakan SSL. Situs web apa pun yang dimulai dengan "https: //," misalnya, menggunakan protokol HTTPS, yang mengenkripsi semua data yang dikirim antara server web dan browser Anda. SFTP, yang merupakan versi FTP yang aman, mengenkripsi semua transfer data.

Ada banyak jenis algoritma enkripsi, tetapi beberapa yang paling umum termasuk AES (Advanced Encryption Standard), DES (Data Encryption Standard), Blowfish, RSA, dan DSA (Digital Signature Algorithm). Meskipun sebagian besar metode enkripsi cukup untuk mengamankan data pribadi Anda, jika keamanan sangat penting, yang terbaik adalah menggunakan algoritma modern seperti AES dengan enkripsi 256-bit.

2.6.2 Dekripsi

Dekripsi adalah proses mengubah data yang telah dibuat tidak dapat dibaca melalui enkripsi kembali ke bentuk yang tidak dienkripsi. Dalam dekripsi, sistem

mengekstraksi dan mengubah data yang rusak dan mengubahnya menjadi teks dan gambar yang mudah dimengerti tidak hanya oleh pembaca tetapi juga oleh sistem. Dekripsi dapat dilakukan secara manual atau otomatis. Ini juga dapat dilakukan dengan seperangkat kunci atau kata sandi.

Salah satu alasan utama untuk menerapkan sistem enkripsi-dekripsi adalah privasi. Ketika informasi menyebar melalui World Wide Web, informasi tersebut menjadi subyek pengawasan dan akses dari individu atau organisasi yang tidak berwenang. Akibatnya, data dienkripsi untuk mengurangi kehilangan dan pencurian data. Beberapa item umum yang dienkripsi termasuk pesan email, file teks, gambar, data pengguna dan direktori. Orang yang bertanggung jawab atas dekripsi menerima prompt atau jendela di mana kata sandi dapat dimasukkan untuk mengakses informasi yang dienkripsi.

Dekripsi adalah prosedur memodifikasi data yang telah dicapai sebagai materi yang tidak dapat diuraikan melalui enkripsi ke keadaan yang dapat diuraikan. Dalam proses dekripsi, sistem memperoleh dan mengubah data yang membingungkan menjadi kata-kata dan gambar yang hanya dapat dipahami baik untuk pembaca dan sistem. Mungkin dilakukan secara otomatis atau manual. Itu bahkan dapat diselesaikan dengan bermacam-macam kode atau kata sandi. Dekripsi adalah suatu proses untuk mengungkap data yang diamankan dan untuk itu, struktur memperoleh dan mengubah data yang tercampur dan memodifikasinya menjadi bahasa dan gambar yang dapat diakses oleh pembaca bersama dengan sistem. Data yang didekripsi diterima oleh siapa pun di mana jendela akan muncul untuk memasukkan kata sandi yang diperlukan untuk mendapatkan data yang dienkripsi.

Ini dapat dilakukan secara otomatis atau manual dan juga dapat dilakukan melalui kumpulan kata sandi atau kode.

Penyebab paling signifikan untuk menjalankan proses enkripsi prosesor dekripsi adalah privasi. Ini menjadi masalah analisis dan aksesibilitas dari orang atau perusahaan yang tidak disetujui saat data bermigrasi di World Wide Web. Akibatnya, informasi dienkripsi untuk mengurangi kehilangan dan pencurian data. Beberapa item yang biasa dienkripsi terdiri dari gambar, direktori; pesan email, data pengguna, dan file teks. Individu yang menangani dekripsi mendapatkan jendela langsung di mana ia harus memencetnya untuk mendapatkan data terenkripsi.

Pengembangan algoritma kontinu untuk enkripsi substansial memiliki persyaratan yang lebih besar untuk spesialis intelijen dan penegakan hukum dalam perlombaan senjata dalam perhitungan. Selain itu, organisasi yang membutuhkan untuk menangani pemeriksaan keamanan digital atau untuk memulihkan kata sandi yang hilang memenuhi tantangan pemasangan yang serupa. Selain itu, dengan menggunakan cara terdekripsinya yang paling canggih, persyaratan untuk perhitungan yang luas tidak dapat dihindari yang merupakan alasan untuk dekripsi lebih lanjut. Badan-badan Federal dan ISV merangkul Frontier sebagai pilihan amunisi mereka.

Selain itu, kemampuannya adalah untuk membantu lembaga untuk memiliki dekripsi in-house atau algoritma steganografis dengan Frontier. Serta Paragon disertakan dengan beberapa decoder komersial besar untuk menyediakan jaringan turnkey perusahaan yang memberikan dekripsi pada banyak komputer di seluruh

perusahaan. Tidak ada metode yang unggul untuk mengarahkan sumber komputasi untuk tingkat yang sangat besar dengan kekuatan besar dari kemajuan dekripsi

.

2.7 Vigenere Cipher

Cipher Vigenere adalah bentuk teks-sederhana dari pengkodean yang menggunakan substitusi alfabet untuk menyandikan teks. Bentuk kuno kriptografi ini berasal dari tahun 1400-an dan didokumentasikan dalam karya-karya penulis terkenal pada zaman itu seperti Trithemius. Cipher Vigenere, seperti cipher kriptografi kontemporer lainnya, menggunakan sesuatu yang disebut tabula recta, kotak karakter alfabet di mana penyandi dapat menggeser garis untuk substitusi alfabet. Strategi dasar ini juga merupakan bagian dari sandi Trithemius, dan sandi Caesar, dinamai dengan nama Julius Caesar. Alih-alih melakukan pergeseran yang konsisten menurut abjad, Vigenere menggeser huruf sesuai dengan kata kunci berulang, yang berfungsi untuk membuat enkripsi lebih kompleks dan lebih sulit untuk diterjemahkan.

Cipher Vigenere adalah substitusi polialfabet dengan abjad yang berasal dari sepasang abjad primer dengan menggeser (seperti dalam Vigenère tableau) yang rumus pengunciannya yang biasa adalah P + K = C di mana P adalah posisi huruf plaintext dalam komponen polos, C dari huruf ciphertext dalam urutan cipher, dan K dari huruf kunci dalam alfabet normal dan di mana posisi diberi nomor dari 0 hingga 25 dan 26 dikurangkan dari jumlah di atas 25 (Hidayat, 2012).

Rumus enkripsi vigenere cipher :

Pi = (Ci-Ki) mod 26

atau

Ci = (Pi + Ki) – 26, kalau hasil penjumlahan Pi dan Ki lebih dari 26

Rumus dekripsi vigenere cipher :

Pi = (Ci-Ki) mod 26

atau

Pi = (Ci – Ki) + 26, kalau hasil pengurangan Ci dengan Ki minus

Keterangan:

Ci = nilai desimal karakter ciphertext ke-i

Pi = nilai desimal karakter plaintext ke-i

Ki = nilai desimal karakter kunci ke-i

Nilai desimal karakter: A=0 B=1 C=2 ... Z=25

2.8 Unified Modelling Language (UML)

Unified Modeling Language (UML) adalah bahasa pemodelan standar yang memungkinkan pengembang menentukan, memvisualisasikan, membuat, dan mendokumentasikan artefak sistem perangkat lunak (Technopedia, 2019). Dengan demikian, UML membuat artefak ini dapat diskalakan, aman, dan kuat dalam eksekusi. UML adalah aspek penting yang terlibat dalam pengembangan perangkat lunak berorientasi objek. Ini menggunakan notasi grafis untuk membuat model

visual dari sistem perangkat lunak. Arsitektur UML didasarkan pada fasilitas meta-objek, yang mendefinisikan dasar untuk membuat bahasa pemodelan. Mereka cukup tepat untuk menghasilkan seluruh aplikasi. UML yang sepenuhnya dapat dieksekusi dapat digunakan untuk berbagai platform menggunakan teknologi yang berbeda dan dapat digunakan dengan semua proses sepanjang siklus pengembangan perangkat lunak. UML dirancang untuk memungkinkan pengguna mengembangkan bahasa pemodelan visual yang ekspresif, siap pakai. Selain itu, mendukung konsep pengembangan tingkat tinggi seperti kerangka kerja, pola, dan kolaborasi (Wasserkrug et al., 2009).

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

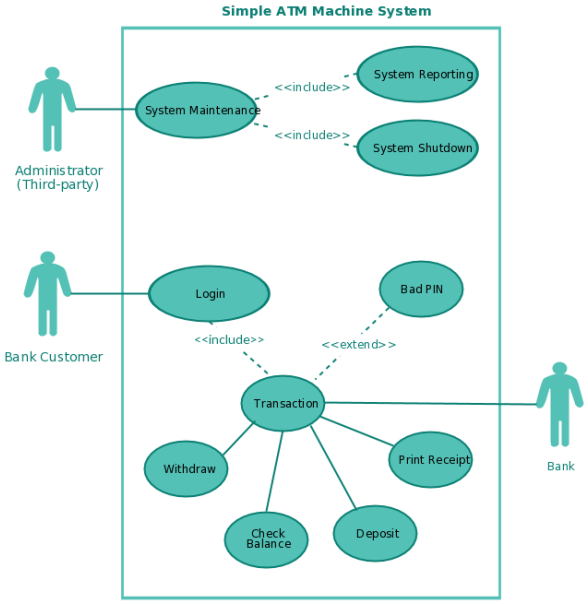
2.8.1 Model Use-Case

Model use-case adalah model tentang bagaimana berbagai jenis pengguna berinteraksi dengan sistem untuk memecahkan masalah. Dengan demikian, ini menggambarkan tujuan pengguna, interaksi antara pengguna dan sistem, dan perilaku sistem yang diperlukan dalam memenuhi tujuan-tujuan ini. Model use-case terdiri dari sejumlah elemen model. Elemen model yang paling penting adalah kasus penggunaan, aktor dan hubungan di antara mereka. Diagram use-case digunakan untuk menggambarkan secara grafis subset dari model untuk menyederhanakan komunikasi. Biasanya akan ada beberapa diagram kasus

penggunaan yang terkait dengan model yang diberikan, masing-masing menunjukkan subset elemen model yang relevan untuk tujuan tertentu. Elemen model yang sama dapat ditampilkan pada beberapa diagram use-case, tetapi setiap instance harus konsisten. Jika alat digunakan untuk mempertahankan model use-case, kendala konsistensi ini otomatis sehingga setiap perubahan pada elemen model (mengubah nama misalnya) akan secara otomatis tercermin dalam setiap diagram use-case yang menunjukkan elemen itu (UTM, 2019).

