PERANCANGAN APLIKASI ENKRIPSI DAN DESKRIPSI DENGAN TEKNIK TRANSPOSISI BARIS DAN KOLOM

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	:	SRI AWINDA
NPM	:	1514370477
PROGRAM STUDI	:	SISTEM KOMPUTER

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2019

ABSTRAK

SRI AWINDA
Perancangan Aplikasi Enkripsi dan Deskripsi Dengan Teknik Transposisi Baris Dan Kolom
2019

Keamanan data perlu diciptakan agar seseorang merasa nyaman dalam bertukar informasi di dunia maya. Data merupakan suatu kumpulan informasi yang berbentuk digital yang tidak memiliki bentuk fisik. Informasi digital dapat diduplikatkan kapan saja. Informasi ini dapat beredar di jaringan internet dengan bebas. Karena berada di jaringan bebas, setiap data rentan akan disalahgunakan. Teknik kriptografi sangat diperlukan untuk mengamankan data agar terhindar dari pencurian. Teknik transposisi kolom dan baris adalah salah satu teknik yang dapat digunakan untuk mengamankan data dari pencurian. Cara kerja metode ini sangat sederhana tapi sangat baik untuk diterapkan. Deretan-deretan karakter pada plaintext akan diacak susunannya sesuai dengan kunci yang diberikan sehingga menghindari peretasan dari pihak asing. Dengan menerapkan teknik transposisi kolom dan baris, keamanan data dapat ditingkatkan.

Kata Kunci: algoritma, keamanan, transposisi, enkripsi, dekripsi, kolom

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pengamanan sangat perlu dilakukan terhadap data-data baik data pribadi atau data perusahaan. Untuk mengamankan data dibutuhkan suatu cara yang dapat menghindari penyalahgunaan data tersebut. Teknik kriptografi adalah salah satu yang dapat digunakan untuk menghindari data dari penyalahgunaan tersebut. Setiap data memiliki kandungan informasi yang bernilai sehingga perlu dijaga kerahasiaannya.

Proses enkripsi dan dekripsi adalah proses yang terlibat dalam mengamankan data. Proses enkripsi berfungsi untuk menjadikan data tersebut menjadi data yang tidak dapat difahami atau ciphertext. Dalam melakukan proses ini ada banyak algoritma yang dapat digunakan untuk mengganti karakter teks tersebut. Banyak jenis dari algoritma yang dapat digunakan. Salah satunya adalah jenis kriptografi transposisi. Kriptografi jenis ini akan bekerja dengan cara mengubah posisi dari karakter-karakter yang ada dalam suatu deretan kata . Susunan dari posisi karakter tersebut akan saling dipertukarkan.

Ada banyak algoritma berjenis transposisi yang dapat dimanfaatkan dalam mengamankan informasi. Salah satunya adalah algoritma transposisi baris dan kolom. Plaintext akan dibentuk berdasarkan kunci yang ditentukan. Kunci merupakan kedalaman pembentukan matriks dua dimensi yang menentukan posisi karakter tersebut.

Transposisi akan mengacak posisi karakter tersebut sesuai dengan jumlah baris dan kolom yang digunakan. Lebar baris dan kolom akan digunakan sebagai kata kunci yang akan membuka ciphertext menjadi plaintext. Dengan menerapkan algoritma transposisi baris dan kolom, diharapkan keamanan informasi dapat terjamin. Berdasarkan latar belakang yang sudah dikemukakan, maka penulis mengambil penelitian dengan judul **"PERANCANGAN APLIKASI ENKRIPSI DAN DESKRIPSI DENGAN TEKNIK TRANSPOSISI BARIS DAN KOLOM".**

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 teknik transposisi baris dan kolom?
2. Bagaimana menentukan jumlah lebar baris dan kolom?
3. Bagaimana melakukan transposisi karakter menggunakan teknik transposisi baris dan kolom?
4. Bagaimana menentukan pertambahan karakter (*padding*) pada teknik transposisi baris dan kolom?
5. Bagaimana melakukan transposisi ciphertext kembali menjadi bentuk plaintext seperti semula?

1.3 Batasan Masalah

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

1. Lebar baris dan kolom maksimal adalah 10.
2. Pesan yang dienkripsi adalah berupa pesan teks.
3. Program aplikasi yang digunakan adalah menggunakan Microsoft Visual Basic.Net 2010.

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 teknik transposisi baris dan kolom.
2. Untuk menentukan jumlah lebar baris dan kolom.
3. Untuk melakukan transposisi karakter menggunakan teknik transposisi baris dan kolom.
4. Untuk menentukan pertambahan karakter (*padding*) pada teknik transposisi baris dan kolom.
5. Untuk melakukan transposisi ciphertext kembali menjadi bentuk plaintext seperti semula.

1.5 Manfaat Penelitian

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

1. Penelitian ini bermanfaat untuk memberikan informasi tentang kriptografi dengan teknik transposisi baris dan kolom.
2. Meningkatkan keamanan pesan sebelum mengalami pengiriman pada jaringan komputer.
3. Memberikan kenyamanan bagi pemilik pesan tersebut.

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.

2.2 Pencurian Data

Pencurian data adalah istilah yang digunakan untuk menggambarkan ketika informasi disalin atau diambil secara ilegal dari bisnis atau orang lain. Biasanya, informasi ini adalah informasi pengguna seperti kata sandi, nomor jaminan sosial, informasi kartu kredit, informasi pribadi lainnya, atau informasi rahasia perusahaan lainnya. Karena informasi ini diperoleh secara ilegal, ketika orang yang mencuri informasi ini ditangkap, ia akan dituntut secara hukum sepenuhnya (Yakub, 2012).

Pencurian data adalah transfer ilegal atau penyimpanan informasi apa pun yang bersifat rahasia, pribadi, atau finansial, termasuk kata sandi, kode perangkat lunak, atau algoritme, informasi berorientasi proses, atau teknologi eksklusif. Dianggap sebagai pelanggaran keamanan dan privasi yang serius, konsekuensi dari pencurian data bisa sangat parah bagi individu dan bisnis.

2.3 Sistem Informasi

Sistem informasi, seperangkat komponen terintegrasi untuk mengumpulkan, menyimpan, dan memproses data dan untuk menyediakan informasi, pengetahuan, dan produk digital. Perusahaan bisnis dan organisasi lain bergantung pada sistem informasi untuk melaksanakan dan mengelola operasi mereka, berinteraksi dengan pelanggan dan pemasok mereka, dan bersaing di pasar. Sistem informasi digunakan untuk menjalankan rantai pasokan antar organisasi dan pasar elektronik. Misalnya, perusahaan menggunakan sistem informasi untuk memproses akun keuangan, untuk mengelola sumber daya manusia mereka, dan untuk menjangkau pelanggan potensial mereka dengan promosi online. Banyak perusahaan besar dibangun sepenuhnya di sekitar sistem informasi. Ini termasuk eBay, pasar lelang besar; Amazon, mal elektronik yang berkembang dan penyedia layanan cloud computing; Alibaba, e-marketplace bisnis-ke-bisnis; dan Google, perusahaan mesin pencari yang memperoleh sebagian besar pendapatannya dari iklan kata kunci di pencarian Internet. Pemerintah menggunakan sistem informasi untuk menyediakan layanan yang hemat biaya bagi warga negara. Barang digital — seperti buku elektronik, produk video, dan perangkat lunak — dan layanan online, seperti game dan jejaring sosial, dikirimkan dengan sistem informasi. Individu mengandalkan sistem informasi, umumnya berbasis Internet, untuk melakukan banyak kehidupan pribadi mereka: untuk bersosialisasi, belajar, berbelanja, perbankan, dan hiburan (Zwass, 2019).

2.4 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.

2.4.1 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.

2.4.2 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:

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

6. Keamanan Pembayaran - Solusi menyediakan enkripsi dan tokenisasi point-to-point lengkap untuk transaksi pembayaran ritel, memungkinkan pengurangan lingkup PCI.
7. 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.
8. Keamanan Aplikasi Seluler - Melindungi data sensitif di aplikasi seluler asli sembari menjaga data dari ujung ke ujung.
9. 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.
10. 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.

2.4.3 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.

2.4.4 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 seseorang 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.

2.4.5 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.

2.4.6 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
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

2.5 Algoritma

Untuk membuat komputer melakukan apa pun, seseorang harus menulis program komputer. Untuk menulis program komputer, seseorang harus memberi

tahu komputer, langkah demi langkah, persis apa yang seseorang inginkan. Komputer kemudian "mengeksekusi" program, mengikuti setiap langkah secara mekanis, untuk mencapai tujuan akhir. Ketika seseorang memberi tahu komputer apa yang harus dilakukan, seseorang 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 seseorang memiliki seorang teman yang tiba di bandara, dan teman seseorang perlu pergi dari bandara ke rumah. Berikut adalah empat algoritma berbeda yang mungkin akan diberikan kepada orang lain untuk sampai ke rumah:

1. Algoritma taksi:
    a. Pergi ke tempat taksi.
    b. Naik taksi.
    c. Berikan alamat saya pada pengemudi.

2. Algoritma panggilan-saya:
    a. Ketika pesawat Anda tiba, hubungi ponsel saya.
    b. Temui saya di luar klaim bagasi.

3. Algoritma rent-a-car:
    a. Naik shuttle ke tempat rental mobil.
    b. Menyewa mobil.

c. Ikuti petunjuk untuk sampai ke rumah saya.

4. Algoritma bus:
    a. Di luar klaim bagasi, naik bus nomor 70.
    b. Transfer ke bus 14 di Main Street.
    c. Turun di Elm street.
    d. 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:

1. Bin sort
2. Gabungkan semacam
3. Semacam gelembung

4. Semacam shell
5. 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.

2.5.1 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.

2.5.2 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."

2.5.3 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.

2.6 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, 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.

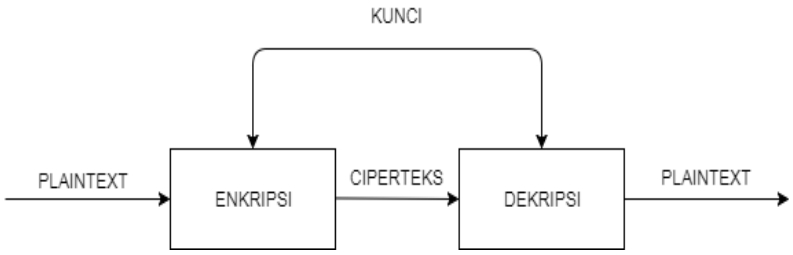
7. Kriptanalisis

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.

2.6.1 Kriptografi Simetris

Algoritma kriptografi disebut juga *cipher* yaitu aturan untuk *enchipering* dan *dechipering* atau fungsi matematika yang digunakan untuk enkripsi dan deskripsi. Beberapa *cipher* memerlukan algoritma yang berbeda untuk *enciphering* dan *dechiphering*. Algoritma Simetris sering disebut dengan algoritma klasik, karena memakai kunci yang sama untuk kegiatan enkripsi dan deskripsinya. Gambar 2.1 adalah skema algoritma simetris.

