



**SIMULASI PENGAMANAN TEXT DALAM PROSES
ENKRIPSI DAN DESKRIPSI METODE VIGENERE CIPHER**

*Dibuat dan Disajikan Untuk Memenuhi Persyaratan Ujian Akhir
Memperoleh Gelar Sarjana Pada Fakultas Sains dan Teknologi
Universitas Pembangunan Panca Budi Medan*

SKRIPSI

OLEH

NAMA : FAJAR AZMI SYAHPUTRA
N.P.M : 1414370374
PROGRAM STUDI : SISTEM KOMPUTER

**FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2019**

LEMBAR PENGESAIAN
SIMULASI PENGAMANAN TEXT DALAM PROSES
ENKRIPSI DAN DESKRIPSI METODE VIGENERE CIPHER

SKRIPSI

OLEH

NAMA : FAJAR AZMI SYAHPUTRA
NPM : 1414370374
PROGRAM STUDI : ILMU KOMPUTER

Skripsi telah disetujui oleh Dosen Pembimbing Skripsi pada
tanggal.....:

Dosen Pembimbing I



Andriah P. U. Sihaban, S.Kom, M.Kom, Ph.D

Dosen Pembimbing II



Dian Kurnia, S.Kom, M.Kom

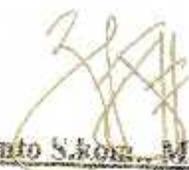
Mengetahui :

Dekan Fakultas Sains dan Teknologi



Sri Shindi Indira, ST., M.sc.

Ketua Program Studi



Eko Hariyanto S.Kom., M.Kom

SURAT PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : FAJAR AZMI SYAHPUTRA
Mata No : 1414370374
Bidang : SISTEM KOMPUTER
Konsentrasi : KEAMANAN JARINGAN KOMPUTER
Judul Skripsi : SIMULASI PENGAMANAN TEXS DALAM PROSES ENKRIPSI DAN DESKRIPSI METODE VIGENERE CIPHER

Yang ini menyatakan bahwa :

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

Dengan demikian pernyataan ini saya perbuat dengan sebenar-benarnya, terima kasih

Medan, 14 November 2019

Yang membuat pernyataan



FAJAR AZMI SYAHPUTRA



UNIVERSITAS PEMBANGUNAN PANCA BUDI FAKULTAS SAINS & TEKNOLOGI

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

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

PERMOHONAN JUDUL TESIS / SKRIPSI / TUGAS AKHIR*

Saya yang bertanda tangan di bawah ini :

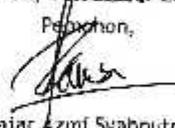
Nama Lengkap : FAJAR AZMI SYAHPUTRA
 Tempat/Tgl. Lahir : Medan, 30-september-1996 / 30 September 1996
 Nomor Pokok Mahasiswa : 1414370374
 Program Studi : Sistem Komputer
 Konsentrasi : Keamanan Jaringan Komputer
 Jumlah Kredit yang telah dicapai : 143 SKS, IPK 3.09
 Nomor Hp : 087867062772
 Dengan ini mengajukan judul sesuai bidang ilmu sebagai berikut :

No.	Judul
1.	Simulasi Pengamanan Text dalam Proses Enkripsi dan Deskripsi Metode Vigenere Cipher.

Catatan : Diisi Oleh Dosen Jika Ada Perubahan Judul

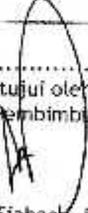
*Coret Yang Tidak Perlu


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

07 November 2018
 Medan, ~~30 September~~ 2019
 Pemohon,

 (Fajar Azmi Syahputra)

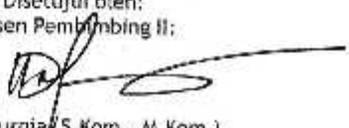
Tanggal :
 Disahkan oleh
 Dekan

 (Sri Hartono, S.T., M.Sc.)

Tanggal :
 Disetujui oleh:
 Dosen Pembimbing I :

 (Andyah Putera Utama Siahaan, S.Kom., M.Kom., Ph.D.)

Tanggal :
 Disetujui oleh:
 Ka. Prodi Sistem Komputer

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

Tanggal :
 Disetujui oleh:
 Dosen Pembimbing II:

 (Dian Kurnia, S.Kom., M.Kom.)

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



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

Universitas : Universitas Pembangunan Panca Budi
 Fakultas : SAINS & TEKNOLOGI
 Dosen Pembimbing I : Anisya Putri Utami Sihuman, S.Kom, M.Kom
 Dosen Pembimbing II : Dian Kusuma, S.Kom, M.Kom
 Nama Mahasiswa : FAJAR AZMI SYAHPUTRA
 Jurusan/Program Studi : Sistem Komputer
 Nomor Pokok Mahasiswa : 1414370374
 Jenjang Pendidikan :
 Judul Tugas Akhir/Skripsi : Simulasi Pengamanan Text dalam Proses Enkripsi dan Deskripsi

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
15/1	Revisi Bab I		
12/2	Revisi Bab II		
20/2	Revisi Bab II, III		
1/3	Revisi Bab III, IV		
5/3	Revisi Bab IV, V		
14/3	Revisi Summary		
16/10	Revisi Sider		
11/11	Revisi Jilid		

Medan, 20 Februari 2019
 Diketahui/Disetujui oleh :
 Dekan,

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



UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI

Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571
 website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id
 Medan - Indonesia

Universitas : Universitas Pembangunan Panca Budi
 Fakultas : SAINS & TEKNOLOGI
 Dosen Pembimbing I : Andyah Kusuma Utami Sihana, S.kom, M.kom
 Dosen Pembimbing II : Dian Kurnia S.kom, M.kom
 Nama Mahasiswa : FAJAR AZMI SYAHPUTRA
 Jurusan/Program Studi : Sistem Komputer
 Nomor Pokok Mahasiswa : 1414370374
 Jenjang Pendidikan : STRATA satu (S1)
 Judul Tugas Akhir/Skripsi : Simulasi Pengamanan Teks dalam Proses Enkripsi dan Deskripsi

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
30/03-2019	Berkas latar belakang masalah kegiatan kutipan dengan daftar pustaka	h	
27/04-2019	berita perbandingan penelitian sebelumnya dengan sekarang perbaikan bab 1 dan 2 g dan akan aplikasi mendeley untuk sitasi, lanjut bab 3	h	
16/07-2019	Ace bab 1, 2, 3, lanjut bab 4,	h	
18/07-2019	Ace bab 4 lanjut bab 5	h	
20/07-2019	perbaikan daftar pustaka Ace bab 5	h	
27/07-2019	lengkapinya berkas skripsi ke-4 Ace bab 1, 2, 3, 4, 5,	h	Ace skripsi no 2
21/10-2019	perbaikan skripsi dengan panduan skripsi	h	
23/10-2019	lengkapinya berkas sidang tugas akhir	h	Ace sidang
16/11-2019	Ace judul	h	

Medan, 22 Maret 2019
 Diketahui/Dijetujui oleh :
 Dekan,

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

Telah Diperiksa oleh LPMU
dengan Plagiarisme... 51... %

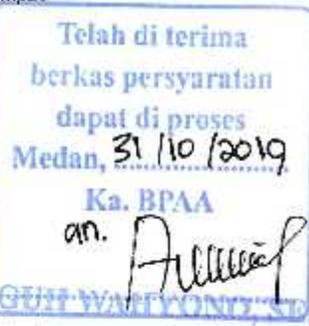
31 OKTOBER 2019

FM-BPAA-2012-041

Hal : Permohonan Meja Hijau



Medan, 21 Oktober 2019
Kepada Yth : Bapak/Ibu Dekan
Fakultas SAINS & TEKNOLOGI
UNPAB Medan
Di -
Tempat



Dengan hormat, saya yang bertanda tangan di bawah ini :

Nama : FAJAR AZMI SYAHPUTRA
Tempat/Tgl. Lahir : Medan / 30 September 1996
Nama Orang Tua : SUKAPRI
N. P. M : 1414370374
Fakultas : SAINS & TEKNOLOGI
Program Studi : Sistem Komputer
No. HP : 087867062772
Alamat : Jl. Cinta Karya Gg. Utama Kel. Satri Rejo Kec. Medan Polonia

Datang bermohon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul Stimulasi Pengamanan Text dalam Proses Enkripsi dan Deskripsi Metode Vigenere Cipher. Selanjutnya saya menyatakan :