Model use-case dapat berisi paket yang digunakan untuk menyusun model untuk menyederhanakan analisis, komunikasi, navigasi, pengembangan, pemeliharaan, dan perencanaan. Faktanya, sebagian besar model use-case adalah tekstual, dengan teks yang ditangkap dalam Spesifikasi Use-Case yang terkait dengan setiap elemen model use-case. Spesifikasi ini menjelaskan alur peristiwa use case. Model use-case berfungsi sebagai utas pemersatu sepanjang pengembangan sistem. Ini digunakan sebagai spesifikasi utama dari persyaratan fungsional untuk sistem, sebagai dasar untuk analisis dan desain, sebagai input untuk perencanaan iterasi, sebagai dasar mendefinisikan kasus uji dan sebagai dasar untuk dokumentasi pengguna. (Kurniawan, 2018).

Use case diagram merupakan suatu diagram yang berisi *use case, actor*, serta *relationship* diantaranya. *Use Case Diagram* dapat digunakan untuk kebutuhan apa saja yang diperlukan dalam suatu sistem, sehingga sistem dapat digambarkan dengan jelas bagaimana proses dari sistem tersebut, bagaimana cara aktor menggunakan sistem, serta apa saja yang dapat dilakukan pada suatu sistem.

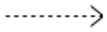
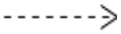
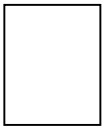


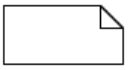
Gambar 2.2 Use-case Diagram ATM
Sumber: (Uml-diagrams.org, 2019)

Gambar 2.2 adalah contoh dari penggunaan use-case diagram pada mesin ATM. Use-case memiliki beberapa simbol untuk menyatakan kegiatan dari use-case tersebut. Adapun simbol dari *use case* adalah sebagai berikut:

Tabel 2.1 Simbol Use-case Diagram

No	Gambar	Nama	Keterangan
1		*Actor*	Menspesifikasikan himpunan peran yang pengguna mainkan ketika berinteraksi dengan *use case*.

2		*Dependency*	Hubungan dimana perubahan yang terjadi pada suatu elemen mandiri *(independent)* akan mempengaruhi elemen yang bergantung padanya elemen yang tidak mandiri.
3		*Generalization*	Hubungan dimana objek anak berbagi perilaku dan struktur data dari objek yang ada diatasnya.
4		*Include*	Menspesifikasikan bahwa *use case* sumber secara *eksplisit*.
5		*Extend*	Menspesifikasikan bahwa *use case* target memperluas perilaku dari *use case* sumber pada suatu titik yang diberikan.
6		*Association*	Apa yang menghubungkan antara objek satu dengan objek lainnya.
7		*System*	Menspesifikasikan paket yang menampilkan sistem secara terbatas.
8		*Use Case*	Deskripsi dari urutan aksi-aksi yang ditampilkan sistem yang

			menghasilkan suatu hasil yang terukur bagi suatu actor
9		*Collaboration*	Interaksi aturan-aturan dan elemen lain yang bekerja sama untuk menyediakan prilaku yang lebih besar dari jumlah dan elemen-elemennya (sinergi).
10		*Note*	Elemen fisik yang eksis saat aplikasi dijalankan dan mencerminkan suatu sumber daya komputasi

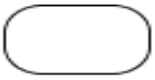
Sumber: (Kurniawan, 2018)

2.8.2 Activity Diagram

Activity Diagram (Diagram Aktifitas) menggambarkan berbagai alir aktifitas dalam sistem yang sedang dirancang, bagaimana masing-masing alir berawal, *decision* yang mungkin terjadi, dan bagaimana mereka berakhir (Ladjamudin, 2005).

Activity diagram menurut adalah salah satu cara untuk memodelkan *event-event* yang terjadi dalam suatu *use case*. Diagram ini juga dapat digantikan dengan sejumlah teks.

Tabel 2.2. Simbol Activity Diagram

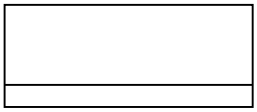
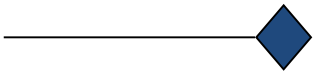
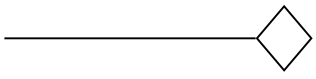
No	Gambar	Nama	Keterangan
1		*Actifity*	Memperlihatkan bagaimana masing-masing kelas antarmuka saling berinteraksi satu sama lain
2		*Action*	State dari sistem yang mencerminkan eksekusi dari suatu aksi
3		*Initial Node*	Bagaimana objek dibentuk /diawali.
4		*Actifity Final Node*	Bagaimana objek dibentuk dan dihancurkan
5		*Fork Node*	Satu aliran yang pada tahap tertentu berubah menjadi beberapa aliran

Sumber: (Kurniawan, 2018)

2.1.1 Class Diagram

Class diagram digunakan untuk menggambarkan perbedaan yang mendasar antara *class*, hubungan antara *class*, dan di mana *sub-sistem class* tersebut (Jogiyanto, 2006). Simbol yang digunakan dalam *class diagram* adalah sebagai berikut:

Tabel 2.3 Simbol yang digunakan dalam Class Diagram

Simbol	Nama	Fungsi
	*Class*	Menggambarkan *Class* baru pada diagram.
	*Association*	Menggambarkan relasi antar asosiasi
	*Composition*	Jika sebuah *class* tidak bisa berdiri sendiri dan harus merupakan bagian dari *class* yang lain, maka class tersebut memiliki relasi *Composition* terhadap *class* tempat dia bergantung tersebut.
	Depedency	Umumnya penggunaan *dependency* digunakan untuk menunjukkan operasi pada suatu *class* yang menggunakan *class* yang lain.
	*Aggregation*	*Aggregation* mengindikasikan keseluruhan bagian *relationship* dan biasanya disebut sebagai relasi.

Sumber: (Kurniawan, 2018)

2.1.2 Flowchart

Flowchart digunakan dalam mendesain dan mendokumentasikan proses atau program sederhana. Seperti jenis diagram lainnya, diagram membantu memvisualisasikan apa yang sedang terjadi dan dengan demikian membantu memahami suatu proses, dan mungkin juga menemukan fitur-fitur yang kurang jelas dalam proses tersebut, seperti kekurangan dan hambatan. Ada berbagai jenis diagram alur: masing-masing jenis memiliki set kotak dan notasi sendiri. Dua jenis kotak yang paling umum dalam diagram alur adalah:

1. langkah pemrosesan, biasanya disebut aktivitas dan dilambangkan sebagai kotak persegi panjang.
2. keputusan biasanya dilambangkan sebagai berlian.

Diagram alir digambarkan sebagai "lintas fungsional" ketika bagan dibagi menjadi bagian vertikal atau horizontal yang berbeda, untuk menggambarkan kontrol unit organisasi yang berbeda. Simbol yang muncul di bagian tertentu berada dalam kendali unit organisasi itu. Flowchart lintas fungsional memungkinkan penulis untuk menemukan tanggung jawab untuk melakukan suatu tindakan atau membuat keputusan dengan benar, dan untuk menunjukkan tanggung jawab masing-masing unit organisasi untuk bagian berbeda dari satu proses tunggal.

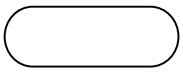
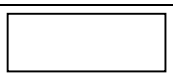
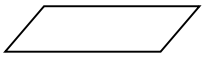
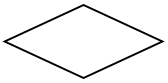
Diagram alir menggambarkan aspek-aspek tertentu dari proses dan biasanya dilengkapi dengan jenis diagram lainnya. Misalnya, Kaoru Ishikawa, mendefinisikan diagram alir sebagai salah satu dari tujuh alat dasar kendali mutu, di sebelah histogram, diagram Pareto, lembar periksa, diagram kontrol, diagram

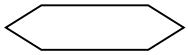
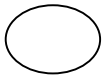
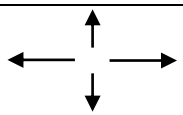
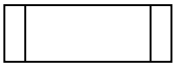
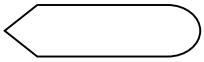
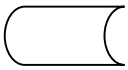
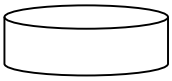
sebab-akibat, dan diagram sebaran. Demikian pula, di UML, notasi pemodelan konsep standar yang digunakan dalam pengembangan perangkat lunak, diagram aktivitas, yang merupakan jenis diagram alur, hanyalah salah satu dari banyak jenis diagram yang berbeda.

Diagram Nassi-Shneiderman dan Drakon-chart adalah notasi alternatif untuk aliran proses. Nama alternatif umum termasuk diagram alir, diagram alur proses, diagram alur fungsional, peta proses, diagram proses, diagram proses fungsional, model proses bisnis, model proses, diagram alir proses, diagram alur kerja, diagram alir bisnis. Istilah "diagram alur" dan "diagram alir" digunakan secara bergantian (Nakatsu, 2009).

Struktur grafik yang mendasari diagram alur adalah grafik aliran, yang mengabstraksi jenis simpul, isinya, dan informasi tambahan lainnya. Adapun simbol-simbol flowchart lihat pada tabel sebagai berikut :

Tabel 2.4 Simbol Flowchart

NO	SIMBOL	FUNGSI
1.		**Terminal**, untuk memulai atau mengakhiri suatu program
2.		**Proses**, suatu simbol yang menunjukkan setiap pengolahan yang dilakukan.
3.		**Input-Output**, untuk memasukkan menunjukkan hasil dari suatu proses
4.		**Decision**, suatu kondisi yang akan menghasilkan beberapa kemungkinan jawaban atau pilihan

5.		**Preparation,** suatu symbol yang menyediakan tempat pengolahan
6.		**Connector**, suatu prosedur penghubung yang akan masuk atau keluar melalui symbol ini dalam lembar yang sama
7.		**Off-Page Connector**, merupakan symbol masuk atau keluarannya suatu prosedur pada lembaran kertas lainnya
8.		**Arus/Flow**, dari pada prosedur yang dapat dilakukan atas ke bawah dari bawah ke atas, ke atas dari kiri ke kanan ataupun dari kanan ke kiri
9.		**Predefined Process**, untuk menyatakan sekumpulan langkah proses yang ditulis sebagai prosedur
10.		Simbol untuk output, yang ditunjukkan ke suatu device, seperti printer, dan sebagainya
11		Penyimpanan file secara sementara
12		Menunjukkan input / Output Hardisk (media penyimpanan)

Sumber: (Kurniawan, 2018)

2.9 Visual Basic.Net

Visual Basic.Net merupakan salah satu *tool development Microsoft* yang dapat digunakan untuk membuat aplikasi di lingkungan kerja berbasis sistem

operasi *Windows*. Visual Basic.Net menyediakan *tools* bagi para *developer* untuk membangun aplikasi yang berjalan di *.Net Framework*.