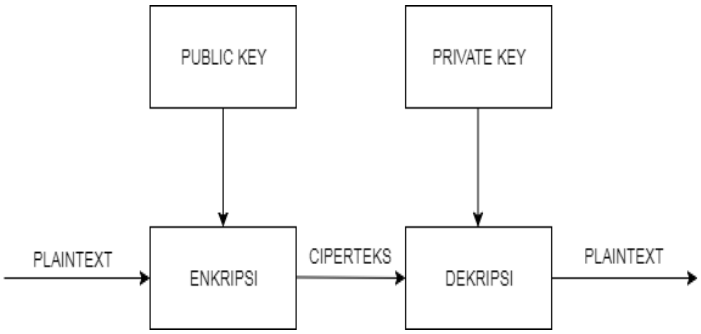


Gambar 2.1 Skema kriptografi simetris
Sumber: (Putri, Setyorini, & Rahayani, 2018)

2.6.2 Kriptografi Asimetris

Algoritma tak simetris sering juga disebut dengan algoritma kunci publik, dengan arti kata kunci yang digunakan untuk melakukan enkripsi dan dekripsinya berbeda (Ayushi, 2010) (S., L. Ribeiro, & David, 2012). Pada algoritma tak simetri kunci terbagi menjadi 2 (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)

2.7 Pengertian Enkripsi

Enkripsi adalah metode yang digunakan untuk mengubah informasi menjadi kode rahasia yang menyembunyikan makna sebenarnya dari informasi tersebut. Ilmu mengenkripsi dan mendekripsi informasi disebut kriptografi. Dalam komputasi, data yang tidak terenkripsi juga dikenal sebagai plaintext, dan data terenkripsi disebut ciphertext. Rumus yang digunakan untuk menyandikan dan mendekode pesan disebut algoritma enkripsi atau sandi. Agar efektif, sandi

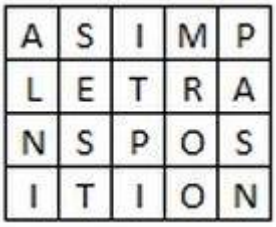
menyertakan variabel sebagai bagian dari algoritma. Variabel, yang disebut kunci, adalah apa yang membuat output cipher unik. Ketika pesan terenkripsi dicegat oleh entitas yang tidak sah, penyusup harus menebak cipher pengirim mana yang digunakan untuk mengenkripsi pesan, serta kunci apa yang digunakan sebagai variabel. Waktu yang diperlukan untuk menebak informasi ini adalah yang menjadikan enkripsi sebagai alat keamanan yang sangat berharga. Pada awal proses enkripsi, pengirim harus memutuskan cipher apa yang paling baik menyamarkan makna pesan dan variabel apa yang digunakan sebagai kunci untuk membuat pesan yang dikodekan menjadi unik. Jenis cipher yang paling banyak digunakan terbagi dalam dua kategori: simetris dan asimetris.

2.8 Pengertian Dekripsi

Dekripsi adalah proses mengambil teks yang disandikan atau dienkripsi atau data lain dan mengubahnya kembali menjadi teks yang dapat Anda baca dan pahami oleh komputer. Istilah ini dapat digunakan untuk menggambarkan metode tidak mengenkripsi data secara manual atau tidak mengenkripsi data menggunakan kode atau kunci yang tepat. Data dapat dienkripsi untuk menyulitkan seseorang untuk mencuri informasi. Beberapa perusahaan juga mengenkripsi data untuk perlindungan umum data perusahaan dan rahasia dagang. Jika data ini perlu dapat dilihat, mungkin memerlukan dekripsi. Jika kode sandi atau kunci dekripsi tidak tersedia, perangkat lunak khusus mungkin diperlukan untuk mendekripsi data menggunakan algoritme untuk memecahkan dekripsi dan membuat data dapat dibaca (Amin, 2016).

2.9 Transposisi Kolom dan Baris

Transposisi Kolom melibatkan penulisan plaintext dalam baris, dan kemudian membaca ciphertext dalam kolom. Dalam bentuk yang paling sederhana, itu adalah Rute Cipher di mana rute tersebut untuk membaca setiap kolom secara berurutan. Misalnya, plaintext "transposisi sederhana" dengan 5 kolom terlihat seperti pada ilustrasi berikut ini.



Jika sekarang kita membaca setiap kolom kita mendapatkan ciphertext "ALNISESTITPIMROOPASN". Sejauh ini tidak ada bedanya dengan cipher rute tertentu. Transposisi Kolom dibangun dalam kata kunci untuk memesan cara kita membaca kolom, serta untuk memastikan berapa banyak kolom yang digunakan.

2.9.1 Proses Enkripsi

Pertama, pilih kata kunci untuk enkripsi. Plaintext akan ditulis dalam kisi di mana jumlah kolom adalah jumlah huruf dalam kata kunci. Kami kemudian memberi judul pada setiap kolom dengan huruf masing-masing dari kata kunci. Kami mengambil huruf dalam kata kunci dalam urutan abjad, dan membaca kolom dalam urutan ini. Jika sebuah surat diulang, kita lakukan yang muncul pertama, lalu

yang berikutnya dan seterusnya. Sebagai contoh, mari kita mengenkripsi pesan "THE TOMATO IS A PLANT IN THE NIGHTSHADE FAMILY" menggunakan kata kunci tomat. Bentuk baris dan kolom dapat dilihat pada berikut ini.

T	O	M	A	T	O
5	3	2	1	6	4
T	H	E	T	O	M
A	T	O	I	S	A
P	L	A	N	T	I
N	T	H	E	N	I
G	H	T	S	H	A
D	E	F	A	M	I
L	Y	X	X	X	X

Plaintext ditulis dalam kotak di bawah kata kunci. Angka-angka tersebut mewakili urutan abjad kata kunci, dan urutan kolom yang akan dibaca. Kami telah menulis kata kunci di atas kisi plaintext, dan juga angka yang memberi tahu kami urutan kolom mana yang harus dibaca. Perhatikan bahwa "O" pertama adalah 3 dan "O" kedua adalah 4, dan hal yang sama untuk dua "T". Dimulai dengan kolom yang dimulai oleh "A", ciphertext kami mulai "TINESAX" dari kolom ini. Kami sekarang pindah ke kolom yang dipimpin oleh "M", dan seterusnya melalui huruf-huruf kata kunci dalam urutan abjad untuk mendapatkan ciphertext "TINESAX / EOAHTFX / HTLTHEY / MAIIAIX / TAPNGDL / OSTNHMX" (di mana / memberi tahu Anda di mana yang baru kolom dimulai). Dengan demikian,

ciphertext terakhir adalah "TINES AXEOA HTFXH TLTHE YMAII AIXTA PNGDL OSTNH MX".

2.9.2 Proses Dekripsi

Proses dekripsi jauh lebih mudah jika nulls digunakan untuk mengganti pesan dalam proses enkripsi. Di bawah ini kita akan berbicara tentang bagaimana cara mendekripsi pesan di kedua skenario. Pertama, jika nulls telah digunakan, maka Anda mulai dengan menuliskan kata kunci dan urutan abjad dari kata kunci. Anda kemudian harus membagi panjang ciphertext dengan panjang kata kunci. Jawabannya adalah jumlah baris yang perlu Anda tambahkan ke kisi. Anda kemudian menulis ciphertext di kolom pertama sampai Anda mencapai baris terakhir. Huruf berikutnya menjadi huruf pertama di kolom kedua (dengan urutan abjad kata kunci), dan seterusnya.

Sebagai contoh, kita akan mendekripsi ciphertext "ARESA SXOST HEYLO IIAIE XPENG DLLTA HTFAX TENHM WX" yang diberi kata kunci kentang. Kita mulai dengan menuliskan kata kunci dan urutan huruf. Ada 42 huruf dalam ciphertext, dan kata kunci memiliki enam huruf, jadi kita perlu 42 ÷ 6 = 7 baris.

Ketika tidak ada nol yang digunakan, kita harus melakukan perhitungan yang sedikit berbeda. Kami membagi panjang ciphertext dengan panjang kata kunci, tetapi ini sepertinya bukan angka keseluruhan. Jika ini masalahnya, maka kami membulatkan jawabannya ke seluruh nomor berikutnya. Kami kemudian mengalikan angka ini dengan panjang kata kunci, untuk mencari tahu berapa

banyak kotak yang ada dalam kisi. Akhirnya, kami mengambil panjang ciphertext dari jawaban ini. Nomor pencuri (yang seharusnya kurang dari panjang kunci) adalah berapa banyak nol yang akan ada jika digunakan, jadi kita perlu menghapus beberapa kotak terakhir ini, jadi kita tidak memasukkan huruf ke dalamnya saat mendekripsi.

Untuk mendekripsi teks sandi "ARESA SOSTH EYLOI IAIEP ENGDL LTAHT FATEN HMW", kami mulai dengan cara yang sama di atas, dengan mengepalai kolom dengan kentang kata kunci. Kali ini, untuk menemukan berapa baris yang kita butuhkan, kita melakukan 38 ÷ 6 = 6.3333. Kami membulatkannya ke angka berikutnya, yaitu 7, jadi kami membutuhkan 7 baris. Jika kita mengalikan 6 x 7, kita mendapatkan 42, dan 42 - 38 = 4. Karenanya kita membutuhkan 4 placeholder di baris terakhir. Kami mendapatkan kisi di bawah ke kiri. Setelah memasukkan huruf ciphertext ke dalam, dengan cara yang sama seperti di atas, kita mendapatkan grid di sebelah kanan.

2.10 Unified Modelling Language (UML)

Unified Modeling Language adalah Metodologi kolaborasi antara metoda-metoda Booch, OMT (*Object Modeling Technique*), serta OOSE (*Object Oriented Software Engineering*) dan beberapa metoda lainnya, merupakan metodologi yang paling sering digunakan saat ini untuk analisa dan perancangan sistem dengan metodologi berorientasi objek mengadaptasi maraknya penggunaan bahasa “pemrograman berorientasi objek” (OOP) (Wasserkrug et al., 2009).

Beberapa literature menyebutkan bahwa UML menyediakan sembilan jenis diagram, yang lain menyebutkan delapan karena ada beberapa diagram yang digabung, misalnya diagram komunikasi, diagram urutan dan diagram pewaktuan digabung menjadi diagram interaksi (Sukmawati & Priyadi, 2019).

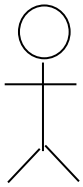
2.10.1 Use Case Diagram

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

Tabel 2.1 Simbol Use Case Diagram

No	Simbol	Deskripsi
1	*Use case* Nama *Use*	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)

2.10.2 Activity Diagram

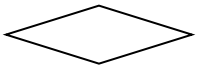
Menurut Indra Griha Tofik Isa dan George Pri Hartawan, Activity Digram menggambarkan rangkaian aliran dari aktivitas, digunakan untuk mendeskripsikan

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 2.2 Simbol Activity Diagram

No	Simbol	Deskripsi
1	Status awal 	Status awal aktivitas sistem, sebuah diagram aktivitas memiliki sebuah status awal.
2	Aktivitas 	Aktivitas yang dilakukan sistem, aktivitas biasanya diawali dengan kata kerja.

3	Percabangan / *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)

2.11 Pengertian Pesan

Pesan adalah komunikasi atau pernyataan yang disampaikan dari satu orang atau kelompok ke yang lain. Jika Anda menelepon telepon rumah saya dan saya sedang menjalankan tugas, Anda akan diminta untuk "silakan tinggalkan pesan setelah bunyi bip."

2.12 Visual Basic

Visual Basic .NET (VB.NET) adalah bahasa pemrograman berorientasi objek Microsoft (OOP). Ini berkembang dari Visual Basic 6 (VB6) untuk memenuhi kebutuhan yang meningkat akan layanan web dan pengembangan web yang mudah. VB.Net dirancang untuk memanfaatkan kelas berbasis NET framework dan lingkungan run-time. Itu direkayasa ulang oleh Microsoft sebagai bagian dari grup produk .NET. VB.NET mendukung abstraksi, pewarisan, dan polimorfisme. Modifikasi VB6 ke VB.NET yang paling substansial adalah OOP,

yang memungkinkan untuk pembuatan kelas dan objek dan peningkatan penggunaan kembali kode. Banyak kontrol baru ditambahkan untuk merampingkan pengembangan program. VB.NET juga mendukung layanan pengembangan multithreading dan Web, seperti formulir dan layanan Web. Penanganan data VB.NET direpresentasikan dan dipertukarkan melalui ADO.NET berbasis XML, yang memungkinkan penanganan data dalam jumlah besar secara efisien dan mudah melalui Web. Ada basis besar pengembang VB mengingat sejarahnya yang panjang. Banyak yang memilih C #, tetapi ini bisa menjadi perdebatan yang agak subyektif tentang manfaat dari masing-masing bahasa (Wibowo, 2014).

