IMPLEMENTASI ALGORITMA KRIPTOGRAFI VIGENERE CIPHER DALAM MENGAMANKAN PENGIRIMAN DATA 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	:	**ARNO PANDI**
NPM	:	**1414370555**
PROGRAM STUDI	:	**SISTEM KOMPUTER**

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2019

ABSTRAK

ARNO PANDI
Implementasi Algoritma Kriptografi Vigenere Cipher Dalam Mengamankan Pengiriman Data Teks
2019

Pencurian data adalah tindakan mencuri informasi berbasis komputer dari korban yang tidak mengetahui dengan tujuan membahayakan privasi atau mendapatkan informasi rahasia. Pencurian data semakin menjadi masalah bagi pengguna komputer individu, serta perusahaan besar. Setiap individu tidak tertutup kemungkinan akan kecurian informasi karena kelalaian seseorang tersebut. Dalam menjaga data, dibutuhkan suatu teknik yang dapat membantu seseorang dalam merahasiakan data tersebut. Pencurian data tidak dapat dihindari, tetapi keamanan data dapat ditingkatkan agar tidak terjadi penyalahgunaan data. Algoritma Vigenere yang merupakan salah satu teknik kriptografi dapat memantu mengamankan data dari penyalahgunaan data. Algoritma ini bekerja dengan cara menggeser tiap karakter pada plaintext sebesar kunci yang disediakan. Kunci yang digunakan dapat berupa deretan karakter atau merupakan kata-kata yang sulit untuk ditebak oleh orang yang ingin melakukan kejahatan. Dengan menerapkan algoritma Vigenere Cipher, keamanan data akan lebih terjamin.

Kata Kunci: algoritma, keamanan, ekripsi, enkripsi, kriptografi, Vigenere

DAFTAR ISI

KATA PENGANTAR ..... **i**
DAFTAR ISI ..... **ii**
DAFTAR GAMBAR ..... **iv**
DAFTAR TABEL ..... **v**
BAB I PENDAHULUAN **1**
1.1 Latar Belakang 1
1.2 Rumusan Masalah 2
1.3 Batasan Masalah 2
1.4 Tujuan Penelitian 3
1.5 Manfaat Penelitian 3

BAB II LANDASAN TEORI **4**
2.1 Data 4
2.1.1 Bagaimana Data Disimpan 5
2.1.2 Jenis data 6
2.1.3 Pengelolaan dan Penggunaan Data 7
2.2 Keamanan Data 8
2.2.1 Pentingnya Keamanan Data 9
2.2.2 Solusi Keamanan Data 10
2.2.3 Kerahasiaan 11
2.2.4 Integritas 12
2.2.5 Ketersediaan 13
2.2.6 Kontrol Akses 13
2.3 Algoritma 14
2.3.1 Desain Konseptual 16
2.3.2 Tugas Algoritma 17
2.3.3 Rekayasa Algoritma 18
2.4 Kriptografi 18
2.4.1 Kriptografi Simetris 20
2.4.2 Kriptografi Asimetris 21
2.5 Vigenère Cipher 22
2.5.1 Enkripsi 22
2.5.2 Dekripsi 23
2.6 Unified Modelling Language (UML) 24
2.6.1 Use Case Diagram 25
2.6.2 Activity Diagram 28
2.6.3 Flowchart 29
2.6.4 Class Diagram 32

BAB III METODE PENELITIAN **34**
3.1 Kerangka Penelitian 34
3.2 Perancangan Penelitian 36

3.2.1 Use Case Diagram 37
3.2.2 Activity Diagram 38
3.2.3 Flowchart Enkripsi 40
3.2.4 Flowchart Dekripsi 41
3.3 Desain Interface 42
3.3.1 Menu Utama 42
3.3.2 Menu Vigenere Cipher 43
3.3.3 Menu Info 44
3.3.4 Menu About 45

BAB IV HASIL DAN PEMBAHASAN 46
4.1 Spesifikasi Sistem 46
4.1.1 Spesifikasi Perangkat Keras 47
4.1.2 Spesifikasi Perangkat Lunak 47
4.2 Implementasi Antarmuka 48
4.2.1 Halaman Menu Utama 48
4.2.2 Halaman Info 49
4.2.3 Halaman About 50
4.2.4 Halaman Vigenere Cipher 50
4.2.5 Hasil Enkripsi 51
4.2.6 Hasil Dekripsi 52
4.3 Test Perhitungan 53

BAB V PENUTUP 59
5.1 Kesimpulan 59
5.2 Saran 59

DAFTAR PUSTAKA

DAFTAR GAMBAR

Gambar 2.1 Skema kriptografi simetris 21
Gambar 2.2 Skema kriptografi asimetris 21
Gambar 2.3 Tabel Vigenere 23
Gambar 2.4. Use-case Diagram ATM 26
Gambar 3.1 Kerangka Penelitian 35
Gambar 3.2 Use Case Diagram 38
Gambar 3.3 Activity Diagram 39
Gambar 3.4 Flowchart enkripsi algoritma Vigenere 40
Gambar 3.5 Flowchart dekripsi algoritma Vigenere 41
Gambar 3.6 Tampilan Menu Utama 42
Gambar 3.7 Tampilan Menu Vigenere Cipher 43
Gambar 3.8 Tampilan Menu Info 44
Gambar 3.9 Tampilan Menu About 45
Gambar 4.1 Halaman Menu Utama 49
Gambar 4.2 Halaman Info 49
Gambar 4.3 Halaman About 50
Gambar 4.4 Halaman kriptografi stream cipher algoritma Vigenere 51
Gambar 4.5 Halaman enkripsi algoritma Vigenere Cipher 52
Gambar 4.6 Halaman dekripsi algoritma Vigenere Cipher 53

DAFTAR TABEL

Tabel 2.1 Simbol Use Case Diagram 27
Tabel 2.2 Simbol Activity Diagram 29
Tabel 2.3 Simbol Flowchart 31
Tabel 2.4 Simbol Class Diagram 33
Tabel 4.1 Spesifikasi perangkat keras 47
Tabel 4.2 Spesifikasi perangkat lunak 47
Tabel 4.3 Hasil enkripsi pengujian pertama 54
Tabel 4.4 Hasil dekripsi pengujian pertama 55
Tabel 4.5 Hasil enkripsi pengujian kedua 56
Tabel 4.6 Hasil dekripsi pengujian kedua 57

KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Kuasa, karena dengan berkat dan rahmatNya penulis masih diberikan kesempatan untuk menyelesaikan skripsi ini sebagaimana mestinya. Skripsi ini berjudul "**IMPLEMENTASI ALGORITMA KRIPTOGRAFI VIGENERE CIPHER DALAM MENGAMANKAN PENGIRIMAN DATA TEKS**". Dalam kesempatan ini, penulis mengucapkan rasa terima kasih yang tak terhingga kepada pihak-pihak yang telah membantu dalam penyelesaian skripsi ini. Penulis ingin mengucapkan terima kasih kepada :

1. Orang tua saya yang selalu memberikan semangat, dukungan dan motivasi dalam penyusunan skripsi ini.
2. Bapak Dr. H. Muhammad Isa Indrawan, S.E, M.M., selaku Rektor Universitas Pembangunanan Panca Budi Medan.
3. Rektor I Bapak Ir. Bhakti Alamsyah, M.T, Ph.D.
4. Bapak Hamdani, ST., M.T., selaku Dekan Fakultas Sains dan Teknologi Universitas Pembangunan Panca Budi Medan.
5. Bapak Eko Hariyanto, S.Kom., M.Kom, selaku Ketua Program Studi Sistem Komputer Universitas Pembangunan Panca Budi Medan.
6. Bapak Andysah Putera Utama Siahaan, S.Kom., M.Kom., Ph.D., selaku Dosen Pembimbing I yang telah memberikan arahan dan membimbing dalam peyelesaian skripsi ini.
7. Bapak Supiyandi, S.Kom., M.Kom, selaku Dosen Pembimbing II yang telah memberikan ilmu pengetahuan, serta bimbingan dalam penyelesaian skripsi ini.
8. Dosen-dosen pada Program Studi Sistem Komputer Fakultas Sains dan Teknologi Universitas Pembangunan Panca Budi Medan.
9. Seluruh staff dan karyawan pada Universitas Pembangunan Panca Budi Medan.
10. Seluruh teman-teman penulis dari program studi Sistem Komputer, Fakultas Ilmu Komputer Universitas Pembangunan Panca Budi, Medan

Penulis juga menyadari bahwa penyusunan skripsi ini belum mendapaatkan kesempurnaan dalam segi penulisan ataupun isi. Hal ini disebebkan pengetahuan penulis yang sangat terbatas. Penulis sangat mengharapkan adanya kritik dan saran dari pembaca untuk dapat memperbaiki isi skripsi.

Medan, 19 Desember 2019
Penulis

Arno Pandi
1414370555

BAB I

PENDAHULUAN

1.1 Latar Belakang

Informasi merupakan harta yang paling berharga untuk dijaga. Data dapat berupa informasi-informasi penting yang tidak boleh tersebar luas karena memiliki kandungan yang berbahaya atau vital. Pengiriman informasi jenis ini harus dilakukan dengan cara seksama dan tidak diketahui oleh orang lin. Jika informasi ini jauth ke tangan orang yang tidak bertanggung jawab, maka informasi ini dapat disalahgunakan atau dijadikan sumber pencarian uang secara ilegal. Untuk mengamankan informasi tersebut, dibutuhkan teknik yang baik dalam mengubah informasi tersebut menjadi untaian kata yang tidak dapat dimengerti oleh orang lain. Dalam dunia komputer, alat bantu untuk melakukan ini disebut dengan kriptografi. Kriptografi adalah seni dalam mengubah pesan asli menjadi pesan tak terbaca sehingga pesan tersebut tidak dapat dimengerti pada saat diambil oleh orang yang tidak bertanggung jawab. Kriptografi merupakan hal yang tidak mudah secara umum. Tetapi ada banyak teknik dalam melakukan kriptografi yang mudah. Metode kriptografi cukup aman untuk digunakan dan dapat menjadi pertahanan untuk menghindari serangan. Metode yang digunakan untuk pengamanan data pada penelitian ini adalah Vigenere Cipher. Metode ini adalah salah satu metode substitusi dimana karakter plaintext akan digantikan dengan karakter yang ada pada tabel ASCII dengan cara menggeser posisi karakter tersebut dengan sebuah kunci.

Dalam proses enkripsi, algoritma ini menggunakan cara mengenkripsi plaintext menjadi ciphertext sehingga pesan asli tersandikan. Algoritma dari enkripsi adalah fungsi-fungsi yang digunakan untuk melakukan fungsi enkripsi dan dekripsi.

Untuk mendukung pembuktian proses enkripsi dan dekripsi, maka akan diciptakan suatu aplikasi yang akan dibuat oleh penulis adalah dengan menggunakan Visual Studio 2010 dengan menggunakan kriptografi Vigenere Cipher. Berdasarkan latar belakang di atas maka penulis tertarik untuk memilih judul "**Implementasi Algoritma Kriptografi Vigenere Cipher Dalam Mengamankan Pengiriman Data Teks**".

1.2 Rumusan Masalah

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

1. Bagaimana melakukan proses enkripsi dan dekripsi dengan algoritma Vigenere Cipher?
2. Bagaimana menentukan pergeseran kunci sebagai pengaman algoritma Vigenere Cipher?
3. Bagaimana menentukan modulo pada algoritma Vigenere Cipher?

1.3 Batasan Masalah

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

1. Algoritma Vigenere mengunakan karakter berdasarkan tabel ASCII.
2. Batas karakter yang digunakan adalah sebanyak 1000 karakter.
3. Pesan yang digunakan sebagai plaintext adalah pesan berbasis teks.

1.4 Tujuan Penelitian

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

1. Untuk melakukan proses enkripsi dan dekripsi dengan algoritma Vigenere Cipher.
2. Untuk menentukan pergeseran kunci sebagai pengaman algoritma Vigenere Cipher.
3. Untuk menentukan modulo pada algoritma Vigenere Cipher.

1.5 Manfaat Penelitian

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

1. Dapat mengamankan pesan yang akan dikirim ke orang lain.
2. Informasi yang dikirimkan tidak mudah dapat dipecahkan sehingga terjadi penyalahgunaan informasi.