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

1. [102] Ujian Meja Hijau	: Rp.	250.000	
2. [170] Administrasi Wisuda	: Rp.	1.500.000	
3. [202] Bebas Pustaka	: Rp.	100.000	
4. [221] Bebas LAB	: Rp.	5.000	
Total Biaya	: Rp.	2.000.000	1.855.000
5. Disk. 10% (dari 1.855.000)	: Rp.	185.500	
	Rp.	5.905.000	

31 OKTOBER
2019 (Fm)

Ukuran Toga : L



Hormat saya
FAJAR AZMI SYAHPUTRA
1414370374

Catatan :

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





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

KARTU BEBAS PRAKTIKUM

Yang bertanda tangan di bawah ini Ka. Laboratorium Komputer dengan ini menerangkan bahwa

Nama : FAJAR AZMI SYAHPUTRA
N.P.M. : 1414370374
Tingkat/Semester : Akhir
Fakultas : SAINS & TEKNOLOGI
Jurusan/Prodi : Sistem Komputer

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

Medan, 21 Oktober 2019
Ka. Laboratorium



Eachrid Widly S. Kom

ABSTRAK

FAJAR AZMI SYAHPUTRA

SIMULASI PENGAMANAN TEXT DALAM PROSES ENKRIPSI DAN DESKRIPSI METODE VIGENERE CIPHER

2019

Kriptografi merupakan salah satu metode mengamankan data yang dapat digunakan untuk menjaga kerahasiaan data, keaslian data serta keaslian pengirim. Metode ini bertujuan agar informasi yang bersifat rahasia yang dikirim melalui telekomunikasi umum seperti LAN atau Internet. Kriptografi biasanya dalam bentuk enkripsi dan Deskripsi. Untuk menyembunyikan tulisan, biasanya menggunakan algoritma. Algoritma yang dipakai dalam aplikasi ini adalah Algoritma Vigenere Cipher. Dalam hal ini, penulis berkeinginan mengangkat topik enkripsi dan deskripsi menjadi sebuah penulisan ilmiah skripsi dengan menggunakan visual studio yang berkembang saat ini. Diharapkan dengan adanya aplikasi ini, mahasiswa serta dosen dapat melakukan uji coba enkripsi menggunakan algoritma Vigenere Cipher.

Kata Kunci: Kriptografi, Vigenere Cipher

DAFTAR ISI

Halaman

COVER

LEMBAR PENGESAHAN

ABSTRAK

KATA PENGANTAR..... i

DAFTAR ISI ii

DAFTAR GAMBAR..... iv

DAFTAR TABEL..... vi

BAB I PENDAHULUAN..... 1

1.1 Latar Belakang 1

1.2 Rumusan Masalah 3

1.3 Batasan Masalah 3

1.4 Tujuan Penelitian 4

1.5 Manfaat Penelitian 4

BAB II LANDASAN TEORI..... 5

2.1 Keamanan data..... 5

2.2 Kriptografi 6

2.3 Kriptografi Vigenere Cipher..... 7

2.4 Enkripsi..... 12

2.5 Kriptografi Klasik..... 13

2.6 One Time Pad (OTP)..... 13

2.7	Algoritma.....	14
2.8	Unified Modeling Language (UML)	17
2.9	Pengertian Informasi	24
2.10	Pengertian Visual Studio.....	25
2.11	Tabel ASCII	28
2.12	Peneliti-Peneliti Sebelumnya	37
BAB III	METODE PENELITIAN.....	41
3.1	Tahapan peniliitian	41
3.2	Metode Pengumpulan Data.....	42
3.3	Analisis Permasalahan Yang Berjalan.....	42
3.4	Analisa Kelemahan Yang Berjalan.....	43
3.5	Solusi Pemecahan Masalah.....	43
3.6	Analisa Kebutuhan Sistem.....	45
3.7	Analisa Proses Sistem Yang Berjalan.....	46
3.8	Flowchart Sistem	49
3.9	Flowchart Vigenere Cipher	49
3.10	Perancangan Antarmuka	50
BAB IV	HASIL DAN PEMBAHASAN.....	56
4.1	Implementasi Sistem.....	56
4.2.	Pengujian Sistem	56
4.3.	Validas Sistem.....	64

BAB V PENUTUP	69
5.1 Kesimpulan.....	69
5.2 Saran	69

DAFTAR ISI

BIOGRAFI PENULIS

LAMPIRAN

DAFTAR GAMBAR

Judul	Hal
Proses Enkripsi dan Deskripsi	13
Contoh Use Case Diagram	16
Contoh Activity Diagram	20
Contoh Sequence Diagram.....	22
Tampilan Toolbox	27
Tahapan Penelitian	41
Skema Pengiriman Pesan	43
Flowchart Vigenere Cipher.....	50
Rancangan Halaman Judul	51
Rancangan Halaman Menu Utama.....	52
Rancangann Halaman Materi.....	53
Rancangan Halaman Enkripsi.....	54
Rancangan Halaman Deskripsi	54
Tampilan Awal/Home	57
Tampilan Halaman Judul.....	58
Tampilan Materi.....	58
Tampilan Aturan Penggunaan Aplikasi	59

4.5. Tampilan Halaman Utama Algoritma Vigenere	60
4.6. Tombol Pencarian Data	60
4.7. Tampilan Memilih File.....	61
4.8. Tampilan Tombol Baca File	61
4.9. Tampilan Enkripsi Dengan Algoritma Vigenere	62
4.10. Tampilan Deskripsi Vigenere Cipher.....	63
4.11. Tampilan Tombol Tutup.....	63

DAFTAR TABEL

No	Judul	Hal
2.1.	Tabel Alphabet dan Konversinya.....	12
2.2.	Tabel Enkripsi.....	12
2.3.	Simbol Use Case Diagram.....	18
2.4.	Simbol Activity Diagram	20
2.5.	Sequence Diagram	21
2.6.	Simbol Class Diagram.....	22
2.7.	Tolboox Visual Studio.....	27
3.1.	Tabel Perencanaan Rancangan	44

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada zaman sekarang ini, menjaga kerahasiaan informasi merupakan hal yang sangat penting. Sebagai contoh bagi perusahaan besar, penyimpanan dokumen serta data–data penting adalah kewajiban yang mesti dilakukan. Penyalahgunaan data–data rahasia perusahaan tersebut oleh pihak tertentu tentunya bisa saja menimbulkan kerugian yang sangat besar pada perusahaan tersebut. Contoh lainnya adalah komunikasi suara lewat jaringan internet. Kemungkinan pihak lain untuk mengetahui informasi yang disampaikan lewat komunikasi elektronik tersebut sangat besar mengingat belum adanya sekuritas khusus terhadap aplikasi tersebut. Karenanya, salah satu alternatif yang dapat digunakan untuk menjaga kerahasiaan informasi tersebut adalah dengan menyamakannya menjadi bentuk tersandi yang tidak bermakna. Hal tersebut dapat dilakukan dalam kriptografi.

Kriptografi merupakan salah satu metode pengamanan data yang dapat digunakan untuk menjaga kerahasiaan data, keaslian data serta keaslian pengirim. Metode ini bertujuan agar informasi yang bersifat rahasia yang dikirim melalui telekomunikasi umum seperti LAN atau internet, tidak dapat diketahui atau dimanfaatkan oleh orang yang tidak berkepentingan atau yang tidak berhak menerimanya. Kriptografi biasanya dalam bentuk enkripsi. Proses enkripsi merupakan proses untuk meng-*encode* dalam bentuk yang hanya

dapat dibaca oleh sistem yang mempunyai kunci untuk membaca data tersebut. Proses enkripsi dapat dengan menggunakan *software* atau *hardware*. (Sitinjak, 2015).

Berdasarkan penelitian (Pradipta, 2016). Vigenere cipher ini menggunakan teknik substitusi dalam pengenkripsian pesannya dimana setiap karakter plainteks pada pesan akan dienkripsi mejadi karakter lain pada cipherteks berdasarkan kunci yang digunakan. Selanjutnya adalah metode penyandian transposisi adalah metode penyandian dengan cara mengubah letak dari teks pesan yang akan disandikan. Dan untuk membaca pesan aslinya kembali, cukup dengan mengembalikan letak dari pesan tersebut berdasarkan kunci dan algoritma pergeseran huruf yang telah disepakati. Pada penelitian ini dilakukan pengamanan data yang dikirimkan melalui jaringan ke server yang rentan untuk di serang hacker. Metode enkripsi yang diterapkan adalah vigenere cipher yang dikombinasikan dengan metode transposisi untuk mendapatkan data yang sudah diacak atau disebut dengan cipher text yang menghasilkan pengacakan data yang lebih kompleks dan sulit untuk di pecahkan pada saat pesan chatting memasuki server.