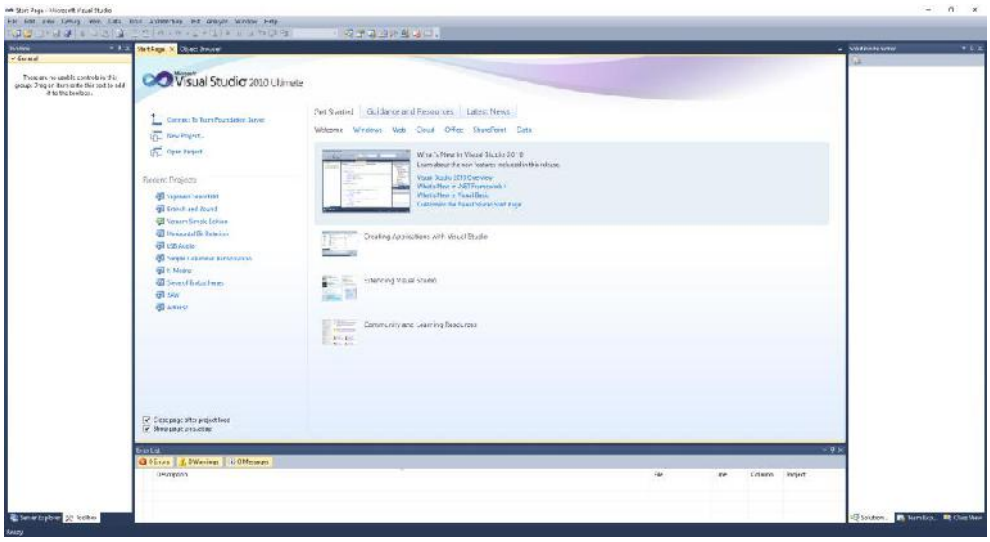
2.12.1 Sejarah Visual Basic

Visual Basic adalah bahasa pemrograman berbasis acara generasi ketiga yang pertama kali dirilis oleh Microsoft pada tahun 1991. Versi terakhir adalah Visual Basic 6. VB adalah bahasa pemrograman yang ramah pengguna yang dirancang untuk pemula. Oleh karena itu, ini memungkinkan siapa saja untuk mengembangkan aplikasi jendela GUI dengan mudah. Banyak pengembang masih lebih menyukai VB6 daripada VB.NET penggantinya. Pada tahun 2002, Microsoft merilis Visual Basic.NET (VB.NET) untuk menggantikan Visual Basic 6. Setelah itu, Microsoft menyatakan VB6 bahasa pemrograman lawas pada tahun 2008. Namun, Microsoft masih menyediakan beberapa bentuk dukungan untuk VB6. VB.NET adalah bahasa pemrograman berorientasi objek sepenuhnya diimplementasikan dalam .NET Framework. Itu dibuat untuk memenuhi pengembangan web serta aplikasi mobile.

Selanjutnya, Microsoft telah merilis banyak versi VB.NET. Mereka adalah VB2005, VB2008, VB2010, VB2012, VB2013, VB2015 dan VB2017. Meskipun bagian .NET dibuang pada tahun 2005, semua versi bahasa pemrograman Visual Basic yang dirilis sejak tahun 2002 dianggap sebagai bahasa pemrograman VB.NET. Setiap versi VB.NET dibundel dengan bahasa pemrograman Microsoft lainnya yang mencakup C #, C ++, F #, JavaScript, Python, dan lainnya di Lingkungan Pengembangan Terpadu Microsoft (IDE) yang dikenal sebagai Visual Studio. Microsoft telah menambahkan banyak fitur baru dalam Visual Studio 2017 terbaru, terutama fitur-fitur tersebut untuk membangun aplikasi seluler. Visual Basic dapat diunduh secara bebas pada Free Visual Studio Community 2017 RC dari https://www.visualstudio.com/downloads.

2.12.2 Lingkungan kerja Visual Basic.Net

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.



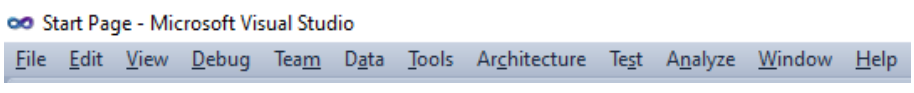
Gambar 2.3 Tampilan Microsoft Visual Studio 2010

2.12.3 Komponen Visual Basic.Net

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

1. Menu Bar

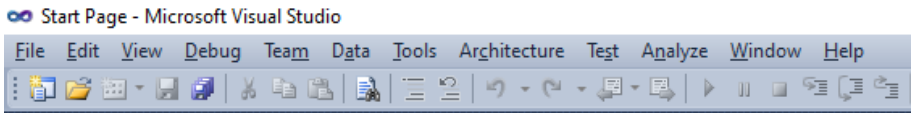
   Menu Bar adalah bagian dari *IDE* yang terdiri atas perintah-perintah untuk mengatur *IDE*, mengedit kode, dan mengeksekusi program. Menu yang terdapat pada menu bar adalah *menu file, edit, view, project, build, debug, data, tools, window* dan *help*. *Menu bar* pada *Visual Sudio* 2010 seperti terlihat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



Gambar 2.4 Tampilan Menu Bar

2. Toolbar

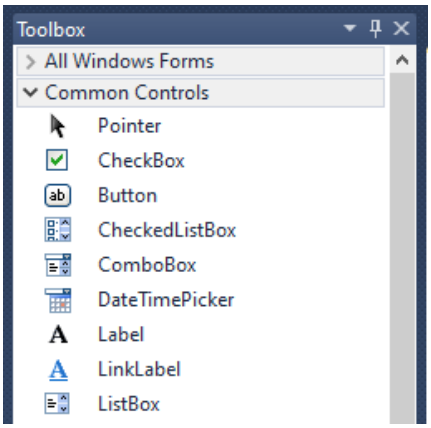
   Fasilitas ini dapat mempercepat pengaksesan perintah-perintah yang ada dalam pemrograman seperti terlihat pada gambar 2.6.



Gambar 2.5 Tampilan Toolbar

3. Toolbox

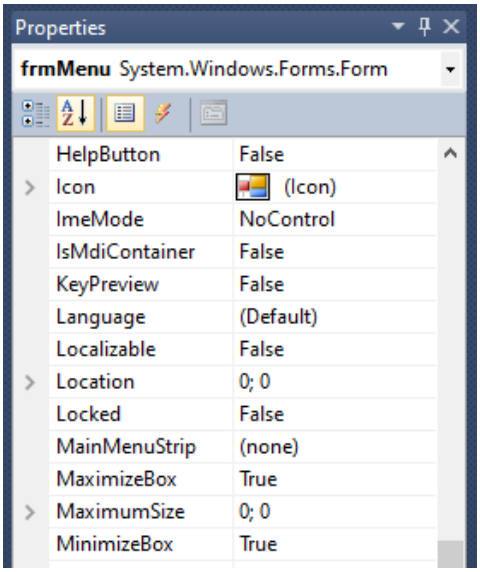
   Sebuah *window* yang berisi tombol-tombol kontrol yang akan Anda gunakan untuk mendesain atau membangun sebuah *form* atau *report* seperti terlihat pada gambar 2.7.



Gambar 2.6 Tampilan Toolbox

4. Properties Window

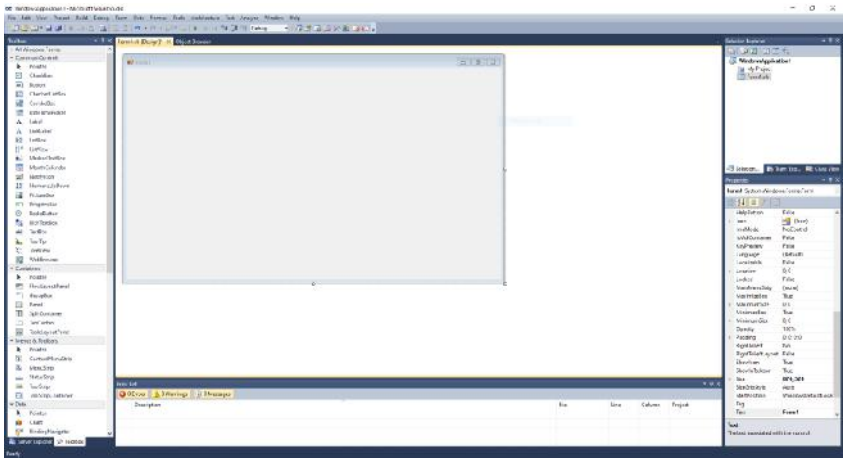
   Properties window adalah tempat menyimpan *property* dari setiap objek control dan komponen.



Gambar 2.7 Tampilan Properties

5. Form

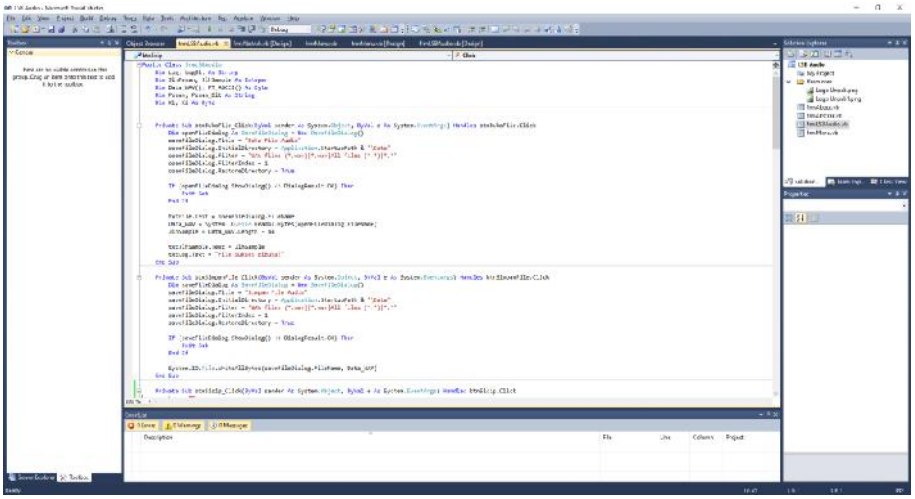
   Form merupakan tempat di mana kontrol-kontrol diletakkan. Form juga berfungsi sebagai tempat pembuatan tampilan atau antarmuka (*user interface)* dari sebuah aplikasi *windows*.