BAB II

LANDASAN TEORI

2.1 Data

Data, dalam konteks komputasi, mengacu pada bagian informasi digital yang berbeda. Data biasanya diformat dengan cara tertentu dan dapat ada dalam berbagai bentuk, seperti angka, teks, dll. Ketika digunakan dalam konteks media transmisi, data merujuk ke informasi dalam format digital biner. Data adalah istilah luas dalam teknologi komputer, tetapi sering digunakan untuk mengidentifikasi dan memisahkan informasi dari bit belaka. Dalam telekomunikasi, data sering merujuk pada informasi digital, bukan analog. Tidak seperti transmisi analog, yang memerlukan koneksi garis keras selama durasi transmisi, data digital dikirim dalam paket (Sun, Zhang, Xiong, & Zhu, 2014).

Dalam komputasi, data adalah informasi yang telah diterjemahkan ke dalam bentuk yang efisien untuk pergerakan atau pemrosesan. Relatif terhadap komputer dan media transmisi saat ini, data adalah informasi yang diubah menjadi bentuk digital biner. Data dapat diterima untuk digunakan sebagai subjek tunggal atau subjek jamak. Data mentah adalah istilah yang digunakan untuk menggambarkan data dalam format digital paling dasar.

Konsep data dalam konteks komputasi berakar pada karya Claude Shannon, seorang ahli matematika Amerika yang dikenal sebagai bapak teori informasi. Dia mengantarkan konsep digital biner berdasarkan penerapan logika Boolean dua nilai ke sirkuit elektronik. Format digit biner mendasari CPU,

memori semikonduktor dan disk drive, serta banyak perangkat periferal yang umum dalam komputasi saat ini. Input komputer awal untuk kontrol dan data berupa kartu punch, diikuti oleh pita magnetik dan hard disk.

Pada awalnya, pentingnya data dalam komputasi bisnis menjadi jelas dengan popularitas istilah "pemrosesan data" dan "pemrosesan data elektronik," yang, untuk beberapa waktu, datang untuk mencakup keseluruhan dari apa yang sekarang dikenal sebagai teknologi informasi. Selama sejarah komputasi perusahaan, spesialisasi terjadi, dan profesi data yang berbeda muncul seiring dengan pertumbuhan pemrosesan data perusahaan.

2.1.1 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 megabita dan gigabita.

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).

2.1.2 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.

2.1.3 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 analis bisnis dan pemimpin bisnis. Meningkatnya penekanan pada menemukan pola dan memprediksi hasil bisnis telah mengarah pada pengembangan teknik penambangan data (Barone, Williams, & Micklos, 2017).

2.2 Keamanan Data

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 (Rao & Selvamani, 2015).

Keamanan data mengacu pada langkah-langkah privasi digital pelindung yang diterapkan untuk mencegah akses tidak sah ke komputer, database, dan situs web. Keamanan data juga melindungi data dari korupsi. Keamanan data adalah aspek penting dari TI untuk organisasi dari berbagai ukuran dan tipe. Keamanan data juga dikenal sebagai keamanan informasi atau keamanan komputer.

Contoh teknologi keamanan data termasuk backup, masking data dan penghapusan data. Ukuran teknologi keamanan data utama adalah enkripsi, di mana data digital, perangkat lunak / perangkat keras, dan hard drive dienkripsi dan karenanya tidak dapat dibaca oleh pengguna dan peretas yang tidak sah. Salah satu metode yang paling umum dijumpai dalam mempraktikkan keamanan data adalah penggunaan otentikasi. Dengan otentikasi, pengguna harus memberikan kata sandi, kode, data biometrik, atau bentuk data lainnya untuk memverifikasi identitas sebelum akses ke sistem atau data diberikan. Keamanan data juga sangat penting untuk catatan perawatan kesehatan, sehingga pendukung kesehatan dan praktisi medis di AS dan negara-negara lain berupaya menerapkan privasi rekam medis elektronik dengan menciptakan kesadaran tentang hak-hak pasien terkait

dengan pelepasan data ke laboratorium, dokter, rumah sakit dan fasilitas medis lainnya.

2.2.1 Pentingnya Keamanan Data

Semua bisnis saat ini menangani data hingga taraf tertentu. Dari raksasa perbankan yang menangani data pribadi dan keuangan dalam volume besar hingga bisnis satu orang yang menyimpan detail kontak pelanggannya di ponsel, data berperan di perusahaan baik besar maupun kecil.

Tujuan utama keamanan data adalah untuk melindungi data yang dikumpulkan, disimpan, diterima, atau ditransmisikan oleh suatu organisasi. Kepatuhan juga merupakan pertimbangan utama. Tidak masalah perangkat, teknologi, atau proses mana yang digunakan untuk mengelola, menyimpan, atau mengumpulkan data, itu harus dilindungi. Pelanggaran data dapat menyebabkan kasus litigasi dan denda yang sangat besar, belum lagi kerusakan reputasi organisasi. Pentingnya melindungi data dari ancaman keamanan lebih penting saat ini daripada sebelumnya.

Keamanan data mengacu pada proses melindungi data dari akses yang tidak sah dan korupsi data sepanjang siklus hidupnya. Keamanan data termasuk enkripsi data, tokenization, dan praktik manajemen kunci yang melindungi data di semua aplikasi dan platform. Organisasi di seluruh dunia banyak berinvestasi dalam kemampuan pertahanan cyber teknologi informasi untuk melindungi aset penting mereka. Apakah suatu perusahaan perlu melindungi merek, modal intelektual, dan informasi pelanggan atau menyediakan kontrol untuk infrastruktur

penting, sarana untuk mendeteksi insiden dan merespons melindungi kepentingan organisasi memiliki tiga elemen umum: orang, proses, dan teknologi.

2.2.2 Solusi Keamanan Data

Data membutuhkan enkripsi dalam mengamankan informasi yang ada dalam data tersebut. Dengan enkripsi data canggih, tokenization, dan manajemen utama untuk melindungi data di seluruh aplikasi, transaksi, penyimpanan, dan platform big data, Teknik ini menyederhanakan perlindungan data sensitif bahkan dalam kasus penggunaan yang paling kompleks sekalipun. Beberapa model keamanan data antara lain:

- Keamanan akses cloud - Platform perlindungan yang memungkinkan Anda untuk pindah ke cloud dengan aman sambil melindungi data dalam aplikasi cloud.
- Enkripsi data - Solusi keamanan data-sentris dan tokenisasi yang melindungi data di lingkungan perusahaan, cloud, seluler, dan data besar.
- Modul keamanan perangkat keras - Modul keamanan perangkat keras yang menjaga data keuangan dan memenuhi persyaratan keamanan dan kepatuhan industri.
- Manajemen kunci - Solusi yang melindungi data dan memungkinkan kepatuhan regulasi industri.
- Enterprise Data Protection - Solusi yang menyediakan pendekatan data-centric end-to-end untuk perlindungan data perusahaan.

- Keamanan Pembayaran - Solusi menyediakan enkripsi dan tokenisasi point-to-point lengkap untuk transaksi pembayaran ritel, memungkinkan pengurangan lingkup PCI.
- Big Data, Hadoop, dan perlindungan data IofT - Solusi yang melindungi data sensitif di Danau Data - termasuk Hadoop, Teradata, Micro Focus Vertica, dan platform Big Data lainnya.
- Keamanan Aplikasi Seluler - Melindungi data sensitif di aplikasi seluler asli sembari menjaga data dari ujung ke ujung.
- Keamanan Peramban Web - Melindungi data sensitif yang diambil di peramban, dari titik pelanggan memasukkan pemegang kartu atau data pribadi dan menjaganya agar tetap terlindungi melalui ekosistem ke tujuan tuan rumah tepercaya.
- eMail Security - Solusi yang menyediakan enkripsi ujung ke ujung untuk email dan olahpesan seluler, menjaga informasi pribadi dan informasi kesehatan pribadi tetap aman dan pribadi.

2.2.3 Kerahasiaan

Kerahasiaan mengacu pada melindungi informasi agar tidak diakses oleh pihak yang tidak berwenang. Dengan kata lain, hanya orang yang diberi wewenang untuk melakukannya yang dapat memperoleh akses ke data sensitif. Bayangkan catatan bank harus dapat diakses, tentu saja, dan karyawan di bank yang membantu dalam menjalankan transaksi harus dapat mengaksesnya, tetapi tidak ada orang lain yang seharusnya. Kegagalan untuk menjaga kerahasiaan

berarti bahwa seseorang yang seharusnya tidak memiliki akses telah berhasil mendapatkannya, melalui perilaku yang disengaja atau karena kecelakaan. Kegagalan kerahasiaan seperti itu, umumnya dikenal sebagai pelanggaran, biasanya tidak dapat diperbaiki. Setelah rahasia itu terungkap, tidak ada cara untuk mengetahuinya. Jika catatan bank diposting di situs web publik, semua orang dapat mengetahui nomor rekening bank, saldo, dll., Informasi itu tidak dapat dihapus dari pikiran, kertas, komputer, dan tempat lain mereka. Hampir semua insiden keamanan utama yang dilaporkan di media saat ini melibatkan kerugian besar kerahasiaan. Jadi, secara ringkas, pelanggaran kerahasiaan berarti bahwa seseorang memperoleh akses ke informasi yang seharusnya tidak memiliki akses ke sana.

2.2.4 Integritas

Integritas mengacu pada memastikan keaslian informasi — bahwa informasi tidak diubah, dan bahwa sumber informasi itu asli. Bayangkan jika seseorang memiliki situs web dan Anda menjual produk di situs itu. Sekarang bayangkan penyerang dapat berbelanja di situs web dan dengan jahat mengubah harga produk Anda sehingga mereka dapat membeli apa pun dengan harga berapa pun yang mereka pilih. Itu akan menjadi kegagalan integritas karena informasi dalam hal ini, harga suatu produk telah diubah dan perubahan ini tidak dapat digagalkan. Contoh lain dari kegagalan integritas adalah ketika sesorang mencoba terhubung ke situs web dan penyerang jahat antara Anda dan situs web

mengalihkan lalu lintas ke situs web yang berbeda. Dalam hal ini, situs yang dituju tidak asli.

2.2.5 Ketersediaan

Ketersediaan berarti informasi dapat diakses oleh pengguna yang berwenang. Jika penyerang tidak dapat mengkompromikan dua elemen pertama dari keamanan informasi (lihat di atas) mereka dapat mencoba melakukan serangan seperti penolakan layanan yang akan menurunkan server, membuat situs web tidak tersedia untuk pengguna yang sah karena kurangnya ketersediaan.

2.2.6 Kontrol Akses

Kesalahan terbesar yang bisa dilakukan oleh perancang aplikasi adalah mengabaikan kontrol akses sebagai bagian dari fungsionalitas yang diperlukan. Jarang bahwa setiap pengguna atau sistem yang berinteraksi dengan suatu aplikasi harus memiliki hak yang sama di seluruh aplikasi itu. Beberapa pengguna mungkin memerlukan akses ke data tertentu dan bukan yang lain; beberapa sistem harus atau tidak dapat mengakses aplikasi. Akses ke komponen, fungsi, atau modul tertentu dalam aplikasi juga harus dikontrol. Kontrol akses juga penting untuk kepatuhan audit dan peraturan. Beberapa cara umum mengelola kontrol akses adalah:

1. Baca, tulis, dan jalankan hak istimewa: File
2. Kontrol akses berbasis peran: administrator, pengguna
3. Alamat IP akses berbasis host, nama mesin

4. Objek kode kontrol akses tingkat objek, banyak pembaca / penulis tunggal

2.3 Algoritma

Untuk membuat komputer melakukan apa pun, sesorang harus menulis program komputer. Untuk menulis program komputer, sesorang harus memberi tahu komputer, langkah demi langkah, persis apa yang sesorang inginkan. Komputer kemudian "mengeksekusi" program, mengikuti setiap langkah secara mekanis, untuk mencapai tujuan akhir. Ketika sesorang memberi tahu komputer apa yang harus dilakukan, sesorang juga harus memilih bagaimana melakukannya. Di situlah algoritma komputer masuk. Algoritma adalah teknik dasar yang digunakan untuk menyelesaikan pekerjaan (Gurevich, 2012). Mari kita ikuti contoh untuk membantu mendapatkan pemahaman tentang konsep algoritma. Katakanlah sesorang memiliki seorang teman yang tiba di bandara, dan teman sesorang perlu pergi dari bandara ke rumah. Berikut adalah empat algoritma berbeda yang mungkin akan diberikan kepada orang lain untuk sampai ke rumah:

- Algoritma taksi:
    - Pergi ke tempat taksi.
    - Naik taksi.
    - Berikan alamat saya pada pengemudi.