Kelebihan dari pada penelitian ini adalah Implementasi program enkripsi data dengan metode vigenere dan transposisi dapat meningkatkan keamanan pengiriman pesan ke server dan Kombinasi dengan metode transposisi membuat metode vigenere menjadi lebih sulit untuk di pecahkan karena cipher text yang dihasilkan di awal akan dilakukan pengenkripsian kembali dengan merubah letak posisi karakter menggunakan cara transposisi. Kenyataan dalam proses

pengamanan data dengan metode kriptografi sering kali dibutuhkan waktu yang relatif lama dibandingkan tanpa menggunakan metode kriptografi. Oleh karena itu, diusahakan membuat sistem yang sandi lebih cepat dalam kriptografi tanpa mengabaikan kaidah kerahasiaan yang ingin dicapai.

Berdasarkan berbagai pertimbangan tersebut maka dalam penyusunan skripsi ini, penulis memilih judul “Simulasi Pengamanan Text dalam Proses Enkripsi dan Deskripsi Metode Vigenere Cipher”.

1.2 Rumusan Masalah

Dalam pelaksanaan penelitian Skripsi ini terdapat beberapa permasalahan yang menjadi titik utama pembahasan, diantaranya adalah sebagai berikut:

1. Bagaimana aspek kerahasiaan pada algoritma Vigenere Cipher yang ditinjau berdasarkan: kompleksitas algoritma, karakteristik penyandian *plaintext* terhadap *chipertext*.
2. Membangun sistem yang dapat menjaga kerahasiaan data menggunakan algoritma Vigenere Cipher berbasis android.

1.3 Batasan Masalah

Batasan masalah dalam penulisan skripsi ini adalah sebagai berikut:

1. Menggunakan metode Vigenere Cipher dengan teknik angka dan huruf.
2. Menggunakan kunci dalam penyandian
3. Data yang dienkrpsi berupa hanya berupa plainteks.
4. Sistem penyandian berbasis Desktop.

5. Tidak menggunakan database

1.4 Tujuan Penelitian

Adapun manfaat yang dapat diambil dari penulisan skripsi ini adalah sebagai berikut:

1. Membuat sistem penyandian tulisan menggunakan metode Vigenere Cipher
2. Untuk Mengubah proses pengiriman data penting.

1.5 Manfaat Penelitian

Adapun manfaat yang dapat diambil dari penulisan skripsi ini adalah sebagai berikut:

1. Memberi kemudahan bagi pengguna dalam menyandi tulisan.
2. Menjadi contoh program bagi pengajar dalam memberi materi pengajaran kriptographi.

BAB II

LANDASAN TEORI

2.1 Kemanan Data

Pada zaman teknologi informasi sekarang, data atau informasi merupakan suatu asset yang sangat berharga dan harus dilindungi. Hal ini juga diikuti oleh kemajuan teknologi komputer. Kemajuan teknologi komputer membantu semua aspek kehidupan manusia. Dengan adanya kemajuan dalam teknologi informasi, komunikasi dan komputer maka kemudian muncul masalah baru, yaitu masalah keamanan akan data dan informasi dan dalam hal ini akan membuka peluang bagi orang-orang yang tidak bertanggung jawab untuk menggunakannya sebagai tindak kejahatan. Dan tentunya akan merugikan pihak tertentu. Dalam keamanan data ada beberapa aspek yang berkaitan dengan persyaratan kemanan yaitu (Pabokory, 2015):

- a. *Secrecy*. Berhubungan dengan akses membaca data dan informasi. Data dan informasi di dalam suatu sistem komputer hanya dapat diakses dan dibaca oleh orang yang berhak.
- b. *Integrity*. Berhubungan dengan akses merubah data dan informasi. Data dan informasi di dalam suatu sistem komputer hanya dapat diubah oleh orang yang berhak.

- c. *Availability*. Berhubungan dengan ketersediaan data dan informasi. Data dan informasi yang berada dalam suatu sistem komputer tersedia dan dapat dimanfaatkan oleh orang yang berhak. (Pabokory, 2015).
- d. Lebih lanjut menurut (Pabokory, 2015), terdapat lima langkah keamanan komputer yang baik untuk diperhitungkan yaitu; aset, analisis resiko, perlindungan, alat dan prioritas.

2.2 *Kriptografi*

Kriptografi merupakan kata dari bahasa Yunani yaitu *cryptography*, terdiri dari dua suku kata yaitu kripto dan graphia. Kripto artinya menyembunyikan, sedangkan graphia artinya tulisan. Sehingga, bila digabungkan akan menjadi kata yang berarti menyembunyikan/merahasiakan tulisan. *Kriptografi* adalah suatu ilmu ataupun seni mengamankan pesan dan dilakukan oleh *cryptographer* (Anonim, 2014).

Menurut (Rhee, 2013). *kriptografi* digunakan untuk memastikan privasi dan autentifikasi data dalam komunikasi antar sistem komputer. Terdapat dua proses dasar dalam *kriptografi* yaitu:

- a. *Enkripsi*, adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca). (Pabokory, 2015)
- b. *Deskripsi*, adalah kebalikan dari *Enkripsi* yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal. (Pabokory, 2015).

Sebuah pesan atau data yang masih asli dan belum mengalami penyandian dikenal dengan istilah *plaintext*. Kemudian setelah disamarkan dengan suatu cara penyandian, maka *plaintext* ini disebut sebagai *chipertext*. Proses penyamaran dari *plaintext* ke *ciphertext* disebut *Enkripsi (encryption)*, dan proses pengembalian dari *ciphertext* menjadi *plaintext* kembali disebut dekripsi (*decryption*). (Pabokory, 2015). *File* yang dapat di *Enkripsi* dapat berupa teks, gambar maupun audio dan video.

2.3 Kriptografi Vigenere Cipher

Kriptografi *Vigenere Cipher* merupakan bagian dari kriptografi polialfabetik yang ditemukan pertama kali pada tahun 1586 oleh diplomat Perancis bernama *Blaise de Vigenere* (1523-1596). Menurut (Prade E, 2014) *Vigenere Cipher* merupakan jenis *cipher* abjad majemuk yang paling sederhana. *Vigenere Cipher* menerapkan metode substitusi poli alfabetik dan termasuk kedalam kategori kunci simetris dimana kunci yang digunakan untuk proses enkripsi adalah sama dengan kunci yang digunakan untuk proses dekripsi. Tujuan utama dari *vigenere cipher* ini adalah menyembunyikan keterhubungan antara *plaintext* dan *ciphertext* dengan menggunakan kata kunci sebagai penentu pergeseran karakternya.

Tabel yang digunakan merupakan tabel 26 huruf alfabetik standart, yang dimulai dari A sampai Z. Panjang kunci tersebut bisa lebih pendek ataupun sama dengan *plaintext*, maka kunci tersebut akan diulang secara periodik hingga

panjang kunci tersebut sama dengan panjang *plaintext*nya. Berikut ini rumus enkripsi dan dekripsi Vigenere Cipher :

$$\text{Enkripsi : } C_i = P_i + k_i \text{ mod } 26$$

$$\text{Dekripsi : } P_i = C_i - k_i \text{ mod } 26$$

C_i : *Ciphertext*

P_i : *Plaintext*

k_i : *Key* atau kunci

Menurut (Teady, 2015) dalam jurnalnya yang berjudul *Vigenere Cipher Menggunakan Spreadsheet*, penyandian *Vigenere* atau *Vigenere Cipher* merupakan salah satu teknik penyandian dengan cara substitusi. Bruen (Bruen, 2015) dalam bukunya *Cryptography, Information Theory, and Error-Correction*, serta Martin (Martin 2015) dalam bukunya *Everyday Cryptography*, mengatakan bahwa *vigenere cipher* adalah sebuah metode dari *enkripsi* teks alfabetik menggunakan serangkaian penyandian berbasis *caesar* pada huruf-huruf dari sebuah kata kunci, dan merupakan bentuk sederhana dari substitusi *polyalphabetic*. Teknik substitusinya 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 *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.

Berbeda dengan caesar cipher, input *key vigenere cipher* berupa sebuah kata yang merupakan rangkaian huruf.

Contoh :

Input Kunci : cerdas

Pengulangan : cerdascerdascerdasc

Plainteks : belajarsupayapandai

cipherteks : didcjstwlmaqctrqdk

Key akan diulang-ulang sampai sejumlah huruf pada plaintext.