Visual basic merupakan turunan bahasa pemrograman BASIC yang menawarkan pengembangan perangkat lunak computer berbasis grafik dengan cepat. Dengan menggunakan bahasa pemrograman VB, para *programmer* dapat membangun aplikasi dengan menggunakan komponen-komponen yang di sediakan VB.

Microsoft Visual Basic (sering disingkat sebagai VB saja) merupakan sebuah bahasa pemrograman yang menawarkan *Integrated Development Environment* (*IDE*) *visual* untuk membuat program perangkat lunak berbasis sistem operasi *Microsoft Windows* dengan menggunakan model pemrograman (*COM*), *Visual Basic* merupakan turunan bahasa pemrograman *BASIC* dan menawarkan pengembangan perangkat lunak computer berbasis grafik dengan cepat, beberapa bahasa skrip seperti *Visual Basic for Applications* (*VBA*) dan *Visual Basic Scripting Edition* (*VBScript*), mirip seperti halnya *Visual Basic*, tetapi cara kerjanya yang berbeda.

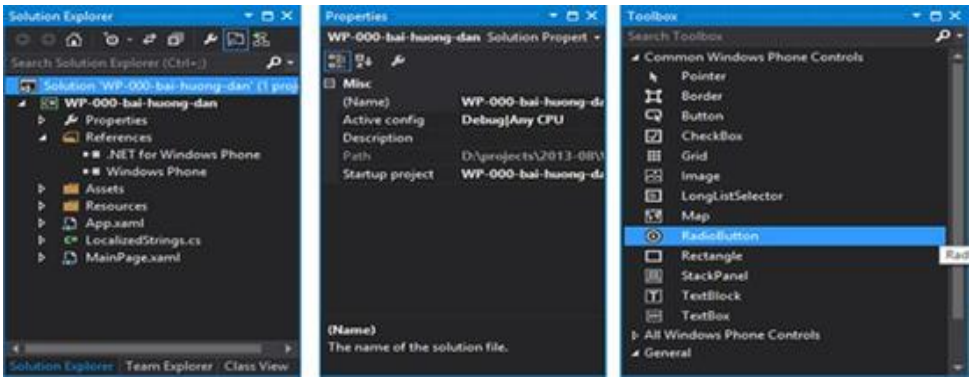
Para *programmer* dapat membangun aplikasi dengan menggunakan komponen-komponen yang disediakan oleh *Microsoft Visual Basic*. Program-program yang ditulis dengan *Visual Basic* juga dapat menggunakan *Windows API*, tapi membutuhkan deklarasi fungsi luar tambahan.

Dalam pemrograman untuk bisnis, *Visual Basic* memiliki pangsa pasar yang sangat luas. Dalam sebuah survey yang dilakukan pada tahun 2005, 62%

pengembang perangkat lunak dilaporkan menggunakan berbagai bentuk *Visual Basic* yang diikuti oleh C++, JavaScript, dan Java.

Beberapa komponen kerja program *visual basic* 2010 telah ditampilkan sebagai tampilan standard. Masih banyak lagi komponen yang masih tersembunyi sehingga memerlukan perintah tertentu untuk menampilkannya. Kita dapat mengatur komponen di dalam program *visual basic* 2010 sesuai dengan yang kita butuhkan. Berikut ini adalah beberapa komponen kerja dari *visual basic* 2010 adalah.

Toolbox adalah sebuah panel yang menampung tombol-tombol yang berguna untuk membuat suatu desain mulai dari tombol *label*, *pointer*, *button*, dan lain-lain. Berikut ini adalah gambaran *toolbox* pada *visual basic* 2010.



Gambar 2.3 Tampilan Toolbox
Sumber: (Rahmel, 2008)

Berikut ini adalah *table* yang berisi nama tombol yang terdapat di dalam *toolbox* beserta fungsinya.

Tabel 2.5 Toolbox Visual Basic.Net

Nama tombol	Fungsi
Pointer	Memilih, mengatur ukuran dan memindahkan posisi yang terpasang di bagian *form*.
Bindingsources	Untuk mengkoneksikan program ke *database.*
Label	Menampilkan teks, dimana pengguna program tidak bisa mengubah teks tersebut.
Groupbox	Untuk mengelompokkan *item* yang ada di *form.*
Checkbox	Membuat kotak periksa, dimana pengguna program dapat memilih sekaligus.
Listbox	Membuat daftar pilihan.
Timer	Membuat kontrol waktu dan interval yang diperlukan.
Image	Menampilkan gambar pada *form* dalam format *bitmap*, *icone*, atau *metafile.*
Picturebox	Menampilkan gambar dari sebuah *file.*
Textbox	Membuat teks, dimana teks tersebut dapat diubah oleh pembuat program.
Button	Membuat tombol perintah.
Combobox	Menambahkan kontrol kotak *combo* yang merupakan kontrol gabungan antara *textbox* dan *listbox.*

Sumber: (Rahmel, 2008)

BAB III

METODE PENELITIAN

3.1 Tahapan Penelitian

Memahami proses penelitian adalah langkah penting menuju pelaksanaan penelitian atau penelitian yang menyeluruh. Berbagai fase dalam perencanaan penelitian serta tahapan yang terlibat dalam proses penelitian harus dikerjakan dengan baik. Pemahaman yang lebih mendalam tentang proses penelitian akan membantu mengidentifikasi fitur-fitur serupa yang terjadi di berbagai bidang, dan variasi dalam tujuan dan pendekatan untuk beberapa studi. Memahami proses penelitian akan membantu memahami implikasi penyimpangan dari pendekatan sistematis untuk penelitian, serta konsekuensi yang terkait dari penelitian yang tidak efektif dan tidak efektif.

Mengadopsi model yang diusulkan oleh Rummel dan Ballaine (1963), ada enam langkah yang terlibat dalam proses penelitian. Ini termasuk mengidentifikasi bidang studi, memilih topik, merumuskan rencana penelitian, mengumpulkan dan kemudian menganalisis data dan akhirnya menulis penelitian. Langkah-langkah ini dapat direpresentasikan dalam tiga fase, yaitu fase perencanaan dan fase penelitian dan akhirnya fase presentasi. Semua tahapan ini harus dapat dilakukan dengan baik agar hasil penelitian dapat berguna dan tidak menyalahi aturan bagaimana suatu penelitian harus dilakukan (Rummel & Ballaine, 1963). Tahapan berikut ini adalah proses yang dilakukan dalam penelitian ini:

- Studi Literatur

  Bagian akan dilakukan pencarian literatur dan buku yang berhubungan dengan algoritma Vigenere Cipher. Sumber-sumber bahan referensi dapat diambil dari web dan buku.

- Analisa

  Bagian ini menjelaskan proses analisa permasalahan dan penentuan cara penyelesaian terhadap masalah yang dialami. Proses ini melakukan analisis terhadap permasalahan yang terjadi dan bagaimana permasalahan tersebut akan diselesaikan.

- Pembahasan

  Bagian ini membahas tentang perhitungan algoritma Vigenere cipher pada proses enkripsi dan dekripsi. Hasil perhitungan akan disesuaikan dengan uji manual.

- Implementasi dan pengujian

  Bagian ini dilakukan pengujian hasil yang dikeluarkan oleh program aplikasi yang sudah dibuat menggunakan Microsoft Visual Basic.Net 2010. Hasil akan dibandingkan dengan perhitungan yang dilakukan secara manual.

3.2 Metode Pengumpulan Data

Pengumpulan data didefinisikan sebagai "proses mengumpulkan dan mengukur informasi tentang variabel yang diminati, dengan cara sistematis yang mapan yang memungkinkan seseorang untuk menjawab pertanyaan, menyatakan

pertanyaan penelitian, menguji hipotesis, dan mengevaluasi hasil". Tahapan yang dilakukan dalam melakukan pengumpulan data adalah sebagai berikut:

1. Studi Kepustakaan

   Studi kepustakaan dilakukan dengan cara mengumpulkan informasi dari berbagai sumber, mempelajari, dan membaca berbagai materi seperti buku, jurnal, majalah, dan internet.

2. Wawancara

   Wawancara satu lawan satu (atau tatap muka) adalah salah satu jenis metode pengumpulan data yang paling umum dalam penelitian kualitatif. Di sini, data dikumpulkan langsung dari orang yang diwawancarai. Karena itu menjadi pendekatan yang sangat pribadi, teknik pengumpulan data ini sangat cocok ketika ingin mengetahui lebih dalam algoritma Vigenere Cipher.

3. Survei

   Survei tertutup didasarkan pada pertanyaan yang memberikan responden pilihan jawaban yang telah ditentukan untuk dipilih. Ada dua jenis utama survei tertutup-survei berdasarkan kategori dan survei berdasarkan pertanyaan yang berhubungan dengan algoritma Vigenere Cipher.