- Algoritma panggilan-saya:
    - Ketika pesawat Anda tiba, hubungi ponsel saya.

  - Temui saya di luar klaim bagasi.

- Algoritma rent-a-car:
  - Naik shuttle ke tempat rental mobil.
  - Menyewa mobil.
  - Ikuti petunjuk untuk sampai ke rumah saya.

- Algoritma bus:
  - Di luar klaim bagasi, naik bus nomor 70.
  - Transfer ke bus 14 di Main Street.
  - Turun di Elm street.
  - Berjalanlah dua blok ke utara ke rumah saya.

Keempat algoritma ini mencapai tujuan yang persis sama, tetapi masing-masing algoritma melakukannya dengan cara yang sama sekali berbeda. Setiap algoritma juga memiliki biaya dan waktu perjalanan yang berbeda. Naik taksi, misalnya, mungkin adalah cara tercepat, tetapi juga yang paling mahal. Naik bus jelas lebih murah, tetapi jauh lebih lambat. Anda memilih algoritma berdasarkan keadaan.

Dalam pemrograman komputer, seringkali ada banyak cara berbeda - algoritma - untuk menyelesaikan tugas yang diberikan. Setiap algoritma memiliki kelebihan dan kekurangan dalam situasi yang berbeda. Penyortiran adalah satu tempat di mana banyak penelitian telah dilakukan karena komputer menghabiskan

banyak daftar penyortiran waktu. Berikut adalah lima algoritma berbeda yang digunakan dalam penyortiran:

- Bin sort
- Gabungkan semacam
- Semacam gelembung
- Semacam shell
- Quicksort

Jika ada sejuta nilai integer antara 1 dan 10 dan perlu diurutkan, jenis bin sort adalah algoritma yang tepat untuk digunakan. Jika Anda memiliki sejuta judul buku, quicksort mungkin merupakan algoritma terbaik. Dengan mengetahui kekuatan dan kelemahan dari berbagai algoritma, Anda memilih yang terbaik untuk tugas yang ada.

2.3.1 Desain Konseptual

Algoritma adalah serangkaian instruksi, sering disebut sebagai "proses," yang harus diikuti ketika memecahkan masalah tertentu. Meskipun secara teknis tidak dibatasi oleh definisi, kata itu hampir selalu terkait dengan komputer, karena algoritma yang diproses komputer dapat mengatasi masalah yang jauh lebih besar daripada manusia, jauh lebih cepat. Karena komputasi modern menggunakan algoritma jauh lebih sering daripada pada titik lain dalam sejarah manusia, bidang telah tumbuh di sekitar desain, analisis, dan penyempurnaan. Bidang desain algoritma membutuhkan latar belakang matematika yang kuat, dengan gelar ilmu

komputer yang sangat dicari kualifikasi. Ini menawarkan semakin banyak pilihan karir yang sangat dikompensasi, karena kebutuhan akan lebih banyak (dan juga lebih canggih) algoritma terus meningkat.

Pada tingkat yang paling sederhana, algoritma pada dasarnya hanya seperangkat instruksi yang diperlukan untuk menyelesaikan tugas. Pengembangan algoritma, meskipun umumnya tidak disebut demikian, telah menjadi kebiasaan yang populer dan pengejaran profesional untuk semua catatan sejarah. Jauh sebelum fajar era komputer modern, orang menetapkan rutinitas yang telah ditentukan untuk bagaimana mereka akan melakukan tugas sehari-hari, sering menuliskan daftar langkah-langkah yang harus diambil untuk mencapai tujuan penting, mengurangi risiko melupakan sesuatu yang penting. Ini, pada dasarnya, adalah apa itu algoritma. Desainer mengambil pendekatan yang mirip dengan pengembangan algoritma untuk tujuan komputasi: pertama, mereka melihat masalah. Kemudian, mereka menguraikan langkah-langkah yang akan diperlukan untuk menyelesaikannya. Akhirnya, mereka mengembangkan serangkaian operasi matematika untuk mencapai langkah-langkah tersebut.

2.3.2 Tugas Algoritma

Tugas sederhana dapat diselesaikan dengan algoritma yang dihasilkan dengan beberapa menit, atau paling banyak pekerjaan pagi. Tingkat kompleksitas menjalankan tantangan yang panjang, namun, sampai pada masalah yang sangat rumit sehingga mereka telah menghalangi matematikawan yang tak terhitung jumlahnya selama bertahun-tahun - atau bahkan berabad-abad. Komputer modern

menghadapi masalah pada tingkat ini di bidang-bidang seperti keamanan dunia maya, serta penanganan data besar - penyortiran set data yang efisien dan menyeluruh sedemikian besar sehingga bahkan komputer standar tidak dapat memprosesnya secara tepat waktu. Contoh data besar mungkin termasuk "setiap artikel di Wikipedia," "setiap halaman web yang diindeks dan diarsipkan akan kembali ke tahun 1998," atau "enam bulan terakhir pembelian online yang dilakukan di Amerika."

2.3.3 Rekayasa Algoritma

Ketika desain algoritma baru diterapkan dalam istilah praktis, disiplin terkait dikenal sebagai rekayasa algoritma. Kedua fungsi tersebut sering dilakukan oleh orang yang sama, meskipun organisasi yang lebih besar (seperti Amazon dan Google) mempekerjakan desainer dan insinyur khusus, mengingat tingkat kebutuhan mereka akan algoritma baru dan khusus. Seperti proses desain, rekayasa algoritma sering kali melibatkan akreditasi sains komputer, dengan latar belakang yang kuat dalam matematika: di mana mereka ada sebagai profesi yang terpisah dan terspesialisasi, insinyur algoritma mengambil ide-ide konseptual dari desainer dan proses kreatif dari mereka yang akan dipahami oleh komputer. Dengan kemajuan teknologi digital yang mantap, para insinyur yang berdedikasi akan terus menjadi semakin umum.

2.4 Kriptografi

Kriptografi adalah teknik mengubah dan mentransmisikan data rahasia dengan cara disandikan sehingga hanya pengguna yang berwenang dan dimaksudkan dapat memperoleh atau bekerja di dalamnya. Ini adalah kata asal Yunani di mana "crypto" berarti tersembunyi dan "graphy" berarti menulis, jadi kriptografi berarti tulisan tersembunyi atau rahasia. Ini memperkenalkan triad seperti kerahasiaan, non-penolakan, integritas dan keaslian dalam komunikasi data yang sedang berlangsung.

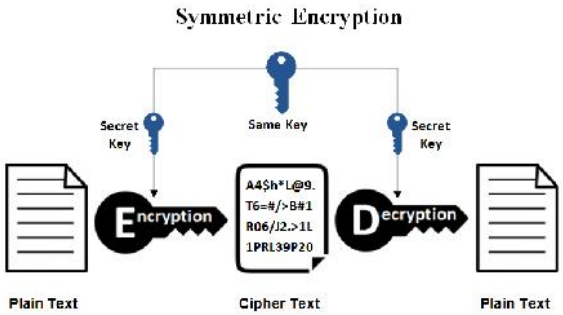
Kriptografi adalah disiplin atau teknik yang digunakan dalam melindungi integritas atau kerahasiaan pesan elektronik dengan mengubahnya menjadi bentuk (ciphertext) yang tidak dapat dibaca. Hanya penggunaan kunci rahasia yang dapat mengubah teks sandi menjadi bentuk yang dapat dibaca manusia (teks jelas). Perangkat lunak kriptografi dan / atau perangkat keras menggunakan rumus matematika (algoritma) untuk mengubah teks dari satu bentuk ke bentuk lainnya.

Komunikasi yang aman dapat disediakan menggunakan teknik, di hadapan konten pihak ketiga berbahaya yang disebut musuh. Teknik-teknik ini dapat disebut sebagai Kriptografi. Pesan pribadi apa pun dapat disembunyikan dari publik atau pihak ketiga, menggunakan seperangkat protokol. Protokol-protokol ini perlu dianalisis dan dibangun dengan cara yang efisien untuk menjaga kerahasiaan pesan yang dikirim. Kriptografi modern memiliki aspek tertentu yang merupakan pusatnya seperti integritas data, otentikasi, kerahasiaan dll. Di dunia modern, kriptografi sangat bergantung pada mata pelajaran seperti matematika dan ilmu komputer. Algoritma untuk Kriptografi dirancang sedemikian rupa

sehingga sulit untuk dipecahkan dalam praktik oleh pihak ketiga jahat yang juga dikenal sebagai musuh. Pendekatan praktis terhadap pemecahan algoritma semacam itu akan gagal, namun, pendekatan teoritis mungkin memecahkan sistem tersebut. Dengan demikian, algoritma apa pun dapat disebut sebagai aman, jika sifat kuncinya tidak dapat disimpulkan, dengan ciphertext yang diberikan. Kriptografi dapat dikategorikan menjadi dua cabang: Symmetric dan Asymmetric. Dengan pendekatan simetris, satu kunci digunakan untuk proses enkripsi dan dekripsi yaitu pengirim dan penerima harus memiliki kunci bersama. Namun, dengan pendekatan ini, distribusi kunci adalah tautan yang lemah, yang memunculkan pendekatan baru.

2.4.1 Kriptografi Simetris

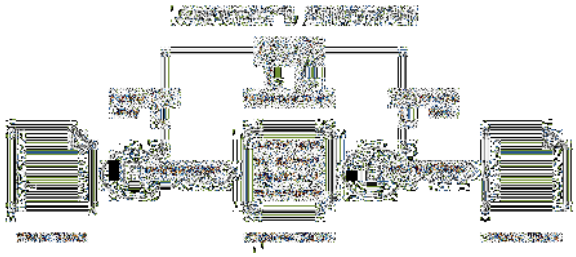
Kriptografi kunci simetris adalah setiap algoritma kriptografi yang didasarkan pada kunci bersama yang digunakan untuk mengenkripsi atau mendekripsi teks / cyphertext, dalam kontrak dengan kriptografi kunci asimetris, di mana kunci enkripsi dan dekripsi dihubungkan oleh berbeda. Enkripsi simetris umumnya lebih efisien daripada enkripsi asimetris dan karenanya lebih disukai ketika sejumlah besar data perlu dipertukarkan. Membuat kunci bersama sulit menggunakan hanya algoritma enkripsi simetris, sehingga dalam banyak kasus, enkripsi asimetris digunakan untuk membuat kunci bersama antara dua pihak. Contoh untuk kriptografi kunci simetris termasuk AES, DES, dan 3DES. Protokol pertukaran kunci yang digunakan untuk membangun kunci enkripsi bersama termasuk Diffie-Hellman (DH), Eliptic Curve (EC) dan RSA. Berikut ini skema dari kriptografi simetris (Ayushi, 2010).



Gambar 2.1 Skema kriptografi simetris
Sumber: (Ayushi, 2010)

2.4.2 Kriptografi Asimetris

Dalam versi kriptografi asimetris, pengirim dan penerima memiliki dua kunci, publik dan pribadi. Kunci pribadi dirahasiakan sedangkan kunci publik terbuka ke dunia luar. Set data apa pun, yang dienkripsi dengan kunci publik hanya dapat didekripsi menggunakan kunci pribadi yang sesuai. Ketika datang ke perbandingan, pendekatan simetris lebih cepat daripada yang asimetris. Contoh - tanda tangan digital menggunakan kriptografi asimetris untuk mengenkripsi pesan dalam hash alih-alih pesan lengkap. Berikut ini skema kriptografi asimetris (S., L. Ribeiro, & David, 2012).



