IMPLEMENTASI KRIPTOGRAFI DENGAN KUNCI BERTINGKAT DALAM MELAKUKAN PENYANDIAN PESAN

Disusun dan Diajukan untuk Memenuhi Salah Satu Syarat Guna Memperoleh
Gelar Sarjana Komputer pada Fakultas Sains dan Teknologi
Universitas Pembangunan Panca Budi
Medan

SKRIPSI

OLEH

NAMA	**: RICKY ARISANDI**
N.P.M	**: 1614370296**
PROGRAM STUDI	**: SISTEM KOMPUTER**

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2022

Halaman Pengesahan

PENGESAHAN SKRIPSI

JUDUL : IMPLEMENTASI KRIPTOGRAFI DENGAN KUNCI BERTINGKAT DALAM MELAKUKAN PENYANDIAN PESAN

NAMA : RICKY ARISANDI
N.P.M : 1614370296
FAKULTAS : SAINS & TEKNOLOGI
PROGRAM STUDI : Sistem Komputer
TANGGAL KELULUSAN : 13 April 2022

DIKETAHUI

DEKAN

Hamdani, ST., MT.

KETUA PROGRAM STUDI

Eko Hariyanto, S.Kom., M.Kom

DISETUJUI
KOMISI PEMBIMBING

PEMBIMBING I

Hafni, S.Kom.,M.Kom.

PEMBIMBING II

Randi Rian Putra, S.Kom., M.Kom

honan Meja Hijau

Medan, 08 Mei 2022
Kepada Yth : Bapak/Ibu Dekan
Fakultas SAINS & TEKNOLOGI
UNPAB Medan
Di -
Tempat

mat, saya yang bertanda tangan di bawah ini :

	: RICKY ARISANDI
L Lahir	: Aek nabara / 11 Maret 1997
g Tua	: Endra wianto
	: 1614370296
	: SAINS & TEKNOLOGI
di	: Sistem Komputer
	: 082277446428
	: Jalan Gaperta lewat lapagan zipur GG pngkas all no 7

hon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul **IMPLEMENTASI KRIPTOGRAFI DENGAN KUNCI BERTINGKAT DALAM MELAKUKAN PENYANDIAN**
njutnya saya menyatakan :

mpirkan KKM yang telah disahkan oleh Ka. Prodi dan Dekan
akan menuntut ujian perbaikan nilai mata kuliah untuk perbaikan indek prestasi (IP), dan mohon diterbitkan ijazahnya setelah lulus ujian meja hijau.
tercap keterangan bebas pustaka
mpir surat keterangan bebas laboratorium
mpir pas photo untuk ijazah ukuran 4x6 = 5 lembar dan 3x4 = 5 lembar Hitam Putih
mpir foto copy STTB SLTA dilegalisir 1 (satu) lembar dan bagi mahasiswa yang lanjutan D3 ke S1 lampirkan ijazah dan transkipnya sebanyak 1 lembar.
mpir pelunasan kwintasi pembayaran uang kuliah berjalan dan wisuda sebanyak 1 lembar
si 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
tuan fakultas yang berlaku) dan lembar persetujuan sudah di tandatangani dosen pembimbing, prodi dan dekan
Copy Skripsi disimpan di CD sebanyak 2 disc (Sesuai dengan Judul Skripsinya)
mpir surat keterangan BKKOL (pada saat pengambilan ijazah)
ah menyelesaikan persyaratan point-point diatas berkas di masukan kedalam MAP
dia melunaskan biaya-biaya uang dibebankan untuk memproses pelaksanaan ujian dimaksud, dengan perincian sbb :

1. [102] Ujian Meja Hijau	: Rp.	1,000,000
2. [170] Administrasi Wisuda	: Rp.	1,750,000
Total Biaya	**: Rp.**	**2,750,000**

Ukuran Toga : M

setujui oleh :

MT.
s SAINS & TEKNOLOGI

Hormat saya

RICKY ARISANDI
1614370296

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

SURAT PERNYATAAN

Saya yang bertandatangan di bawah ini :

Nama : Ricky Arisandi

NPM : 1614370296

Prodi : Sistem Komputer

Judul Skripsi : Implementasi Kriptografi Dengan Kunci Bertingkat Dalam Melakukan Penyandian Pesan

Dengan ini menyatakan bahwa :

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

Demikian pernyataan ini saya perbuat dengan sebenar-benarnya, terimakasih.

Medan, 08 Mei 2022

Yang membuat pernyataan

Ricky Arisandi

1614370296

PERNYATAAN ORISINALITAS

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

Medan, 08 Mei 2022

Ricky Arisandi

1614370296

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)
PROGRAM STUDI TEKNOLOGI INFORMASI	(TERAKREDITASI)

PERMOHONAN JUDUL TESIS / SKRIPSI / TUGAS AKHIR*

nda tangan di bawah ini :

	: RICKY ARISANDI
nir	: Aek nabara / 11 Maret 1997
ahasiswa	: 1614370296
	: Sistem Komputer
	: Keamanan Jaringan Komputer
ang telah dicapai	: 147 SKS, IPK 3.49
	: 082277446428
gajukan judul sesuai bidang ilmu sebagai berikut	:

Judul

ENTASI KRIPTOGRAFI DENGAN KUNCI BERTINGKAT DALAM MELAKUKAN PENYANDIAN PESAN

Dosen Jika Ada Perubahan Judul

Perlu

Rektor I,

(Cahyo Pramono, S.E., M.M.)

Medan, 08 Mei 2022

Pemohon,

(Ricky Arisandi)

Tanggal : .....

Disahkan oleh :

Dekan

(Hamdani, ST., MT.)

Tanggal : 14 Mei 2022

Disetujui oleh :

Dosen Pembimbing I :

(Hafni, S.Kom., M.Kom.)

Tanggal : .....

Disetujui oleh:

Ka. Prodi Sistem Komputer

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

Tanggal : 14 Mei 2022

Disetujui oleh:

Dosen Pembimbing II:

(Randi Rian Putra, S.Kom., M.Kom)

No. Dokumen: FM-UPBM-18-02	Revisi: 0	Tgl. Eff: 22 Oktober 2018

Sumber dokumen: *http://mahasiswa.pancabudi.ac.id*

Dicetak pada: *Minggu, 08 Mei 2022 20:36:46*

ABSTRAK

RICKY ARISANDI

Implementasi Kriptografi Dengan Kunci Bertingkat Dalam Melakukan Penyandian Pesan

2021

Kunci merupakan hal yang penting dalam proses enkripsi dan dekripsi. Kunci tidak boleh diketahui oleh orang lain. Terkadang penggunaan kunci tunggal dapat memberikan peluang kepada orang lain untuk melakukan penyadapan pesan. Ada banyak cara untuk mengamankan pesan agar terhindar dari pencurian data. Penelitian ini menggunakan teknik kunci bertingkat dalam hal memberi tambahan keamanan pada plaintext. Ciphertext yang dihasilkan pada enkripsi pertama akan dienkripsi kembali menggunakan kunci berikutnya sehingga menghasilkan ciphertext kedua. Hasil ciphertext ini adalah yang digunakan dan dikirimkan sehingga jauh lebih aman dari plaintext yang hanya mengalami sekali proses enkripsi saja. Algoritma yang dipakai pada proses enkripsi dan dekripsi adalah *Vigenere* dan *Gronsfeld Cipher*. Dengan menerapkan kunci bertingkat pada proses enkripsi dan dekripsi, keamanan informasi akan selalu terjamin kerahasiaannya.

Kata Kunci: algoritma, keamanan, bertingkat, cipher, enkripsi, dekripsi

KATA PENGANTAR

Puji syukur penulis ucapkan ke hadirat Tuhan YME karena berkat rahmat kesehatan dan hidayah-Nya, sehingga penulis dapat menyelesaikan penulisan skripsi tepat pada waktunya. Dalam penulisan skripsi ini, penulis memilih judul **"IMPLEMENTASI KRIPTOGRAFI DENGAN KUNCI BERTINGKAT DALAM MELAKUKAN PENYANDIAN PESAN"**.

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

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

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

Medan, 05 April 2021
Penulis

Ricky Arisandi
1614370296

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pesan merupakan berita atau informasi yang akan disampaikan atau dikabarkan kepada orang yang berhak menerima pesan tersebut. Dalam mengirimkan pesan ada beberapa tindakan yang harus dilaksanakan agar pesan tersebut benar-benar sah. Pesan terkadang bisa berbeda penyampaiannya. Orang yang menerima pesan belum tentu memiliki persepsi yang sama dengan orang yang mengirimkan pesan. Hal ini terjadi karena intonasi tidak dapat dikirim kan melalui pesan tersebut. Hal berikutnya adalah bagaimana seandainya pesan tersebut sudah dimodifikasi oleh orang yang tidak bertanggung jawab. Hal ini akan mengakibatkan kerugian yang besar bagi pemilik pesan tersebut. Terlebih-lebih apabila pesan atau berita yang disampaikan menyangkut hal finansial dan keuangan; hal ini dapat mengakibatkan kerugian yang fatal bagi setiap pihak.

Pesan perlu diamankan dengan suatu teknik kriptografi. Kadang-kadang pesan harus diamankan dengan memiliki sistem yang bertingkat atau ganda. Pesan yang diamankan dengan menggunakan sebuah kunci belum tentu aman dari pembongkaran paksa. Penelitian ini mencoba untuk menggunakan kunci bertingkat dalam hal mengamankan pesan yang akan dikirimkan. Kunci ganda merupakan dua teknik kriptografi yang dikombinasikan agar memiliki sistem pertahanan yang lebih kuat. Ciphertext yang dihasilkan ada dua buah, ciphertext hasil enkripsi dari

plaintext dan ciphertext hasil enkripsi dari ciphertext sebelumnya. Proses enkripsi ada dua kali dan begitu juga pada proses dekripsi, ada sebanyak dua tahapan juga.

Penggunaan kunci bertingkat merupakan teknik yang mudah untuk dilakukan dan juga sangat meningkatkan keamanan pada plaintext. Dengan menerapkan kunci bertingkat, diharapkan keamanan informasi akan lebih terjamin. Berdasarkan latar belakang yang telah dijabarkan, penulis mengambil penelitian dengan judul "**IMPLEMENTASI KRIPTOGRAFI DENGAN KUNCI BERTINGKAT DALAM MELAKUKAN PENYANDIAN PESAN**".

1.2 Rumusan Masalah

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

1. Bagaimana merancang penyandian pesan menggunakan kunci bertingkat?
2. Bagaimana menentukan algoritma enkripsi dan dekripsi pada masing-masing kunci?
3. Bagaimana menentukan karakter yang digunakan pada sistem kunci bertingkat?
4. Bagaimana mengembalikan ciphertext menjadi plaintext?

1.3 Batasan Masalah

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

1. Kunci yang digunakan ada sebanyak dua tingkat dengan menggunakan algoritma *Vigenere dan Gronsfeld Cipher*.
2. Karakter yang dapat diproses adalah 1000 karakter.
3. Plaintext merupakan informasi yang diketik langsung pada objek textbox.
4. Bahasa pemrograman yang digunakan adalah menggunakan Microsoft Visual Basic.Net 2010.
5. Program aplikasi berbasis desktop dan tidak berbasis daring.

1.4 Tujuan Penelitian

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

1. Untuk merancang penyandian pesan menggunakan kunci bertingkat.
2. Untuk menentukan algoritma enkripsi dan dekripsi pada masing-masing kunci.
3. Untuk menentukan karakter yang digunakan pada sistem kunci bertingkat.
4. Untuk mengembalikan ciphertext menjadi plaintext.

1.5 Manfaat Penelitian

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

1. Pesan yang akan dikirimkan akan lebih terlindungi menggunakan kunci bertingkat.
2. Memberi kenyamanan bagi pengirim dan penerima pesan.
3. Menambah ilmu kriptografi tentang teknik memberikan pengamanan dengan teknik kunci bertingkat.

BAB II

LANDASAN TEORI

2.1 Pengertian Aplikasi

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

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

2.2 Data

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

tersebut masih belum dilaporkan secara terperinci kepada manajemen. Untuk keperluan pengambilan keputusan, maka faktur-faktur tersebut perlu diolah lebih lanjut untuk menjadi suatu informasi (Sun et al., 2014).

2.2.1 Bagaimana Data Disimpan

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

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

2.2.2 Jenis data

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

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

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

2.2.3 Pengelolaan dan Penggunaan Data

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

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

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

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

2.3 Logika dan Algoritma

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

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

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

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

2.4 Kriptografi

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

1. *Plaintext*

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

2. *Ciphertext*

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

3. Enkripsi

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

4. Deskripsi

   Deskripsi merupakan proses yang dilakukan untuk memperoleh kembali plaintext dari ciphertext.

5. Kunci

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

6. Kriptosistem

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

7. Kriptanalisis

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

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

2.4.1 Sejarah Kriptografi

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

susunan huruf-huruf di dalam pesan, sedangkan *cipher* substitusi mengganti setiap huruf atau kelompok huruf dengan sebuah huruf atau kelompok huruf lain (Pabokory et al., 2015).