3.3 Perancangan Penelitian

Desain penelitian adalah serangkaian metode dan prosedur yang digunakan dalam mengumpulkan dan menganalisis ukuran variabel yang ditentukan dalam penelitian masalah. Desain penelitian mendefinisikan jenis penelitian (deskriptif,

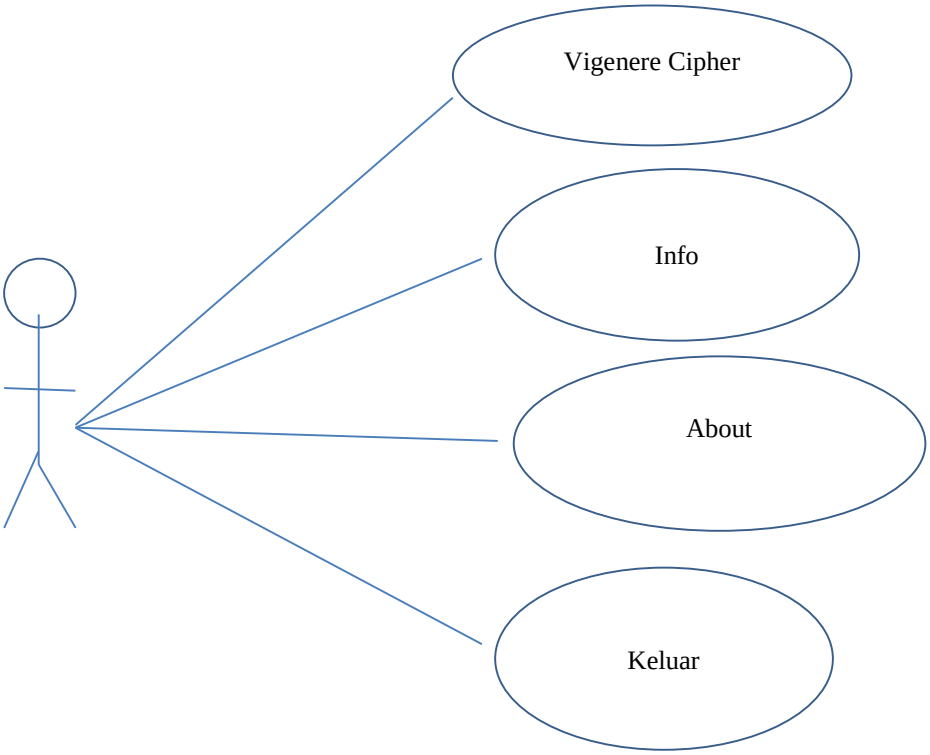
korelasi, semi-eksperimental, eksperimental, ulasan, meta-analitik) dan sub-tipe (misalnya, studi kasus deskriptif-longitudinal), masalah penelitian, hipotesis, variabel independen dan dependen, desain eksperimental, dan, jika berlaku, metode pengumpulan data dan rencana analisis statistik. Desain penelitian adalah kerangka kerja yang telah dibuat untuk menemukan jawaban atas pertanyaan penelitian.

Unified Modeling Language (UML) adalah bahasa pemodelan visual standar untuk pengembangan sistem berorientasi objek, tetapi telah dikritik karena kompleksitasnya, semantik yang tidak konsisten, dan konstruksi yang ambigu. Analisis kompleksitas dirumuskan berdasarkan jumlah konstruksi, asosiasi, peran, dan sebagainya, dalam metode pemodelan. Kami berpendapat bahwa kumpulan metrik ini memberikan indikasi kompleksitas teoritis dari metode pemodelan. Di sisi lain, kompleksitas teoretis dari metode pemodelan tidak selalu berhubungan dengan kompleksitas praktis. Selain kompleksitas teoretis, serangkaian metrik untuk memperkirakan kompleksitas praktis dapat dikembangkan, berdasarkan konstruksi yang paling umum digunakan (bukan semua konstruksi). Dalam penelitian ini, kami menggunakan data sekunder untuk menguji hipotesis kami bahwa kompleksitas praktis berbeda dari kompleksitas teoritis.

Dalam konteks desain pemrograman, memenuhi tuntutan antarmuka untuk praktik langsung dengan diagram UML menghadirkan hasil yang menarik. Berbagai diagram pada UML dapat gunakan untuk menggambarkan alur penelitian. Penelitian ini akan dijelaskan dalam bentuk diagram agar dapat memudahkan pembuatan program aplikasi.

3.3.1 Use Case Diagram

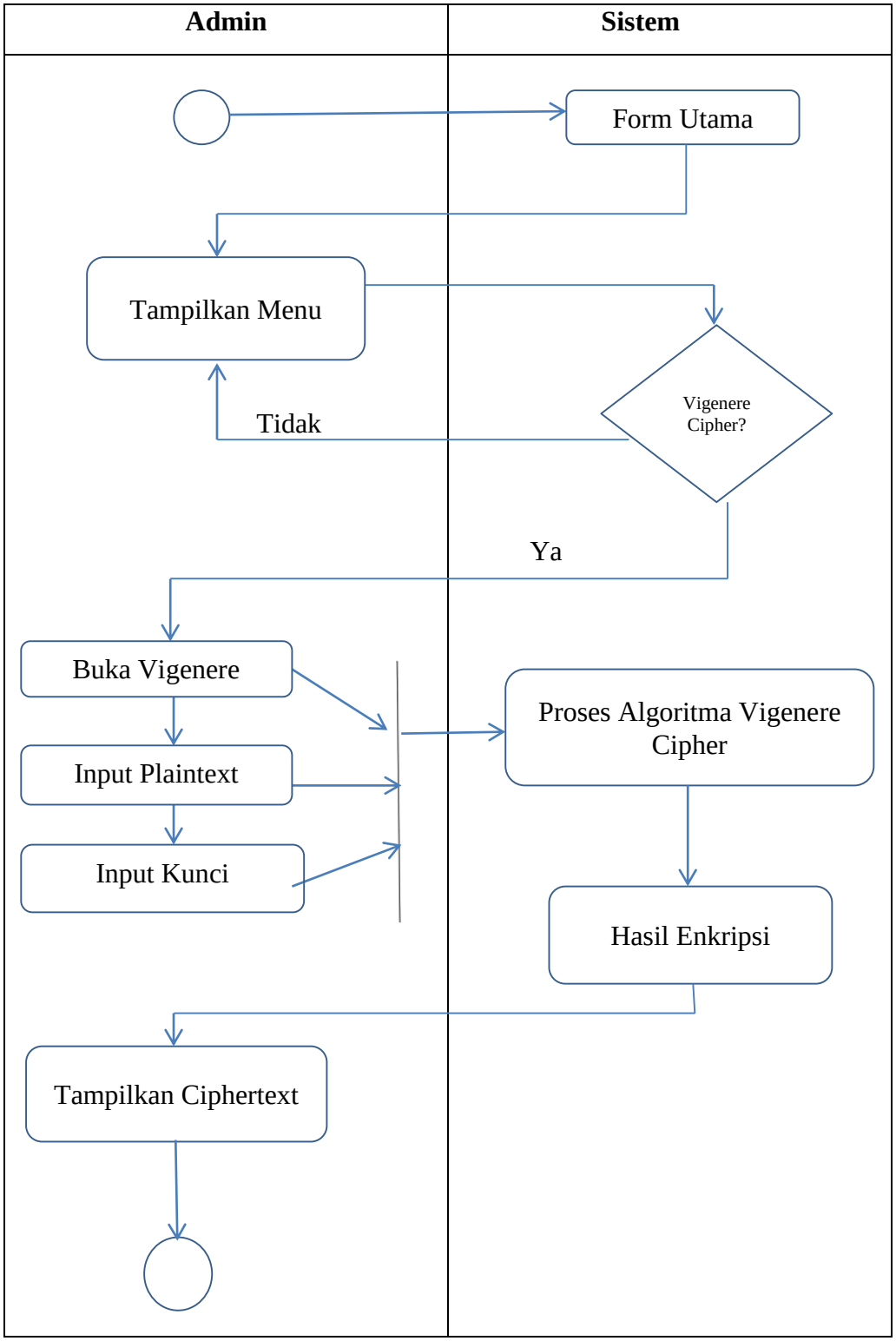
Use Case adalah penjelasan fungsi dari sebuah sistem dari segi pengguna. *Use Case* bekerja dengan cara menjelaskan interaksi antar *User* (pengguna) dengan sistemnya sendiri melalui sebuah bagan bagaimana suatu sistem dipakai. Gambar 3.1 adalah perancangan *Use Case* untuk admin dari algoritma Vigenere Cipher.



Gambar 3.1 Use Case Diagram

3.3.2 Activity Diagram

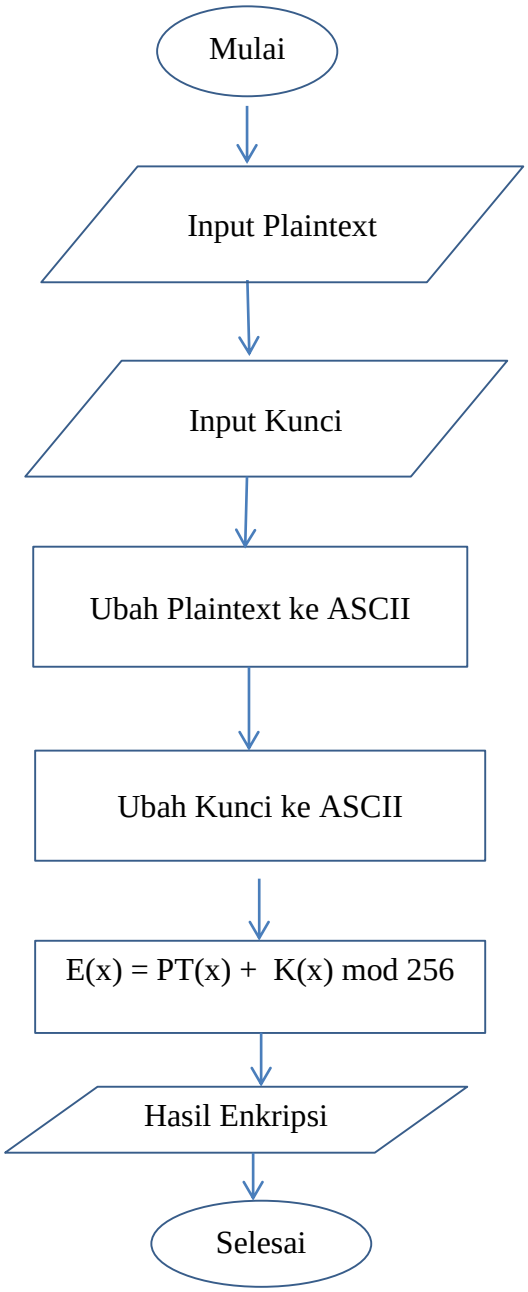
Activity diagram akan menggambarkan alur aktifitas dari sistem, untuk *Activity diagram* dari kriptrografi simetris dengan menggunakan algoritma Vigenere cipher. Gambar berikut ini akan menjelaskan *Activity diagram* tersebut.