Gambar 2.2 Skema kriptografi asimetris
Sumber: (Ayushi, 2010)

2.5 Vigenère Cipher

Vigenère Cipher adalah metode mengenkripsi teks alfabet. Ini menggunakan bentuk substitusi polyalphabetic sederhana. Cipher polyalphabetic adalah cipher yang didasarkan pada substitusi, menggunakan beberapa huruf substitusi. Enkripsi teks asli dilakukan dengan menggunakan Vigenère square atau Vigenère table. Tabel ini terdiri dari alfabet yang ditulis 26 kali dalam baris yang berbeda, setiap alfabet bergeser secara siklis ke kiri dibandingkan dengan alfabet sebelumnya, sesuai dengan 26 kemungkinan Caesar Ciphers. Pada titik berbeda dalam proses enkripsi, sandi menggunakan alfabet yang berbeda dari salah satu baris. Alfabet yang digunakan pada setiap titik tergantung pada kata kunci berulang (Pratama & Tamatjita, 2015).

2.5.1 Enkripsi

Huruf pertama dari plaintext, G dipasangkan dengan A, huruf pertama dari kunci. Jadi gunakan baris G dan kolom A dari kotak Vigenère, yaitu G. Demikian pula, untuk huruf kedua dari plaintext, huruf kedua dari kunci digunakan, huruf pada baris E dan kolom Y adalah C. Sisa dari plaintext dienkripsi

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Gambar 2.3 Tabel Vigenere
Sumber: (Ayushi, 2010)

2.5.2 Dekripsi

Dekripsi dilakukan dengan pergi ke baris dalam tabel yang sesuai dengan kunci, menemukan posisi huruf ciphertext di baris ini, dan kemudian menggunakan label kolom sebagai plaintext. Misalnya, di baris A (dari AYUSH), ciphertext G muncul di kolom G, yang merupakan huruf plaintext pertama. Selanjutnya, kita pergi ke baris Y (dari AYUSH), cari ciphertext C yang ditemukan di kolom E, jadi E adalah huruf plaintext kedua.

2.6 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).

2.6.1 Use Case Diagram

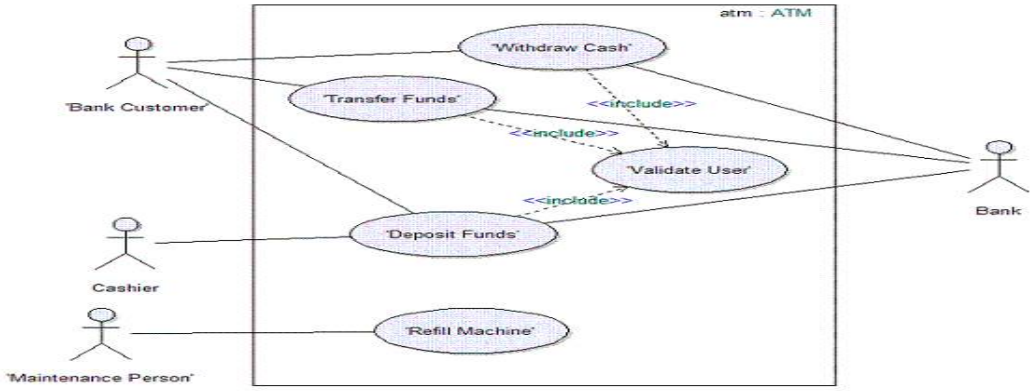
Use Case Diagram adalah model tentang bagaimana berbagai jenis pengguna berinteraksi dengan sistem untuk memecahkan masalah. Dengan demikian, ini menggambarkan tujuan pengguna, interaksi antara pengguna dan sistem, dan perilaku sistem yang diperlukan dalam memenuhi tujuan-tujuan ini.

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.

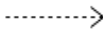
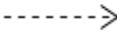
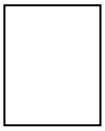


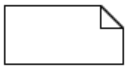
Gambar 2.4. Use-case Diagram ATM
Sumber: (Uml-diagrams.org, 2019)

Gambar di atas 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 himpuan 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

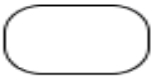
Sumber: (Kurniawan, 2018)

2.6.2 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)

2.6.3 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:

- langkah pemrosesan, biasanya disebut aktivitas dan dilambangkan sebagai kotak persegi panjang.

- 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.

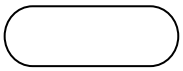
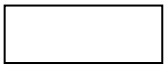
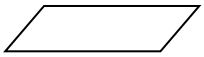
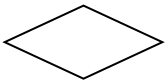
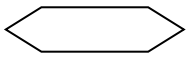
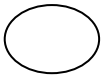
Diagram alir menggambarkan aspek-aspek tertentu dari proses dan biasanya dilengkapi dengan jenis diagram lainnya. Misalnya, Kaoru Ishikawa, mendefinisikan diagram alir sebagai salah satu dari tujuh alat dasar kendali mutu, di sebelah histogram, diagram Pareto, lembar periksa, diagram kontrol, diagram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

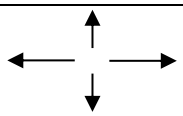
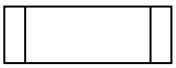
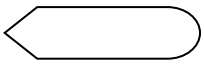
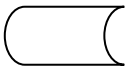
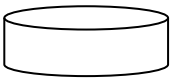
Diagram Nassi-Shneiderman dan Drakon-chart adalah notasi alternatif untuk aliran proses. Nama alternatif umum termasuk diagram alir, diagram alur proses, diagram alur fungsional, peta proses, diagram proses, diagram proses fungsional, model proses bisnis, model proses, diagram alir proses, diagram alur

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 2.3 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

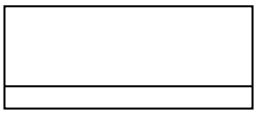
8.		**Arus/Flow**, dari pada prosedur yang dapat dilakukan atas ke bawah dari bawah ke atas, ke atas dari kiri ke kanan ataupun dari kanan ke kiri
9.		**Predefined Process**, untuk menyatakan sekumpulan langkah proses yang ditulis sebagai prosedur
10.		Simbol untuk output, yang ditunjukkan ke suatu device, seperti printer, dan sebagainya
11		Penyimpanan file secara sementara
12		Menunjukkan input / Output Hardisk (media penyimpanan)

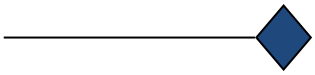
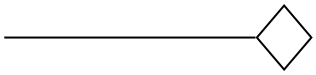
Sumber: (Kurniawan, 2018)

2.6.4 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 2.4 Simbol 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.

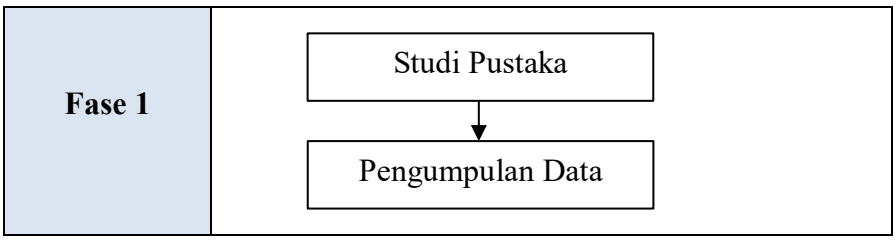
BAB III

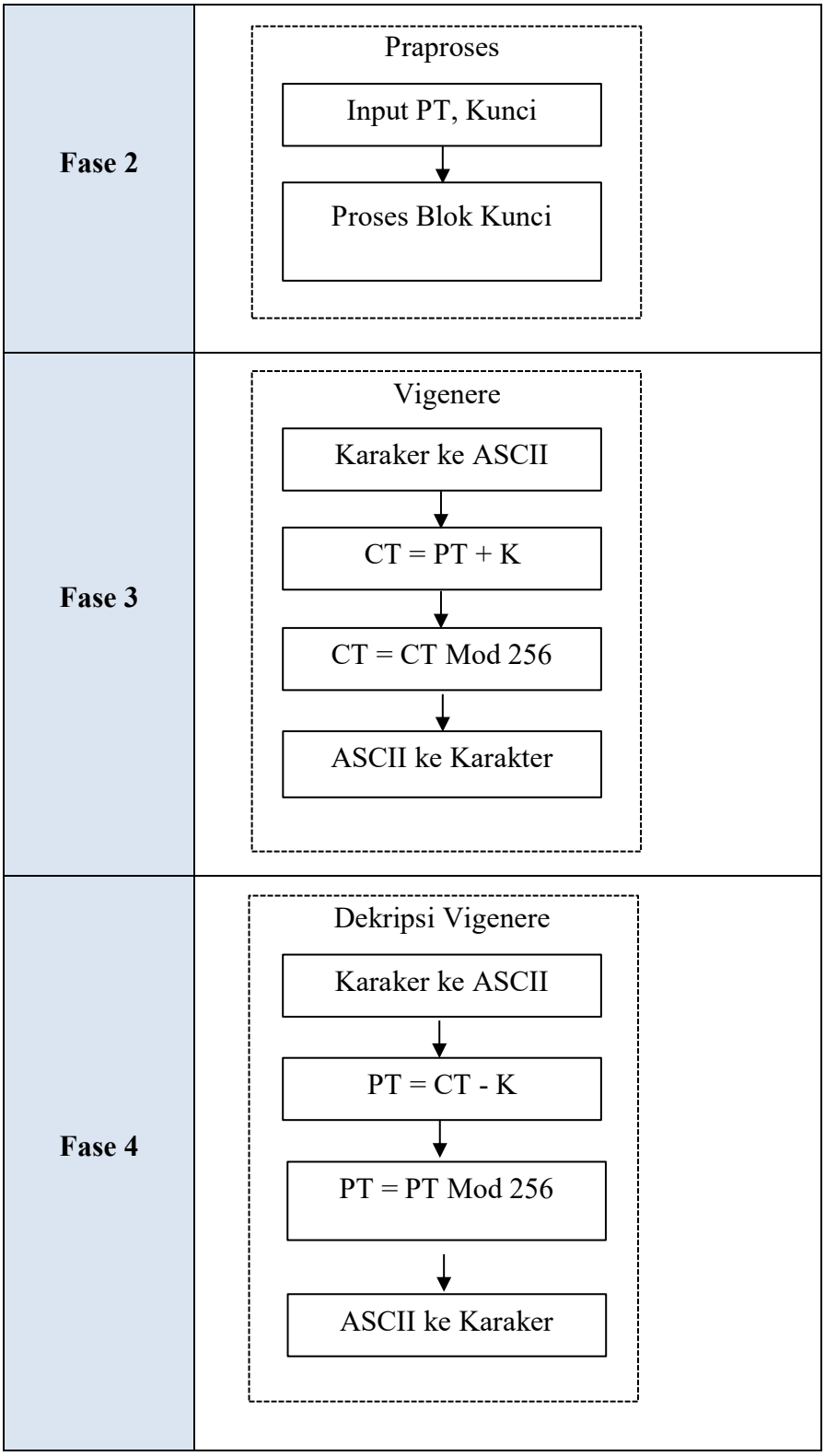
METODE PENELITIAN

3.1 Kerangka Penelitian

Bagian Kerangka Metode Penelitian adalah sumber daya online yang dirancang untuk membantu para peneliti dari semua jenis merancang metodologi penelitian khusus untuk proyek khusus mereka. Sementara kerangka kerja penelitian disusun menjadi beberapa fase dengan keterkaitan yang jelas, proses pengembangan desain penelitian yang baik adalah proses yang terarah dan terstruktur.

Kerangka penelitian dengan jelas menggambarkan struktur rencana penelitian dan membantu peneliti merumuskan pertanyaan penelitian yang relevan. Kerangka kerja penelitian studi kasus induktif berbeda dari kerangka kerja penelitian studi kasus deduktif. Berikut ini adalah kerangka penelitian yang dilakukan:





Gambar 3.1 Kerangka Penelitian

Berikut adalah tahapan penelitian yang dilakukan:

- Studi Literatur

  Studi literatur dilakukan untuk mendapatkan teori-teori tentang ilmu kriptografi khususnya algoritma Vigenere Cipher. Studi ini dapat dilakukan melalui buku dan informasi yang ada di internet.