Kemudian setiap huruf satu persatu akan dicari pada table vigenere sesuai dengan keynya.

Dalam jurnalnya yang berjudul Implementasi *Enkripsi* Data Dengan Algoritma *Vigenere Cipher*. Vigenere Cipher termasuk dalam cipher abjad majemuk (*polyalphabetic substitution Cipher*) yang dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, *Blaise de Vigenere* pada abad 16 (tahun 1586).

Vigenere Cipher menggunakan suatu kunci yang memiliki panjang tertentu. Panjang kunci tersebut bias lebih pendek ataupun sama dengan plainteksnya. Jika panjang kunci kurang dari panjang plainteks, maka kunci tersebut akan diulang secara periodic sehingga panjang kunci tersebut akan sama panjang dengan plainteksnya.

Formula atau rumus enkripsi *Vigenere Cipher*

$$C_i = (P_i + K_i) \bmod 26$$

Formula atau rumus deskripsi *Vigenere Cipher*

$$P_i = (C_i - K_i) \bmod 26 ; \text{ untuk } C_i \geq K_i$$

$$P_i = (C_i + 26 - K_i) \bmod 26 ; \text{ untuk } C_i < K_i$$

Dengan penjelasan:

C_i = nilai decimal karakter *ciphertext* ke- i

P_i = nilai decimal karakter *ciphertext* ke- i

K_i = nilai decimal karakter *ciphertext* ke- i

Contoh bila kita ingin memberi sandi pada kata ILMU KOMPUTER dan kunci yang kita inginkan adalah UNPAB maka enkripsi dilakukan sebagai berikut:

Plainteks : ILMUKOMPUTER

Kunci : UNPAB

Karena metode yang diterapkan pada *Vigenere Cipher* adalah dengan menyusun kunci yang panjangnya akan disesuaikan dengan panjang plainteksnya, maka kunci akan mengalami perulangan sampai memenuhi banyak karakter yang terdapat pada plainteks.

Plainteks : ILMUKOMPUTER

Kunci : UNPABUNPABUN

Langkah selanjutnya adalah masuk ke proses enkripsi dengan metode *vigenere* menggunakan formula atau rumus $C_i = (P_i + K_i) \bmod 26$.

Plainteks : I L M U K O M P U T E R

Kunci : U N P A B U N P A B U N

Cipherteks : B Y B U L I Z E U U Y E

Cipherteks didapatkan dengan cara menggunakan formula $C_i = (P_i + K_i) \bmod 26$

$$C_1 = (I + U) \bmod 26 = (8+20) \bmod 26 = 2 = B$$

$$C_2 = (L + N) \bmod 26 = (11+13) \bmod 26 = 24 = Y$$

Setelah seluruh karakter mendapatkan *cipherteks*, maka proses *enkripsi* sudah selesai.

Proses *deskripsi* dilakukan untuk memecahkan *cipherteks* kembali menjadi *plainteks*. Untuk proses deskripsi digunakan rumus atau formula $P_i = (C_i - K_i) \bmod 26$; untuk $C_i \geq K_i$ dan/atau $P_i = (C_i + 26 - K_i) \bmod 26$; untuk $C_i < K_i$

Cipherteks : B Y B U L I Z E U U Y E

Kunci : U N P A B U N P A B U N

Plainteks : I L M U K O M P U T E R

Seperti pada karakter pertama dimana C_1 bernilai 2 dan K_1 bernilai 20 maka digunakan formula atau rumus $P_i = (C_i + 26 - K_i) \bmod 26$ karena nilai $C_1 < K_1$

$$P_1 = (2 + 26 - 20) \bmod 26 = 8 = I$$

Sementara pada karakter kedua dimana C_2 bernilai 24 dan K_2 bernilai 13 maka digunakan formula atau rumus $P_i = (C_i - K_i) \bmod 26$ karena nilai $C_2 \geq K_2$

$$P_2 = (24 - 13) \bmod 26 = 11 = L$$

Selain itu kunci juga dapat berupa angka, berikut adalah table huruf beserta angka yang akan membantu proses enkripsi

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2
										0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5

Tabel 2.1 Tabel Alphabet dan Konversinya (sumber: Arjana, 2013)

Misalkan plainteksnya adalah ilmu komputer dan kunci yang ingin diberikan adalah 5,15,8,0 maka selanjutnya didapatkan tabel enkripsi sebagai berikut.

I	L	M	U	K	O	M	P	U	T	E	R
8	11	12	20	10	14	12	15	20	19	4	17
5	15	8	0	5	15	8	0	5	15	8	0

Tabel 2.2 Tabel Enkripsi

Ciphertext yang dihasilkan adalah sebagai berikut

Ciphertext : 13,1,20,20,15,29,20,15,25,9,12,17

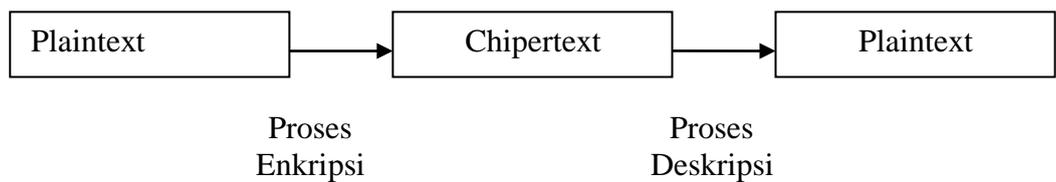
Untuk proses deskripsi dapat dilakukan dengan rumus atau formula yang sama seperti *vigenere cipher* dengan menggunakan huruf . Misalkan untuk angka pertama *chipertext* adalah 13 dan mau didapatkan plainteksnya maka;

$$P1 = (13-5) \text{ modulo } 26 = 8 = I$$

2.4 Enkripsi

Enkripsi merupakan hal yang sangat penting dalam *kriptografi* supaya keamanan data yang dikirimkan bisa terjaga kerahasiaannya. Pesan asli (plaintext) diubah menjadi kode-kode yang tidak dimengerti. *Enkripsi* bisa diartikan dengan chiper atau kode. Sama halnya dengan kita yang tidak mengerti sebuah kata, kita akan dapat melihatnya di dalam kamus atau daftar istilah-istilah. Berbeda halnya

dengan *Enkripsi*, untuk mengubah plaintext ke bentuk ciphertext, kita harus menggunakan algoritma yang dapat mengkodekan data yang kita inginkan. Berikut adalah penggambaran proses *Enkripsi*.



Gambar 2.1. Proses *Enkripsi* dan *Deskripsi*

Sumber : (Pabokory, 2015)

2.5 *Kriptografi Klasik*

Menurut (Bishop, 2014). *kriptografi* klasik adalah *kriptografi* yang disebut juga sebagai *kriptografi* kunci tunggal atau *kriptografi* simetris yang menggunakan kunci yang sama untuk *Enkripsi* maupun *Deskripsi*. *Kriptografi* klasik merupakan *kriptografi* yang digunakan pada zaman dahulu sebelum komputer ditemukan atau sudah ditemukan namun belum secanggih sekarang. *Kriptografi* ini melakukan pengacakan huruf pada kata terang / plaintext.

2.6 *One Time Pad (OTP)*

Algoritma *One Time Pad* (OTP) merupakan algoritma berjenis *Symmetric key* yang artinya bahwa kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama. Dalam proses enkripsi, algoritma ini menggunakan cara *stream Cipher* yang berasal dari hasil XOR antara *bit plaintext* dan *bit key*. Pada metode ini *plain text* diubah kedalam kode ASCII dan kemudian

dikenakan operasi XOR terhadap kunci yang sudah diubah ke dalam kode ASCII. (Hamokwarong, 2014).

One-time pad adalah salah satu stream *Cipher* klasik yang secara matematis terbukti sempurna aman. *Cipher* teksnya tidak mungkin dapat dipecahkan. Keamanan algoritma *one-time pad* terletak pada penggunaan barisan bilangan acak sejati (*trully random*) sebagai kunci enkripsi, panjang kunci sama dengan panjang pesan dan tidak ada perulangan kunci sebagaimana pada *Vernam Cipher* atau *Vigenere Cipher*. (Munir, 2014)

Sayangnya *one-time pad* tidak dapat diimplementasikan secara praktis sebab pembangkitan bilangan acak sejati tidak dapat diulang kembali di sisi penerima pesan. Oleh karena itu kunci (*pad*) harus dikirim melalui saluran komunikasi yang kedua (misalnya melalui kurir), sayangnya saluran kedua itu umumnya lambat dan ongkosnya mahal. *One-time pad* masih dapat diterapkan namun kunci yang berupa barisan bilangan acak diganti dengan barisan bilangan semi-acak (*pseudo-random*) dengan syarat barisan kunci itu tidak boleh berulang. (Munir, 2014)

2.7 Algoritma

Penyelesaian permasalahan dengan menggunakan alat bantu system computer paling tidak akan melibatkan lima tahapan, yaitu:

- a. Analisis masalah
- b. Merancang algoritma
- c. Membuat program computer

d. Menguji hasil program computer

e. Dokumentasi

Poin kedua menerangkan bahwa dalam perancangan sebuah system komputer dibutuhkan adanya perancangan algoritma. Sehingga setelahnya dapat dilanjutkan ke tahap-tahap berikutnya hingga dokumentasi.