Gambar 3.2 Activity Diagram

3.3.3 Flowchart Enkripsi

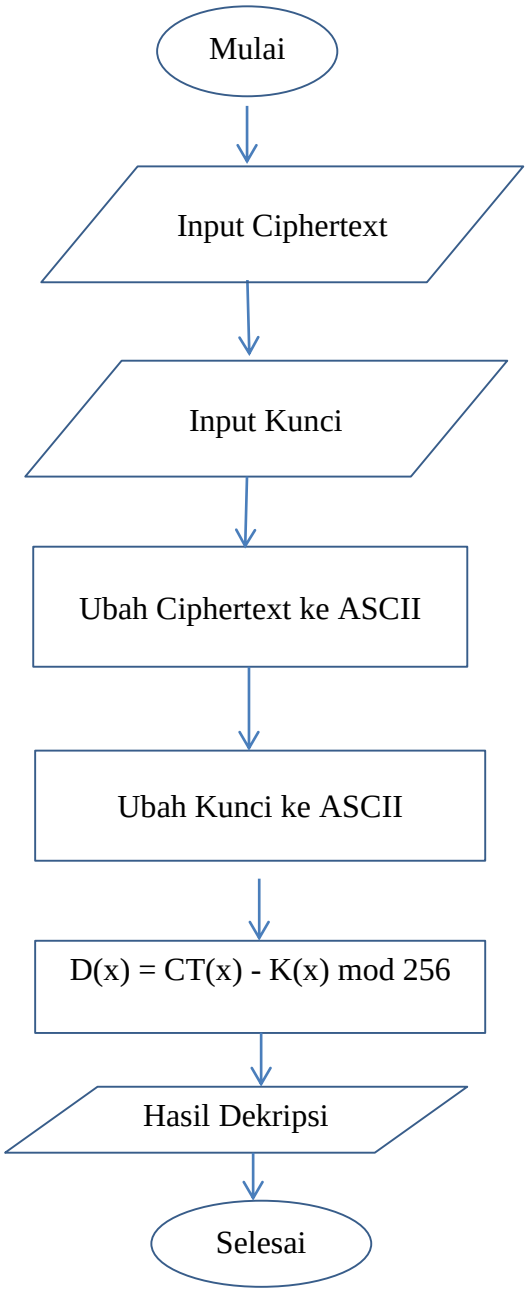
Flowchart enkripsi akan menerangkan proses enkripsi dengan metode substitusi dengan algoritma Vigenere Cipher. *Flowchart* enkripsi dapat dilihat pada gambar berikut ini.



Gambar 3.3 Flowchart enkripsi algoritma Vigenere

3.3.4 Flowchart Dekripsi

Flowchart dekripsi akan menjelaskan alur dari proses dekripsi dengan metode substitusi dengan algoritma Vigenere Cipher. *Flowchart* dekripsi dapat dilihat pada gambar berikut ini.



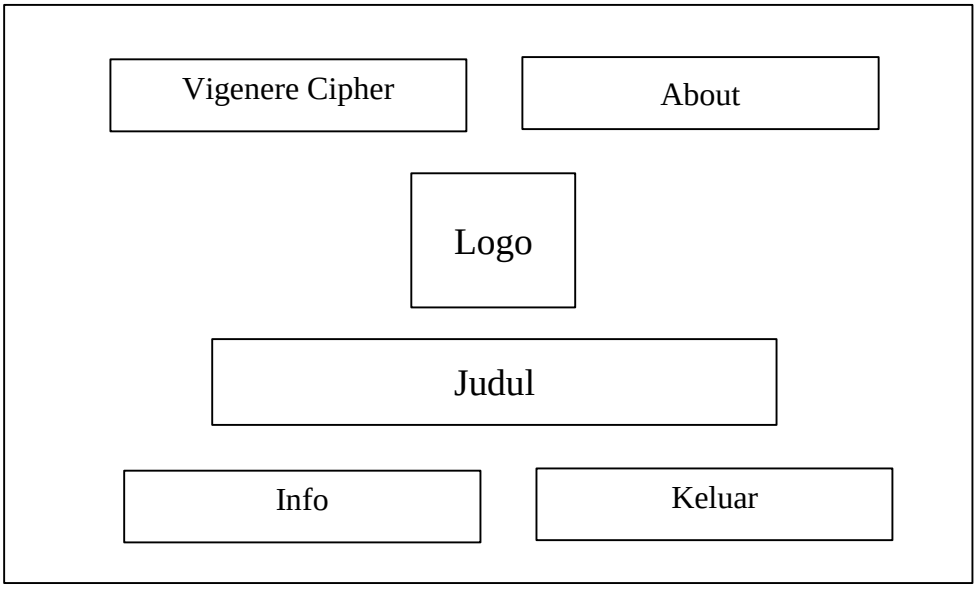
Gambar 3.4 Flowchart dekripsi algoritma Vigenere

3.4 Desain Interface

Desain *interface* adalah perancangan program aplikasi yang akan dibuat. Kode program akan dibuat menggunakan Microsoft Visual Basic.Net 2010. Desain *interface* ini terbagi menjadi beberapa sub-menu dan memiliki sebuah menu utama yang berfungsi sebagai menjalankan program utama. Tahapan berikut ini merupakan desain *interface* dari menu-menu yang ada pembuatan program aplikasi algoritma Vigenere Cipher.

3.4.1 Menu Utama

Menu utama adalah tampilan yang pertama sekali muncul pada saat progam aplikasi dijalankan. Tampilan pada gambar berikut ini adalah hasil perancangan menu utama yang memiliki beberapa komponen lainnya.



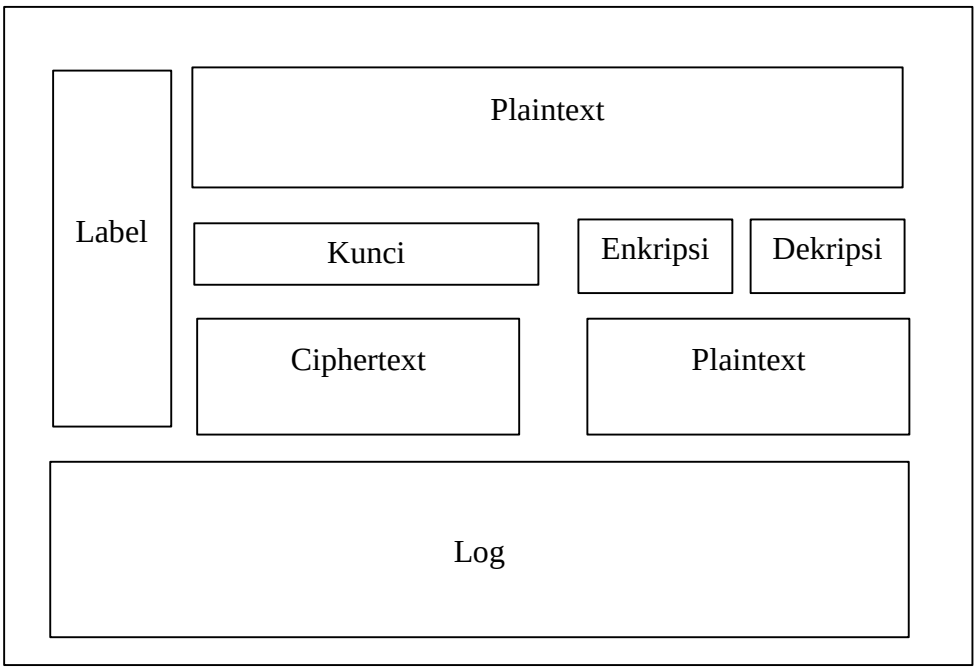
Gambar 3.5 Tampilan Menu Utama

Menu ini memiliki berapa sub-menu antara lain:

- Vigenere Cipher
- About
- Logo
- Info
- Keluar

3.4.2 Menu Vigenere Cipher

Menu ini adalah yang terpenting dalam program aplikasi karena menjalankan tugas utama yaitu Vigenere Cipher. Menu ini berfungsi untuk melakukan proses enkripsi dan dekripsi. Menu ini terdiri dari input, proses, output dan riwayat perhitungan. Gambar 3.6 adalah tampilan menu ini.



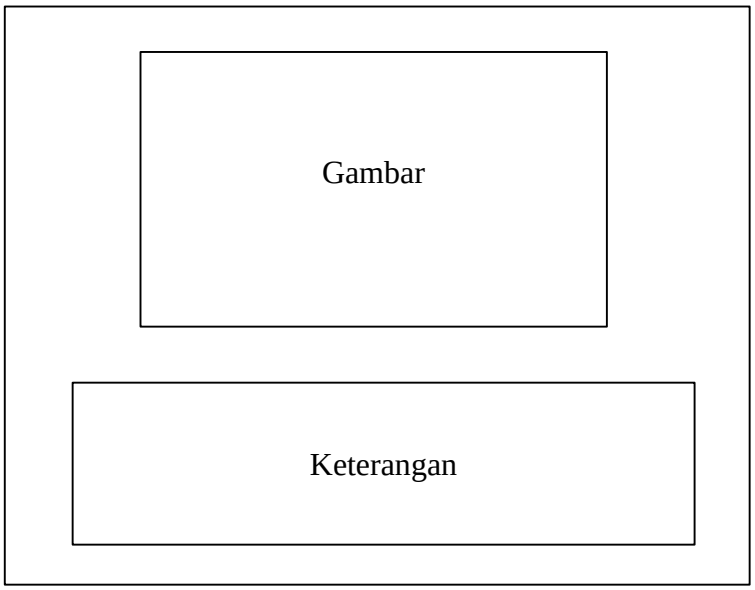
Gambar 3.6 Tampilan Menu Vigenere Cipher

Menu algoritma Vigenere Cipher memiliki beberapa bagian antara lain:

- Plaintext
- Ciphertext
- Kunci
- Tombol Enkripsi
- Tombol Dekripsi
- Log

3.4.3 Menu Info

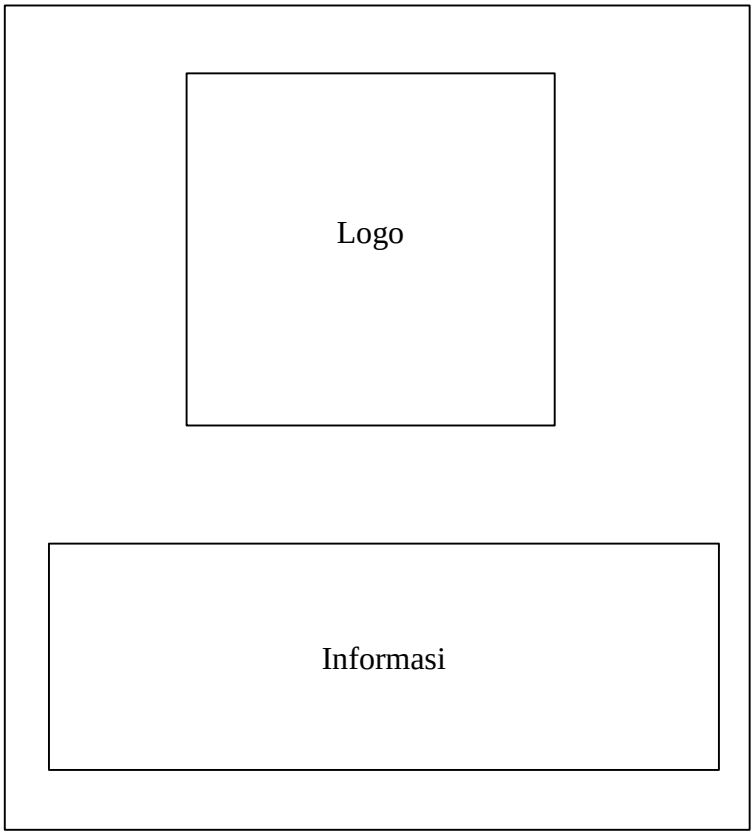
Menu ini menampilkan tentang keterangan singkat algoritma Vigenere Cipher. Menu ini memiliki dua buah objek, yaitu objek gambar dan keterangan. Gambar berikut ini adalah hasil perancangan menu Info.