- Analisa

  Bagian ini menjelaskan proses analisa permasalahan dan bagaimana permasalahan dapat diselesaikan dengan baik. Analisa akan memeriksa kebenaran dari rancangan yang akan dibuat.

- Pembahasan

  Bagian ini membahas tentang formula yang digunakan oleh pengguna tentang algoritma Vigenere cipher untuk melakukan proses enkripsi dan dekripsi terhadap plaintext dan ciphertext.

- Implementasi dan pengujian

  Bagian ini dilakukan pengujian kebenaran output yang dihasilkan oleh program aplikasi Microsoft Visual Basic.Net 2010. Hasil akan dibandingkan berdasarkan rumus yang telah ditetapkan dalam melakukan perhitungan.

3.2 Perancangan Penelitian

Perancangan penelitian adalah bagaimana suatu penelitian dimodelkan dalam suatu alur atau diagram. Banyak cara yang dapat dilakukan untuk merancang penelitian agar lebih terarah dan terstruktur. Perancangan ini

membutuhkan ketelitian yang tinggi agar tidak menyalahi aturan yang ada. Hal ini bertujuan agar program aplikasi yang telah dibuat dapat bekerja secara efisien dan efektif. Desain penelitian dapat digambarkan dengan bentuk Unified Modelling Language (UML). Pada UML, setiap arah penelitian tergambarkan dengan jelas dan terstruktur. Hal ini dapat memudahkan peneliti dalam menghasilkan output yang benar.

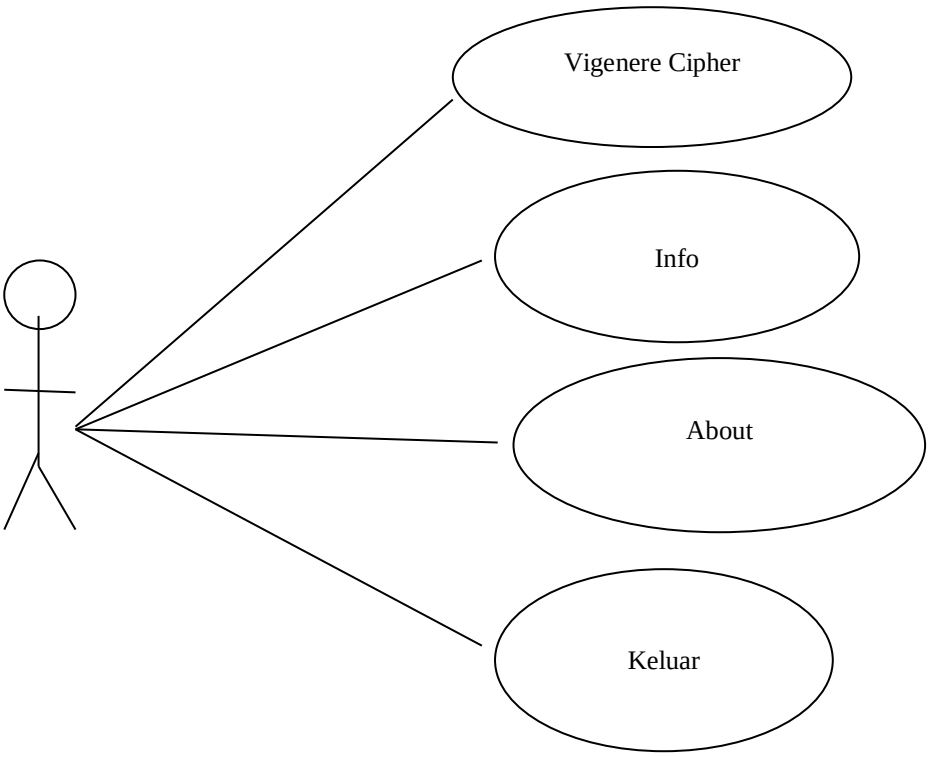
Perancangan penelitian yang menghasilkan batas kesalahan terkecil dalam penelitian disebut sebagai hasil perancangan yang terbaik. Perancangan penelitian berikut ini berfunsi untuk mendefinisikan setiap tahapan untuk melengkapi kegiatan kerja pengguna terhadap rancangan penelitian yang akan dilaksanakan.

3.2.1 Use Case Diagram

Use Case diagram didefinisikan sebagai diagram yang menangkap fungsionalitas dan persyaratan sistem dalam UML. Use-cases adalah konsep inti dari pemodelan bahasa Unified Modeling. Use Case terdiri dari use case, orang, atau berbagai hal yang menggunakan fitur yang disebut sebagai aktor dan elemen yang bertanggung jawab untuk mengimplementasikan use case. Use case diagram menangkap perilaku dinamis dari sistem live. Ini memodelkan bagaimana entitas eksternal berinteraksi dengan sistem untuk membuatnya bekerja. Use case diagram bertanggung jawab untuk memvisualisasikan hal-hal eksternal yang berinteraksi dengan bagian dari sistem.

Use case digunakan untuk mewakili fungsionalitas tingkat tinggi dan bagaimana pengguna akan menangani sistem. Sebuah use case mewakili fungsionalitas yang berbeda dari suatu sistem, komponen, paket, atau kelas.

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. Gamabr 3.1 adalah perancangan *Use Case* untuk admin dari algoritma Vigenere Cipher.

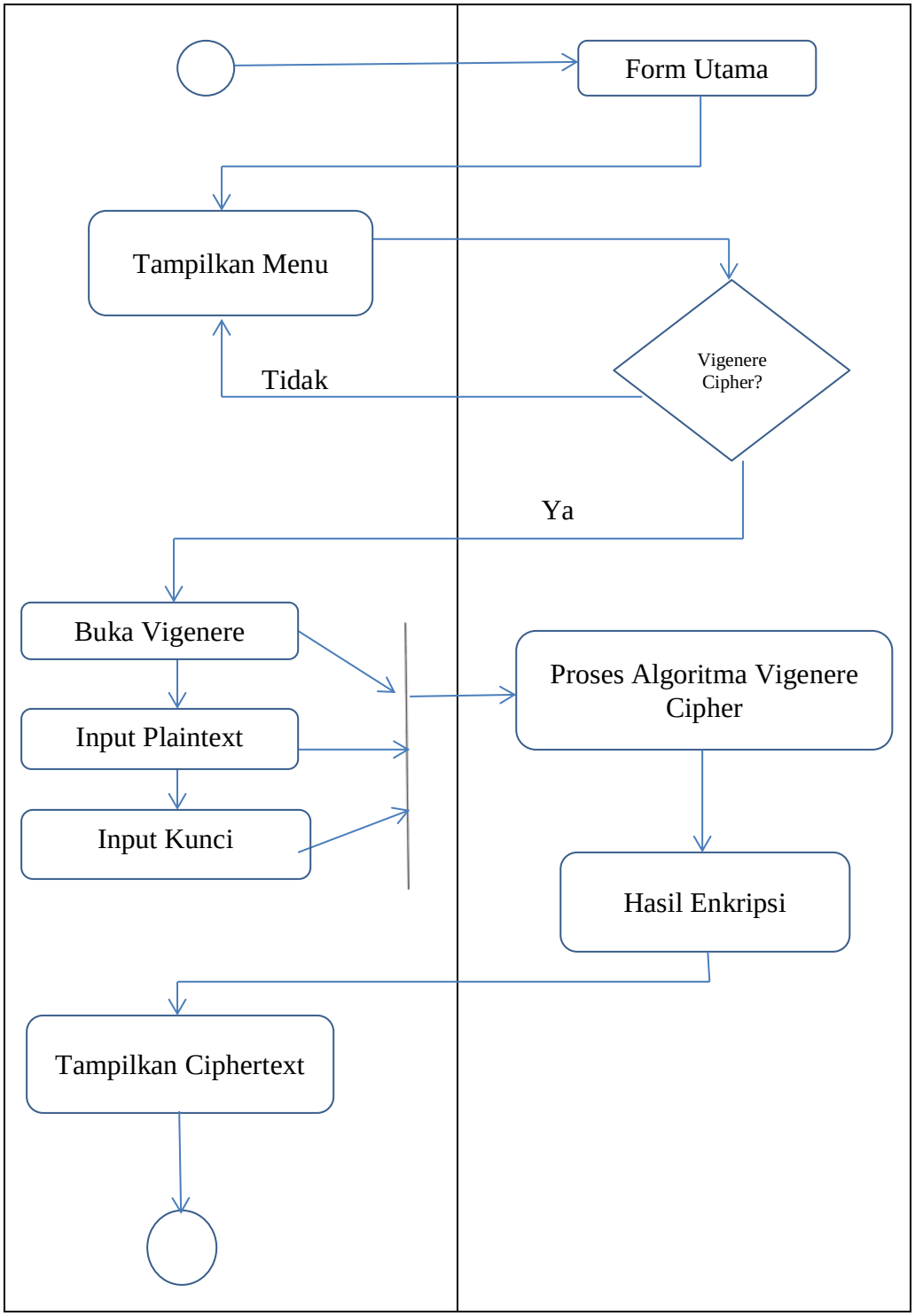


Gambar 3.2 Use Case Diagram

3.2.2 Activity Diagram

Activity diagram menggambarkan perilaku alur kerja aktual suatu sistem dalam Teknologi Informasi. Diagram ini menggambarkan keadaan aktual dari suatu sistem dengan menunjukkan semua urutan kegiatan yang dilakukan. Juga, diagram ini dapat menunjukkan aktivitas yang kondisional atau paralel. Gambar berikut ini akan menjelaskan *Activity diagram* tersebut.