2.4.2 Tujuan Kriptografi

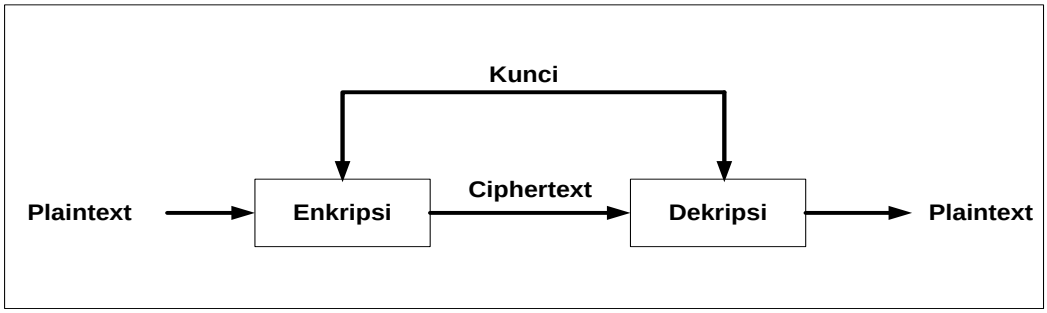
Dari paparan awal dapat dirangkumkan bahwa kriptografi bertujuan untuk member layanan keamanan. Yang dinamakan aspek-aspek keamanan:

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

2.4.3 Kriptografi Simetris

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

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



Gambar 2.1 Skema kriptografi simetris
Sumber: (Putri et al., 2018)

Kelebihan kriptografi simetris adalah:

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

Kelemahan kriptografi simetris antara lain:

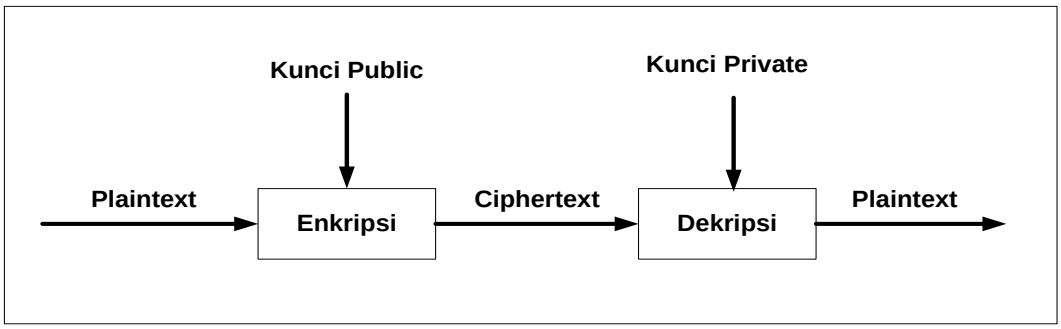
1. Kunci simetris harus dikirim melalui saluran komunikasi yang aman, dan kedua entitas yang berkomunikasi harus menjaga kerahasiaan kunci.
2. Kunci harus sering diubah, setiap kali melaksanakan komunikasi. Apabila kunci tersebut hilang atau lupa, maka pesan tersebut tidak dapat dibuka.

2.4.4 Kriptografi Asimetris

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

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

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



Gambar 2.2 Skema kriptografi asimetris
Sumber: (Putri et al., 2018)

Kelebihan kriptografi asimetris adalah:

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

Kelemahan kriptografi asimetris adalah:

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

2.5 Enkripsi

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

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

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

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

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

Langkah-langkah pada proses enkripsi adalah sebagai berikut:

1. *Plaintext* diubah ke dalam bentuk bilangan. Untuk mengubah plaintext yang berupa huruf menjadi bilangan dapat digunakan kode *ASCII* dalam sistem bilangan desimal.
2. *Plaintext* m dinyatakan menjadi blok-blok m1,m2,m3,...., sedemikian sehingga setiap blok merepresentasikan nilai di dalam selang [0, n-1] , sehingga transformasinya menjadi satu ke satu.
3. Setiap blok mi dienkripsi menjadi blok ci dengan rumus mi = ci e mod n

2.6 Dekripsi

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

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

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

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

1. Setiap blok *ciphertext* ci *didekripsi* kembali menjadi blok mi dengan rumus mi = ci d mod n
2. Kemudian blok-blok m1,m2,m3,...., diubah kembali ke bentuk huruf dengan melihat kode *ASCII* hasil *dekripsi*. (Yuza, dkk, 2018)

2.7 Vigenere Cipher

Menurut (Teady, 2013) dalam jurnalnya yang berjudul *Vigenere Cipher* Menggunakan *Spreadsheet*, penyandian *Vigenere* atau *Vigenere Cipher* merupakan salah satu teknik penyandian dengan cara subtitusi. Bruen dalam bukunya *Cryptography, Information Theory*, and *Error-Correction*, serta Martin dalam bukunya *Everyday Cryptography*, mengatakan bahwa *vigenere cipher* adalah sebuah metode dari enkripsi teks alfabetik menggunakan serangkaian penyandian bebasis caesar pada huruf-huruf dari sebuah kata kunci, dan merupakan bentuk sederhana dari subtitusi *polyalphabetic*.

Teknik subtitusinya serupa dengan semua penyandian berbasis caesar. Seperti penyandian berbasis caesar lainnya, *vigenere cipher* sebenarnya juga melakukan pergeseran, tetapi pergeseran dilakukan perhuruf dengan huruf berikutnya pada *plaintext* berbeda. Dengan demikian jika pada *caesar cipher*

seseorang dengan mudah menebak kuncinya dengan melakukan pergeseran abjad mulai dari 1 s/d 26 secara cara *try* and *error*, sampai ditemukan nilai kunci yang tepat. Maka pada pada *vigenere cipher* akan lebih sulit menebak kuncinya dengan *try* and *error* mencari nilai pergeseran seperti pada *Caesar cipher*, karena antara huruf yang satu dengan huruf berikutnya mempunyai nilai pergeseran yang berbeda.

Vigenere Cipher menggunakan suatu kunci yang memiliki panjang tertentu. Panjang kunci tersebut biasa lebih pendek ataupun sama dengan *Plaintext* nya. Jika panjang kunci kurang dari panjang *Plaintext*, maka kunci tersebut akan diulang secara *periodic* sehingga panjang kunci tersebut akan sama panjang dengan *Plaintext* nya.

Formula atau rumus Enkripsi *Vigenere Cipher*

$$Ci = (Pi + Ki) \bmod 26$$

Formula atau rumus Dekripsi *Vigenere Cipher*

$$Pi = (Ci-Ki) \bmod 26 \text{ ; untuk } Ci >= Ki$$

$$Pi = (Ci+26-Ki) \bmod 26 \text{ ; untuk } Ci <= Ki$$

Dengan penjelasan:

Ci = nilai *decimal* karakter *ciphertext* ke-i

Pi = nilai *decimal* karakter *ciphertext* ke-i

Ki = nilai *decimal* karakter *ciphertext* ke-i

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

R	S	T	U	V	W	X	Y	Z
17	18	19	20	21	22	23	24	25

2.8 Gronsfeld Cipher

Gronsfeld Cipher adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi *Caesar* berdasarkan huruf-huruf pada kata kunci. Sandi *Vigenère* merupakan bentuk sederhana dari sandi substitusi *polialfabetik*. Kelebihan sandi ini dibanding sandi *Caesar* dan sandi *monoalfabetik* lainnya adalah sandi ini tidak begitu rentan terhadap metode pemecahan sandi yang disebut analisis frekuensi. Giovan Batista Belaso menjelaskan metode ini dalam buku La cifra del. Sig. Giovan Batista Belaso (1553); dan disempurnakan oleh diplomat Perancis Blaise de Vigenère, pada 1586. Pada abad ke-19, banyak orang yang mengira *Vigenère* adalah penemu sandi ini, sehingga, sandi ini dikenal luas sebagai "sandi *Vigenère*". Sandi ini dikenal luas karena cara kerjanya mudah dimengerti dan dijalankan, dan bagi para pemula sulit dipecahkan. Pada saat kejayaannya, sandi ini dijuluki le chiffre indéchiffrable (bahasa Prancis: 'sandi yang tak terpecahkan'). Metode pemecahan sandi ini baru ditemukan pada abad ke-19. Pada tahun 1854, Charles Babbage menemukan cara untuk memecahkan sandi Vigenère. Metode ini dinamakan tes Kasiski karena Friedrich Kasiski-lah yang pertama

mempublikasikannya. Tabel Vigenère, atau tabula recta, dapat digunakan untuk enkripsi maupun dekripsi sandi Vigenère. Sandi Vigenère sebenarnya merupakan pengembangan dari sandi Caesar. Pada sandi Caesar, setiap huruf teks terang digantikan dengan huruf lain yang memiliki perbedaan tertentu pada urutan alfabet. Misalnya pada sandi Caesar dengan geseran 3, A menjadi D, B menjadi Eand dan seterusnya. Sandi Vigenère terdiri dari beberapa sandi Caesar dengan nilai geseran yang berbeda. Untuk menyandikan suatu pesan, digunakan sebuah tabel alfabet yang disebut tabel Vigenère. Tabel Vigenère berisi alfabet yang dituliskan dalam 26 baris, masing-masing baris digeser satu urutan ke kiri dari baris sebelumnya, membentuk ke-26 kemungkinan sandi Caesar. Setiap huruf disandikan dengan menggunakan baris yang berbeda-beda, sesuai kata kunci yang diulang Misalnya, teks terang yang hendak disandikan adalah perintah "Serbu Berlin" Sedangkan kata kunci antara pengirim dan tujuan adalah "PIZZA" diulang sehingga jumlah hurufnya sama banyak dengan plaintext nya yaitu PIZZAPIZZAP.

Huruf pertama pada teks terang, S, disandikan dengan menggunakan baris berjudul P, huruf pertama pada kata kunci. Pada baris P dan kolom S di tabel Vigenère, terdapat huruf H. Demikian pula untuk huruf kedua, digunakan huruf yang terletak pada baris I (huruf kedua kata kunci) dan kolom E (huruf kedua teks terang), yaitu huruf M. Proses ini dijalankan terus sehingga:

Plaintext	:	serbuberlin
Kata kunci	:	PIZZAPIZZAP
Ciphertext	:	HMQAUQMQKIC

Proses sebaliknya (disebut dekripsi), dilakukan dengan mencari huruf teks bersandi pada baris berjudul huruf dari kata kunci. Misalnya, pada contoh di atas, untuk huruf pertama, kita mencari huruf H (huruf pertama teks tersandi) pada baris P(huruf pertama pada kata kunci), yang terdapat pada kolom S, sehingga huruf pertama adalah S. Lalu M terdapat pada baris I di kolom E, sehingga diketahui huruf kedua teks terang adalah E, dan seterusnya hingga didapat perintah "*serbuberlin*".

Salah satu cipher substitusi sederhana *polyalphabetic* adalah *Gronsfeld*. *Gaspar Schot* adalah seorang *kriptografer* abad ke 17 di Jerman, yang belajar *cipher* ini selama perjalanan antara *Mainz* dan *Frankfurt* dengan menghitung *Gronsfeld*, maka terciptalah nama dari cipher tersebut yaitu *Gronsfeld* (*Optimal Cryptography Technique*, Abhishek P.S. Rathore dan K. Avinash Muthuswamy).

Algoritma Gronsfeld menggunakan suatu kunci numerik yang biasanya cukup pendek misalnya 7341, kunci ini diulang secara priodik, sesuai dengan jumlah kata plainteks. Idenya adalah dengan mengganti huruf dengan bilangan desimal maka akan melainkan hanya berupa susunan angka. Kemudian enkripsi menggunakan prinsip yang sama dengan *Algoritma Vigenère* yaitu menggunakan tabel yang hanya berukuran 10x10. (Azanuddin, 2015).

Tabel 2.1 Gronsfeld Tabel

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1

3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

2.8.1 Proses Enkripsi

Untuk mengenkripsi, hanya menambahkan jumlah huruf yang akan dienkripsi sesuai dengan jumlah kunci tetapi terlebih dahulu pesan tersebut diubah ke kode nilai desimal, plainteks yang dihasilkan akan menjadi *chiperteks*. Langkah-langkah proses enkripsi adalah sebagai berikut:

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

Algoritma enkripsi Gronsfeld cipher : $Ci = (Pi + Ki) \bmod 256$

Contoh Proses Enkripsi :

Plaintext : GRO

Kunci : 734

G = 71

R = 82

O = 79

Key : 7,3,4

C1 = (G + k1) mod 256

= (71 + 7) mod 256

= 78 mod 256

= 78 = N

C2 = (R + k2) mod 256

= (82 + 3) mod 256

= 85 mod 256

= 85 = U

C3 = (O + k3) mod 256

= (79 + 4) mod 256

= 83 mod 256

= 83 = S

Chipertext : NUS

2.8.2 Proses Dekripsi

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

1. Terlebih dahulu mengubah *chiperteks* ke nilai desimal.
2. Kemudian nilai desimal *chiperteks* nya dikurangi sesuai dengan kunci
3. Setelah dikurangi dengan kunci maka langkah berikutnya adalah mengubah kembali kebentuk karakter

Contoh Proses Dekripsi :

C1 = (N - k1) mod 256

= (78 - 7) mod 256

= 71 mod 256

= 71 = G

C2 = (U - k2) mod 256

= (85 - 3) mod 256

= 83 mod 256

= 83 = R

C3 = (S - k3) mod 256

= (83 - 4) mod 256

= 79 mod 256

= 79 = O

Plaintext : GRO

2.9 Unified Modelling Language (UML)

Unified Modelling Language (UML) adalah sebuah "bahasa" yg telah menjadi standar dalam industri untuk visualisasi, merancang dan mendokumentasikan sistem piranti lunak (Mallu, 2015). UML menawarkan sebuah standar untuk merancang model sebuah system. Notasi UML merupakan sekumpulan bentuk khusus untuk menggambarkan berbagai diagram piranti lunak. Notasi UML terutama diturunkan dari 3 notasi yang telah ada sebelumnya: Grady Booch OOD (*Object-Oriented Design*), Jim Rumbaugh OMT (*Object Modeling Technique*), dan Ivar Jacobson OOSE (*Object-Oriented Software Engineering*) (Isa & Hartawan, 2017).

Unifed Modeling Language (UML) adalah keluarga notasi grafis yang didukung oleh meta-model tunggal, yang membantu pendekskripsian dan desain sistem perangkat lunak, khususnya sistem yang dibangun menggunakan pemrograman berorientasi objek.

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).