Gambar 2.8 Tampilan Form

6. Code Editor

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



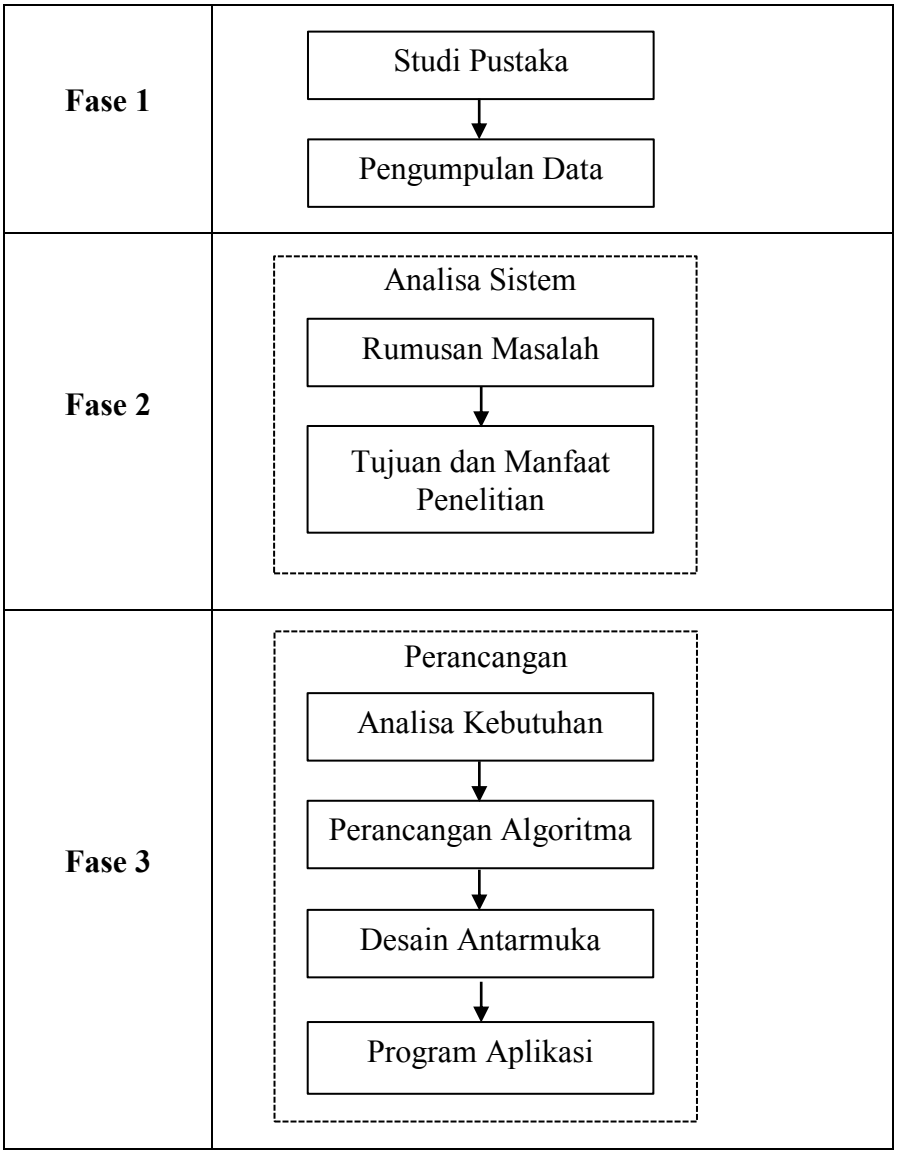
Gambar 2.9 Tampilan Code Editor

BAB III

METODE PENELITIAN

3.1. Tahapan Penelitian

Tahapan penelitian terdiri dari beberapa fase seperti pada gambar 3.1.



Gambar 3.1 Tahapan Penelitian

Berikut merupakan penjelasan dari tahapan penelitian yang sudah dikemukakan:

1. Studi pustaka, dalam skripsi ini penulis ambil dari berbagai referensi.
2. Pengumpulan data, dalam skripsi ini penulis mengumpulkan data yang berhubungan dengan teknik yang digunakan.
3. Analisa sistem, masalah yang diangkat dalam skripsi adalah bagaimana melakukan proses enkripsi dan dekripsi dengan teknik transposisi baris dan kolom.
4. Analisa kebutuhan, untuk membuat sistem ini penulis membutuhkan beberapa perangkat keras dan perangkat lunak yang digunakan.
5. Metode, metode algoritma yang penulis gunakan dalam penulisan skripsi adalah dengan menggunakan teknik transposisi kolom dan baris.
6. Desain sistem, penulis memulai proses mendesain sistem dengan menggunakan *UML* agar terlihat alur proses enkripsi dan dekripsi dengan teknik transposisi kolom dan baris.
7. Pembuatan sistem, penulis membuat sistem dengan menggunakan Microsoft Visual Basic.Net 2010.
8. Program aplikasi berfungsi untuk menguji teknik transposisi kolom dan baris. Penulis mengimplementasikan sistem dengan menjalankan program aplikasi yang dibuat dan menguji kebenaran hasil yang diperoleh pada saat pengujian dengan menggunakan program aplikasi tersebut.

3.2. Teknik Pengumpulan Data

Teknik pengumpulan bertujuan untuk mengumpulkan berbagai referensi yang dapat digunakan untuk membuat program aplikasi sesuai dengan topik transposisi kolom dan baris. Teknik dapat dilakukan dengan beberapa cara, antara lain:

1. Studi Literatur

   Studi literatur adalah mencari teori-teori pendukung yang relevan agar proses dari pembuatan program aplikasi berjalan dengan baik dan benar.

2. Studi Lapangan

   Studi lapangan yaitu pengumpulan data yang diperoleh dari penelitian lapangan.

3. Observasi

   Observasi merupakan teknik yang digunakan untuk mengumpulkan data dengan melakukan pengamatan terhadap fenomena yang terjadi pada teknik transposisi kolom dan baris.

3.3. Analisa Sistem

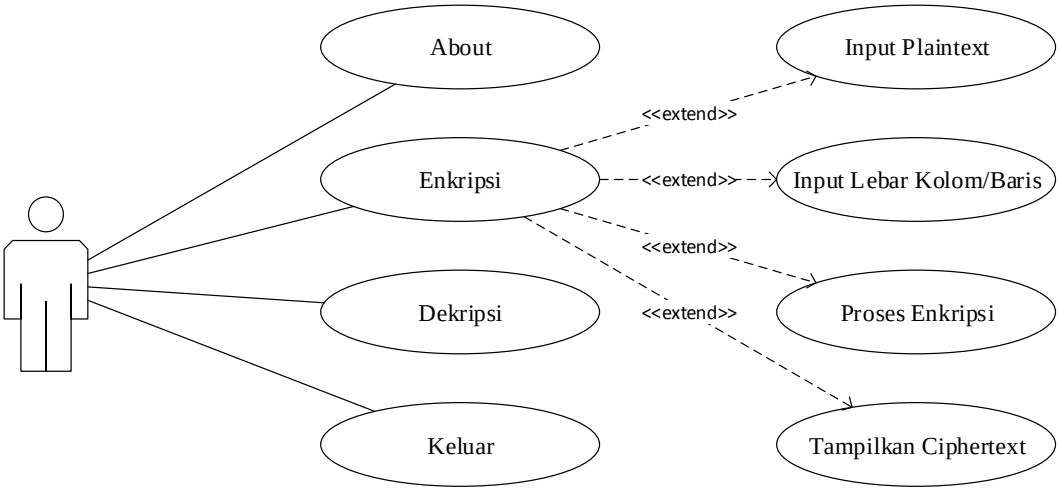
Sistem yang dirancang diharapkan dapat melakukan proses enkripsi dan dekripsi dengan menggunakan teknik transposisi kolom dan baris. Pada sistem terdapat input, proses dan output. Ketiga bagian tersebut harus terhubung secara baik dan benar. Pada penggunaan enkripsi tersebut, sistem akan mengenkripsi karakter yang ada pada pesan sehingga berubah menjadi ciphertext. Pesan ciphertext tidak akan dapat difahami oleh orang yang membaca. Teknik transposisi

kolom dan baris akan diterapkan pada saat pengguna mulai melakukan proses enkripsi atau dekripsi pada pesan yang diinputkan pada textbox. Pengguna dapat melihat hasil ciphertext pada textbox hasil.

3.4. Rancangan Model Diagram

3.4.1. Use Case Diagram Enkripsi

Pada bagian ini akan dijelaskan use case diagram yang digunakan dalam melakukan proses enkripsi transposisi kolom dan baris.

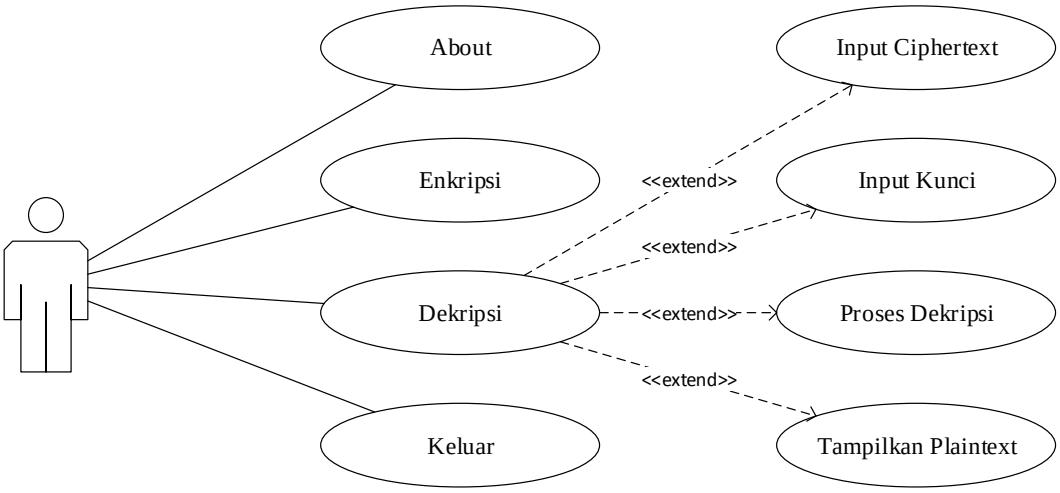


Gambar 3.2 Use Case Diagram Enkripsi

Gambar 3.2 menjelaskan proses enkripsi yang dilakukan. Pengguna dapat memilih menu enkripsi. Dalam menu tersebut, pengguna harus memasukkan plaintext dan kunci agar dapat diproses. Tombol enkripsi akan dapat digunakan untuk memulai proses transposisi baris dan kolom. Hasil akan ditampilkan setelah proses transposisi selesai.

3.4.2. Use Case Diagram Dekripsi

Pada bagian ini akan dijelaskan use case diagram yang digunakan dalam melakukan proses dekripsi transposisi kolom dan baris.

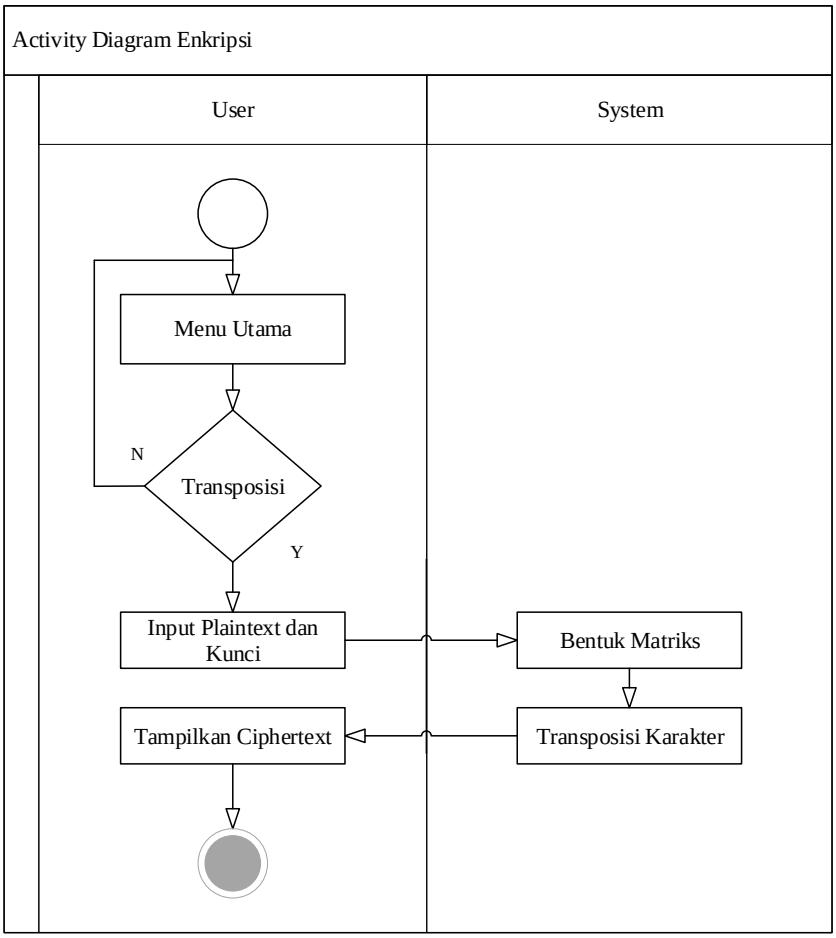


Gambar 3.3 Use Case Diagram Dekripsi

Gambar 3.3 adalah proses dari dekripsi dengan teknik transposisi kolom dan baris. Pengguna harus memasukkan kembali ciphertext yang sudah diperoleh pada proses enkripsi. Pengguna memasukkan kunci untuk menentukan hasil dekripsi. Proses dekripsi yang benar kan menghasilkan hasil yang benar jika menggunakan kunci yang benar juga. Setiap proses dekripsi yang sudah ditentukan sebelumnya akan menghasilkan kembali plaintext yang sama percis dengan plaintext sebelum dilakukan proses enkripsi tersebut. Hasil proses dekripsi akan ditampilkan pada textbox yang tersedia.