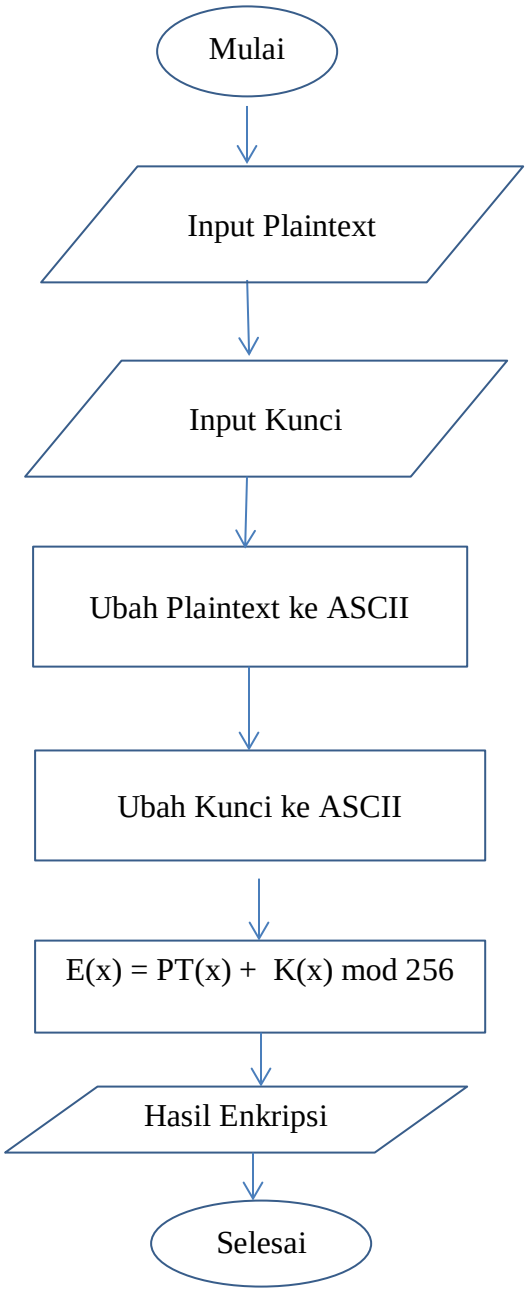
Admin	Sistem



Gambar 3.3 Activity Diagram

3.2.3 Flowchart Enkripsi

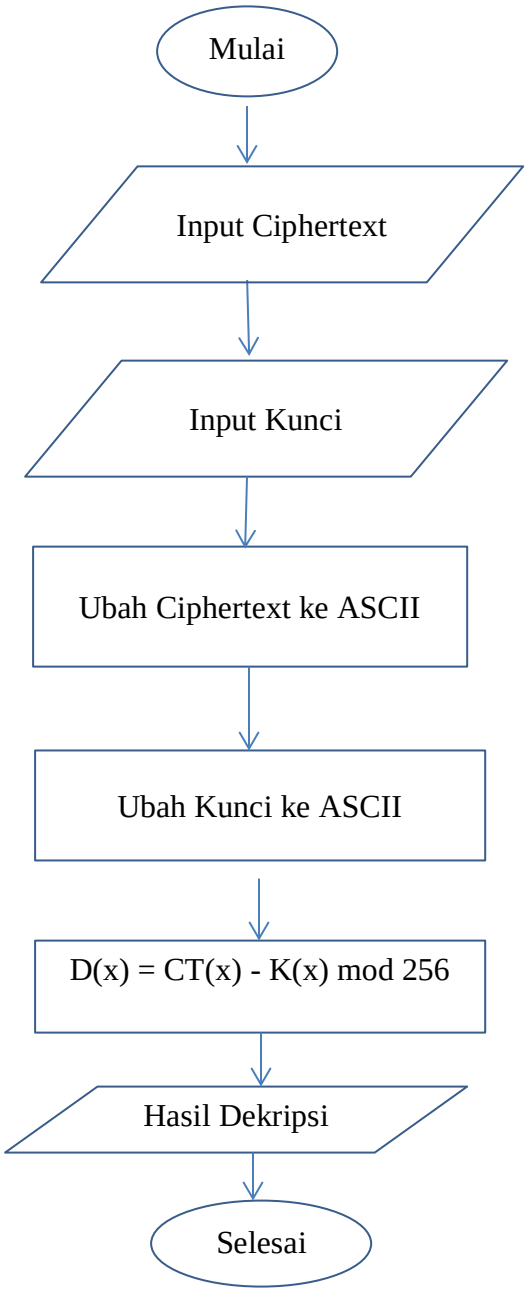
Flowchart enkripsi akan menerangkan cara kerja algoritma Vigenere Cipher dengan proses enkripsi. *Flowchart* enkripsi dapat dilihat pada gambar berikut ini.



Gambar 3.4 Flowchart enkripsi algoritma Vigenere

3.2.4 Flowchart Dekripsi

Flowchart dekripsi akan menjelaskan cara kerja algoritma Vigenere Cipher dengan proses dekripsi. *Flowchart* dekripsi dapat dilihat pada gambar berikut ini.



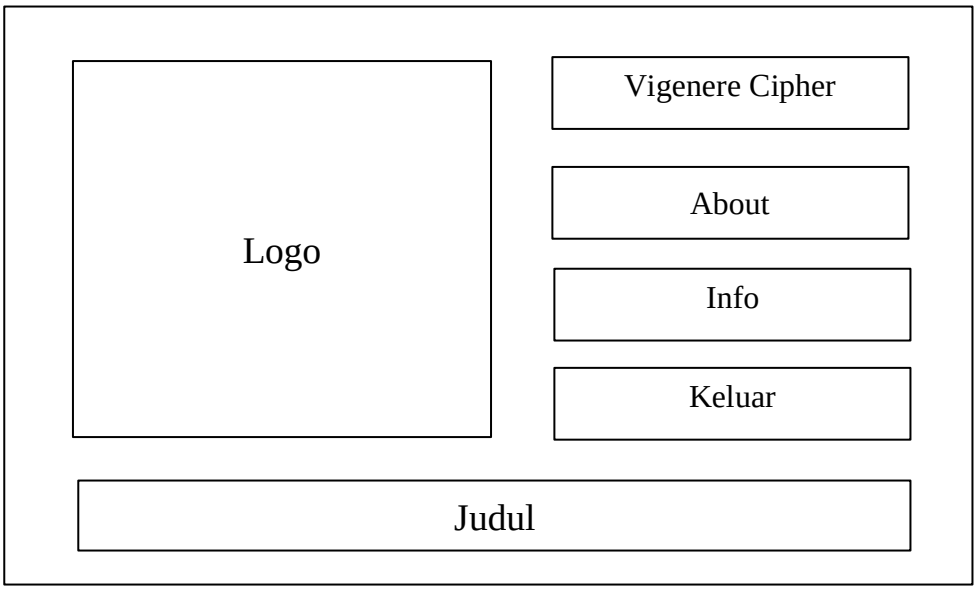
Gambar 3.5 Flowchart dekripsi algoritma Vigenere

3.3 Desain Interface

Desain interface atau perancangan antarmuka adalah bagaimana suatu tampilan pada program aplikasi akan dibuat. Perancangan ini melibatkan beberapa objek yang akan disematkan pada program aplikasi tersebut. Dalam perancangan ini dapat dilihat apa-apa saja yang akan digunakan dalam program aplikasi. Perancangan ini memudahkan penulis dalam menentukan dan memodifikasi apabila terjadi perubahan pada program aplikasi algoritma Vigenere Cipher.

3.3.1 Menu Utama

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



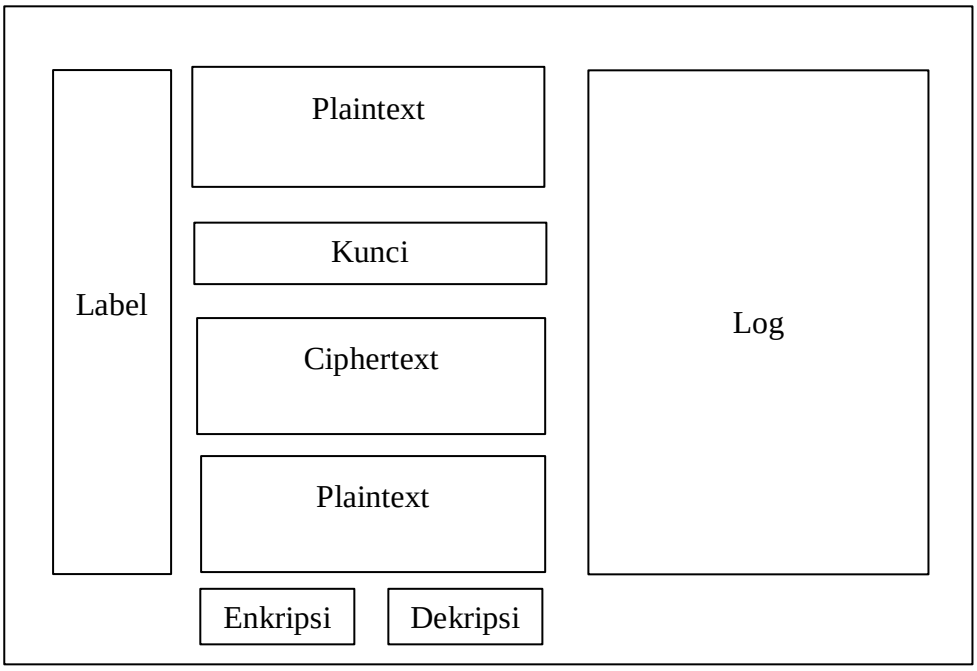
Gambar 3.6 Tampilan Menu Utama

Tampilan ini memiliki berapa sub-menu antara lain:

- Logo
- Vigenere Cipher
- About
- Info
- Keluar
- Judul

3.3.2 Menu Vigenere Cipher

Menu ini adalah perancangan program aplikasi utama yang berfungsi menjalankan algoritma Vigenere Cipher. Tampilan ini adalah tempat untuk melakukan proses enkripsi dan dekripsi. Gambar 3.6 adalah tampilan menu ini.



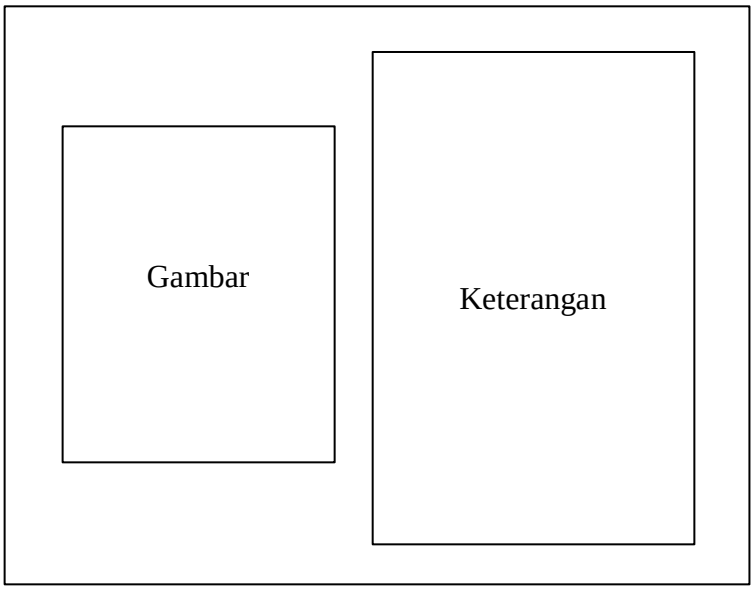
Gambar 3.7 Tampilan Menu Vigenere Cipher

Tampilan algoritma Vigenere Cipher memiliki beberapa bagian antara lain:

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

3.3.3 Menu Info

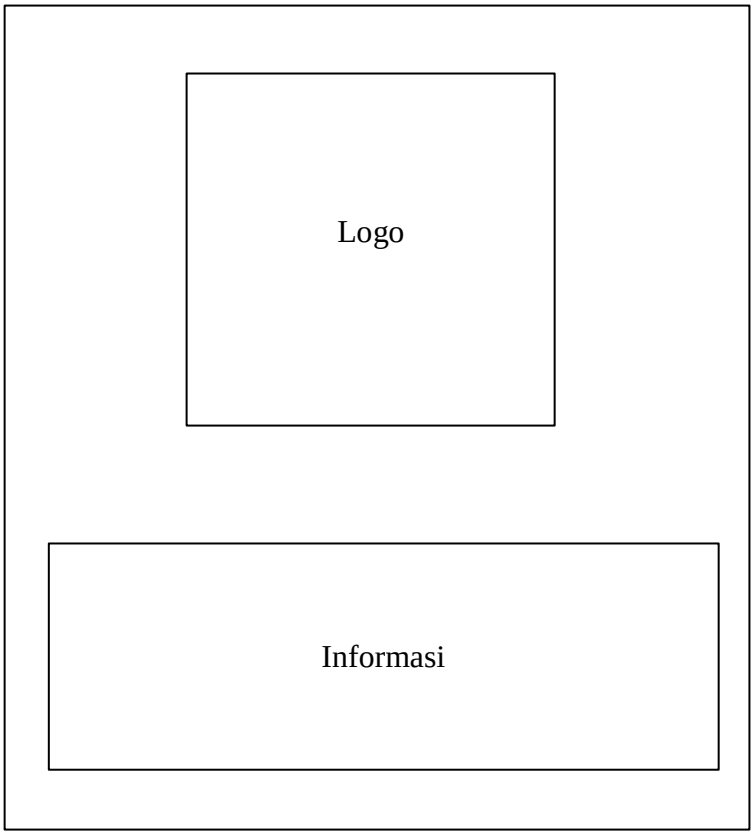
Menu ini menampilkan informasi tentang algoritma Vigenere Cipher. Tampilan ini terdiri dari objek gambar dan keterangan. Gambar berikut ini adalah hasil perancangan menu Info.



Gambar 3.8 Tampilan Menu Info

3.3.4 Menu About

Menu ini menampilkan informasi penulis dan institusi dimana penulis melakukan penelitian. Tampilan ini teridiri dari logo Universitas Pembangunan Panca Budi dan biodata. Gambar berikut ini adalah hasil tampilan dari menu About.



Gambar 3.9 Tampilan Menu About

BAB IV

HASIL DAN PEMBAHASAN

Implementasi adalah pelaksanaan, pelaksanaan, atau praktik rencana, metode, atau desain, ide, model, spesifikasi, standar, atau kebijakan apa pun untuk melakukan sesuatu. Dengan demikian, implementasi adalah tindakan yang harus mengikuti pemikiran awal apa pun agar sesuatu benar-benar terjadi. Dalam konteks teknologi informasi, implementasi perangkat lunak atau perangkat keras mencakup semua proses purnajual yang terlibat dalam sesuatu yang beroperasi dengan baik di lingkungannya, termasuk menganalisis persyaratan, instalasi, konfigurasi, penyesuaian, berjalan, pengujian, integrasi sistem, pelatihan pengguna, pengiriman dan pembuatan yang diperlukan. perubahan.