2.9.1 Use Case Diagram

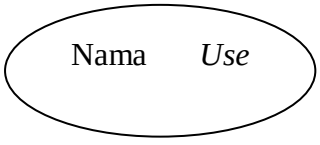
Use Case diagram digunakan untuk menggambarkan sistem dari sudut pandang pengguna sistem tersebut (*user*). sehingga pembuatan use case diagram lebih dititik beratkan pada fungsionalitas yang ada pada sistem, bukan berdasarkan

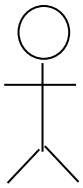
alur atau urutan kejadian. Sebuah use case diagram mempresentasikan sebuah interaksi antara aktor dengan sistem (Isa & Hartawan, 2017).

Use case adalah deskripsi fungsi dari sebuah sistem dari perspektif pengguna. *Use case* bekerja dengan cara mendeskripsikan tipikal interaksi antara *user* (pengguna) sebuah sistem dengan sistemnya sendiri melalui sebuah cerita bagaimana sebuah sistem dipakai. Urutan langkah-langkah yang menerangkan antara pengguna dan sistem disebut skenarion. Setiap skenario mendeskripsikan urutan kejadian. Setiap urutan diinisialisasi oleh orang, sistem yang lain, perangkat keras atau urutan waktu.

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

Tabel 2.2 Simbol Use Case Diagram

No	Simbol	Deskripsi
1	*Use case* 	Gambaran unit yang saling berkaitan antara aktor dengan sistem yang berjalan

2	Aktor  Nama aktor	Orang, proses atau sistem yang lain yang berinteraksi dengan sistem informasi yang akan dibuat.
3	Asosiasi / *Association*	Komunikasi antara aktor dan *use case*.
4	Ekstensi / *Extend* <<extend>>	Kelakuan yang hanya berjalan di bawah kondisi tertentu. Seperti jika akun sesuai, atau jika *session* sesuai.
5	Generalisasi	Elemen yang menjadi spesialisasi elemen lain.
6	*Include* <<include>>	Kelakuan yang harus terpenuhi agar suatu *event* dapat terjadi.

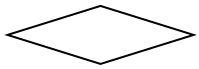
Sumber: (Hendini, 2016)

2.9.2 Activity Diagram

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

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

Tabel 2.3 Simbol Activity Diagram

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

5	Status Akhir 	Tahap akhir dari proses sistem.

Sumber: (Hendini, 2016)

2.10 Visual Basic.Net 2010

Bahasa Pemrograman *Microsoft Visual Basic .NET* adalah sebuah bahasa pemrograman tingkat tinggi untuk *Microsoft .NET Framework*. Walaupun *VB.NET* ini memang dibuat supaya mudah dipahami dan dipelajari, namun bahasa pemrograman ini juga cukup *powerful* untuk memenuhi kebutuhan dari *programmer* yang berpengalaman. Bahasa pemrograman *Visual Basic .NET* mirip dengan bahasa pemrograman *Visual Basic*, namun keduanya tidak sama".

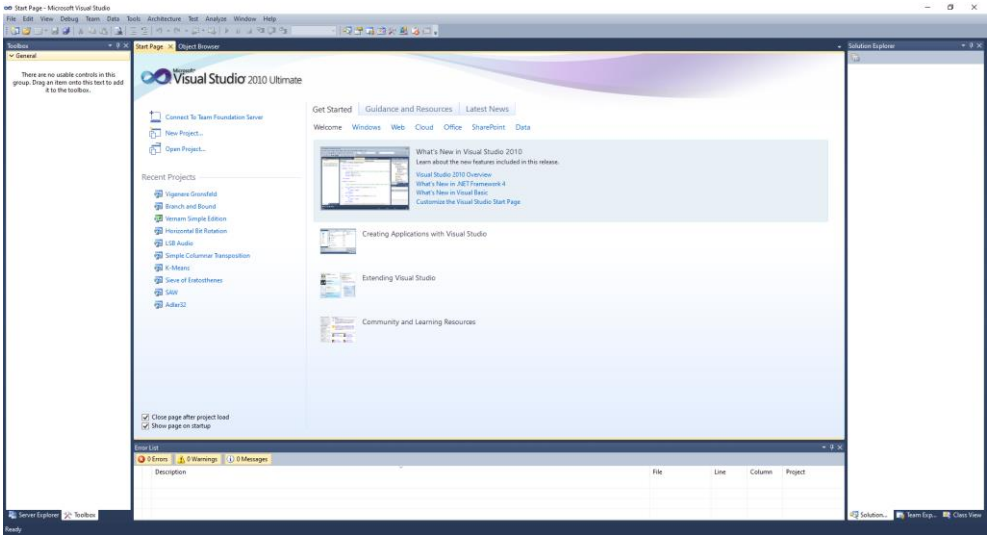
Bahasa pemrograman *Visual Basic .NET* memiliki struktur penulisan yang mirip dengan bahasa Inggris, di mana hal ini juga menyebabkan kemudahan dalam membaca dan mengerti dari sebuah kode. Di mana dimungkinkan, kata ataupun frasa yang memiliki arti digunakan dan bukannya menggunakan singkatan, akronim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

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

2.10.1 Lingkungan kerja Visual Basic.Net 2010

Pada saat pertama kali dijalankan Visual Basic 2010 Ultimate, akan menampilkan sebuah jendela Splash Visual Studio 2010 Ultimate, setelah jendela

Splash Visual Studio 2010 Ultimate muncul kemudian akan keluar sebuah start page Microsoft Visual Studio seperti gambar 2.3.



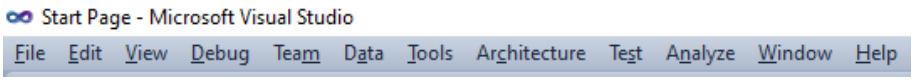
Gambar 2.3 Tampilan Microsoft Visual Studio 2010

2.10.2 Komponen Visual Basic.Net 2010

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

1. Menu Bar

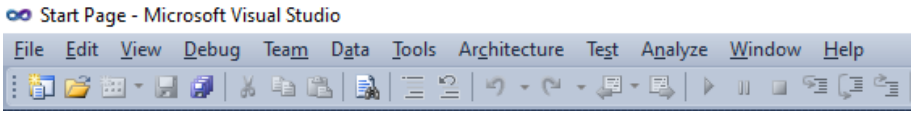
   Menu Bar adalah bagian dari *IDE* yang terdiri atas perintah-perintah untuk mengatur *IDE*, mengedit kode, dan mengeksekusi program. Menu yang terdapat pada menu bar adalah *menu file, edit, view, project, build, debug, data, tools, window* dan *help*. *Menu bar* pada *Visual Sudio* 2010 seperti terlihat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



Gambar 2.4 Tampilan Menu Bar

2. Toolbar

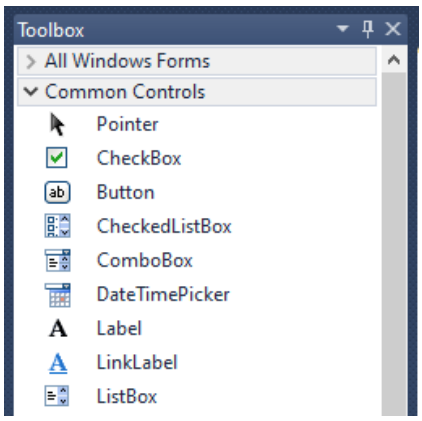
   Fasilitas ini dapat mempercepat pengaksesan perintah-perintah yang ada dalam pemrograman seperti terlihat pada gambar 2.6.



Gambar 2.5 Tampilan Toolbar

3. Toolbox

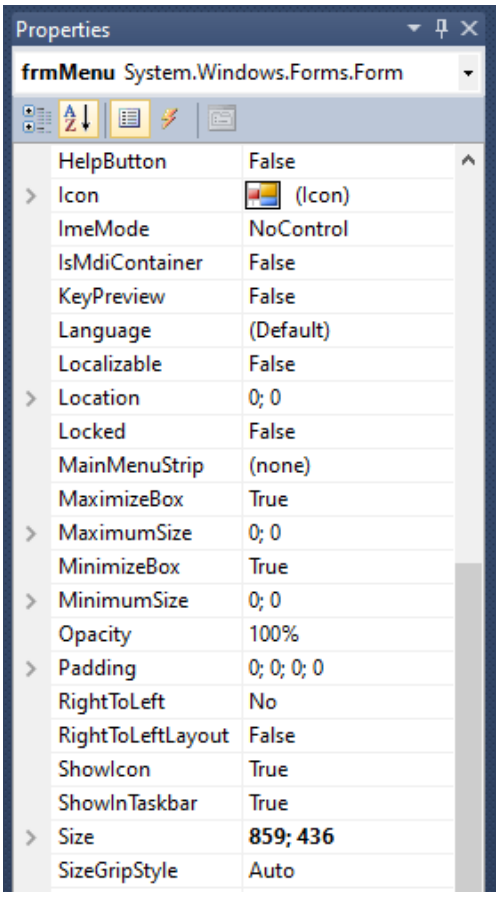
   Sebuah *window* yang berisi tombol-tombol kontrol yang akan Anda gunakan untuk mendesain atau membangun sebuah *form* atau *report* seperti terlihat pada gambar 2.7.



Gambar 2.6 Tampilan Toolbox

4. Properties Window

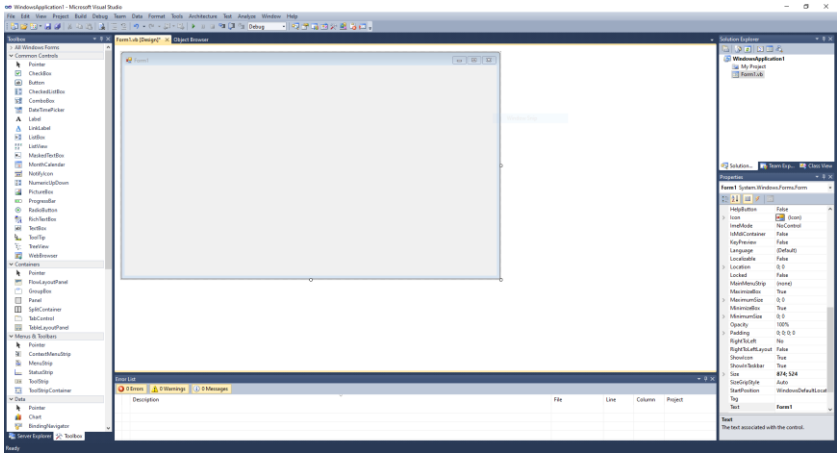
   Properties window adalah tempat menyimpan *property* dari setiap objek control dan komponen.



Gambar 2.7 Tampilan Properties

5. Form

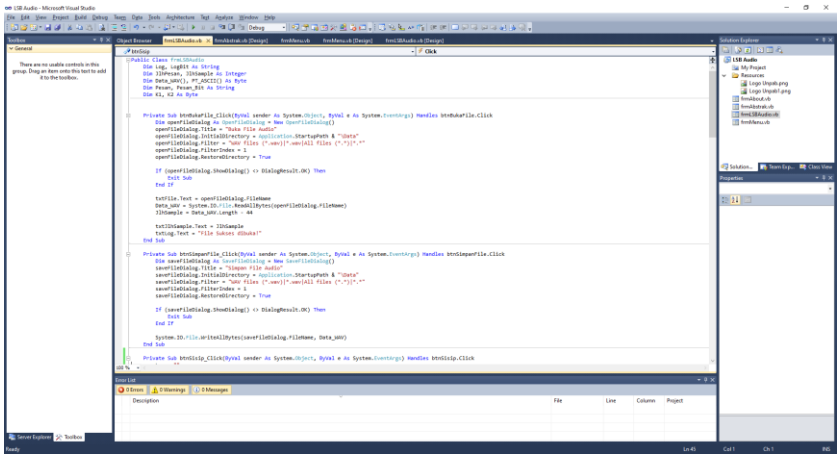
   Form merupakan tempat di mana kontrol-kontrol diletakkan. Form juga berfungsi sebagai tempat pembuatan tampilan atau antarmuka (*user interface)* dari sebuah aplikasi *windows*.



Gambar 2.8 Tampilan Form

6. Code Editor

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



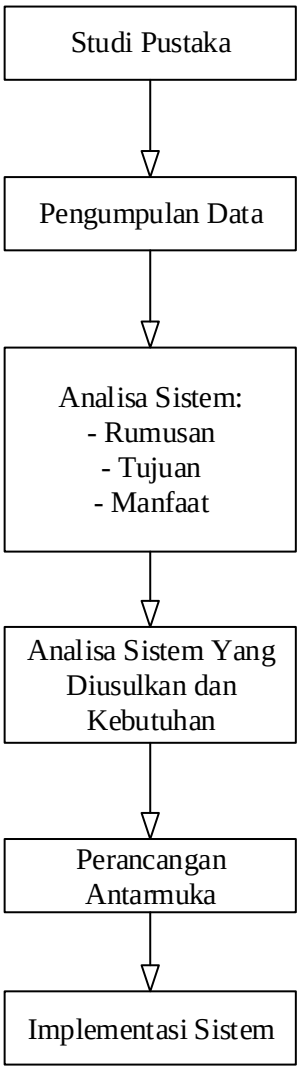
Gambar 2.9 Tampilan Code Editor

BAB III

METODE PENELITIAN

3.1 Tahapan Penelitian

Tahapan penelitian merupakan skema yang dilakukan agar memudahkan pembuatan program aplikasi. Gambar 3.1 adalah tahapan penelitian dilakukan.



Gambar 3.1 Tahapan Penelitian

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

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

3.2 Metode Pengumpulan Data

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

1. Studi Pustaka

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

2. Studi Lapangan

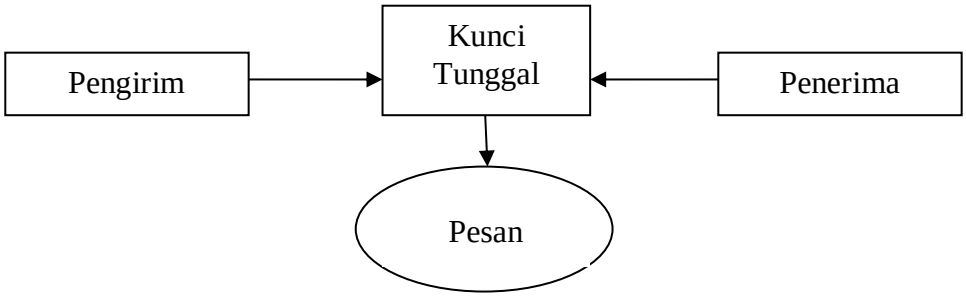
   Studi lapangan yaitu kegiatan terjun secara langsung ke lapangan dengan menggunakan teknik pengumpulan data.