3.4.3. Activity Diagram Enkripsi

Pada bagian ini akan dijelaskan activity diagram proses enkripsi.

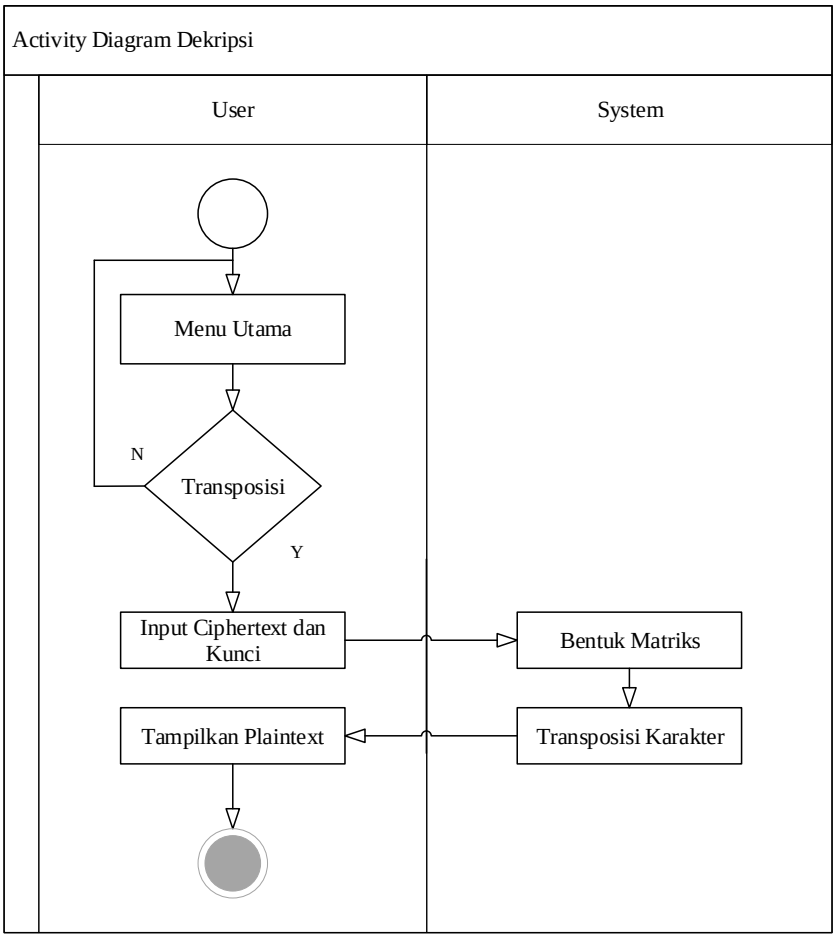


Gambar 3.4 Activity Diagram Enkripsi

Gambar 3.4 adalah hasil activity diagram pada teknik transposisi kolom dan baris untuk melakukan proses enkripsi pesan. Pengguna memilih menu utama terlebih dahulu. Tahap selanjutnya adalah memilih menu transposisi kolom dan baris diikuti memasukkan plaintext dan kunci. Hasil enkripsi akan ditampilkan ketika proses enkripsi selesai.

3.4.4. Activity Diagram Dekripsi

Pada bagian ini akan dijelaskan activity diagram proses dekripsi.

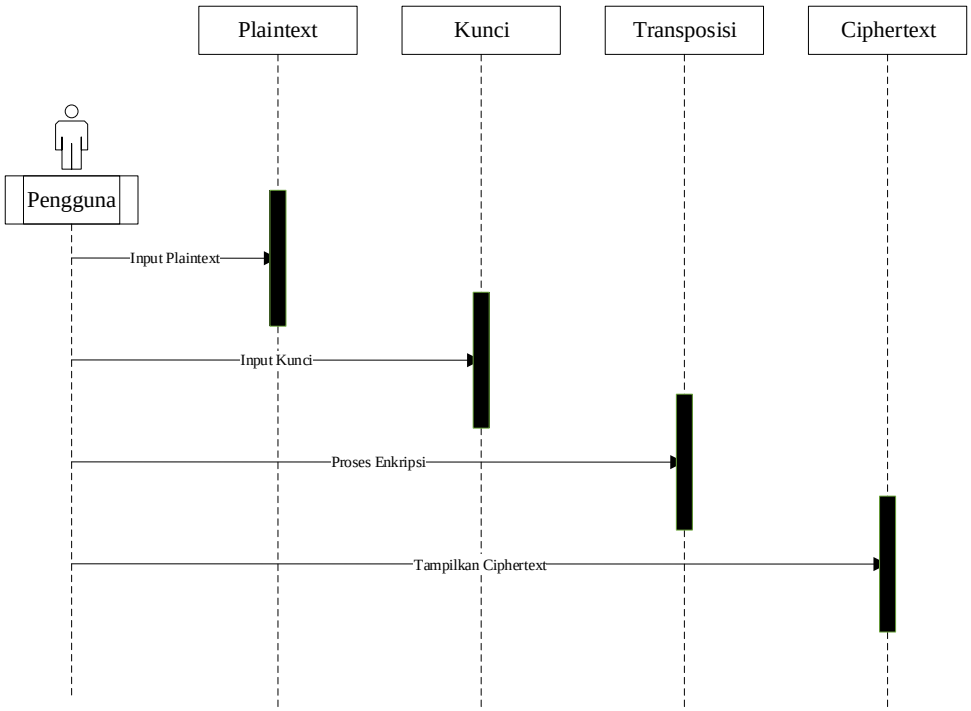


Gambar 3.5 Activity Diagram Dekripsi

Gambar 3.5 adalah activity diagram dari proses dekripsi. Pengguna kembali menggunakan menu utama untuk masuk ke menu transposisi kolom dan baris. Ciphertext dan kunci akan dimasukkan yang kemudian akan diproses untuk mendapatkan plaintext kembali. Hasil plaintext akan ditampilkan setelah proses dekripsi selesai.

3.4.5. Sequence Diagram Enkripsi

Pada bagian ini akan dijelaskan sequence diagram proses enkripsi yang menjelaskan alur dari proses enkripsi dengan teknik transposisi kolom dan baris.

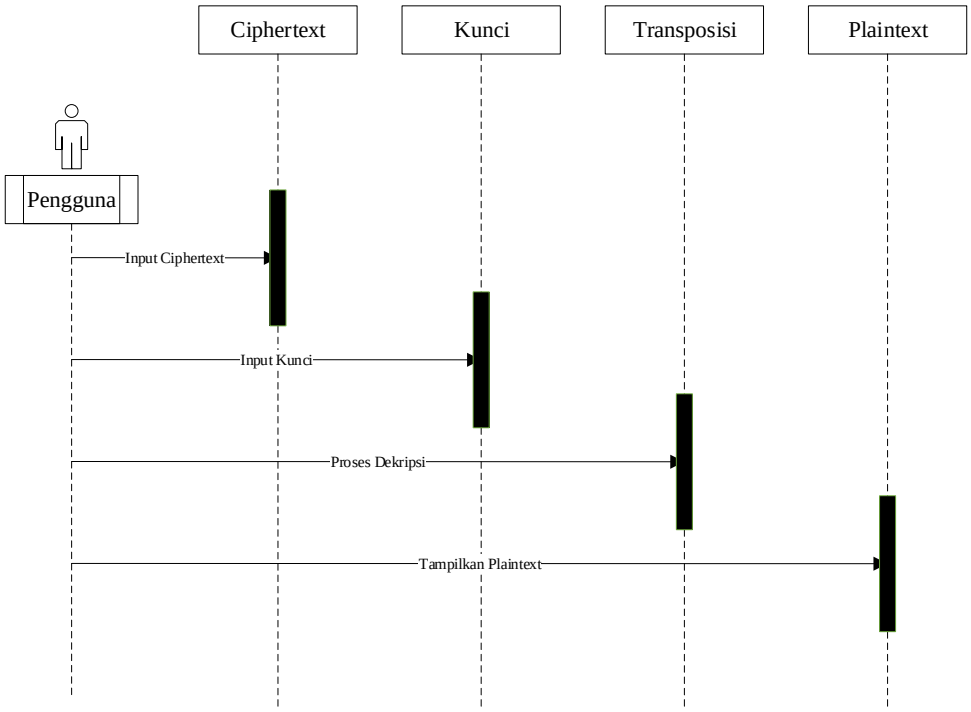


Gambar 3.6 Sequence Diagram Enkripsi

Gambar 3.6 adalah sequence diagram dari proses enkripsi pada teknik transposisi kolom dan baris. Pada sequence diagram enkripsi, ada empat bagian yang akan dilakukan oleh pengguna untuk menyelesaikan proses enkripsi tersebut. Pengguna harus memasukkan plaintext dan kunci. Tahap berikutnya adalah melakukan proses transposisi karakter sehingga menghasilkan ciphertext.

3.4.6. Sequence Diagram Dekripsi

Pada bagian ini akan dijelaskan sequence diagram proses dekripsi yang menjelaskan alur dari proses enkripsi dengan teknik transposisi kolom dan baris.



Gambar 3.7 Sequence Diagram Dekripsi

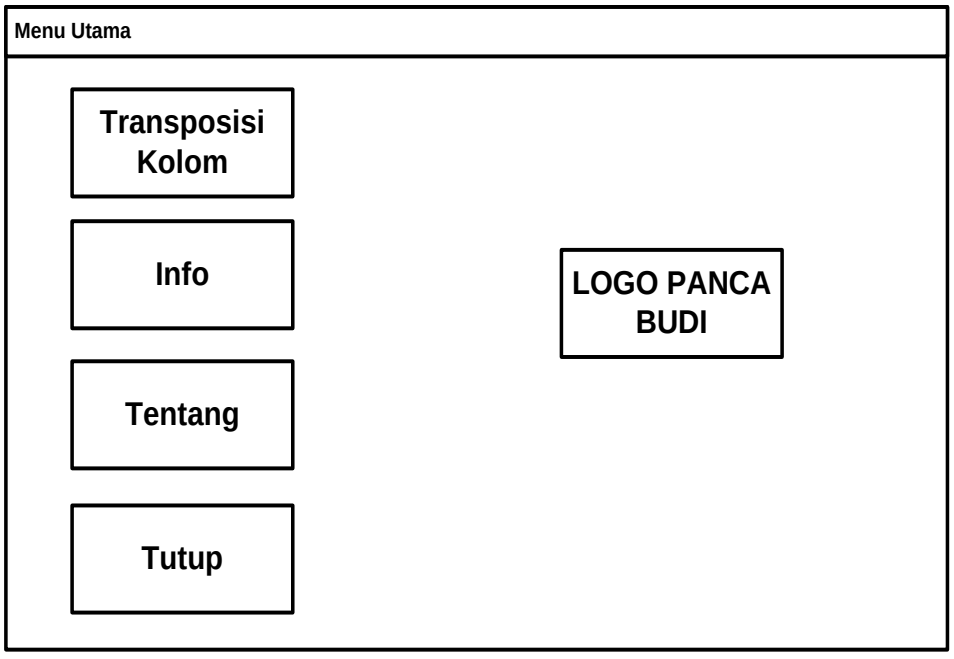
Gambar 3.7 adalah sequence diagram dari proses dekripsi pada teknik transposisi kolom dan baris. Pada sequence diagram dekripsi, ada empat bagian yang akan dilakukan oleh pengguna untuk menyelesaikan proses dekripsi tersebut. Pengguna harus memasukkan ciphertext dan kunci. Tahap berikutnya adalah melakukan proses transposisi karakter sehingga menghasilkan plaintext.