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 program aplikasi. Spesifikasi sistem 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 dapat menentukan akses keamanan. Spesifikasi pada penelitian ini terdiri dari perangkat keras dan lunak.

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.	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 mendukuing hasil keluaran. Tabel 4.2 adalah spsesifikasi perangkat lunak yang digunakan pada penelitian ini.

Tabel 4.2 Spesifikasi perangkat lunak

No.	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 desain berarti benar-benar melakukan pekerjaan untuk mengubah ide (desain) menjadi sesuatu yang nyata. Proses mendesain apa pun akan memiliki langkah-langkah umum termasuk mengumpulkan persyaratan, mengidentifikasi solusi yang mungkin, menganalisis solusi tersebut, dll. Agar proses implementasi berhasil, banyak tugas antara berbagai departemen perlu diselesaikan secara berurutan. Perusahaan berusaha untuk menggunakan metodologi yang telah terbukti dan meminta bantuan profesional untuk membimbing mereka melalui penerapan suatu sistem tetapi kegagalan dari banyak proses implementasi sering berasal dari kurangnya perencanaan yang akurat pada tahap awal proyek karena sumber daya yang tidak memadai atau masalah tak terduga yang muncul .

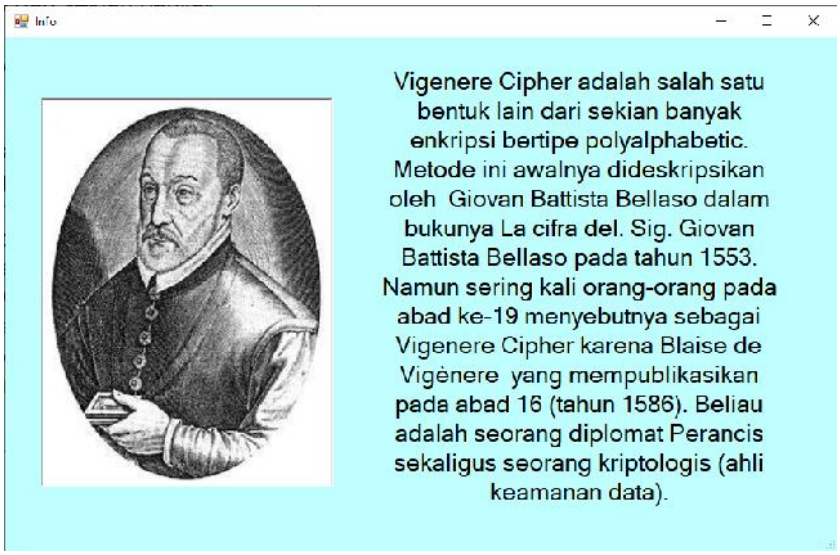
4.2.1 Halaman Menu Utama

Halaman Menu Utama merupakan halaman utama sebuah program aplikasi di mana pengguna dapat menemukan beberapa fungsi atau dapat berpindah ke halaman-halaman yang lain pada program aplikasi tersebut. Secara default, halaman utama merupakan sebuah splashscreen, tetapi dapat juga terdiri dari beberapa tombol navigasi yang mengarah ke menu lain seperti pada tampilan menu utama pada program aplikasi Vigenere Cipher ini. Menu utama terdiri dari tiga buah navigasi tombol dan satu buah tombol untuk keluar dari program 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 sejarah Vigenere Cipher yang awalnya diciptakan oleh Blaise de Vigenere. Gambar 4.2 adalah hasil tampilan dari halaman info.



Gambar 4.2 Halaman Info

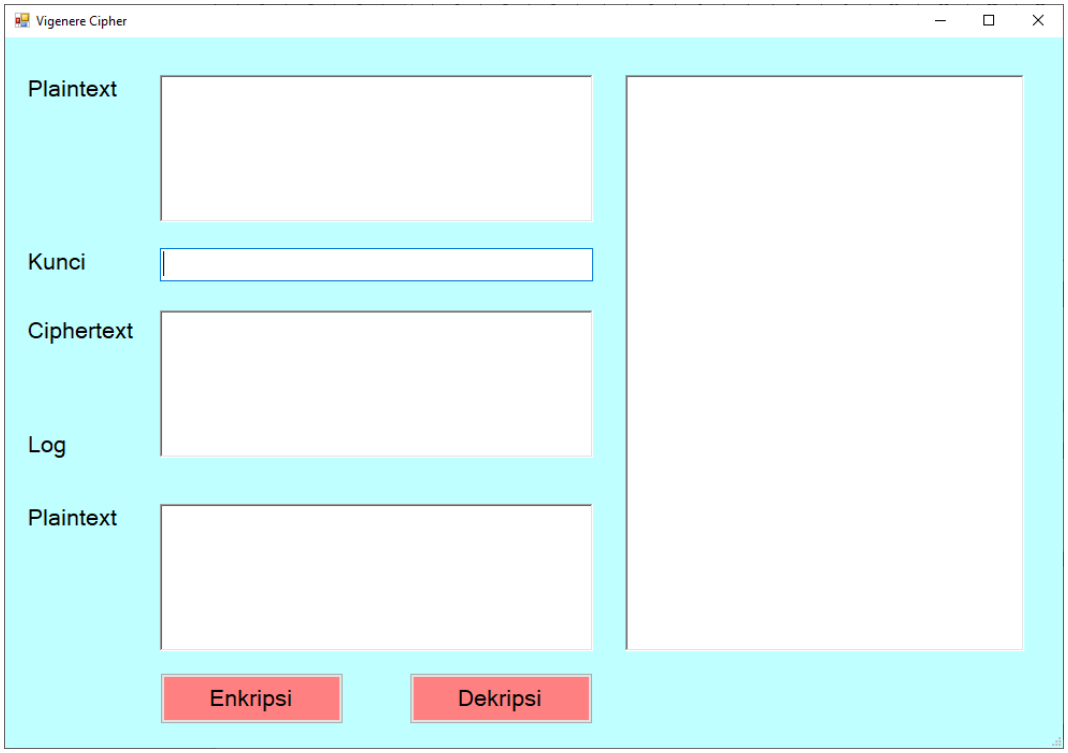
4.2.3 Halaman About

Halaman about menampilkan status dari penulis dalam lingkungan universitas. Form ini memiliki sebuah objek label dan picturebox. Gambar 4.3 adalah tampilan dari halaman About.

Gambar 4.3 Halaman About

4.2.4 Halaman Vigenere Cipher

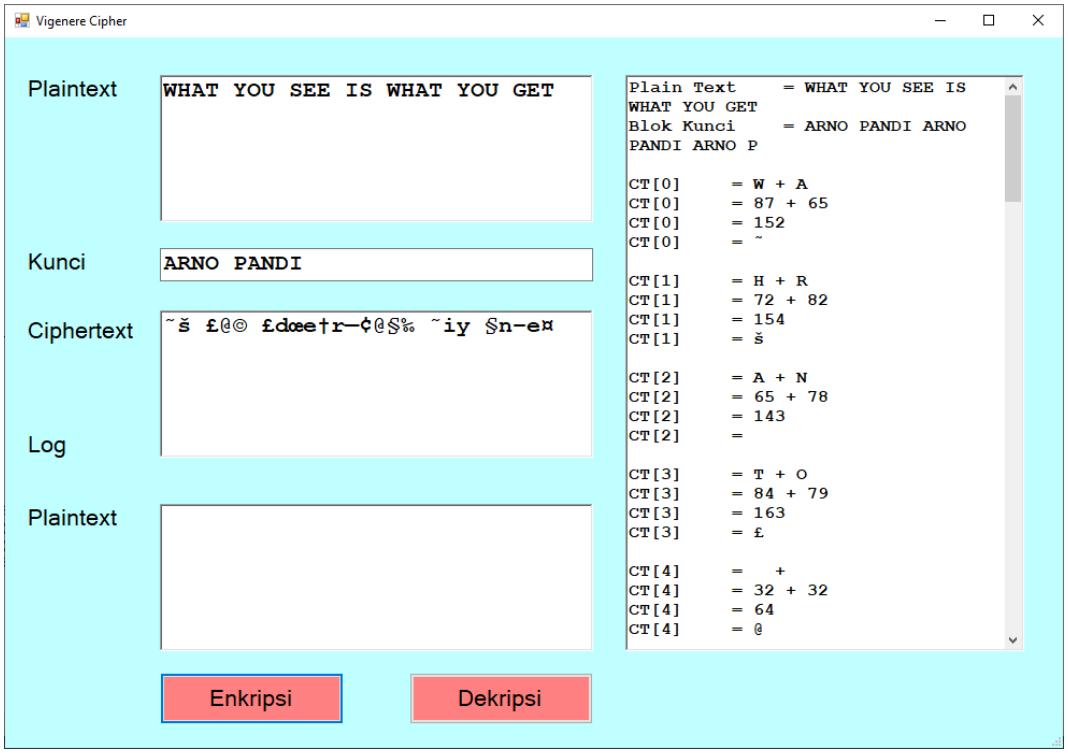
Halaman ini adalah bagian terpenting dari program aplikasi. Halaman ini berupa proses transformasi dari plaintext ke ciphertext dan juga pengembalian chipertext itu sendiri menuju plaintext. Bagian ini terdiri dari dua buah plaintext, sebuah kunci dan sebuah ciphertext yang termasuk dari bagian input dan output. Proses enkripsi dan dekripsi dilakukan dengan memberikan 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 Enkripsi

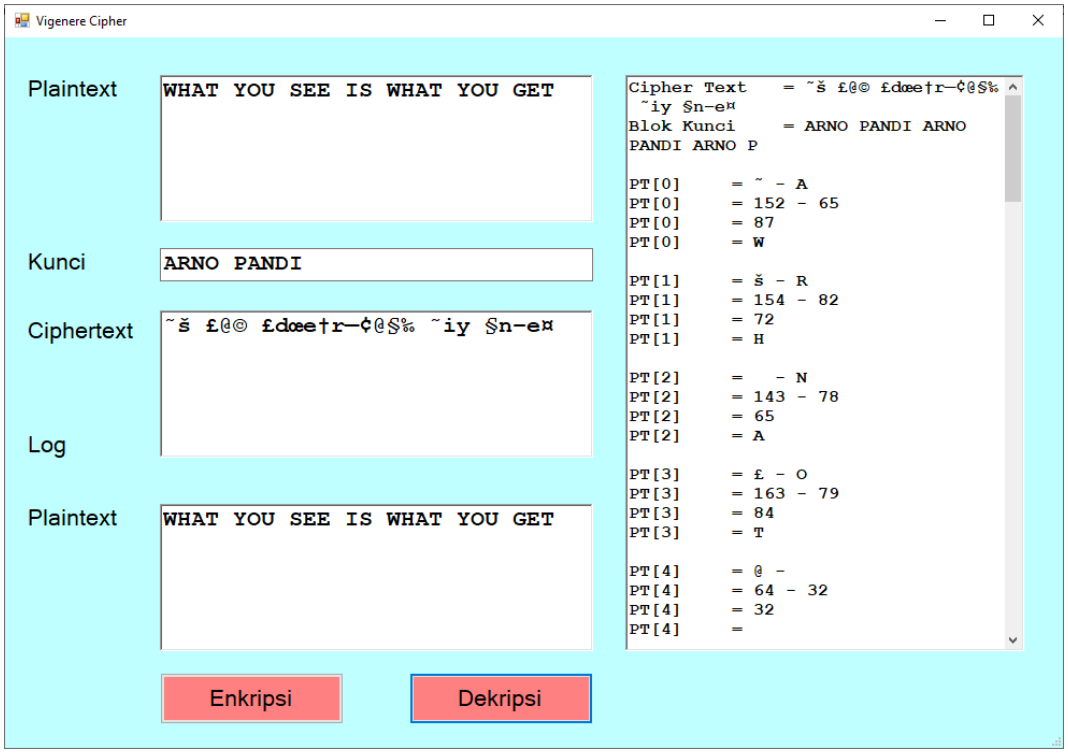
Bagian ini berisi tentang hasil proses enkripsi dengan plaintext dan kunci yang telah dimasukkan pada textbox. Plaintext dan Kunci adalah dua bagian yang harus dipenuhi agar ciphertext dapat ditentukan. Blok kunci dibentuk sesuai dengan jumlah panjang Kunci dan Plaintext. Blok kunci harus memiliki panjang yang sama dengan plaintext agar setiap karakter pada plaintext dapat dilakukan proses enkripsi. Gambar 4.5 adalah tampilan dari hasil perhitungan proses enkripsi algoritma Vigenere Cipher.