3. Observasi

   Observasi melakukan pengamatan dalam melakukan penyandian pesan dengan kunci bertingkat.

3.3 Analisa Permasalahan yang Berjalan

Pengiriman pesan dengan kunci tunggal dapat memberi peluang dalam mencoba mengetahui kunci tersebut.



Gambar 3.2 Skema Pengiriman Pesan

Gambar 3.2 menjelaskan kunci yang digunakan hanya satu buah dan ini berpotensi memberikan peluang kepada pihak ketiga dalam usaha melakukan pembobolan terhadap data.

3.4 Analisa Kelemahan Yang Berjalan

Ada beberapa kelemahan dengan sistem yang berjalan saat ini. Berikut ini kelemahan sistem yang ada yaitu:

- Penggunaan kata kunci tunggal berpotensi terjadinya salah pemahaman. Dalam hal ini kemungkinan penerima salah mengartikan kunci yang diberikan oleh pengirim adalah hal yang dapat terjadi.
- Pertukaran kata kunci yang dikirimkan oleh pengirim ke penerima memiliki peluang untuk dapat disadap oleh orang yang ingin membobol pesan sehingga pesan rahasia dapat diketahui kemudian.

3.5 Analisa Sistem Yang Diusulkan

Pemecahan masalah yang penulis lakukan adalah dengan melakukan penerapan metode kunci bertingkat yang memiliki dua buah algoritma *Vigenere Cipher* dan *Gronsfeld Cipher*. Penggunaan kunci bertingkat dapat digunakan sebagai solusi agar pengirim dan penerima tidak lagi harus bertukar kunci tunggal untuk melakukan penyandian pesan melainkan dapat memiliki kata kunci masing-masing sehingga kunci tersebut tidak dapat disadap oleh orang yang berniat untuk membobol pesan tersebut.

Tabel 3.1 Rancangan Sistem

No.	Sistem yang Berjalan	Sistem yang Diusulkan	Hasil yang Ingin Dicapai
1.	Penggunaan kunci tunggal yang harus diketahui oleh pengirim dan penerima untuk membuka pesan.	Pengirim dan penerima memiliki kunci masing-masing untuk membuka pesan	Tidak ada lagi kesalahan pemahaman atau salah tafsir kunci tunggal karena pengirim dan penerima memiliki kunci yang dapat ditetapkan masing-masing pihak.
2.	Pertukaran kunci tunggal menggunakan media komunikasi yang rentan untuk dapat diketahui orang lain.	Pengirim dan penerima dapat menentukan sendiri kunci yang ingin digunakan untuk membuka pesan.	Kemungkinan bocornya kunci saat proses pertukaran informasi kunci tunggal dapat dihindari.

3.6 Analisa Proses

Pada analisa proses ini penggunaan kunci bertingkat digunakan sebagai metode yang di dalamnya terdapat kombinasi dari algoritma *Vigenere cipher* dengan algoritma *Gronsfeld cipher*. Algoritma *Vigenere cipher* digunakan oleh pengirim untuk mengenkripsi pesan yang akan dikirimkan. Sementara Algoritma *Gronsfeld cipher* akan digunakan oleh penerima untuk mendeskripsikan pesan,

sehingga penerima dapat membaca pesan asli yang dikirimkan oleh pihak pengirim tanpa perlu mengetahui kunci apa yang digunakan oleh pengirim.

Perhitungan matematika dilakukan sebagai penggambaran proses yang akan terjadi pada perhitungan kunci bertingkat. Berikut adalah langkah-langkah dalam melakukan penyandian dengan kunci bertingkat:

1. Pengirim melakukan proses enkripsi *Vigenere Cipher* pada pesan menggunakan mod 256.
2. Hasil proses enkripsi *Vigenere Cipher* di terima penerima lalu di enkripsi kembali menggunakan *Gronsfeld Cipher* dengan mod 128.
3. Lalu, hasil dari Proses enkripsi yang dilakukan oleh penerima menggunakan *Gronsfeld Cipher* di dekripsi kembali menggunakan metode *Vigenere Cipher* mod 128.
4. Setelah mendapatkan hasil dekripsi dari *Vigenere Cipher*, maka penerima mendekripsikan pesan menggunakan *Gronsfeld Cipher* dengan menggunakan mod 256 untuk mendapatkan pesan aslinya.

Berikut ini diberikan sebuah contoh perhitungan kunci bertingkat dengan menggunakan dua algoritma tersebut.

Diketahui:

Pesan = TAWA

Kunci = 4A5R

Penyelesaian:

Enkripsi Pesan Menggunakan Vigenere Chiper

T = 84 dan K = 4

Ci = (Pi + Ki) mod 256

Ci = (84 + 4) mod 256

Ci = 88 mod 256

Ci = 88

Ci = X

A = 65 dan K = A = 65

Ci = (Pi + Ki) mod 256

Ci = (65 + 65) mod 256

Ci = 130 mod 256

Ci = 130

Ci = ,

W = 87 dan K =5

Ci = (Pi + Ki) mod 256

Ci = (87 + 5) mod 256

Ci = 92 mod 256

Ci = 92

Ci = \

A = 65 dan K = R = 82

Ci = (Pi + Ki) mod 256

Ci = (65 + 82) mod 256

Ci = 147 mod 256

Ci = 147

Ci = “

Plaintext TAWA dengan kunci 4A5R menghasilkan chipertext = *X*,\“

Enkripsi Pesan Menggunakan Gronsfeld Chiper

X = 88 dan K = 4

Ci = (Pi + Ki) mod 128

Ci = (88 + 4) mod 128

Ci = 92 mod 128

, = 130 dan K = A = 65

Ci = (Pi + Ki) mod 128

Ci = (130 + 65) mod 128

Ci = 195 mod 128

Ci = 92

Ci = \

Ci = 67

Ci = C

\ = 92 dan K =5

Ci = (Pi + Ki) mod 128

Ci = (92 + 5) mod 128

Ci = 97 mod 128

Ci = 97

Ci = a

“ = 147 dan K = R = 82

Ci = (Pi + Ki) mod 128

Ci = (147 + 82) mod 128

Ci = 229 mod 128

Ci = 101

Ci = e

Jadi, plaintext X ï\ ø dengan kunci 4A5 menghasilkan chipertext = \Cae

Dekripsi Pesan Menggunakan Vigenere Chiper

\ = 92 dan K = 4

Ci = (Pi - Ki) mod 128

Ci = (92 - 4) mod 128

Ci = 88 mod 128

Ci = 88

Ci = X

C = 67 dan K = A= 65

Ci = (Pi - Ki) mod 128

Ci = (67 - 65) mod 128

Ci = 2 mod 128

Ci =2

Ci =

a = 97 dan K =5

Ci = (Pi + Ki) mod 128

Ci = (97 - 5) mod 128

e = 101 dan K = R = 82

Ci = (Pi + Ki) mod 256

Ci = (101 - 82) mod 128

Ci = 92 mod 128

Ci = 92

Ci = \

Ci = 19 mod 128

Ci = 19

Ci = !!

Jadi, chipertext \Lam dengan kunci 4A5 menghasilkan plaintext = X\!!

Dekripsi Pesan Menggunakan Gronsfeld Chiper

X = 88 dan K = 4

Ci = (Pi - Ki) mod 128

Ci = (88 - 4) mod 128

Ci = 84 mod 128

Ci = 84

Ci = T

= 2 dan K = A= 65

Ci = (Pi - Ki) mod 128

Ci = (2 - 65) mod 128

Ci = -63 mod 128

Ci = 65

Ci = A

\ = 92 dan K =5

Ci = (Pi - Ki) mod 128

Ci = (92 - 5) mod 128

Ci = 87 mod 128

Ci = 87

Ci = W

!! = 19 dan K = R = 82

Ci = (Pi - Ki) mod 128

Ci = (19 - 82) mod 128

Ci = -63 mod 128

Ci = 65

Ci = A

Jadi, chipertext X LF \ ESC dengan kunci 4A5 menghasilkan plaintext = TAWA

3.7 Analisa Kebutuhan

Analisa kebutuhan merupakan tahap awal dari sebuah penelitian. Pada bagian analisa kebutuhan, akan dijabarkan kebutuhan-kebutuhan apa saja yang harus dicantumkan dalam pembuatan perangkat lunak. Analisa kebutuhan berfungsi untuk memahami apa-apa saja yang diperlukan sebuah perangkat lunak hingga menjabarkan alur atau proses yang akan dibuat oleh perangkat lunak yang dirancang tersebut.

3.7.1 Kebutuhan Fungsional

Kebutuhan fungsional merupakan kebutuhan yang harus dipenuhi oleh sistem, dalam perancangan perangkat lunak ini berikut adalah kebutuhan fungsional yang harus dipenuhi tersebut:

1. Enkripsi pesan, sistem menjalankan proses enkripsi pesan berdasarkan kunci yang telah ditetapkan menggunakan algoritma *Vigenere Cipher*.
2. Dekripsi pesan, pengirim mendekripsikan pesan dari pihak kedua atau pihak penerima dengan menggunakan algoritma *Vigenere Cipher*.

3.7.2 Kebutuhan Non Fungsional

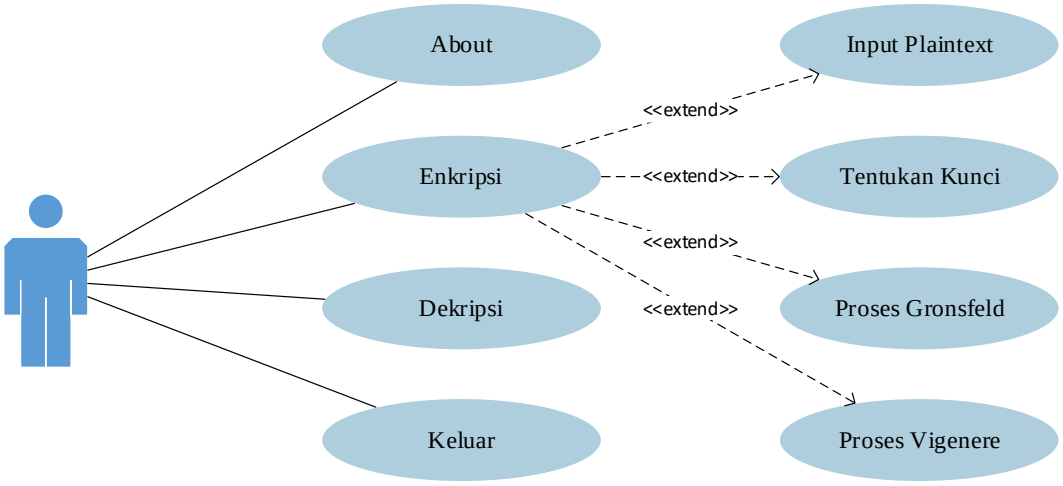
Menjalankan kebutuhan fungsional yang telah dijabarkan sebelumnya, membutuhkan dukungan dari kebutuhan non fungsional. Adapun kebutuhan non fungsional terdiri dari:

1. Sistem operasi menggunakan Windows 10 64 bit
2. Visual Basic 2010

2.8 Rancangan UML

2.8.1 Use Case Diagram Enkripsi

Berikut ini adalah use case diagram yang digunakan dalam melakukan proses enkripsi pesan.

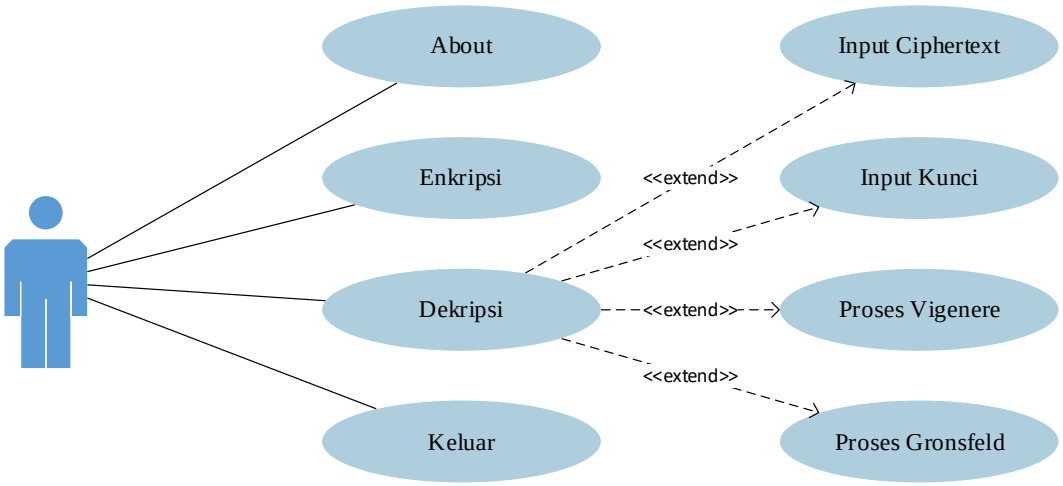


Gambar 3.3 Use Case Diagram Enkripsi

Gambar 3.3 merupakan rancangan *use case* diagram enkripsi. Pada *use case* diagram terebut, tahap pertama yang akan dilakukan oleh pengguna adalah pengguna dapat menginputkan pesan pada textbox yang sudah tersedia. Selanjutnya pengguna menentukan kunci pergeseran pada textbox kunci. Sstem akan secara otomatis memproses enkripsi pesan tersebut dengan menggunakan metode algoritma Gronsfeld dan Vigenere cipher ketika tombol enkripsi ditekan. Setelah proses enkripsi dilakukan, ciphertext hasil enkripsi akan ditampilkan pada textbox yang sudah ditentukan sebelumnya.