Algoritma adalah Sistem kerja komputer memiliki *brainware*, *hardware*, dan *software*. Tanpa salah satu dari ketiga sistim tersebut, komputer tidak akan berguna. Kita akan lebih fokus pada *software* komputer. Software terbangun atas susunan program (silahkan baca mengenai pengertian program) dan syntax (cara penulisan/pembuatan program). Untuk menyusun program atau syntax, diperlukannya langkah-langkah yang sistematis dan logis untuk dapat menyelesaikan masalah atau tujuan dalam proses pembuatan suatu *software*. Maka, Algoritma berperan penting dalam penyusunan program atau syntax tersebut.

Pengertian Algoritma adalah susunan yang logis dan sistematis untuk memecahkan suatu masalah atau untuk mencapai tujuan tertentu. Dalam dunia komputer, Algoritma sangat berperan penting dalam pembangunan suatu *software*. Dalam dunia sehari-hari, mungkin tanpa kita sadari Algoritma telah masuk dalam kehidupan kita.

Pengertian Algoritma adalah susunan yang logis dan sistematis untuk memecahkan suatu masalah atau untuk mencapai tujuan tertentu.

Algoritma adalah kunci dari bidang ilmu komputer, dan pada dasarnya setiap hari kita melakukan aktivitas algoritma. Kata algoritma berasal dari sebutan

Algorizm (Abu Abdullah Muhammad Ibn Musa Al Khwarizmi, ahli matematika Uzbeki

- a. Algoritma adalah urutan langkah-langkah berhingga untuk memecahkan masalah logika atau matematika
- b. Algoritma adalah logika, metode dan tahapan (urutan) sistematis yang digunakan untuk memecahkan suatu permasalahan.
- c. Algoritma adalah urutan langkah-langkah logis penyelesaian masalah yang disusun secara sistematis dan logis.
- d. Algoritma adalah urutan logis pengambilan keputusan untuk pemecahan masalah.

Pembuatan algoritma harus selalu dikaitkan dengan:

- a. Kebenaran algoritma
- b. Kompleksitas (lama dan jumlah waktu proses dan penggunaan memori)

Kriteria Algoritma yang baik:

- a. Tepat, benar, sederhana, standar dan efektif
- b. Logis, terstruktur dan sistematis
- c. Semua operasi terdefinisi
- d. Semua proses harus berakhir setelah sejumlah langkah dilakukan
- e. Ditulis dengan bahasa yang standar dengan format pemrograman agar mudah untuk diimplementasikan dan tidak menimbulkan arti ganda.

2.8 *Unified Modeling Language (UML)*

2.8.1 Pengenalan UML

Unified Modelling Language (UML) adalah suatu alat untuk memvisualisasikan dan mendokumentasikan hasil analisis dan desain yang berisi sintak dalam memodelkan sistem secara visual (Haviluddin, 2015). Banyak orang yang telah membuat bahasa pemodelan pembangunan perangkat lunak sesuai dengan teknologi pemrograman yang berkembang pada saat itu, misalnya yang sempat berkembang dan digunakan oleh banyak pihak adalah *Data Flow Diagram* (DFD) untuk memodelkan perangkat lunak yang menggunakan pemrograman prosedural atau struktur, kemudian juga ada *State Transition Diagram* (STD) yang digunakan untuk memodelkan *real time* (waktu nyata).

Pada perkembangan teknik pemrograman berorientasi objek, muncullah sebuah standarisasi bahasa pemodelan untuk pembangunan perangkat lunak yang dibangun dengan menggunakan teknik pemrograman berorientasi objek, yaitu *Unified Modeling Language (UML)*.

2.8.2 *Use Case Diagram*

Diagram yang menggambarkan *actor*, *use case* dan relasinya sebagai suatu urutan tindakan yang memberikan nilai terukur untuk aktor. Sebuah *use case* digambarkan sebagai elips horizontal dalam suatu diagram *use case diagram* (Haviluddin, 2015).

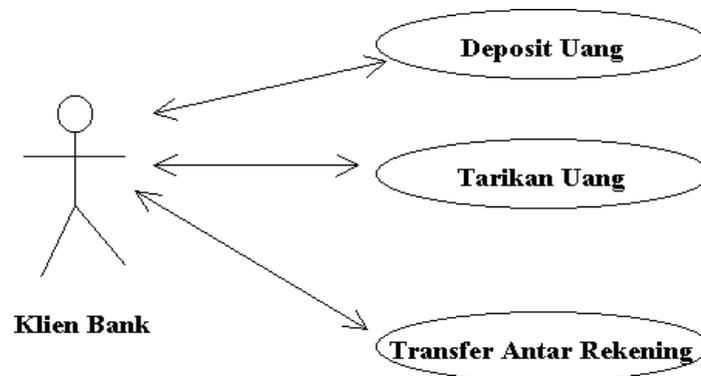
Tabel 2.1 Simbol *Use Case Diagram*

NO	GAMBAR	NAMA	KETERANGAN
1		<i>Actor</i>	Menspesifikasikan himpunan peran yang pengguna mainkan ketika berinteraksi dengan <i>use case</i> .
2		<i>Dependency</i>	Hubungan dimana perubahan yang terjadi pada suatu elemen mandiri (<i>independent</i>) akan mempengaruhi elemen yang bergantung padanya elemen yang tidak mandiri (<i>independent</i>).
3		<i>Generalization</i>	Hubungan dimana objek anak (<i>descendent</i>) berbagi perilaku dan struktur data dari objek yang ada di atasnya objek induk (<i>ancestor</i>).
4		<i>Include</i>	Menspesifikasikan bahwa <i>use case</i> sumber secara <i>eksplisit</i> .
5		<i>Extend</i>	Menspesifikasikan bahwa <i>use case</i> target memperluas perilaku dari <i>use case</i> sumber pada suatu titik yang diberikan.
6		<i>Association</i>	Apa yang menghubungkan antara objek satu dengan objek lainnya.
7		<i>System</i>	Menspesifikasikan paket yang menampilkan sistem secara terbatas.
8		<i>Use Case</i>	Deskripsi dari urutan aksi-aksi yang ditampilkan sistem yang menghasilkan suatu hasil yang terukur bagi suatu aktor
9		<i>Collaboration</i>	Interaksi aturan-aturan dan elemen lain yang bekerja sama untuk menyediakan perilaku yang lebih besar dari jumlah dan elemen-elemennya (sinergi).

10		<i>Note</i>	Elemen fisik yang eksis saat aplikasi dijalankan dan mencerminkan suatu sumber daya komputasi
----	---	-------------	---

Sumber : (Gellysa Urva, 2015)

Contoh Use Case Diagram :



Gambar 2.2. Contoh Use Case Diagram

Sumber : (Haviluddin, 2015)

1. Activity Diagram

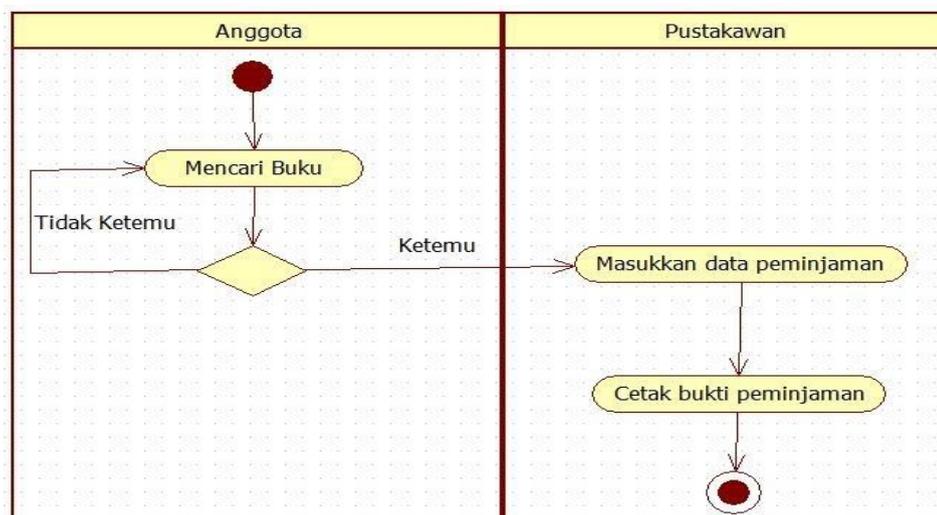
Diagram aktivitas atau *activity diagram* menggambarkan *workflow* (aliran kerja) atau aktivitas dari sebuah sistem atau proses bisnis atau *menu* yang ada pada perangkat lunak. Yang perlu diperhatikan disini adalah bahwa diagram aktivitas menggambarkan aktivitas sistem bukan apa yang dilakukan aktor, jadi aktivitas yang dapat dilakukan oleh sistem.