Gambar 4.5 Halaman enkripsi algoritma Vigenere Cipher

4.2.6 Hasil Dekripsi

Setelah proses enkripsi, ciphertext dihasilkan dan ciphertext ini sudah tidak dapat lagi difahami oleh orang yang berhasil mencuri atau mengambil informasi tersebut. Tetapi untuk dapat dibaca dan difahami oleh penerima, ciphertext tersebut harus dikembalikan kembali ke plaintext dengan proses dekripsi. Dekripsi harus menggunakan kunci yang sama dengan pertama sekali waktu enkripsi. Blok kunci kembali dibentuk agar setiap karakter pada ciphertext dapat dilakukan proses dekripsi. Perhitungasn akan salah jika ada satu karakter yang memiliki perbedaan hasil dengan 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 Test Perhitungan

Tes perhitungan dirancang untuk mengukur kemampuan program aplikasi untuk menambah, mengurangi, membagi, dan mengalikan angka dengan cepat dan akurat. Pada contoh yang akan dipaparkan, plaintext dan kunci akan diberikan untuk diproses mendapatkan ciphertext. Pengujian ini dilakukan untuk melihat seberapa akurat program aplikasi yang diciptakan dan apakah sesuai dengan perhitungan yang dilakukan secara manual. Proses yang dilakukan terdiri dari dua proses, yaitu proses enkripsi dan proses dekripsi. Berikut ini adalah penjelasan dan perhitungan lengkap proses enkripsi dan dekripsi pada algoritma Vigenere Cipher dengan memberikan dua buah plaintext dan kunci.

Pengujian Pertama

Plaintext = UNIVERSITAS PEMBANGUNAN PANCA BUDI

Kunci Vigenere = ARNO PANDI

Hasil Enkripsi

Tabel 4.3 Hasil enkripsi pengujian pertama

PT	PT ASCII	KUNCI	KUNCI ASCII	CT ASCII	CT
U	85	A	65	150	–
N	78	R	82	160	
I	73	N	78	151	—
V	86	O	79	165	¥
E	69		32	101	e
R	82	P	80	162	¢
S	83	A	65	148	”
I	73	N	78	151	—
T	84	D	68	152	˜
A	65	I	73	138	Š
S	83		32	115	s
	32	A	65	97	a
P	80	R	82	162	¢
E	69	N	78	147	“
M	77	O	79	156	œ
B	66		32	98	b
A	65	P	80	145	‘
N	78	A	65	143	•
G	71	N	78	149	•
U	85	D	68	153	™
N	78	I	73	151	—
A	65		32	97	a
N	78	A	65	143	•
	32	R	82	114	r
P	80	N	78	158	ž
A	65	O	79	144	•
N	78		32	110	n

C	67	P	80	147	“
A	65	A	65	130	,
	32	N	78	110	n
B	66	D	68	134	†
U	85	I	73	158	ž
D	68		32	100	d
I	73	A	65	138	Š

Hasil Dekripsi

Tabel 4.4 Hasil dekripsi pengujian pertama

CT	CT ASCII	KUNCI	KUNCI ASCII	PT ASCII	PT
–	150	A	65	85	U
	160	R	82	78	N
—	151	N	78	73	I
¥	165	O	79	86	V
e	101		32	69	E
¢	162	P	80	82	R
”	148	A	65	83	S
—	151	N	78	73	I
˜	152	D	68	84	T
Š	138	I	73	65	A

s	115		32	83	S
a	97	A	65	32	
¢	162	R	82	80	P
“	147	N	78	69	E
œ	156	O	79	77	M
b	98		32	66	B
‘	145	P	80	65	A
•	143	A	65	78	N
•	149	N	78	71	G
™	153	D	68	85	U
—	151	I	73	78	N
a	97		32	65	A
•	143	A	65	78	N
r	114	R	82	32	
ž	158	N	78	80	P
•	144	O	79	65	A
n	110		32	78	N
“	147	P	80	67	C
,	130	A	65	65	A
n	110	N	78	32	
†	134	D	68	66	B
ž	158	I	73	85	U
d	100		32	68	D
Š	138	A	65	73	I

Pengujian Kedua

Plaintext = HALO APA KABAR KAWAN-KAWAN SEMUA

Kunci Vigenere = ARNO PANDI

Hasil Enkripsi

Tabel 4.5 Hasil enkripsi pengujian kedua

PT	PT ASCII	KUNCI	KUNCI ASCII	CT ASCII	CT
H	72	A	65	137	›
A	65	R	82	147	•
L	76	N	78	154	Œ
O	79	O	79	158	ž
	32		32	64	—
A	65	P	80	145	›
P	80	A	65	145	™
A	65	N	78	143	Š
	32	D	68	100	—
K	75	I	73	148	‰
A	65		32	97	¥
B	66	A	65	131	i
A	65	R	82	147	–
R	82	N	78	160	†
	32	O	79	111	•
K	75		32	107	Š
A	65	P	80	145	“
W	87	A	65	152	—
A	65	N	78	143	•
N	78	D	68	146	–
-	45	I	73	118	‘
K	75		32	107	‰
A	65	A	65	130	
W	87	R	82	169	i
A	65	N	78	143	–

N	78	O	79	157	,
	32		32	64	‘
S	83	P	80	163	‹
E	69	A	65	134	“
M	77	N	78	155	i
U	85	D	68	153	ˆ
A	65	I	73	138	–

Hasil Dekripsi

Tabel 4.6 Hasil dekripsi pengujian kedua

CT	PT ASCII	KUNCI	KUNCI ASCII	CT ASCII	PT
›	137	A	65	72	H
•	147	R	82	65	A
Œ	154	N	78	76	L
ž	158	O	79	79	O
—	64		32	32	
›	145	P	80	65	A
™	145	A	65	80	P
Š	143	N	78	65	A
—	100	D	68	32	
‰	148	I	73	75	K
¥	97		32	65	A
i	131	A	65	66	B
–	147	R	82	65	A
†	160	N	78	82	R
•	111	O	79	32	
Š	107		32	75	K
“	145	P	80	65	A

—	152	A	65	87	W
•	143	N	78	65	A
–	146	D	68	78	N
‘	118	I	73	45	-
‰	107		32	75	K
0	130	A	65	65	A
i	169	R	82	87	W
–	143	N	78	65	A
,	157	O	79	78	N
‘	64		32	32	
‹	163	P	80	83	S
“	134	A	65	69	E
i	155	N	78	77	M
ˆ	153	D	68	85	U
–	138	I	73	65	A

BAB V

PENUTUP

5.1 Kesimpulan

Penulis dapat menarik beberapa kesimpulan berdasarkan hasil pengujian yang dilakukan setelah melakukan penelitian. Adapun kesimpulan yang diperoleh adalah antara lain:

1. Vigenere Cipher bekerja dengan dengan cara melakukan pergeseran pada karakter.
2. Vigenere Cipher memiliki kunci yang dapat ditentukan sesuai dengan jumlah kunci yang diinginkan..
3. Vigenere Cipher harus menggunakan modulo agar karakter hasil enkripsi tidak melewati batas karakter pada tabel ASCII.

5.2 Saran

Penelitian juga meiliki kekurangan. Terdapat beberapa saran yang dapat penulis kemukakan untuk meningkatkan kualitas penelitian ini. Adapun saran tersebut adalah antara lain:

1. Sebaiknya algoritma Vigenere Cipher dapat digunakan secara online.
2. Vigenere Cipher akan lebih jika dikombinasikan dengan algoritma lain agar meningkat keamanan.

DAFTAR PUSTAKA

Ayushi, M. (2010). A Symmetric Key Cryptographic Algorithm. *International Journal of Computer Applications*, *1*(15), 1–6. https://doi.org/10.5120/331-502

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

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

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).

Dhany, H. W., Izhari, F., Fahmi, H., Tulus, M., & Sutarman, M. (2017, October). Encryption and decryption using password based encryption, MD5, and DES. In International Conference on Public Policy, Social Computing and Development 2017 (ICOPOSDev 2017) (pp. 278-283). Atlantis Press.

Fuad, R. N., & Winata, H. N. (2017). APLIKASI KEAMANAN FILE AUDIO WAV (WAVEFORM) DENGAN TERAPAN ALGORITMA RSA. InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan, 1(2), 113-119.

Gurevich, Y. (2012). What Is an Algorithm? (pp. 31–42). https://doi.org/10.1007/978-3-642-27660-6_3

Hariyanto, E., Lubis, S. A., & Sitorus, Z. (2017). Perancangan prototipe helm pengukur kualitas udara. KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer), 1(1).

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.

Jogiyanto, H. M. (2006). *Analisis Dan Desain Sistem Informasi, Pendekatan Terstruktur Teori Dan Praktek Aplikasi Bisnis*. Yogyakarta: Andi Offset.

Khairul, K., Haryati, S., & Yusman, Y. (2018). Aplikasi Kamus Bahasa Jawa Indonesia dengan Algoritma Raita Berbasis Android. Jurnal Teknologi Informasi dan Pendidikan, 11(1), 1-6.

Khairul, K., IlhamiArsyah, U., Wijaya, R. F., & Utomo, R. B. (2018, September). IMPLEMENTASI AUGMENTED REALITY SEBAGAI MEDIA PROMOSI PENJUALAN RUMAH. In Seminar Nasional Royal (SENAR) (Vol. 1, No. 1, pp. 429-434).

Kurniawan, H. (2018). Pengenalan Struktur Baru untuk Web Mining dan Personalisasi Halaman Web. Jurnal Teknik dan Informatika, 5(2), 13-19.

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.

Pratama, G. M., & Tamatjita, E. N. (2015). MODIFIKASI ALGORITMA VIGENERE CIPHER MENGGUNAKAN METODE CATALAN NUMBER DAN DOUBLE COLUMNAR TRANSPOSITION. *Compiler*, *4*(1), 31–40.

Rahim, R., Supiyandi, S., Siahaan, A. P. U., Listyorini, T., Utomo, A. P., Triyanto, W. A., ... & Khairunnisa, K. (2018, June). TOPSIS Method Application for Decision Support System in Internal Control for Selecting Best Employees. In Journal of Physics: Conference Series (Vol. 1028, No. 1, p. 012052). IOP Publishing.

Rao, R. V., & Selvamani, K. (2015). Data Security Challenges and Its Solutions in Cloud Computing. *Procedia Computer Science*, *48*, 204–209. https://doi.org/10.1016/j.procs.2015.04.171

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

Sari, R. D., Supiyandi, A. P. U., Siahaan, M. M., & Ginting, R. B. (2017). A Review of IP and MAC Address Filtering in Wireless Network Security. Int. J. Sci. Res. Sci. Technol, 3(6), 470-473.

Sidik, A. P. (2018). Algoritma RSA dan Elgamal sebagai Algoritma Tambahan untuk Mengatasi Kelemahan Algoritma One Time Pad pada Skema Three Pass Protocol.

Sitorus, Z., Saputra, K, S., Sulistianingsih, I. (2018) C4.5 Algorithm Modeling For Decision Tree Classification Process Against Status UKM.

Sitorus, Z. (2018). Kebutuhan Web Service untuk Sinkronisasi Data Antar Sistem Informasi dalam Universitas. Jurnal Teknik dan Informatika, 5(2), 87-90.

Sumartono, I., Siahaan, A. P. U., & Mayasari, N. (2016). An overview of the RC4 algorithm. IOSR J. Comput. Eng, 18(6), 67-73.

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

Tasril, V. (2018). Sistem Pendukung Keputusan Pemilihan Penerimaan Beasiswa Berprestasi Menggunakan Metode Elimination Et Choix Traduisant La Realite. INTECOMS: Journal of Information Technology and Computer Science, 1(1), 100-109.

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

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

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

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

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