2.8.2 Use Case Diagram Dekripsi

Berikut ini adalah use case diagram yang digunakan dalam melakukan proses dekripsi pesan.

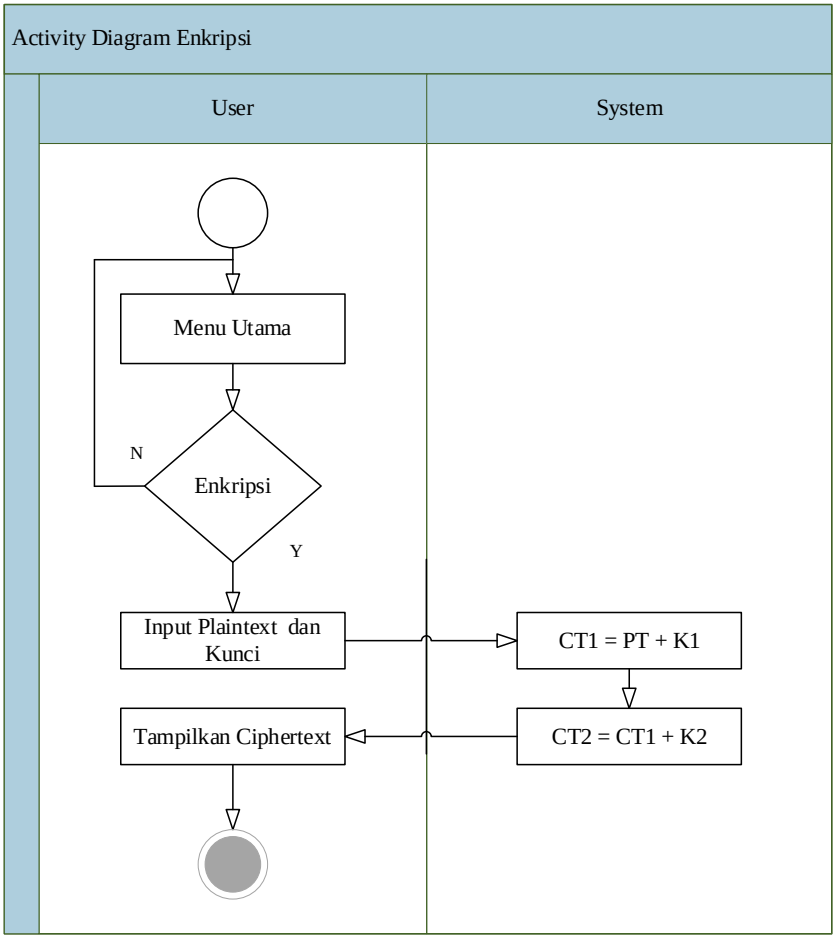


Gambar 3.4 Use Case Diagram Dekripsi

Gambar 3.4 ini merupakan rancangan use case diagram dekripsi. Pada use case diagram dekripsi tersebut, tahap awal yang harus dilakukan oleh pengguna adalah memasukkan ciphertext yang sudah diperoleh sebelumnya pada proses enkripsi. Pengguna juga memasukkan kunci untuk menentukan seberapa besar karakter akan digeser. Proses dekripsi dilakukan dengan cara menekan tombol dekripsi pada tombol yang sudah tersedia. Hasil dekripsi merupakan plaintext yang akan diletakkan pada textbox yang tersedia. Hasil plaintext harus sesuai dengan pesan yang sebelumnya akan dienkripsi.

2.8.3 Activity Diagram Enkripsi

Berikut ini adalah activity diagram proses enkripsi yang dilakukan pada kunci bertingkat.

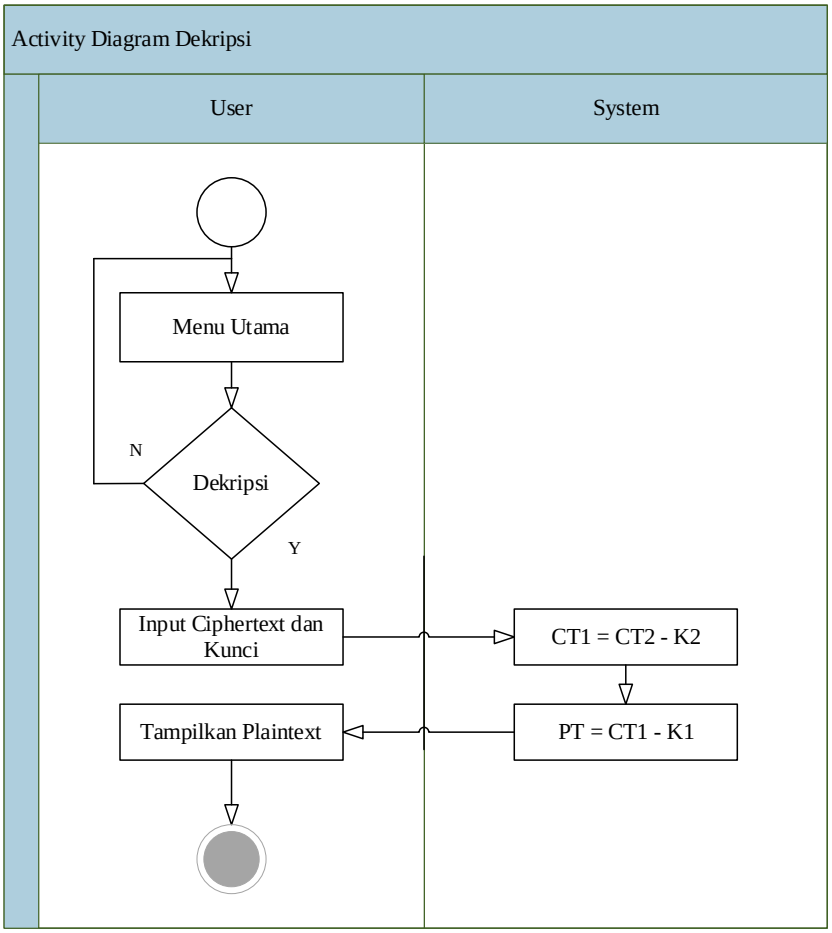


Gambar 3.5 Activity Diagram Enkripsi

Gambar 3.5 merupakan rancangan *activity* diagram enkripsi pesan dengan menggunakan kunci bertingkat. Pada *activity* diagram enkripsi, pengguna akan menginputkan pesan dan kunci yang digunakan untuk proses enkripsi.

2.8.4 Activity Diagram Dekripsi

Berikut ini adalah activity diagram proses dekripsi dengan menggunakan kunci bertingkat.



Gambar 3.6 Activity Diagram Dekripsi

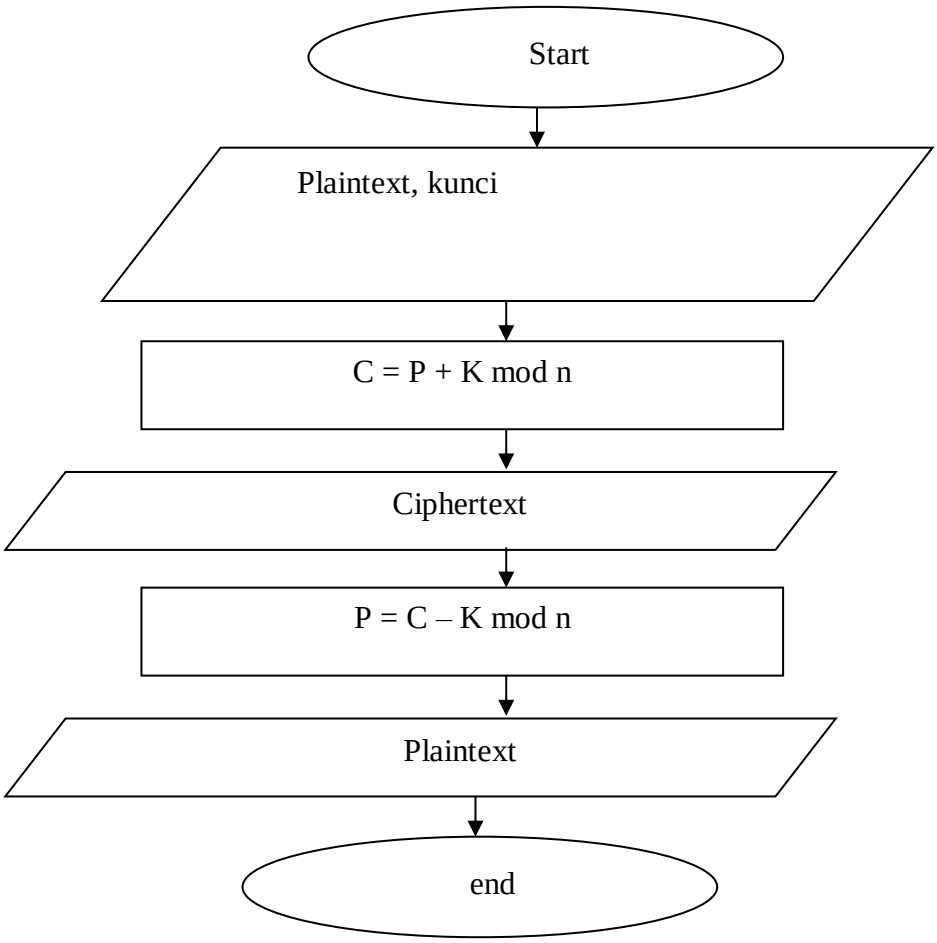
Gambar 3.6 ini merupakan rancangan *activity* diagram dekripsi dengan menggunakan kunci bertingkat. Pada *activity* diagram dekripsi, pengguna memasukkan ciphertext dan kunci.

3.8 Flowchart

Flowchart merupakan urutan-urutan langkah kerja suatu proses yang pada proses enkripsi dan dekripsi menggunakan kunci bertingkat.

3.8.1 Flowchart Vigenere Cipher

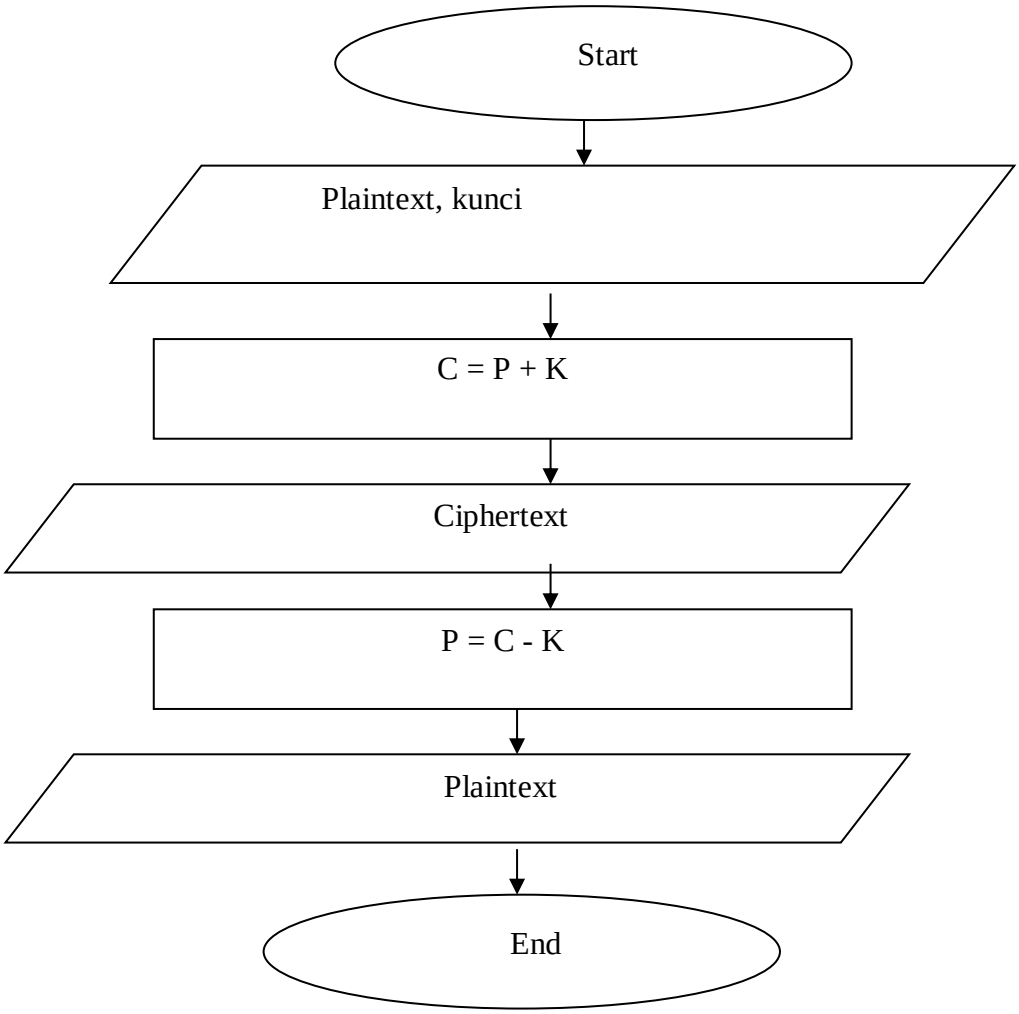
Flowchart *Vigenere Cipher* pada gambar 3.7 digunakan untuk mengenkripsi dan mendekripsi *plaintext* pada tahap pertama.



Gambar 3.7 Flowchart Vigenere Cipher

3.8.2 Flowchart Gronsfeld Cipher

Penggambaran flowchart untuk algoritma *Gronsfeld Cipher* untuk tahap kedua dijelaskan pada gambar 3.8.