3.5. Perancangan Antarmuka

Perancangan antarmuka bertujuan untuk memberikan bayangan bagaimana program aplikasi terlihat. Perancangan ini memiliki komponen-komponen yang akan ditampilkan kemudian pada program aplikasi yang dibuat.

3.5.1. Rancangan Menu Utama

Menu utama merupakan menu yang menampilkan beberapa menu lainya yang memiliki fungsi dan kegunaan masing-masing. Gambar 3.8 adalah hasil perancangan menu utama yang telah dilakukan.



Gambar 3.8 Rancangan Menu Utama

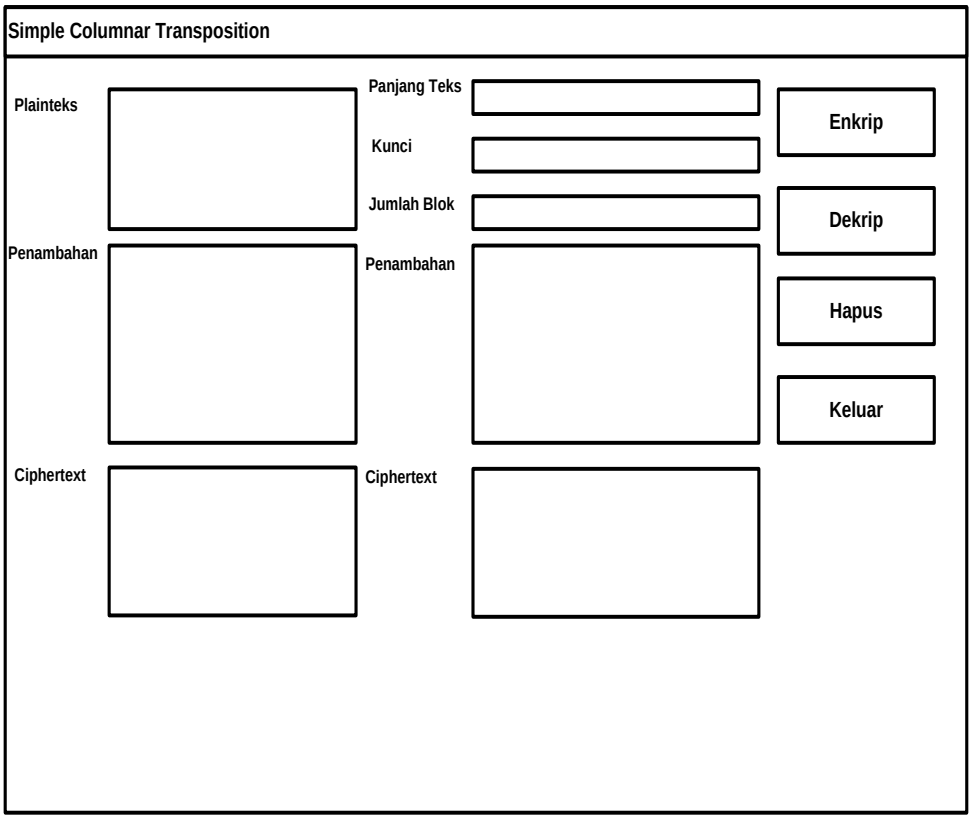
Tampilan ini memiliki berapa sub-menu antara lain:

- Transposisi Kolom

- Info
- Tentang
- Tutup
- Logo

3.5.2. Rancangan Transposisi Kolom dan Baris

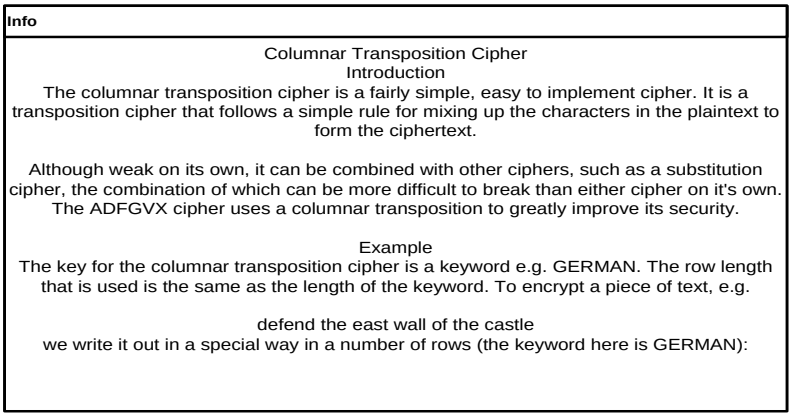
Gambar 3.9 adalah hasil perancangan untuk melakukan proses enkripsi dan dekripsi dengan teknik transposisi kolom. Pada bagian ini terdiri dari beberapa textbox, label dan button yang memiliki peranan masing-masing.



Gambar 3.9 Rancangan Transposisi Kolom dan Baris

3.5.3. Rancangan Info

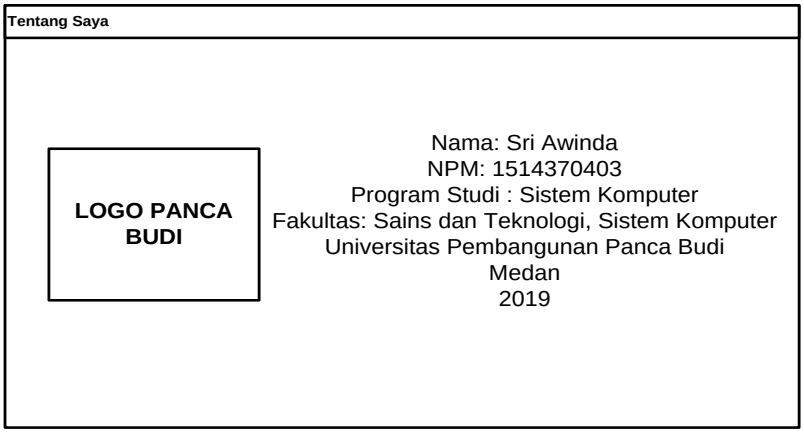
Gambar 3.10 adalah perancangan tampilan info. Tampilan ini akan menjelaskan informasi tentang teknik transposisi kolom dan baris.



Gambar 3.10 Rancangan Info

3.5.4. Rancangan Tentang

Gambar 3.11 adalah rancangan tampilan tentang aplikasi. Tampilan ini menampilkan biodata pengguna.



Gambar 3.11 Rancangan Tentang

BAB IV

HASIL DAN PEMBAHASAN

Implementasi adalah pembuktian hasil program aplikasi yang sudah dilaksanakan. Dalam melakukan implementasi ada beberapa bagian yang harus dipenuhi termasuk kebutuhan perangkat keras dan perangkat lunak.

4.1 Spesifikasi Sistem

Spesifikasi sistem menjelaskan persyaratan yang harus dipenuhi dalam melaksanakan operasional dan kinerja suatu sistem. Spesifikasi diperlukan untuk mengetahui batasan minimal persyaratan sistem yang digunakan. Spesifikasi dapat menentukan kelancaran dari program aplikasi yang dibuat. Spesifikasi pada penelitian ini terdiri dari perangkat keras dan lunak.

4.1.1 Spesifikasi Perangkat Keras

Penerapan teknik transposisi kolom dan baris membutuhkan perangkat keras untuk menciptakan kode program. 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	2048 MB
3	Penyimpanan	500 GB
4	Layar Monitor	14 inch

4.1.2 Spesifikasi Perangkat Lunak

Kebutuhan akan perangkat lunak sangat berarti dalam menciptakan program aplikasi yang lancar dan cepat. Tabel 4.2 adalah spesifikasi 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 2019
5	Pembuatan Diagram	Microsoft Visio 2019
6	Pengetik Naskah	Microsoft Word 2019
7	Browsing	Google Chrome

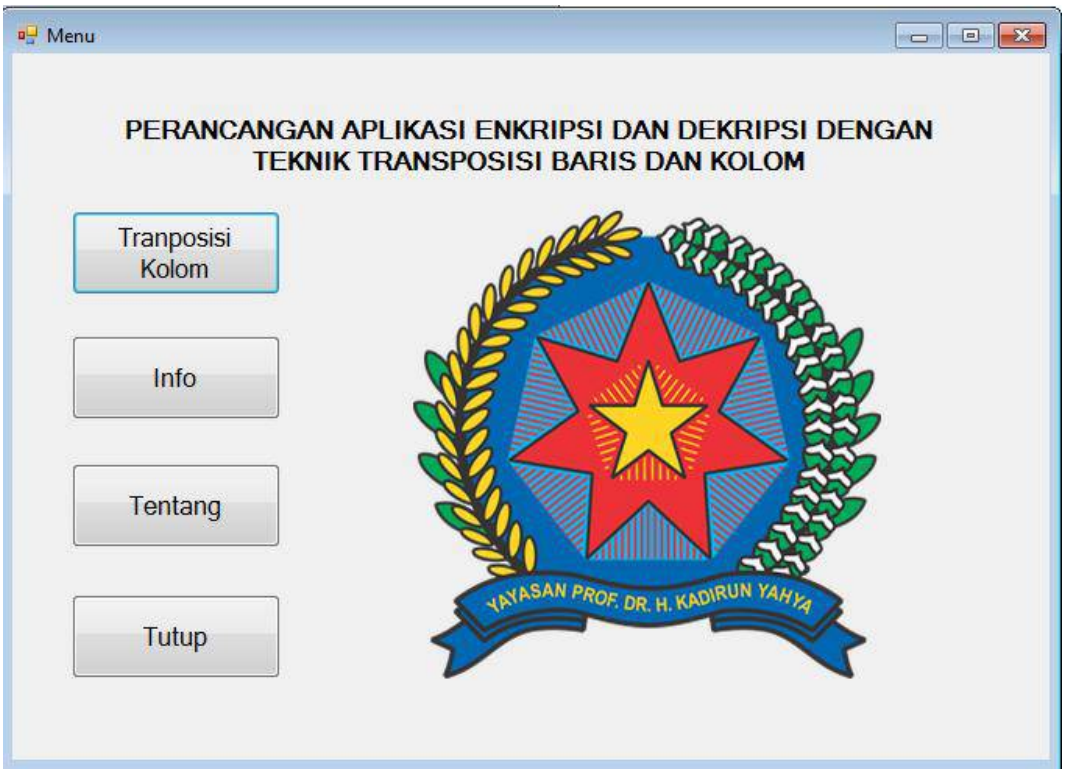
4.2 Tampilan Halaman Antarmuka

Tampilan adalah suatu yang akan muncul dan berinteraksi dengan pengguna. Dalam menyusun tampilan, ada beberapa persyaratan yang harus dilakukan. Tampilan akan dibuat seindah mungkin dan senyaman mungkin agar pengguna aplikasi dapat dengan leluasa menggunakan aplikasi tersebut tanpa mengalami kendala.