Tabel 2.2. Simbol *Activity Diagram*

NO	GAMBAR	NAMA	KETERANGAN
1		<i>Activity</i>	Memperlihatkan bagaimana masing-masing kelas antarmuka saling berinteraksi satu sama lain
2		<i>Action</i>	<i>State</i> dari sistem yang mencerminkan eksekusi dari suatu aksi
3		<i>Initial Node</i>	Bagaimana objek dibentuk atau diawali.
4		<i>Activity Final Node</i>	Bagaimana objek dibentuk dan dihancurkan
5		<i>Fork Node</i>	Satu aliran yang pada tahap tertentu berubah menjadi beberapa aliran

Sumber : (Gellysa Urva, 94 : 2015)

Contoh Activity Diagram :

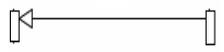
Gambar 2.3. Contoh *Activity Diagram*

Sumber : (Gellysa Urva, 94 : 2015)

2. *Sequence Diagram*

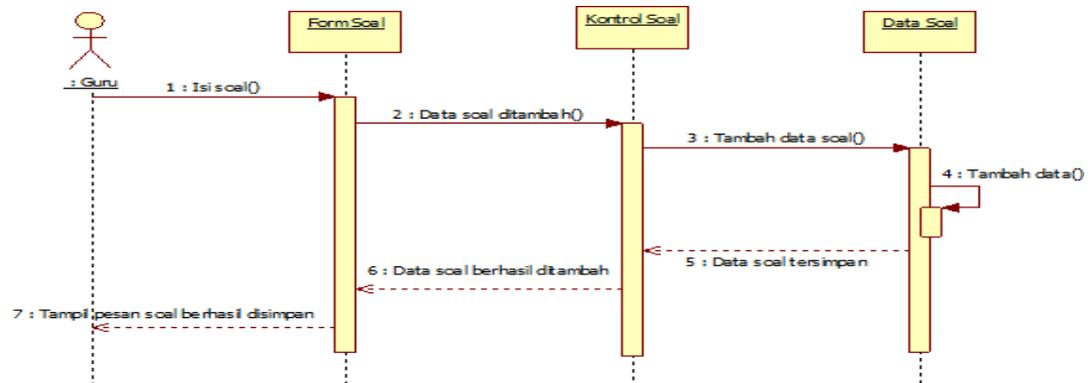
Diagram sekuen menggambarkan kelakuan objek pada *use case* dengan mendeskripsikan waktu hidup objek dan *message* yang dikirimkan dan diterima antar objek. Oleh karena itu untuk menggambar diagram sekuen maka harus diketahui objek-objek yang terlibat dalam sebuah *use case* beserta metode-metode yang dimiliki kelas yang diinstansiasi menjadi objek itu. Membuat diagram sequence juga dibutuhkan untuk melihat skenario yang ada pada *use case*.

Tabel 2.3. Simbol *Sequence Diagram*

NO	GAMBAR	NAMA	KETERANGAN
1		<i>LifeLine</i>	Objek <i>entity</i> , antarmuka yang saling berinteraksi.
2		<i>Message</i>	Spesifikasi dari komunikasi antar objek yang memuat informasi-informasi tentang aktifitas yang terjadi
3		<i>Message</i>	Spesifikasi dari komunikasi antar objek yang memuat informasi-informasi tentang aktifitas yang terjadi

Sumber : (Gellysa Urva, 95 : 2015)

Contoh Sequence Diagram :



Gambar 2.4. Contoh Sequence Diagram

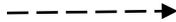
Sumber : (Gellysa Urva, 95 : 2015)

3. Class Diagram

Class diagram menggambarkan struktur statis dari kelas dalam sistem anda dan menggambarkan atribut, operasi dan hubungan antara kelas. Class diagram membantu dalam memvisualisasikan struktur kelas-kelas dari suatu sistem dan merupakan tipe diagram yang paling banyak dipakai. Selama tahap desain, class diagram berperan dalam menangkap struktur dari semua kelas yang membentuk arsitektur sistem yang dibuat.

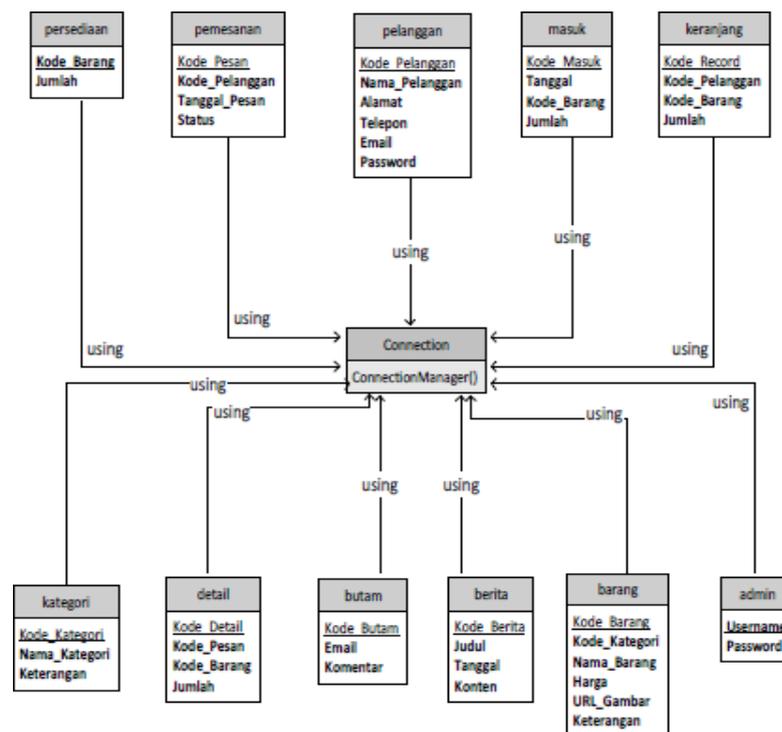
Tabel 2.4. Simbol Class Diagram

NO	GAMBAR	NAMA	KETERANGAN
1		<i>Note</i>	Elemen fisik yang eksis saat aplikasi dijalankan dan mencerminkan suatu sumber daya komputasi

2		<i>dependency</i>	Hubungan dimana perubahan yang terjadi pada suatu elemen mandiri akan mempengaruhi elemen yang bergantung padanya
3		<i>extend</i>	Menspesifikasikan bahwa use case target memperluas perilaku dari use case sumber pada suatu titik yang diberikan.

Sumber : (Gellysa Urva, 95 : 2015)

Contoh *Class Diagram* :



Gambar 2.5. Contoh Class Diagram

Sumber : (Gellysa Urva, 95 : 2015)

2.9 Pengertian Informasi

Secara Etimologi, kata informasi ini berasal dari kata bahasa Perancis kuno *informacion* (tahun 1387) mengambil istilah dari bahasa Latin yaitu *informationem* yang berarti “konsep, ide atau garis besar”. Informasi ini merupakan kata benda dari *informare* yang berarti aktivitas dalam “pengetahuan yang dikomunikasikan”.

Informasi adalah hasil pemrosesan data yang diperoleh dari setiap elemen sistem menjadi bentuk yang mudah dipahami dan merupakan pengetahuan yang relevan dan berguna (Yulansari, 2013).

Informasi bisa menjadi fungsi penting dalam membantu mengurangi rasa cemas pada seseorang. Menurut pendapat (Notoatmodjo, 2018) bahwa semakin banyak memiliki informasi dapat memengaruhi atau menambah pengetahuan terhadap seseorang dan dengan pengetahuan tersebut bisa menimbulkan kesadaran yang akhirnya seseorang itu akan berperilaku sesuai dengan pengetahuan yang dimilikinya.