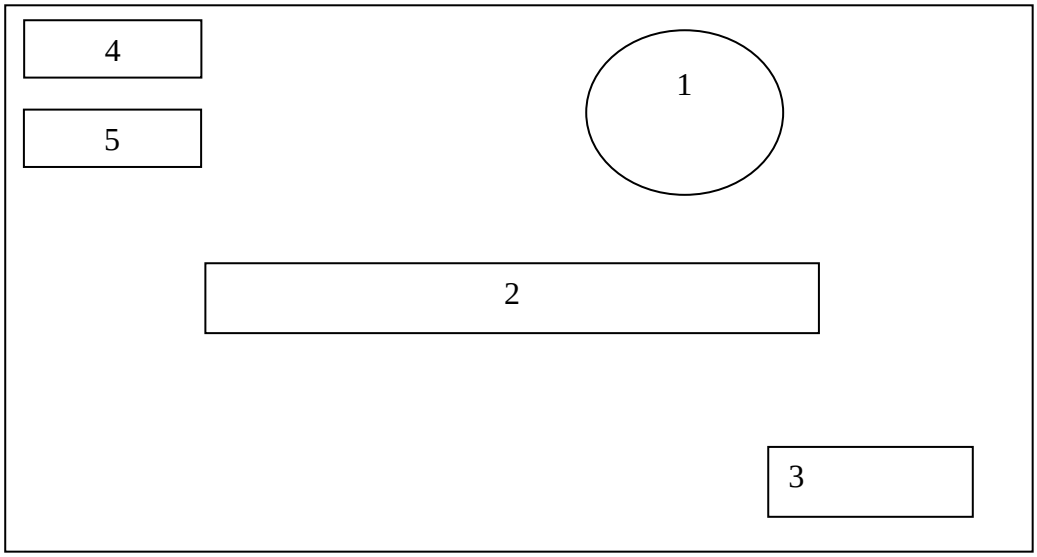
Gambar 3.8 Flowchart Gronsfeld Cipher

3.9 Rancangan Antarmuka

Rancangan antarmuka merupakan pengembangan dari sebuah ide yang bertujuan untuk memudahkan pembuatan sistem dalam hal pembuatan program aplikasi penyandian pesan dengan kunci bertingkat.

3.9.1 Rancangan Halaman Menu Utama

Menu Utama merupakan tampilan awal dari perangkat lunak yang dirancang yang berisi info-info seperti pada gambar 3.9.



Gambar 3.9 Rancangan halaman menu utama

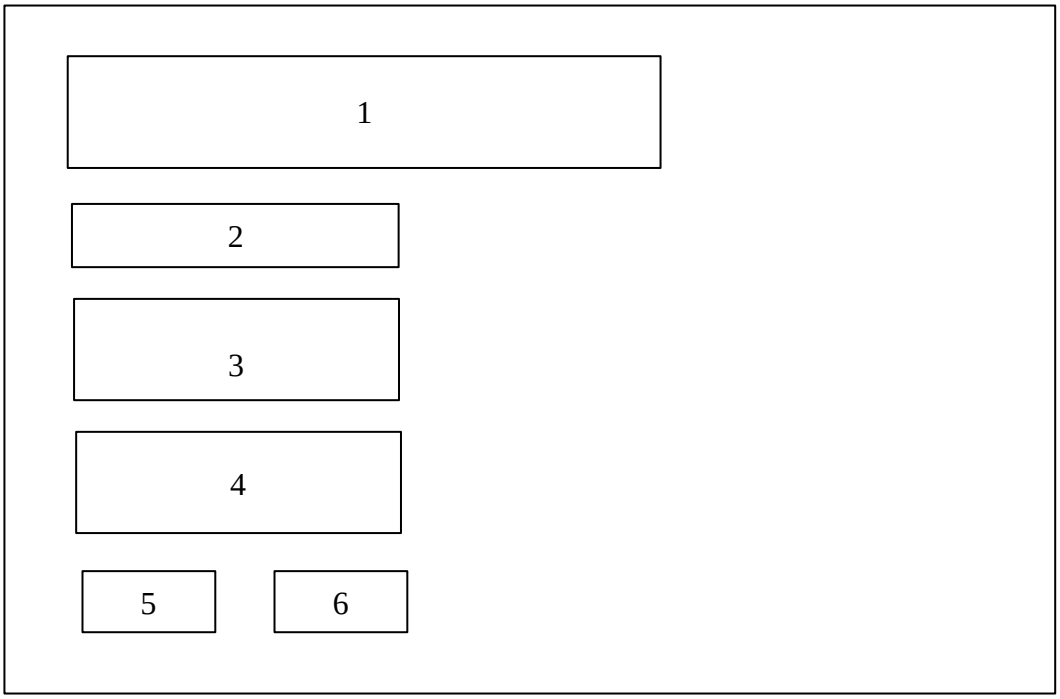
Keterangan:

1. Logo Universitas Pembangunan Panca Budi akan diletakkan sebagai simbol universitas.
2. Judul skripsi terletak pada textbox yang berfungsi menjelaskan topik yang digunakan oleh penulis.

3. Tombol Mulai ke perangkat lunak, merupakan button atau tombol yang mengarahkan pengguna untuk masuk ke proses enkripsi dan dekripsi.
4. Tombol About merupakan button atau tombol yang berfungsi mengarahkan pengguna menuju biodata penulis.
5. Tombol Deskripsi merupakan tombol yang mengarahkan pengguna menuju penjelasan seputar singkat tentang penelitian.

3.9.2 Rancangan Halaman Deskripsi

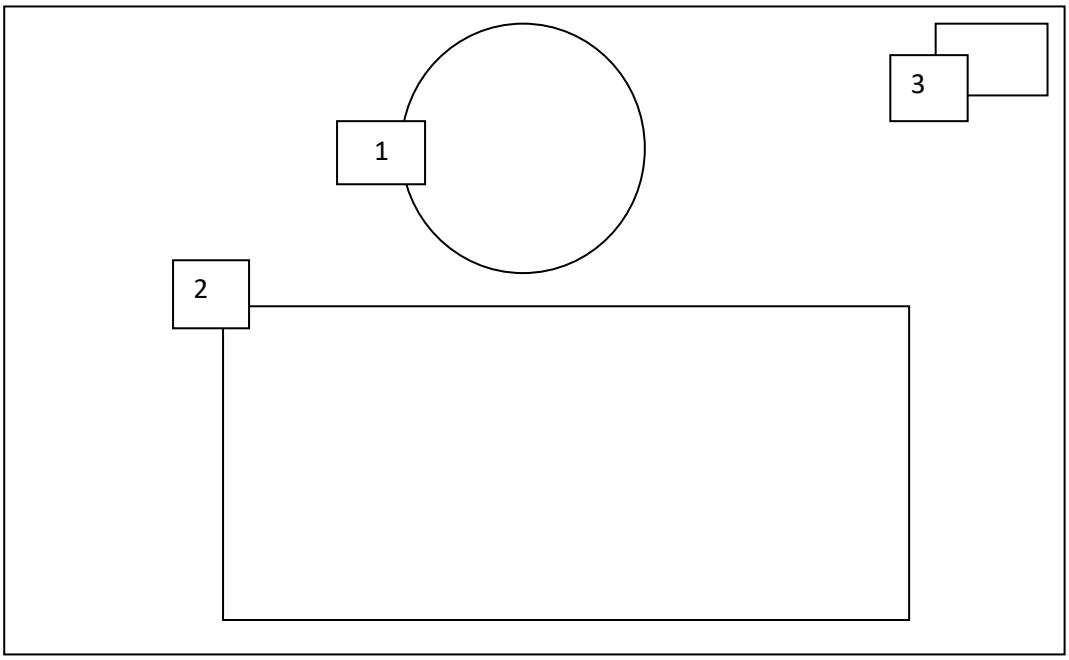
Deskripsi akan menjelaskan secara singkat penelitian yang dilakukan penulis. Rancangan ini dapat dilihat pada gambar 3.10.



Gambar 3.10 Rancangan halaman deskripsi

3.9.3 Rancangan Halaman About

Halaman about akan menjelaskan biodata penulis. Rancangan ini dapat dilihat pada gambar 3.11.



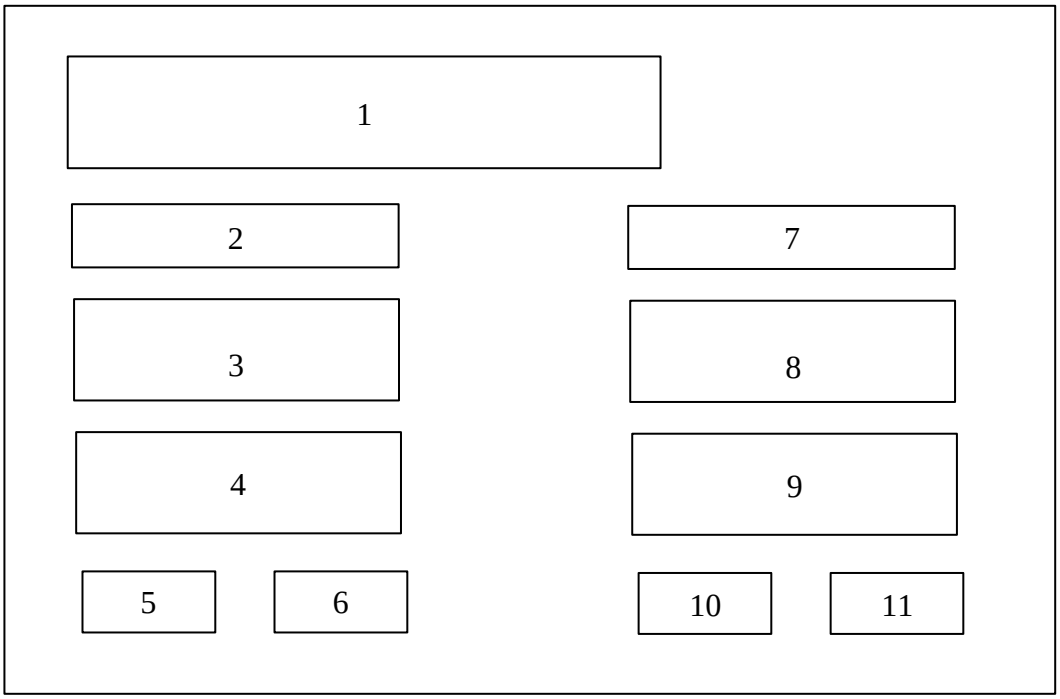
Gambar 3.11 Rancangan halaman about

Keterangan:

1. Gambar yang berfungsi untuk menampilkan logo Universitas Pembangunan Panca Budi.
2. Label yang berfungsi untuk menampilkan penjelasan tentang penulis.
3. Tombol untuk menutup halaman tentang yang berfungsi mengarahkan pengguna untuk kembali ke halaman awal.

3.7.4 Rancangan Halaman Enkripsi dan Deskripsi

Halaman enkripsi dan dekripsi menjelaskan penggunaan kunci bertingkat dalam melakukan penyandian pesan. Rancangan halaman ini dapat dilihat dengan jelas pada gambar 3.12.



Gambar 3.12 Rancangan halaman enkripsi dan deskripsi

Keterangan:

1. Plaintext 1, merupakan isi dari pesan asli yang akan di enkripsi dan dideskripsi.
2. Kunci Vigenere, merupakan kunci proses penyandian pesan asli yang akan merubah pesan asli menjadi teks tidak beraturan sesuai dengan kunci yang digunakan.

3. Ciphertext 1, tempat hasil enkripsi pertama dengan menggunakan algoritma Vigere.
4. Ciphertext 3, tempat hasil dekripsi pertama dengan menggunakan algoritma Vigenere.
5. Tombol enkripsi merupakan proses pengenkripsian pesan menggunakan algoritma Vigenere.
6. Tombol dekripsi merupakan proses pendekripsian pesan menggunakan algoritma Vigenere.
7. Kunci Gronsfeld, merupakan kunci proses penyandian pesan asli yang akan merubah pesan asli menjadi *text* tidak beraturan sesuai dengan kunci yang digunakan.
8. Ciphertext 2, tempat hasil enkripsi kedua dengan menggunakan algoritma Gronfeld.
9. Plaintext 2, tempat hasil dekripsi kedua dengan menggunakan algoritma Gronfeld.
10. Tombol enkripsi merupakan proses pengenkripsian pesan menggunakan algoritma Gronfeld.
11. Tombol dekripsi merupakan proses pendekripsian pesan menggunakan algoritma Gronfeld.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Kebutuhan Perangkat Keras dan Lunak

Sebuah program aplikasi membutuhkan perangkat keras dan perangkat lunak dalam mendukung kinerja program aplikasi tersebut. Berikut ini adalah kebutuhan perangkat tersebut:

1. *Hardware* (Perangkat Keras)

   Untuk menjalankan sistem ini, penulis menggunakan laptop dengan spesifikasi RAM 2GB, Processor Intel Celeron, Hard drive 320GB dan Display 13".

2. Software (Perangkat Lunak)

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

   a. Windows 10 64 Bit
   b. Microsoft Visual Studio 2010
   c. Microsoft Word 2019
   d. Microsoft Excel 2019
   e. Microsoft Visio 2019

4.2 Hasil Tampilan Program

Hasil tampilan program harus sesuai dengan perancangan yang dilakukan pada bab sebelumnya. Ada beberapa tampilan yang dibuat dalam program aplikasi penyandian pesan dengan kunci bertingkat.

4.2.1 Tampilan Menu Utama

Gambar 4.1 merupakan tampilan pertama ketika aplikasi dijalankan. Pada form ini pengguna dapat memilih menu lainnya seperti tombol *About* yang akan menjelaskan biodata dari penulis. Tombol *Deskripsi* akan mengarahkan pengguna untuk memberi gambaran secara singkat penelitian yang penulis lakukan. Berikut ini adalah tampilan menu utama yang akan muncul ketika pertama sekali program aplikasi penyandian pesan dengan kunci bertingkat dieksekusi.