4.2.1 Halaman Menu Utama

Halaman menu utama merupakan halaman utama sebuah program aplikasi di mana pengguna akan menemukan halaman ini pertama sekali pada saat program aplikasi mulai dijalankan. Menu utama memiliki beberapa menu lainnya yang

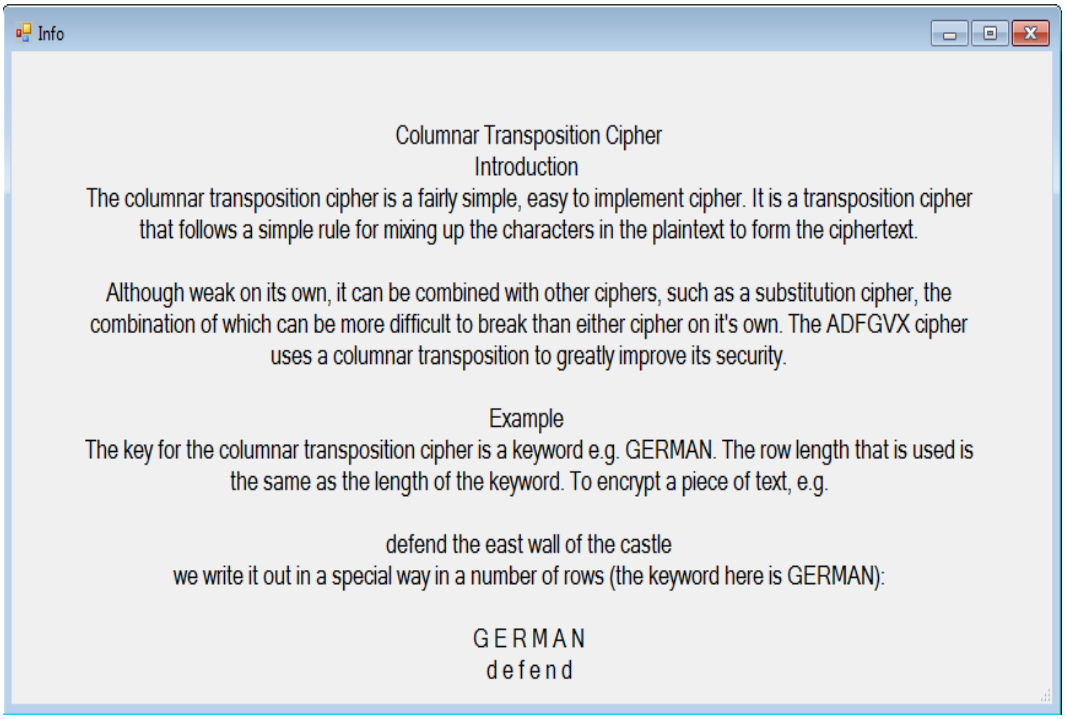
berfungsi untuk menjelaskan teknik transposisi kolom dan baris. Gambar 4.1 adalah hasil tampilan menu utama.



Gambar 4.1 Halaman Menu Utama

4.2.2 Halaman Info

Halaman info adalah halaman yang menjelaskan pengertian dari teknik transposisi kolom dan baris. Pada halaman ini akan dijelaskan secara singkat bagaimana proses kerja dari kriptografi jenis transposisi. Gambar 4.2 adalah hasil tampilan dari halaman info.



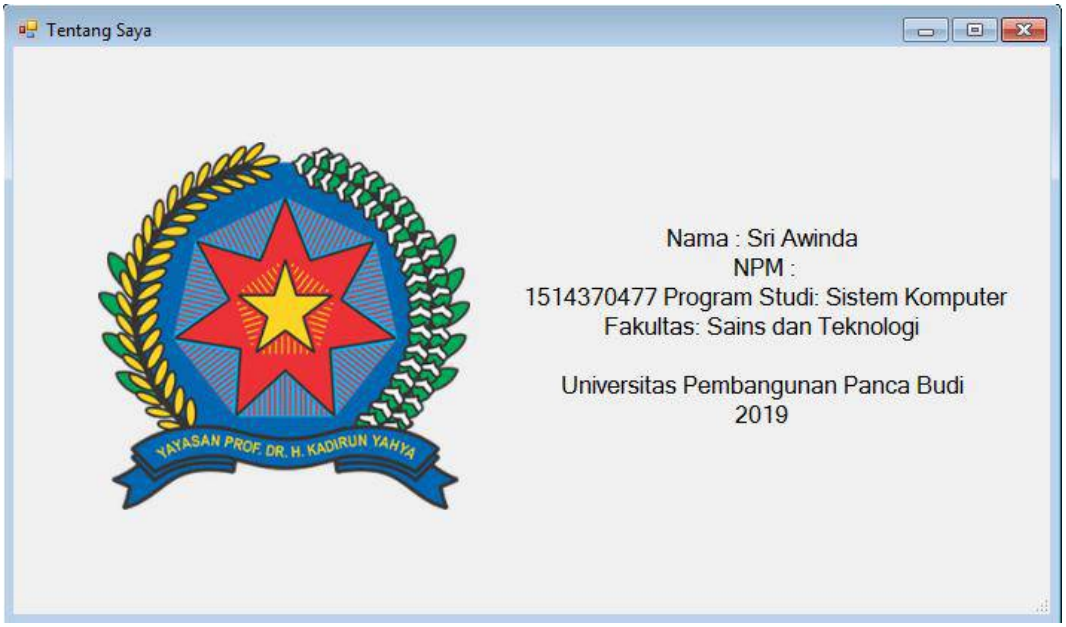
Gambar 4.2 Halaman Info

4.2.3 Halaman Tentang

Halaman Tentang menampilkan biodata singkat penulis sebagai penulis penelitian ini. Ada beberapa komponen yang ditampilkan pada halamam ini antara lain:

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

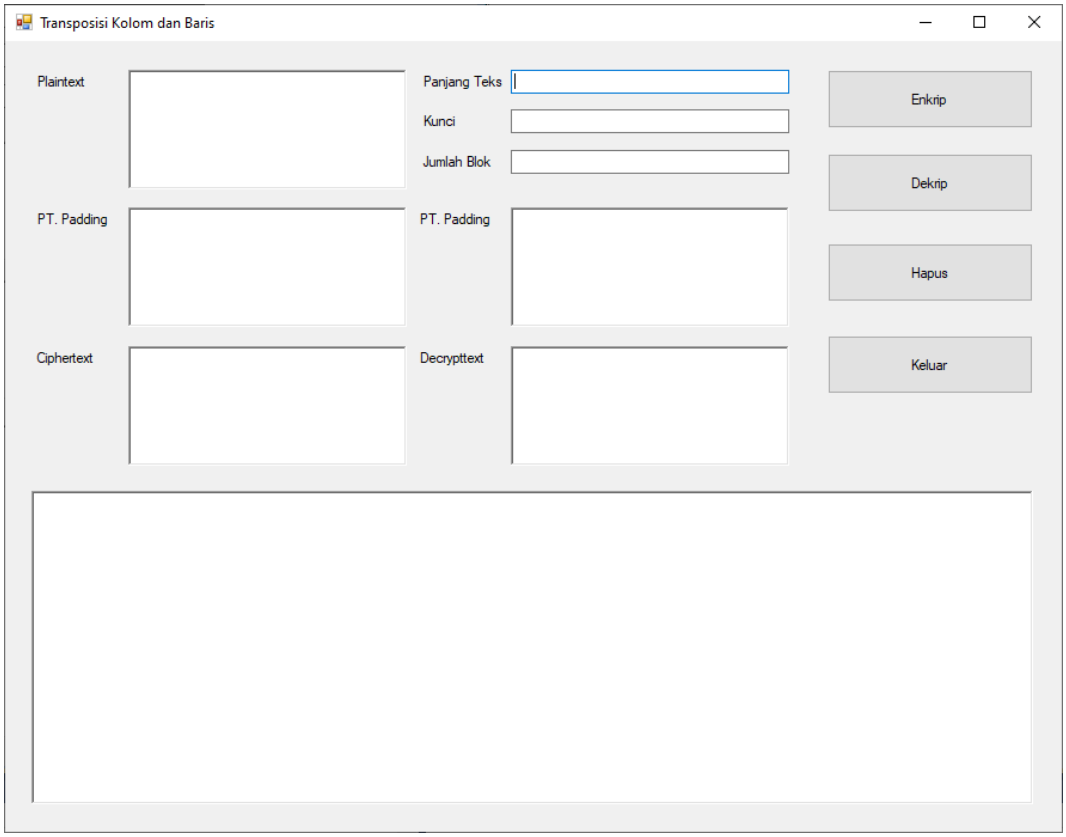
Form ini memiliki sebuah objek label dan picturebox untuk menampilkan logo universitas. Gambar 4.3 adalah tampilan dari halaman Tentang.



Gambar 4.3 Halaman Tentang

4.2.4 Halaman Transposisi Kolom dan Baris

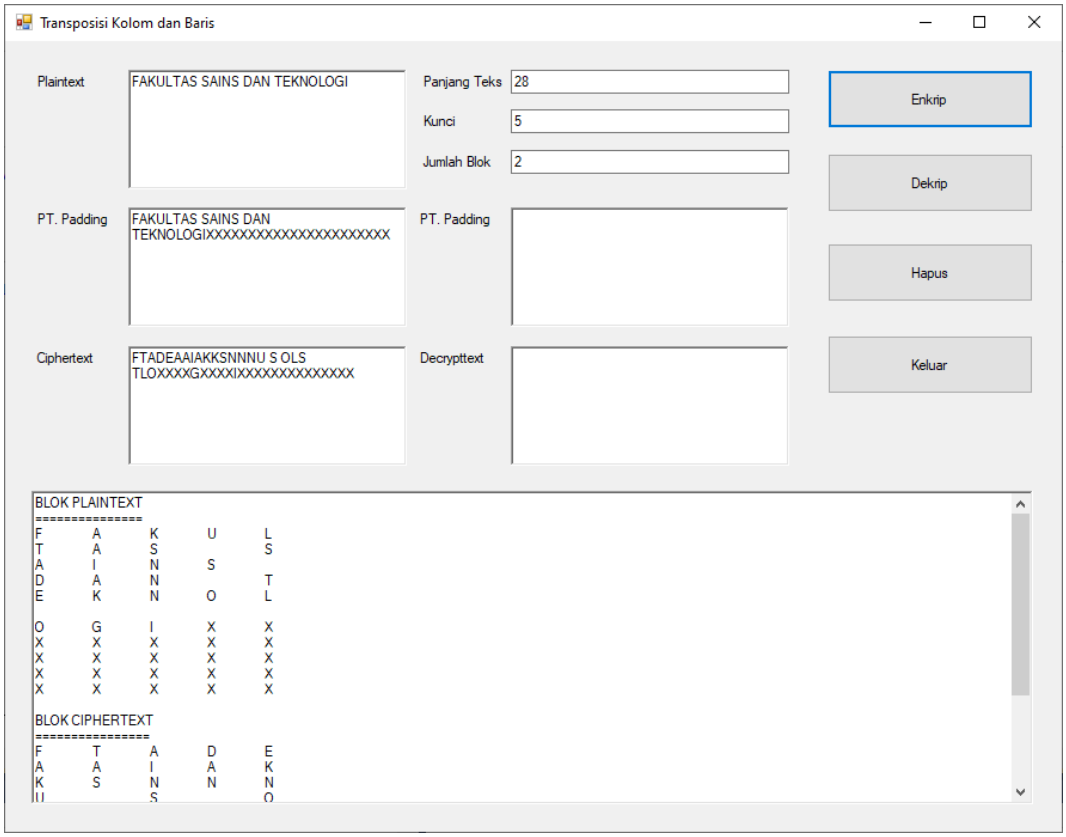
Halaman ini adalah bagian terpenting dari program aplikasi. Halaman ini berupa proses transposisi plaintext ke ciphertext dengan menggunakan kolom dan baris sebagai kunci enkripsi. Pada halaman ini juga ditampilkan textbox yang berfungsi untuk menampilkan plaintext setelah dilakukan pertambahan (*padding*) karakter. Proses pertambahan karakter dilakukan jika karakter plaintext tidak mencukupi hingga K^2. Textbox ciphertext menampung hasil enkripsi yang dilakukan dengan teknik transposisi kolom dan baris. Gambar 4.4 adalah hasil tampilan dari halaman transposisi kolom dan baris.