Gambar 3.7 Tampilan Menu Info

3.4.4 Menu About

Menu ini menampilkan keterangan tentang penulis. Menu ini teridiri dari logo Universitas Pembangunan Panca Budi dan beberapa keterangan singkat. Menu ini terdiri dari dua objek, yaitu logo dan informasi. Gambar berikut ini adalah hasil tampilan dari menu About.



Gambar 3.8 Tampilan Menu About

BAB IV

HASIL DAN PEMBAHASAN

Hasil studi biasanya merujuk pada jawaban langsung untuk pertanyaan penelitian yang dihasilkan dari data. Diskusi adalah tentang menafsirkan hasil studi. Ketika mendiskusikan hasil studi, ini akan menghubungkan temuan studi dengan studi sebelumnya. Hal ini bertujuan mengontekstualisasikan kontribusi studi yang sudah dilakukan. Dalam melakukan implementasi, ada beberapa hal yang harus dipenuhi. Spesifikasi sistem dan implementasi antarmuka adalah dua hal yang saling berhubungan yang harus dilakukan untuk membuktikan kebenaran dari penelitian yang dilakukan.

4.1 Spesifikasi Sistem

Spesifikasi sistem menjelaskan persyaratan operasional dan kinerja suatu sistem, seperti komputer. Ini dianggap sebagai dokumen tingkat tinggi yang menentukan fungsi global. Spesifikasi sistem membantu untuk menentukan pedoman operasional dan kinerja untuk suatu sistem. Ini dapat menguraikan bagaimana sistem diharapkan untuk melakukan, dan apa yang mungkin termasuk. Spesifikasi utama dapat mencakup definisi antarmuka, aturan desain dokumen, dan area fungsional. Spesifikasi sistem dapat diuraikan selama proses evaluasi dan disepakati selama proses pengujian.

4.1.1 Spesifikasi Perangkat Keras

Penerapan algoritma Vigenere Cipher pada metode kriptografi substitusi membutuhkan perangkat keras untuk menjalankan sistem. Hal ini sebagai sarana pendukung utama. Tabel 4.1 adalah spesifikasi perangkat keras yang digunakan pada penelitian ini.

Tabel 4.1 Spesifikasi perangkat keras

No.	Nama Komponen	Spesifikasi
1	Processor	Intel Core i5 2.4 GHz
2	RAM	8192 MB
3	Storage	500 GB
4	Display	14 inch

4.1.2 Spesifikasi Perangkat Lunak

Tahap spesifikasi perangkat lunak memiliki tujuan, deskripsi kebutuhan dan persiapan validasi aplikasi perangkat lunak. Deskripsi kebutuhan memunculkan file spesifikasi aplikasi perangkat lunak. Kebutuhan akan perangkat lunak sebagai sarana non-fisik sangat mendukung hasil keluaran. Tabel 4.2 adalah spesifikasi perangkat lunak yang digunakan pada penelitian ini.

Tabel 4.2 Spesifikasi perangkat lunak

No.	Nama Komponen	Spesifikasi
1	Sistem Operasi	Windows 10 64 Bit
2	IDE Pemrograman	Microsoft Visual Basic.NET 2010
3	Tangkap Gambar	Snipping Tool
4	Data Editor	Microsoft Excel

4.2 Implementasi Antarmuka

Menerapkan antarmuka berarti benar-benar melakukan implementasi untuk membuktikan kebenaran program aplikasi. Proses mendesain apapun akan memiliki langkah-langkah umum termasuk mengumpulkan persyaratan, mengidentifikasi solusi yang mungkin, menganalisis solusi tersebut, dll. Agar proses implementasi berhasil, perlu dilakukan pengujian terhadap data yang sudah diperoleh. Penulis berusaha untuk menggunakan metodologi yang telah terbukti menerapkan kepada sistem. Berikut ini adalah tahapan implementasi antarmuka yang dilakukan dengan beberapa bagian yang terpisah.

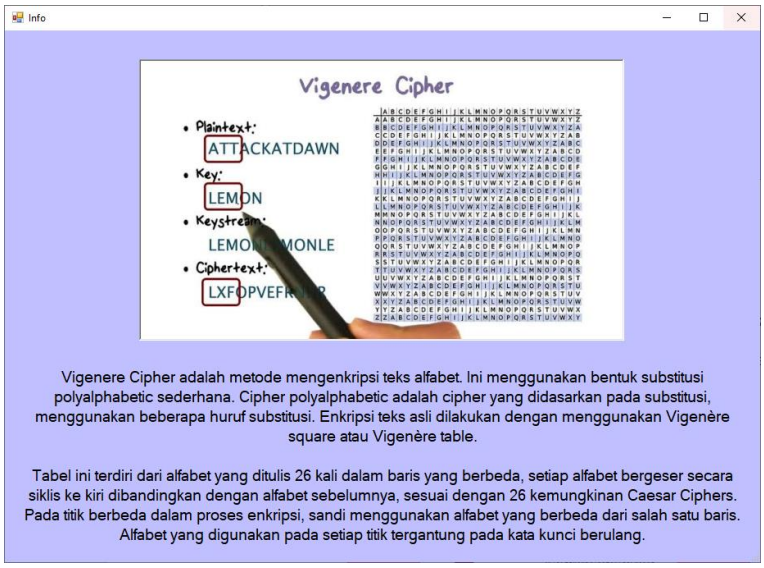
4.2.1 Halaman Menu Utama

Halaman menu utama adalah tampilan yang pertama sekali muncul pada saat program aplikasi dibuka. Ada beberapa menu yang akan dimunculkan untuk menentukan pilihan menu berikutya. Pengguna akan memilih ke bagian mana pengguna tersebut ingin jalankan. Menu utama bertujuan untuk memberikan pilihan fungi dari fasilitas-fasilitas yang ditawarkan pada suatu program aplikasi. Menu utama pada penelitian inii terdiri dari tiga buah sub-menu dan satu buah tombol untuk keluar dari aplikasi tersebut. Gambar 4.1 adalah hasil tampilan menu utama.

Gambar 4.1 Halaman Menu Utama

4.2.2 Halaman Info

Halaman info adalah menu yang menampilkan penjelasan singkat tentang algoritma Vigenere Cipher. Halaman ini akan menampilkan sebuah gambar dan sebuah keterangan. Gambar 4. 2 adalah hasil tampilan dari halaman info.



Gambar 4.2 Halaman Info

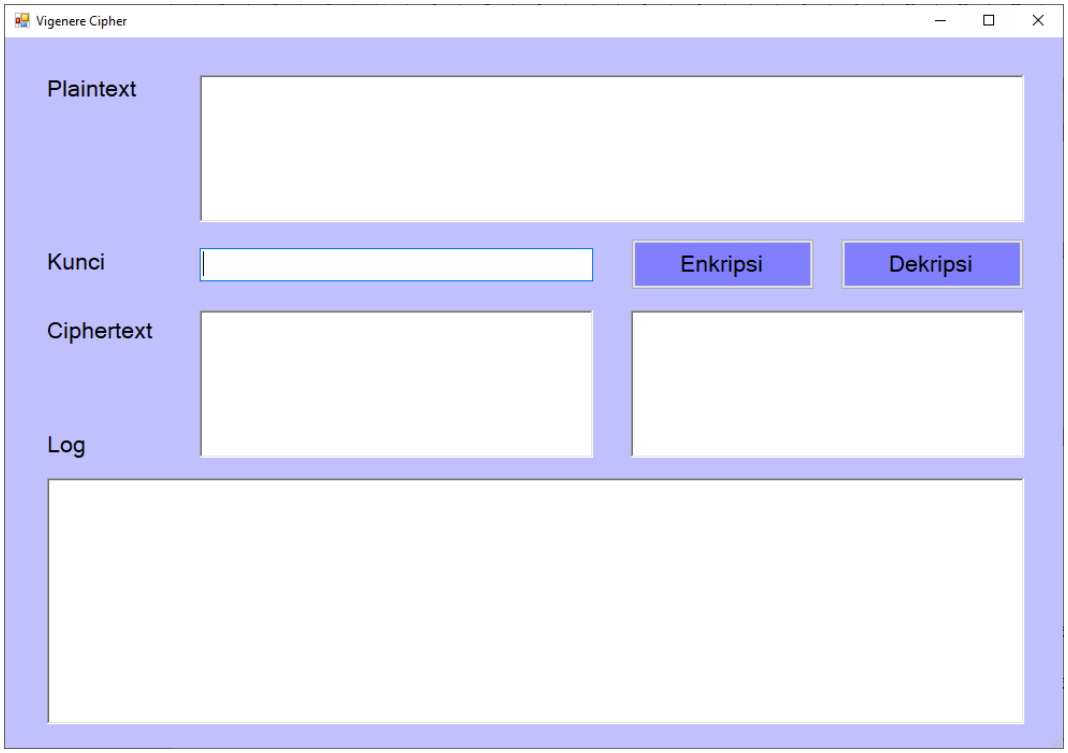
4.2.3 Halaman About

Halaman about adalah tampilan seputar keterangan mengenai penulis. Halaman ini menampilkan nama, NPM, fakutas, program studi dan universitas. Gamabr 4.3 adalah tampilan dari halaman About.