Gambar 4.1 Tampilan menu utama

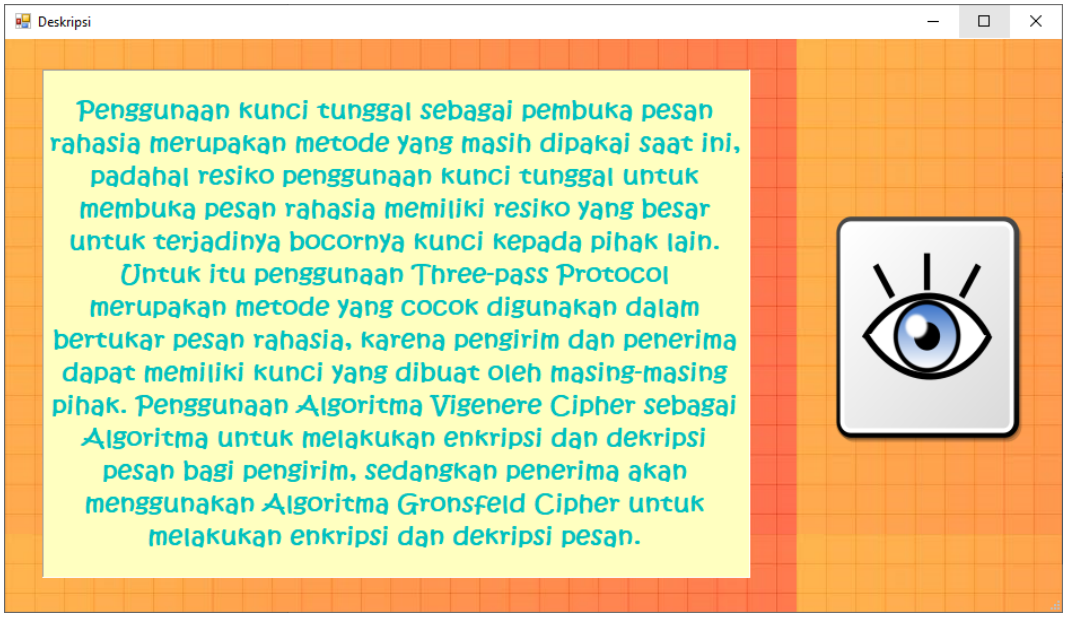
4.2.2 Tampilan About

Tampilan about menjelaskan tentang penulis, seperti judul skripsi, nama dan NPM penulis.

Gambar 4.2 Tampilan about

4.2.3 Tampilan Deskripsi

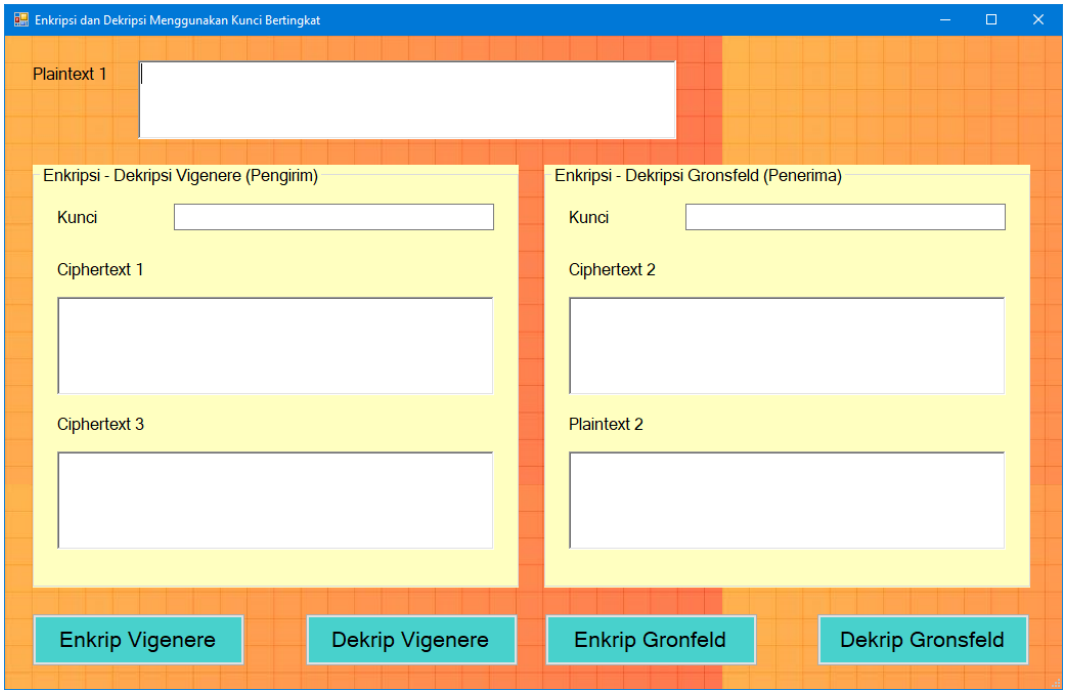
Tampilan deskripsi dari aplikasi merupakan tampilan halaman atau form yang berisi tentang informasi atau abstrak dari judul yang diambil. Pada halaman tersebut dijelaskan apa-apa saja yang menjadi latar belakang, hasil dan kesimpulan dari penyandian pesan denga menggunakan kunci bertingkat. Gambar 4.3 ini adalah tampilan dari deskripsi.



Gambar 4.3 Tampilan deskripsi

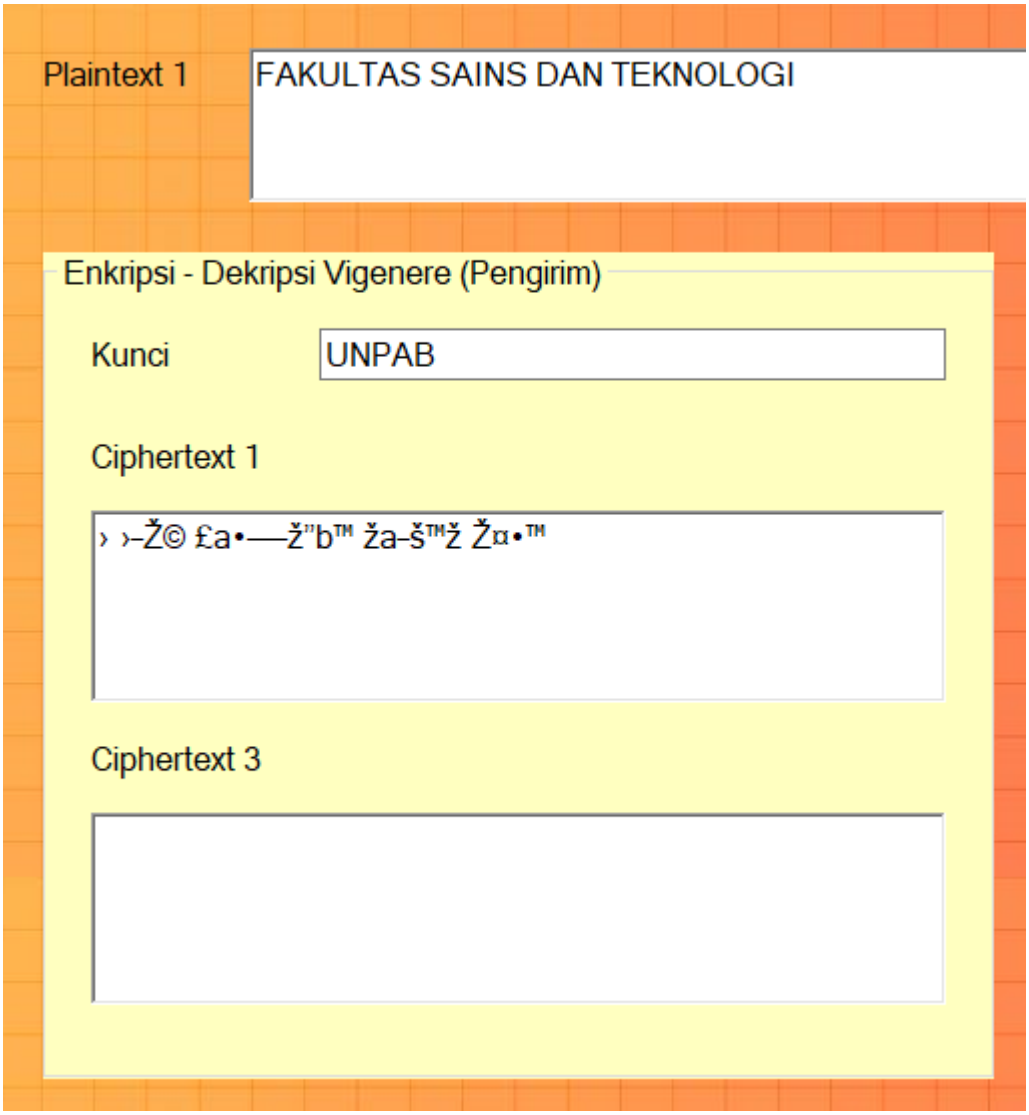
4.2.4 Tampilan Enkripsi dan Dekripsi Kunci Bertingkat

Tampilan pada gambar 4.4 adalah tampilan yang penting dalam penelitian ini. Kunci bertingkat merupakan teknik yang menjamin masing-masing pengirim dan penerima tidak akan pernah melakukan pertukaran kunci antara sesama pada saat melakukan proses enkripsi dan dekripsi. Konsep dasar kunci bertingkat bahwa masing-masing pihak memiliki kunci enkripsi dan deskripsi secara personal. Pihak pengirim dan penerima akan menggunakan kunci mereka masing-masing untuk mengenkripsi dan mendekripsi pesan dan kemudian tanpa perlu mengetahui kunci mereka masing-masing.



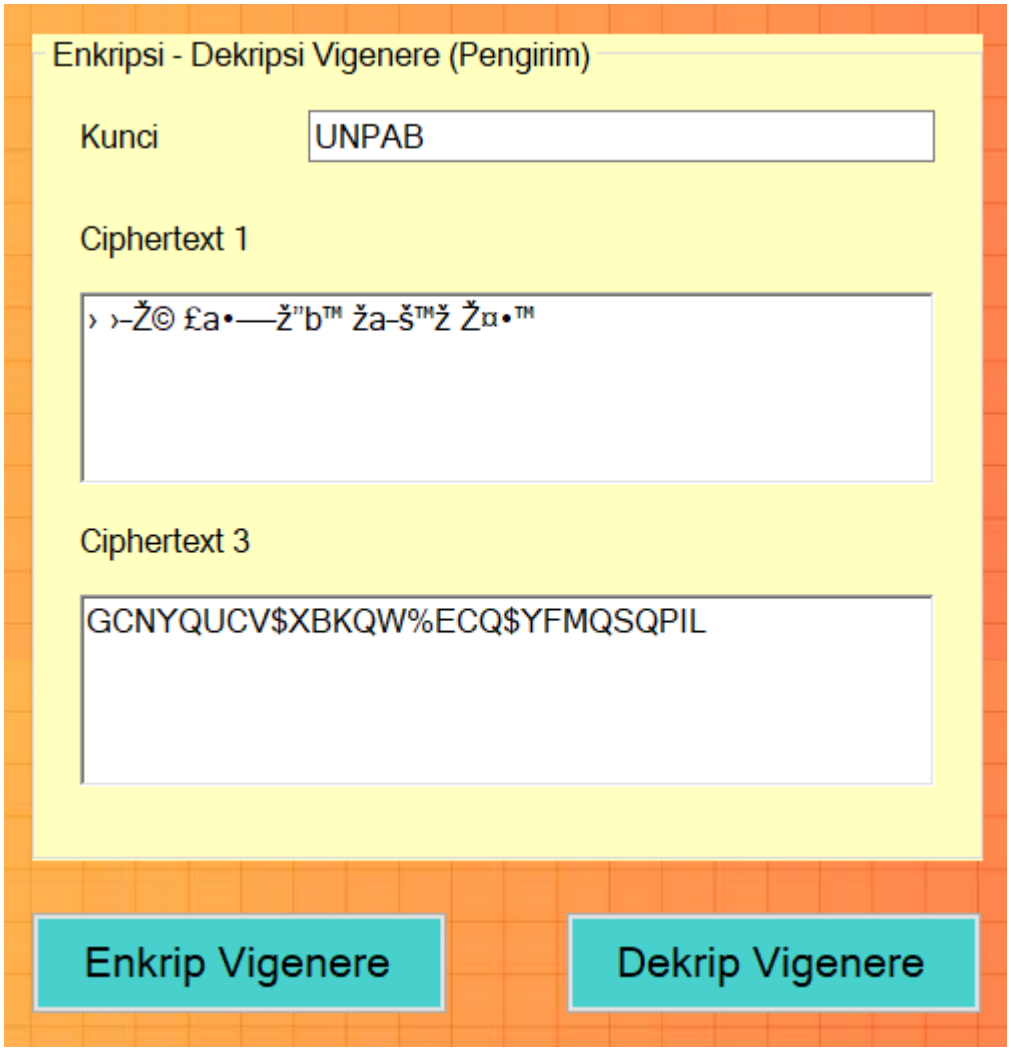
Gambar 4.4 Tampilan enkripsi dan dekripsi kunci bertingkat

Uji coba pada sistem aplikasi ini dilakukan dengan memasukkan input teks. Otomatis rangkaian karakter tersebut akan berpindah ke textbox yang berada di bawahnya. Pada tahap awal rangkaian karakter akan berada di sisi bagian pengirim yang akan mengeksekusi rangkaian karakter tersebut untuk diubah menjadi *ciphertext* menggunakan Algoritma *Vigenere Cipher*. Untuk dapat mengeksekusi dibutuhkan kunci yang hanya dapat diisi karakter angka dari 0 sampai 9.