Gambar 4.4 Halaman Transposisi Kolom dan Baris

4.2.5 Hasil Enkripsi

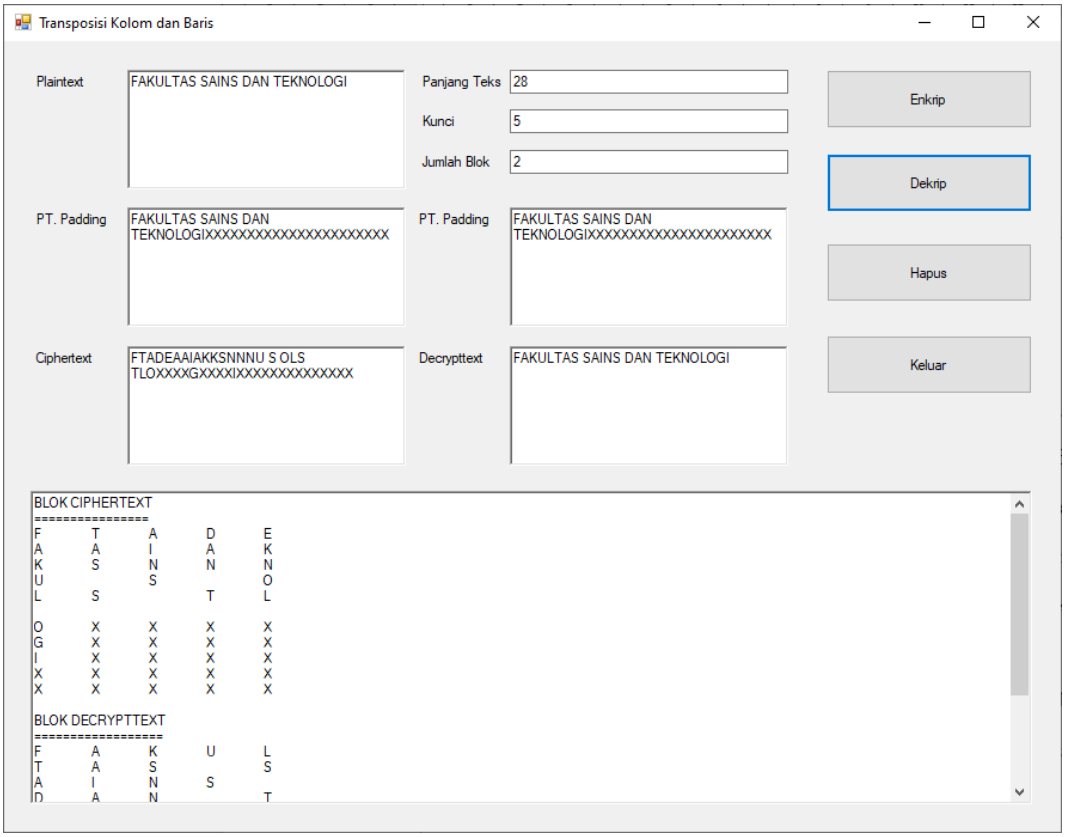
Hasil enkripsi akan ditampilkan menggunakan form yang sama. Enkripsi dilakukan dengan cara memasukkan pesan pada textbox plaintext. Kunci berupa lebar kolom dan baris yang diinputkan pada textbox Kunci. Dalam melakukan proses enkripsi, hanya dua buah textbox yang menjadi input dalam proses ini. Tombol enkrip berfungsi untuk melakukan proses enkripsi. Riwayat cara kerja metode ini akan ditampilkan secara rinci pada textbox log yang berada paling bawah. Gambar 4.5 adalah tampilan dari hasil perhitungan proses enkripsi dari teknik transposisi kolom dan baris.



Gambar 4.5 Hasil tampilan enkripsi

4.2.6 Hasil Dekripsi

Setelah proses enkripsi, ciphertext dihasilkan dan ciphertext ini tidak dapat difahami lagi. Posisi karakter pada plaintext telah berganti dan teracak sehingga hasilnya dapat dilihat pada textbox ciphertext. Dalam mengembalikan ciphertext ke bentuk plaintext. Setiap karakter pada ciphertext akan disusun kembali seperti menyusun plaintext ke dalam bentuk matriks dengan lebar kolom dan baris sesuai dengan kunci yang diinputkan sebelumnya. Tombol dekrip berfungsi untuk menyusun ulang posisi ciphertext yang teracak tersebut hingga menghasilkan plaintext. Gambar 4. 6 adalah tampilan dari hasil perhitungan proses dekripsi dengan teknik transposisi kolom dan baris.



Gambar 4.6 Hasil tampilan dekripsi

4.3 Pembahasan Perhitungan

Pembahasan perhitungan berfungsi untuk menguji hasil yang dikeluarkan oleh program aplikasi apakah sudah sesuai dengan perhitungan sebenarnya. Dengan ini, diperlukan perhitungan manual yang akan membuktikan kebenaran dari teknik transposisi kolom dan baris tersebut. Proses yang dilakukan terdiri dari dua proses, yaitu proses enkripsi dan proses dekripsi. Penjelasan dan perhitungan berikut ini adalah langkah lengkap proses enkripsi dan dekripsi pada teknik transposisi kolom dan baris.

Hasil proses enkripsi dengan teknik transposisi kolom dan baris dapat dilihat pada perhitungan berikut ini.

Plaintext : FAKULTAS SAINS DAN TEKNOLOGI
Panjang Teks : 28
Kunci : 5
Jumlah Blok : 2
Ciphertext :
FTADEAAIAKKSNNNU S OLS TLOXXXXGXXXXIXXXXXXXXXXXXXX

Penjelasan:
BLOK PLAINTEXT
==========

F	A	K	U	L
T	A	S		S
A	I	N	S	
D	A	N		T
E	K	N	O	L
O	G	I	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X

BLOK CIPHERTEXT
==========

F	T	A	D	E
A	A	I	A	K
K	S	N	N	N
U		S		O

L	S		T	L
O	X	X	X	X
G	X	X	X	X
I	X	X	X	X
X	X	X	X	X
X	X	X	X	X

Hasil proses dekripsi dengan teknik transposisi kolom dan baris dapat dilihat pada perhitungan berikut ini.

Ciphertext :
FTADEAAIAKKSNNNU S OLS TLOXXXXGXXXXIXXXXXXXXXXXXXX
Panjang Teks : 28
Kunci : 5
Jumlah Blok : 2

Plaintext : FAKULTAS SAINS DAN TEKNOLOGI
Penjelasan:
BLOK CIPHERTEXT
==========

F	T	A	D	E
A	A	I	A	K
K	S	N	N	N
U		S		O
L	S		T	L
O	X	X	X	X
G	X	X	X	X
I	X	X	X	X
X	X	X	X	X
X	X	X	X	X

BLOK DECRYPTTEXT

==========

F	A	K	U	L
T	A	S		S
A	I	N	S	
D	A	N		T
E	K	N	O	L
O	G	I	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X

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. Teknik transposisi kolom dan baris bekerja dengan cara melakukan pertukaran karakter dari kolom ke baris.
2. Teknik ini memiliki kunci yang merupakan lebar kolom dan baris tersebut.
3. Teknik transposisi kolom dan baris tidak mengganti karakter plaintext dengan karakter lain atau simbol melainkan hanya mengacak posisi karakter plaintext.

5.2 Saran

Penelitian juga masih mengalami kekurangan. Ada beberapa saran yang dapat penulis paparkan untuk memperbaiki penelitian ini. Adapun saran tersebut adalah antara lain:

1. Sebaiknya kunci tidak hanya menggunakan angka, tetapi dapat menggunakan huruf juga.
2. Sebaiknya lebar kolom dan baris dapat bervariasi sehingga meningkatkan keamanan.

DAFTAR PUSTAKA

Amin, M. M. (2016). Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks. *Jurnal Pseudocode*, *3*(2).

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

Fachri, barany, agus perdana windarto, and ikhsan parinduri. "penerapan backpropagation dan analisis sensitivitas pada prediksi indikator terpenting perusahaan listrik." jepin (jurnal edukasi dan penelitian informatika) 5.2 (2019): 202-208.

Fachri, b., windarto, a. P., & parinduri, i. (2019). Penerapan backpropagation dan analisis sensitivitas pada prediksi indikator terpenting perusahaan listrik. Jepin (jurnal edukasi dan penelitian informatika), 5(2), 202-208.

Fachri, barany; windarto, agus perdana; parinduri, ikhsan. Penerapan backpropagation dan analisis sensitivitas pada prediksi indikator terpenting perusahaan listrik. Jepin (jurnal edukasi dan penelitian informatika), 2019, 5.2: 202-208.

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

Hamdi, nurul. "model penyiraman otomatis pada tanaman cabe rawit berbasis programmable logic control." jurnal ilmiah core it: community research information technology 7.2 (2019).

Hendini., A. (2016). Pemodelan UML Sistem Informasi Monitoring Penjualan Dan Stok Barang. *Jurnal Khatulistiwa Informatika*, *4*(2), 107–116. https://doi.org/10.31294/jki.v4i2.1262.g1027

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

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

Permana, aminuddin indra. "kombinasi algoritma kriptografi one time pad dengan generate random keys dan vigenere cipher dengan kunci em2b." (2019).

Putra, randi rian. "sistem informasi web pariwisata hutan mangrove di kelurahan belawan sicanang kecamatan medan belawan sebagai media promosi." jurnal ilmiah core it: community research information technology 7.2 (2019).

Putra, randi rian, et al. "decision support system in selecting additional employees using multi-factor evaluation process method." (2019).

Putra, randi rian. "implementasi metode backpropagation jaringan saraf tiruan dalam memprediksi pola pengunjung terhadap transaksi." jurti (jurnal teknologi informasi) 3.1 (2019): 16-20.

Putri, G. G., Setyorini, W., & Rahayani, R. D. (2018). Analisis Kriptografi Simetris AES dan Kriptografi Asimetris RSA pada Enkripsi Citra Digital. *ETHOS (Jurnal Penelitian Dan Pengabdian)*, *6*(2), 197–207. https://doi.org/10.29313/ethos.v6i2.2909

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

Saputra, muhammad juanda, and nurul hamdi. "rancang bangun aplikasi sejarah kebudayaan aceh berbasis android studi kasus dinas kebudayaan dan pariwisata aceh." journal of informatics and computer science 5.2 (2019): 147-157

Sidik, a. P., efendi, s., & suherman, s. (2019, june). Improving one-time pad algorithm on shamir's three-pass protocol scheme by using rsa and elgamal algorithms. In journal of physics: conference series (vol. 1235, no. 1, p. 012007). Iop publishing.

Sitepu, n. B., zarlis, m., efendi, s., & dhany, h. W. (2019, august). Analysis of decision tree and smooth support vector machine methods on data mining. In journal of physics: conference series (vol. 1255, no. 1, p. 012067). Iop publishing.

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

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

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

Tasril, v., wijaya, r. F., & widya, r. (2019). Aplikasi pintar belajar bimbingan dan konseling untuk siswa sma berbasis macromedia flash. Jurnal informasi komputer logika, 1(3).

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

Wibowo, H. R. (2014). *Visual Basic Database*. Yogyakarta: Jubilee Enterprise.

Yakub. (2012). *Pengantar Sistem Informasi*. Yogyakarta: Graha Ilmu.

Zwass, V. (2019). Information System. Retrieved November 20, 2019, from https://www.britannica.com/topic/information-system