Gambar 4.3 Halaman About

4.2.4 Halaman Vigenere Cipher

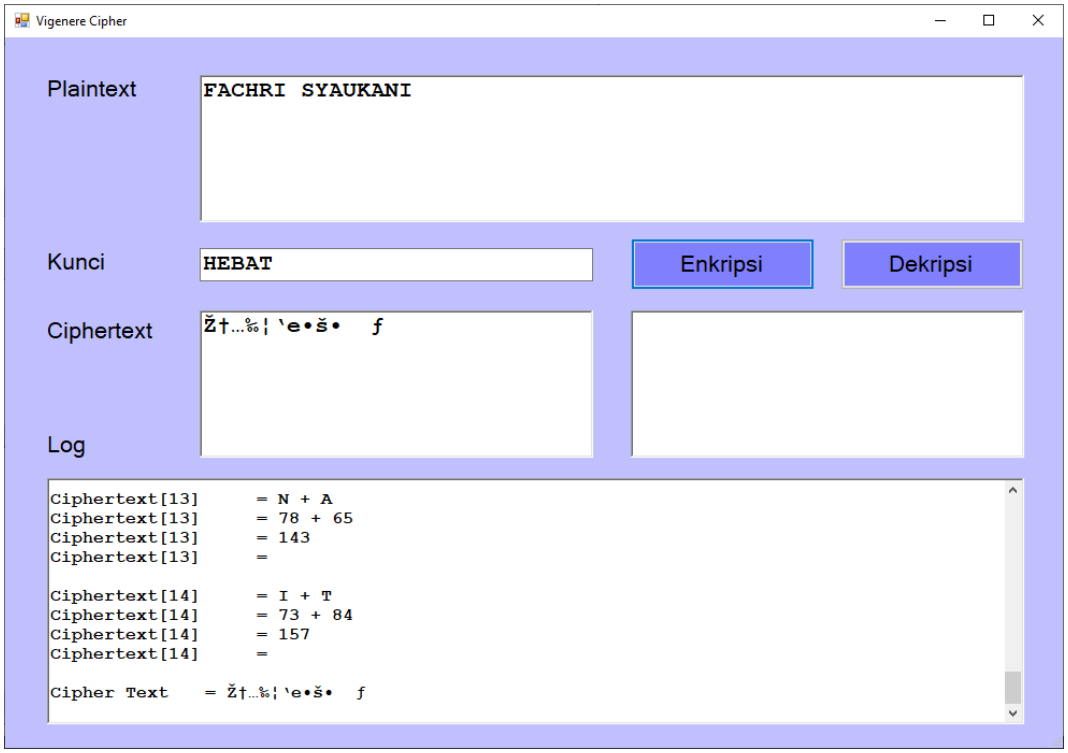
Halaman ini merupakan proses untuk melakukan enkripsi dan dekripsi. Pada halaman ini juga ditampilkan perhitungan lengkap algoritma Vigenere Cipher tersebut. Halaman terdiri dari dua buah plaintext, sebuah kunci dan sebuah ciphertext yang dibentuk dari objek textbox. Sementara untuk proses enkripsi dan dekripsi, halaman ini memiliki beberapa tombol. Gambar 4.4 adalah hasil tampilan dari halaman Vigenere Cipher.



Gambar 4.4 Halaman kriptografi stream cipher algoritma Vigenere

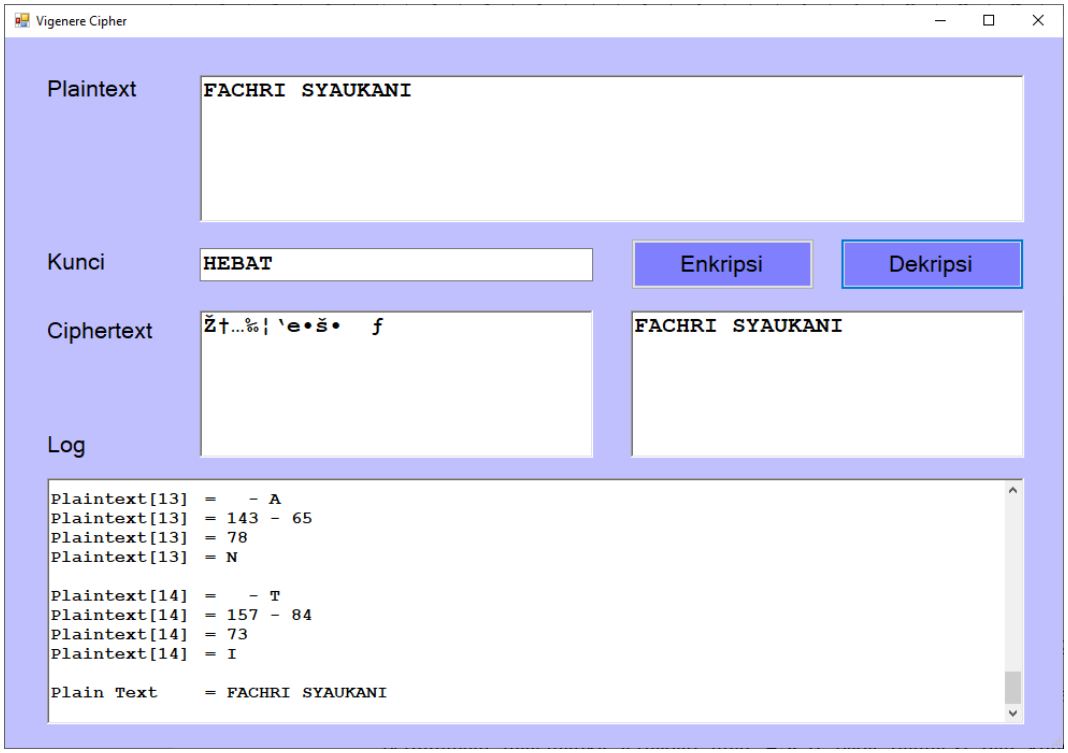
4.2.5 Hasil Perhitungan Algoritma Vigenere

Halaman ini berisi tentang hasil tangkap gambar dari proses yang dikerjakan oleh program aplikasi dalam melakukan proses enkripsi dan dekripsi. Plaintext dan Kunci adalah dua bagian yang harus diisi untuk menentukan ciphertext. Kedua nilai dari parameter ini akan diproses sehingga membentuk blok kunci. Blok kunci akan memiliki panjang yang sama dengan plaintext. Setiap karakter pada plaintext akan dilakukan pergeseran terhadap kunci untuk mendapatkan ciphertext. Gambar 4.5 adalah tampilan dari hasil perhitungan proses enkripsi algoritma Vigenere Cipher.



Gambar 4.5 Halaman enkripsi algoritma Vigenere Cipher

Proses dekripsi akan melakukan hal yang sama yaitu melakukan proses pergeseran ciphertext terhadap blok kunci sebelumnya. Hasil yang benar akan menampilkan bahwa plaintext sebelum proses enkripsi harus sama dengan plaintext yang dihasilkan setelah proses dekripsi. Pada textbox plaintext harus menampilkan nilai yang sama seperti pada plaintext sebelumnya. Perhitungan dinyatakan salah apabila ada satu karakter yang memiliki perbedaan nilai ASCII dengan plaintext sebelumnya. Gambar 4. 6 adalah tampilan dari hasil perhitungan proses dekripsi algoritma Vigenere Cipher.



Gambar 4.6 Halaman dekripsi algoritma Vigenere Cipher

4.3 Pengujian Perhitungan

Pengujian adalah melakukan uji coba hasil perhitungan proses enkripsi dan dekripsi algoritma Vigenere Cipher. Pengujian dilakukan dengan melakukan perhitungan matematika terhadap nilai ASCII pada plaintext dan kunci dan sebaliknya pada proses dekripsi akan melakukan perhitungan nilai ASCII ciphertext dan kunci. Hasil program aplikasi harus sesuai dengan hasil perhitungan yang dilakukan secara manual. Sebelum melakukan perhitungan, ada beberapa tahap yang perlu dilakukan yaitu memberikan nilai pada plaintext dan kunci. Berikut ini adalah penjelasan dan perhitungan lengkap proses dekripsi dan enkripsi pada algoritma Vigenere Cipher.

Pengujian Pertama

Plaintext = UNIVERSITAS PEMBANGUNAN PANCA BUDI

Kunci Vigenere = FACHRI

Hasil Enkripsi

Tabel 4.3 Hasil enkripsi pengujian pertama

PT	PT ASCII	KUNCI	KUNCI ASCII	CT ASCII	CT
U	85	F	70	155	›
N	78	A	65	143	•
I	73	C	67	140	Œ
V	86	H	72	158	ž
E	69	R	82	151	—
R	82	I	73	155	›
S	83	F	70	153	™
I	73	A	65	138	Š
T	84	C	67	151	—
A	65	H	72	137	‰
S	83	R	82	165	¥
	32	I	73	105	i
P	80	F	70	150	–
E	69	A	65	134	†
M	77	C	67	144	•
B	66	H	72	138	Š
A	65	R	82	147	“
N	78	I	73	151	—
G	71	F	70	141	•
U	85	A	65	150	–

N	78	C	67	145	‘
A	65	H	72	137	‰
N	78	R	82	160	
	32	I	73	105	i
P	80	F	70	150	–
A	65	A	65	130	,
N	78	C	67	145	‘
C	67	H	72	139	‹
A	65	R	82	147	“
	32	I	73	105	i
B	66	F	70	136	ˆ
U	85	A	65	150	–
D	68	C	67	135	‡
I	73	H	72	145	‘

Hasil Dekripsi

Tabel 4.4 Hasil dekripsi pengujian pertama

CT	CT ASCII	KUNCI	KUNCI ASCII	PT ASCII	PT
›	155	F	70	85	U
•	143	A	65	78	N
Œ	140	C	67	73	I
ž	158	H	72	86	V
—	151	R	82	69	E
›	155	I	73	82	R
™	153	F	70	83	S
Š	138	A	65	73	I
—	151	C	67	84	T
‰	137	H	72	65	A