Informasi adalah data yang telah diolah melalui proses tertentu menjadi sesuatu yang menambah pengetahuan atau temuan yang mempunyai arti baru bagi pemakainya.

Adapun fungsi-fungsi informasi adalah sebagai berikut:

1. Untuk meningkatkan pengetahuan bagi si pemakai.
2. Untuk mengurangi ketidakpastian dalam proses pengambilan keputusan pemakai.

3. Menggambarkan keadaan yang sebenarnya dari sesuatu hal. Informasi yang berkualitas harus akurat, tepat dan relevan.

Sumber dari informasi adalah data. Data adalah kenyataan yang menggambarkan suatu kejadian-kejadian dan kesatuan nyata. Data merupakan bentuk yang masih mentah, belum dapat bercerita banyak sehingga perlu diolah lebih lanjut. Data diolah melalui suatu metode untuk menghasilkan informasi. Data dapat berbentuk simbol-simbol semacam huruf, angka, bentuk suara, sinyal, gambar, dan sebagainya.

2.10 Pengertian Visual Studio

Visual Studio .Net merupakan salah satu *tool development Microsoft* yang dapat digunakan untuk membuat aplikasi di lingkungan kerja berbasis sistem operasi *Windows*. *Visual Studio .NET* menyediakan tools bagi para *developer* untuk membangun aplikasi yang berjalan di *.Net Framework* (Safik, 2015).

Visual Studio (Beginners All-Purpose Symbolic Instruction Code) merupakan Bahasa pemrograman *Integrated Development Environment (IDE)*, yaitu bahasa pemrograman *visual* yang digunakan untuk membuat program aplikasi atau *software* berbasis sistem operasi *Microsoft Windows*, dengan menggunakan model pemrograman "*Common Object Model (COM)*".

Visual Studio merupakan turunan bahasa pemrograman *STUDIO* yang menawarkan pengembangan perangkat lunak komputer berbasis grafik dengan cepat. Dengan menggunakan bahasa pemrograman VB, para programmer dapat

membangun aplikasi dengan menggunakan komponen-komponen yang di sediakan VB.

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

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

Dalam pemrograman untuk bisnis, *Visual Studio* memiliki pangsa pasar yang sangat luas. Dalam sebuah survey yang dilakukan pada tahun 2005, 62% pengembang perangkat lunak dilaporkan menggunakan berbagai bentuk *Visual Studio*, yang diikuti oleh *C++*, *JavaScript*, *C#*, dan *Java*.

1. Komponen kerja

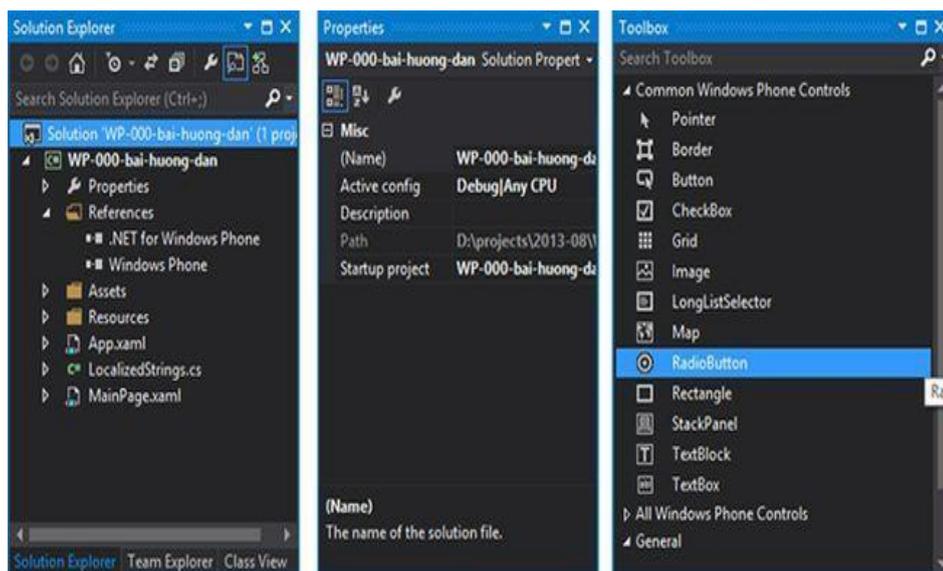
Beberapa komponen kerja program *visual Studio 2015* telah ditampilkan sebagai tampilan standard. Masih banyak lagi komponen yang masih tersembunyi sehingga memerlukan perintah tertentu untuk menampilkannya. Kita dapat

mengatur komponen di dalam program visual Studio 2015 sesuai dengan yang kita butuhkan. Berikut ini adalah beberapa komponen kerja dari visual Studio 2015 adalah :

a. *Toolbox*

Toolbox adalah sebuah panel yang menampung tombol-tombol yang berguna untuk membuat suatu desain mulai dari tombol *label*, *pointer*, *button*, dan lain-lain. Berikut ini adalah gambaran *toolbox* pada *visual Studio 2015* :

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



Gambar 2.6. Tampilan *Toolbox*

Sumber : (Safik, 2015).

Table 2.5. *Toolbox Visual Studio*

Nama tombol	Fungsi
<i>Pointer</i>	Memilih, mengatur ukuran dan memindahkan posisi yang terpasang di bagian form.
<i>Bindingsources</i>	Untuk mengkoneksikan program ke database
<i>Label</i>	Menampilkan teks, dimana pengguna program tidak bisa mengubah teks tersebut

<i>GroupBox</i>	Untuk mengelompokkan item yang ada di form
<i>Checkbox</i>	Membuat kotak periksa, dimana pengguna program dapat memilih sekaligus
<i>Listbox</i>	Membuat daftar pilihan
<i>Timer</i>	Membuat control waktu dan interval yang diperlukan
<i>Image</i>	Menampilkan gambar pada form dalam format <i>bitmap</i> , <i>icone</i> , atau <i>metafile</i>
<i>PictureBox</i>	Menampilkan gambar dari sebuah file
<i>Textbox</i>	Membuat teks, dimana teks tersebut dapat diubah oleh pembuat program
<i>Button</i>	Membuat tombol perintah
<i>Combobox</i>	Menambahkan control kotak combo yang merupakan control gabungan antara <i>textbox</i> dan <i>listbox</i>

Sumber : (Safik, 2015).

2.11 Tabel ASCII

ASCII merupakan kepanjangan dari (American Standard Code for Information Interchange), dan pengertian dari ASCII sendiri adalah suatu standar internasional dalam kode huruf dan simbol seperti Hex dan Unicode tetapi ASCII lebih bersifat universal, contohnya 124 adalah untuk karakter "|". Ia selalu digunakan oleh komputer dan alat komunikasi lain untuk menunjukkan teks. sedangkan fungsi dari kode ASCII ialah digunakan untuk mewakili karakter-karakter angka maupun huruf didalam komputer, sebagai contoh dapat kita lihat pada karakter 1, 2, 3, A, B, C, dan sebagainya.

DEC	OCT	HEX	BIN	Symbol
0	000	00	00000000	NUL
1	001	01	00000001	SOH
2	002	02	00000010	STX
3	003	03	00000011	ETX
4	004	04	00000100	EOT

5	005	05	00000101	ENQ	
6	006	06	00000110	ACK	
7	007	07	00000111	BEL	
8	010	08	00001000	BS	
9	011	09	00001001	HT	
10	012	0A	00001010	LF	
11	013	0B	00001011	VT	
12	014	0C	00001100	FF	
13	015	0D	00001101	CR	
14	016	0E	00001110	SO	
15	017	0F	00001111	SI	
16	020	10	00010000	DLE	
17	021	11	00010001	DC1	
18	022	12	00010010	DC2	
19	023	13	00010011	DC3	
20	024	14	00010100	DC4	
21	025	15	00010101	NAK	
22	026	16	00010110	SYN	
23	027	17	00010111	ETB	
24	030	18	00011000	CAN	
25	031	19	00011001	EM	
26	032	1A	00011010	SUB	
27	033	1B	00011011	ESC	
28	034	1C	00011100	FS	
29	035	1D	00011101	GS	
30	036	1E	00011110	RS	
31	037	1F	00011111	US	
	DEC	OCT	HEX	BIN	Symbol
32	040	20	00100000		Spasi
33	041	21	00100001		!
34	042	22	00100010		"