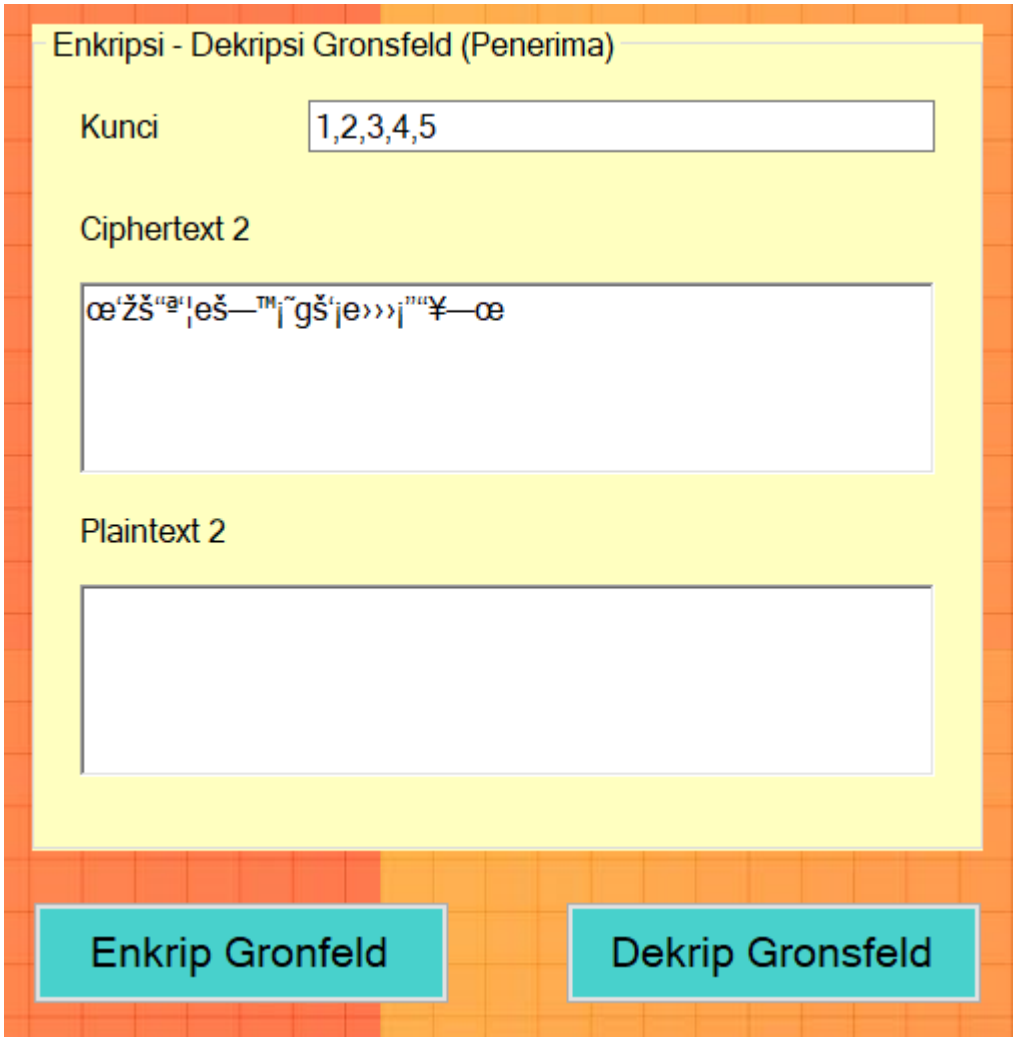
Gambar 4.5 Tampilan enkripsi algoritma Vigenere Cipher

Tombol enkripsi yang ditekan setelah memasukkan kunci berupa karakter angka selanjutnya akan mengeksekusi rangkaian karakter pesan asli yang selanjutnya akan dipanggil *plaintext*. Hasil enkripsi didapatkan pada textbox di bawahnya.



Gambar 4.6 Tampilan hasil dekripsi algoritma Vigenere Cipher

Tombol dekripsi yang ditekan selanjutnya akan memberikan hasil berupa *plaintext* yang berisi rangkaian karakter. Plaintext ini selanjutnya akan diteruskan kepada penerima dengan menekan tombol kirim.

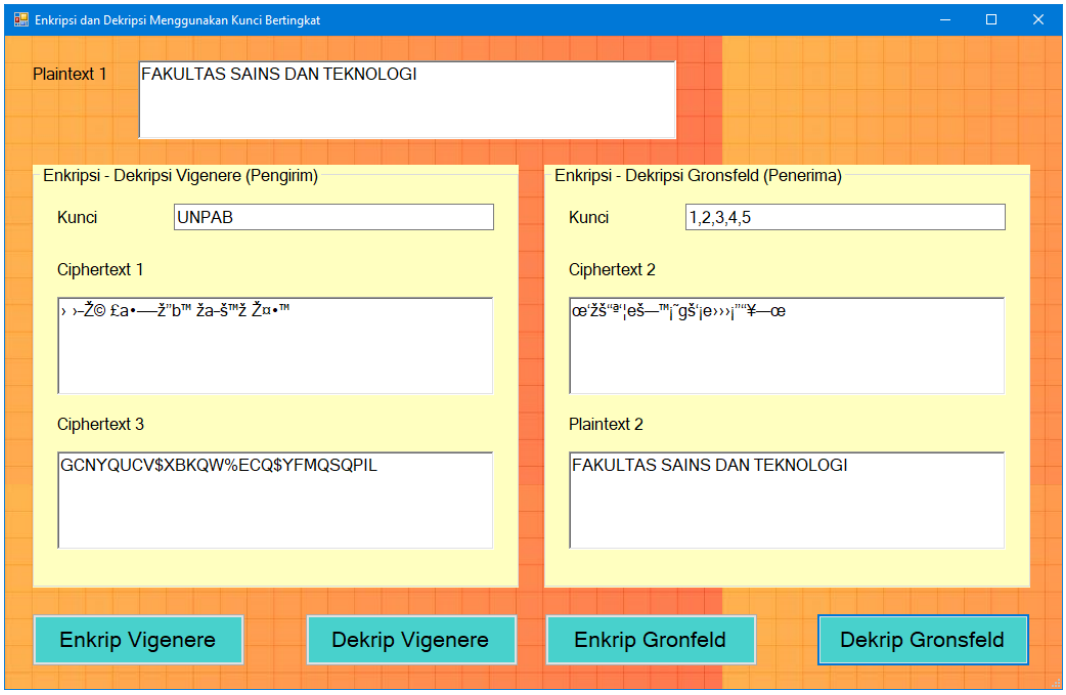


Gambar 4.7 Tampilan hasil enkripsi algoritma Gronsfeld Cipher

Rangkaian karakter yang dikirimkan oleh pengirim selanjutnya diterima oleh penerima yang akan mengeksekusi rangkaian karakter tersebut menjadi pesan asli yang dikirimkan oleh perngirim. Kunci yang digunakan juga harus tetap sama dengan kunci yang digunakan oleh penerima saat melakukan eksekusi enkripsi.

Gambar 4.8 Tampilan hasil dekripsi algoritma Gronsfeld Cipher

Setelah menekan tombol dekkripsi, maka penerima akan mendapatkan pesan asli yang dikirimkan oleh pengirim tanpa perlu bertukar kunci tunggal pada kedua proses enkripsi dan dekripsi tersebut.



Gambar 4.9 Tampilan hasil proses enkripsi dan dekripsi kunci bertingkat

Gambar 4.9 adalah hasil tampilan pada proses enkripsi dan dekripsi dengan menggunakan algoritma Vigenere dan Gronsfeld Cipher dengan teknik kunci bertingkat.

BAB V

PENUTUP

5.1 Kesimpulan

Berikut merupakan kesimpulan yang penulis buat berdasarkan pembahasan pada implementasi penyandian pesan dengan kunci bertingkat:

1. Kunci bertingkat bekerja dengan cara tidak melakukan pertukaran kunci antara penerima dan pengirim.
2. Algoritma yang digunakan untuk proses enkripsi dan dekripsi adalah *Vigenere* dan *Gronsfeld Cipher*.
3. Karakter pada kunci pada algoritma *Vigenere Cipher* menggunakan huruf dan pada algoritma *Gronsfeld Cipher* menggunakan angka.
4. Proses pengembalian *ciphertext* menuju *plaintext* dilakukan dengan cara yang sejajar dengan pada proses enkripsi.

5.2 Saran

Berikut merupakan saran yang penulis paparkan berdasarkan pembahasan dalam implementasi penyandian pesan dengan kunci bertingkat:

1. Sistem ini masih berbasis desktop yang artinya sistem hanya dapat diakses pada perangkat lokal saja, hendaknya sistem dapat dikembangkan berbasis *mobile*.

2. Dalam proses enkripsi dan dekripsi, sistem hanya dapat mengenkripsi dan mendekripsi dengan 1000 karakter, hendaknya dikembangkan menjadi lebih dari 1000 karakter.

DAFTAR PUSTAKA

Aeni Hidayah, N., & Fetrina, E. (2017). RANCANG BANGUN SISTEM PENDUKUNG KEPUTUSAN KENAIKAN JABATAN PEGAWAI DENGAN METODE PROFILE MATCHING (Studi Kasus: Kementerian Agama Kantor Wilayah DKI Jakarta). *Studia Informatika: Jurnal Sistem Informasi*, *10*(2), 127–134.

Destiningrum, M., & Adrian, Q. J. (2017). Sistem Informasi Penjadwalan Dokter Berbassis Web Dengan Menggunakan Framework Codeigniter (Studi Kasus: Rumah Sakit Yukum Medical Centre). *Jurnal Teknoinfo*, *11*(2), 30. https://doi.org/10.33365/jti.v11i2.24

Harison, & Syarif, A. (2016). Sistem Informasi Geografis Sarana Pada Kabupaten Pasaman Barat. *Jurnal TEKNOIF*, *4*(2), 40–50.

Hidayati, A. N. (2013). Analisis Dan Relevansinya Dengan Ekonomi Islam. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Herdianto, H. (2020). Deteksi Pencurian Arus Listrik pada Rumah Tangga Menggunakan Arduino Uno. InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan, 4(2), 227-232.

Isa, I. G. T., & Hartawan, G. P. (2017). Perancangan Aplikasi Koperasi Simpan Pinjam Berbasis Web (Studi. *Jurnal Ilmiah Ilmu Ekonomi*, *5*(10), 139–151.

Kurnia, D. (2020). Analisis Forensik Serangan SQL Injection dan DoS Menggunakan Instrution Detection System Pada Server Berbasis Lokal. InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan, 4(2), 208-212.

Kusumawati, R. (2016). Analisis Kinerja Reksadana Saham Konvensional dan Reksadana Saham Syariah dengan Menggunakan Metode Sharpe. *Analisis Kinerja Reksadana Saham Konvensional Dan Reksadana Saham Syariah Dengan Menggunakan Metode Sharpe*, 151–170.

Mallu, S. (2015). Sistem pendukung keputusan penentuan karyawan kontrak menjadi karyawan tetap menggunakan metode topsis. *Jurnal Ilmiah Teknologi Dan Informasi Terapan*, *1*(2), 36–42.

Palit, R. V, Rindengan, Y. D. Y., & Lumenta, A. S. M. (2015). Rancangan Sistem Informasi Keuangan Gereja Berbasis Web Di Jemaat GMIM Bukit Moria Malalayang. *E-Journal Teknik Elektro Dan Komputer*, *4*(7), 1–7.

Paramitasari, R. (2014). Analisis Faktor-Faktor Yang Mempengaruhi Audit Delay Pada Perusahaan Lq45 Yang Terdaftar Di Bursa Efek Indonesia. *Jurnal Akuntansi Dan Bisnis*, *14*(1), 129–140. https://doi.org/10.20961/jab.v14i1.149

Rizanti, N. P., Sianturi, L. T., & Sianturi, M. (2019). *Sistem Pendukung Keputusan Pemilihan Siswa Pertukaran Pelajar Menggunakan Metode PSI (Preference Selection Index)*. 263–269.

Rozaq, A., Lestari, K. F., & Handayani, S. (2015). Sistem Informasi Produk Dan Data Calon Jamaah Haji Dan Umroh Pada Pt. Travellindo Lusiyana Banjarmasin Berbasis Web. *Jurnal POSITIF*, *1*(1), 1–13.

Rizka, A., Efendi, S., & Sirait, P. (2018, September). Gain ratio in weighting attributes on simple additive weighting. In IOP Conference Series: Materials Science and Engineering (Vol. 420, No. 1, p. 012099). IOP Publishing.

Sonata, F. (2016). Implementasi Metode Simple Additive Weighting (Saw) dengan Proses Fuzzifikasi dalam Penilaian Kinerja Dosen. *Jurnal Teknologi Informasi Dan Komunikasi*, *5*(2), 71–80.

Sriani, & Putri, R. A. (2018). Analisa Sistem Pendukung Keputusan Menggunakan Metode Topsis Untuk Sistem Penerimaan Pegawai Pada Sma Al Washliyah Tanjung Morawa. *Jurnal Ilmu Komputer Dan Informatika*, *02*(April), 40–46.

Virgiawan, I. M. A. (2016). Sistem Pendukung Keputusan Untuk Pemilihan Komputer Dengan Metode Brown Gibson. *Jurnal Teknologi Informasi Dan Komputer*, *1*(1), 20–29. https://doi.org/10.36002/jutik.v1i1.19

Yani, F. (2016). Sistem Pendukung Keputusan Pemilihan Mahasiswa Berprestasi di STMIK Atma Luhur Pangkalpinang dengan Menggunakan Metode Analytical Hierarchy Process (AHP). *Jurnal Nasional Teknologi Dan Sistem Informasi*, *2*(2), 109–118. https://doi.org/10.25077/teknosi.v2i2.2016.109-118.

Zendrato, N., Dhany, H. W., Siagian, N. A., & Izhari, F. (2020, June). Bigdata Clustering using X-means method with Euclidean Distance. In Journal of Physics: Conference Series (Vol. 1566, No. 1, p. 012103). IOP Publishing.