¥	165	R	82	83	S
i	105	I	73	32	
–	150	F	70	80	P
†	134	A	65	69	E
•	144	C	67	77	M
Š	138	H	72	66	B
“	147	R	82	65	A
—	151	I	73	78	N
•	141	F	70	71	G
–	150	A	65	85	U
‘	145	C	67	78	N
‰	137	H	72	65	A
	160	R	82	78	N
i	105	I	73	32	
–	150	F	70	80	P
,	130	A	65	65	A
‘	145	C	67	78	N
‹	139	H	72	67	C
“	147	R	82	65	A
i	105	I	73	32	
ˆ	136	F	70	66	B
–	150	A	65	85	U
‡	135	C	67	68	D
‘	145	H	72	73	I

Pengujian Kedua

Plaintext = THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

Kunci Vigenere = UNPAB

Hasil Enkripsi

Tabel 4.5 Hasil enkripsi pengujian kedua

PT	PT ASCII	KUNCI	KUNCI ASCII	CT ASCII	CT
T	84	U	85	169	©
H	72	N	78	150	–
E	69	P	80	149	•
	32	A	65	97	a
Q	81	B	66	147	“
U	85	U	85	170	ª
I	73	N	78	151	—
C	67	P	80	147	“
K	75	A	65	140	Œ
	32	B	66	98	b
B	66	U	85	151	—
R	82	N	78	160	
O	79	P	80	159	Ÿ
W	87	A	65	152	˜
N	78	B	66	144	•
	32	U	85	117	u
F	70	N	78	148	”
O	79	P	80	159	Ÿ
X	88	A	65	153	™
	32	B	66	98	b

J	74	U	85	159	Ÿ
U	85	N	78	163	£
M	77	P	80	157	•
P	80	A	65	145	‘
S	83	B	66	149	•
	32	U	85	117	u
O	79	N	78	157	•
V	86	P	80	166	¦
E	69	A	65	134	†
R	82	B	66	148	”
	32	U	85	117	u
T	84	N	78	162	¢
H	72	P	80	152	˜
E	69	A	65	134	†
	32	B	66	98	b
L	76	U	85	161	¡
A	65	N	78	143	•
Z	90	P	80	170	ª
Y	89	A	65	154	š
	32	B	66	98	b
D	68	U	85	153	™
O	79	N	78	157	•
G	71	P	80	151	—

Hasil Dekripsi

Tabel 4.6 Hasil dekripsi pengujian kedua

CT	CT ASCII	KUNCI	KUNCI ASCII	PT ASCII	PT
©	169	U	85	84	T
–	150	N	78	72	H
•	149	P	80	69	E
a	97	A	65	32	
“	147	B	66	81	Q
ª	170	U	85	85	U
—	151	N	78	73	I
“	147	P	80	67	C
Œ	140	A	65	75	K
b	98	B	66	32	
—	151	U	85	66	B
	160	N	78	82	R
Ÿ	159	P	80	79	O
˜	152	A	65	87	W
•	144	B	66	78	N
u	117	U	85	32	
”	148	N	78	70	F
Ÿ	159	P	80	79	O
™	153	A	65	88	X
b	98	B	66	32	
Ÿ	159	U	85	74	J
£	163	N	78	85	U
•	157	P	80	77	M
‘	145	A	65	80	P
•	149	B	66	83	S

u	117	U	85	32	
•	157	N	78	79	O
¦	166	P	80	86	V
†	134	A	65	69	E
”	148	B	66	82	R
u	117	U	85	32	
¢	162	N	78	84	T
˜	152	P	80	72	H
†	134	A	65	69	E
b	98	B	66	32	
¡	161	U	85	76	L
•	143	N	78	65	A
ª	170	P	80	90	Z
š	154	A	65	89	Y
b	98	B	66	32	
™	153	U	85	68	D
•	157	N	78	79	O
—	151	P	80	71	G

BAB V

PENUTUP

5.1 Kesimpulan

Penulis memiliki beberapa kesimpulan yang dapat ditarik berdasarkan hasil pengujian yang sudah dilakukan. Beberapa kesimpulan yang diperoleh adalah antara lain:

1. Algoritma Vigenere Cipher bekerja dengan baik dalam melakukan enkripsi dan dekripsi.
2. Panjang kunci dapat diciptakan sepanjang plaintext yang ada.
3. Proses enkripsi algoritma Vigenere Cipher bekerja dengan menggeser karakter dari plaintext sebanyak kunci.
4. Proses dekripsi algoritma Vigenere Cipher bekerja melakukan pengurangan kembali hasil pergeseran.

5.2 Saran

Penelitian juga memiliki beberapa saran dalam pengembangan program aplikasi ini agar menjadi lebih baik. Ada beberapa pengembangan yang dapat penulis paparkan untuk meningkatkan kualitas program aplikasi, antara lain:

1. Hendaknya kunci Vigenere Cipher dikembangkan agar lebih maksimal.
2. Vigenere Cipher akan lebih baik jika dikombinasikan dengan algoritma lainnya untuk meningkatkan tingkat keamanan.
3. Vigenere Cipher hendaknya dapat digunakan sistem operasi Android.

DAFTAR PUSTAKA

Akbar, A. (2018). Pembangunan Model Electronic Government Pemerintahan Desa Menuju Smart Desa. Jurnal Teknik Dan Informatika, 5(1), 1-5.

Aryza, S., Irwanto, M., Lubis, Z., Siahaan, A. P. U., Rahim, R., & Furqan, M. (2018). A Novelty Design Of Minimization Of Electrical Losses In A Vector Controlled Induction Machine Drive. In Iop Conference Series: Materials Science And Engineering (Vol. 300, No. 1, P. 012067). Iop Publishing.

Barus, S., Sitorus, V. M., Napitupulu, D., Mesran, M., & Supiyandi, S. (2018). Sistem Pendukung Keputusan Pengangkatan Guru Tetap Menerapkan Metode Weight Aggregated Sum Product Assesment (Waspas). Jurnal Media Informatika Budidarma, 2(2).

Badawi, A. (2018). Evaluasi Pengaruh Modifikasi Three Pass Protocol Terhadap Transmisi Kunci Enkripsi.

Batubara, S., Wahyuni, S., & Hariyanto, E. (2018, September). Penerapan Metode Certainty Factor Pada Sistem Pakar Diagnosa Penyakit Dalam. In Seminar Nasional Royal (Senar) (Vol. 1, No. 1, Pp. 81-86).

Hidayat, A. (2012). Algoritma Kriptografi Vigenere Cipher. Retrieved November 4, 2019, from https://arfianhidayat.com/algoritma-kriptografi-vigenere-cipher

Ian Ruotsala. (2019). What Are Computer Algorithms, and How Do They Work? Retrieved November 4, 2019, from https://www.howtogeek.com/howto/44052/htg-explains-what-are-computer-algorithms-and-how-do-they-work/

Jogiyanto, H. M. (2006). *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

Ladjamudin, A.-B. bin. (2005). *Analisis dan Desain Sistem Informasi*. Yogyakarta: Graha Ilmu.

Nakatsu, R. T. (2009). *Reasoning with Diagrams : Decision-Making and Problem- Solving with Diagrams.* John Wiley & Sons.

Rahmel, D. (2008). *Visual Basic.NET*. New York: McGraw-Hill.

Rummel, J. F., & Ballaine, W. C. (1963). *Research Methodology in Business*. New York: Harper & Row, Publication.

Saputra, Muhammad Juanda, And Nurul Hamdi. "Rancang Bangun Aplikasi Sejarah Kebudayaan Aceh Berbasis Android Studi Kasus Dinas Kebudayaan Dan Pariwisata Aceh." Journal Of Informatics And Computer Science 5.2 (2019): 147-157.

Sumartono, I. (2019). Analisis Perancangan Sistem Rencana Pembelajaran Terpadu Dalam Mendukung Efektivitas Dan Mutu Pengajaran Dosen (Studi Kasus: Fakultas Ilmu Komputer Universitas Pembangunan Panca Budi). Jurnal Teknik Dan Informatika, 6(1), 12-17.

Sharif, A. (2019). Data Mining Untuk Memprediksi Itemset Promosi Penjualan Barang Menggunakan Metode Market Basket Analysis (Mba)(Studi Kasus: Toko Sentra Ponsel). Jurnal Mantik Penusa, 3(2, Des).

Stallings, W. (2013). *Cryptography and Network Security: Principles and Practice*. New Jersey: Prentice Hall Press.

Stallings, William. (2005). *Cryptography and Network Security Principles and Practices* (4th ed.). Prentice Hall.

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

Technopedia. (2019). Unified Modeling Language (UML). Retrieved from https://www.techopedia.com/definition/3243/unified-modeling-language-uml

Tasril, V., Khairul, K., & Wibowo, F. (2019). Aplikasi Sistem Informasi Untuk Menentukan Kualitas Beras Berbasis Android Pada Kelompok Tani Jaya Makmur Desa Benyumas. Informatika, 7(3), 133-142.

Utomo, R. B. (2019). Aplikasi Pembelajaran Manasik Haji Dan Umroh Berbasis Multimedia Dengan Metode User Centered Design (Ucd). J-Sakti (Jurnal Sains Komputer Dan Informatika), 3(1), 68-79.

UTM. (2019). Concept: Use-Case Model. Retrieved September 19, 2019, from http://www.utm.mx/~caff/doc/OpenUPWeb/openup/guidances/concepts/use_case_model_CD178AF9.html

Uml-diagrams.org. (2019). Use case diagrams are UML diagrams describing units of useful functionality (use cases) performed by a system in collaboration with external users (actors). Retrieved November 3, 2019, from https://www.uml-diagrams.org/use-case-diagrams.html

Wasserkrug, S., Dalvi, N., Munson, E. V., Gogolla, M., Sirangelo, C., Fischer- Hübner, S., … Snodgrass, R. T. (2009). 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

Wijaya, R. F., Utomo, R. B., Niska, D. Y., & Khairul, K. (2019). Aplikasi Petani Pintar Dalam Monitoring Dan Pembelajaran Budidaya Padi Berbasis Android. Rang Teknik Journal, 2(1).

Zen, Muhammad. "Perbandingan Metode Dimensi Fraktal Dan Jaringan Syaraf Tiruan Backpropagation Dalam Sistem Identifikasi Sidik Jari Pada Citra Digital." Jitekh 7.2 (2019): 42-50.