35	043	23	00100011	#
36	044	24	00100100	\$
37	045	25	00100101	%
38	046	26	00100110	&
39	047	27	00100111	'
40	050	28	00101000	(
41	051	29	00101001)
42	052	2A	00101010	*
43	053	2B	00101011	+
44	054	2C	00101100	,
45	055	2D	00101101	-
46	056	2E	00101110	.
47	057	2F	00101111	/
48	060	30	00110000	0
49	061	31	00110001	1
50	062	32	00110010	2
51	063	33	00110011	3
52	064	34	00110100	4
53	065	35	00110101	5
54	066	36	00110110	6
55	067	37	00110111	7
56	070	38	00111000	8
57	071	39	00111001	9
58	072	3A	00111010	:
59	073	3B	00111011	;
60	074	3C	00111100	<
61	075	3D	00111101	=
62	076	3E	00111110	>
63	077	3F	00111111	?
64	100	40	01000000	@
65	101	41	01000001	A
66	102	42	01000010	B

67	103	43	01000011	C
68	104	44	01000100	D
69	105	45	01000101	E
70	106	46	01000110	F
71	107	47	01000111	G
72	110	48	01001000	H
73	111	49	01001001	I
74	112	4A	01001010	J
75	113	4B	01001011	K
76	114	4C	01001100	L
77	115	4D	01001101	M
78	116	4E	01001110	N
79	117	4F	01001111	O
80	120	50	01010000	P
81	121	51	01010001	Q
82	122	52	01010010	R
83	123	53	01010011	S
84	124	54	01010100	T
85	125	55	01010101	U
86	126	56	01010110	V
87	127	57	01010111	W
88	130	58	01011000	X
89	131	59	01011001	Y
90	132	5A	01011010	Z
91	133	5B	01011011	[
92	134	5C	01011100	\
93	135	5D	01011101]
94	136	5E	01011110	^
95	137	5F	01011111	_
96	140	60	01100000	`
97	141	61	01100001	A
98	142	62	01100010	B

99	143	63	01100011	C
100	144	64	01100100	D
101	145	65	01100101	E
102	146	66	01100110	F
103	147	67	01100111	G
104	150	68	01101000	H
105	151	69	01101001	I
106	152	6A	01101010	J
107	153	6B	01101011	K
108	154	6C	01101100	L
109	155	6D	01101101	M
110	156	6E	01101110	N
111	157	6F	01101111	O
112	160	70	01110000	P
113	161	71	01110001	Q
114	162	72	01110010	R
115	163	73	01110011	S
116	164	74	01110100	T
117	165	75	01110101	U
118	166	76	01110110	V
119	167	77	01110111	W
120	170	78	01111000	X
121	171	79	01111001	Y
122	172	7A	01111010	Z
123	173	7B	01111011	{
124	174	7C	01111100	
125	175	7D	01111101	}
126	176	7E	01111110	~
127	177	7F	01111111	
128	200	80	10000000	€
129	201	81	10000001	

130	202	82	10000010	,
131	203	83	10000011	F
132	204	84	10000100	„
133	205	85	10000101	...
134	206	86	10000110	†
135	207	87	10000111	‡
136	210	88	10001000	^
137	211	89	10001001	‰
138	212	8A	10001010	Š
139	213	8B	10001011	‹
140	214	8C	10001100	Œ
141	215	8D	10001101	
142	216	8E	10001110	Ž
143	217	8F	10001111	
144	220	90	10010000	
145	221	91	10010001	‘
146	222	92	10010010	’
147	223	93	10010011	“
148	224	94	10010100	”
149	225	95	10010101	•
150	226	96	10010110	–
151	227	97	10010111	—
152	230	98	10011000	~
153	231	99	10011001	™
154	232	9A	10011010	Š
155	233	9B	10011011	›
156	234	9C	10011100	Œ
157	235	9D	10011101	
158	236	9E	10011110	Ž
159	237	9F	10011111	Ÿ
160	240	A0	10100000	
161	241	A1	10100001	i

162	242	A2	10100010	¢
163	243	A3	10100011	£
164	244	A4	10100100	¤
165	245	A5	10100101	¥
166	246	A6	10100110	¦
167	247	A7	10100111	§
168	250	A8	10101000	¨
169	251	A9	10101001	©
170	252	AA	10101010	^a
171	253	AB	10101011	«
172	254	AC	10101100	¬
173	255	AD	10101101	
174	256	AE	10101110	®
175	257	AF	10101111	¯
176	260	B0	10110000	°
177	261	B1	10110001	±
178	262	B2	10110010	²
179	263	B3	10110011	³
180	264	B4	10110100	´
181	265	B5	10110101	µ
182	266	B6	10110110	¶
183	267	B7	10110111	·
184	270	B8	10111000	¸
185	271	B9	10111001	¹
186	272	BA	10111010	°
187	273	BB	10111011	»
188	274	BC	10111100	¼
189	275	BD	10111101	½
190	276	BE	10111110	¾
191	277	BF	10111111	¿
192	300	C0	11000000	À
193	301	C1	11000001	Á

194	302	C2	11000010	Â
195	303	C3	11000011	Ã
196	304	C4	11000100	Ä
197	305	C5	11000101	Å
198	306	C6	11000110	Æ
199	307	C7	11000111	Ç
200	310	C8	11001000	È
201	311	C9	11001001	É
202	312	CA	11001010	Ê
203	313	CB	11001011	Ë
204	314	CC	11001100	Ì
205	315	CD	11001101	Í
206	316	CE	11001110	Î
207	317	CF	11001111	Ï
208	320	D0	11010000	Ð
209	321	D1	11010001	Ñ
210	322	D2	11010010	Ò
211	323	D3	11010011	Ó
212	324	D4	11010100	Ô
213	325	D5	11010101	Õ
214	326	D6	11010110	Ö
215	327	D7	11010111	×
216	330	D8	11011000	Ø
217	331	D9	11011001	Ù
218	332	DA	11011010	Ú
219	333	DB	11011011	Û
220	334	DC	11011100	Ü
221	335	DD	11011101	Ý
222	336	DE	11011110	Þ
223	337	DF	11011111	ß
224	340	E0	11100000	À
225	341	E1	11100001	Á

226	342	E2	11100010	Â
227	343	E3	11100011	Ã
228	344	E4	11100100	Ä
229	345	E5	11100101	Å
230	346	E6	11100110	Æ
231	347	E7	11100111	Ç
232	350	E8	11101000	È
233	351	E9	11101001	É
234	352	EA	11101010	Ê
235	353	EB	11101011	Ë
236	354	EC	11101100	Ì
237	355	ED	11101101	Í
238	356	EE	11101110	Î
239	357	EF	11101111	Ï
240	360	F0	11110000	Ð
241	361	F1	11110001	Ñ
242	362	F2	11110010	Ò
243	363	F3	11110011	Ó
244	364	F4	11110100	Ô
245	365	F5	11110101	Õ
246	366	F6	11110110	Ö
247	367	F7	11110111	÷
248	370	F8	11111000	Ø
249	371	F9	11111001	Ù
250	372	FA	11111010	Ú
251	373	FB	11111011	Û
252	374	FC	11111100	Ü
253	375	FD	11111101	Ý
254	376	FE	11111110	Þ
255	377	FF	11111111	ÿ

2.12 Peneliti – Peneliti Sebelumnya

Adapaun peneliti – peneliti dari peneliti sebelumnya yang membahas tentang kriptografi vigenere chiper ini adalah sebagai berikut:

No	Penulis	Judul	Nama Jurnal	Hasil Penelitian
1	Gede Angga Pradipta	Penerapan Kombinasi Metode Enkripsi Vigenere Chiper Dan Transposisi Pada Aplikasai Client Server Chatting	Jurnal Sistem Dan Informatika (Jsi)	Setelah Melalui Tahap Demi Tahap Perancangan Dan Penerapan Program Enkripsi Data Dengan Kombinasi Metode Vigenere Dan Transposisi Pada Aplikasi Chatting, Maka Dhasilkan Kesimpulan Yaitu : 1. Implementasi Program Enkripsi Data Dengan Metode Vigenere Dan Transposisi Dapat Meningkatkan Keamanan Pengiriman Pesan Ke Server. 2. Kombinasi Dengan Metode Transposisi Membuat Metode Vigenere Menjadi Lebih Sulit Untuk Di Pecahkan Karena Cipher Text Yang Dhasilkan Di Awal Akan Dilakukan

				<p>Penkripsian Kembali Dengan Merubah Letak Posisi Karakter Menggunakan Cara Transposisi.</p>
2	<p>Andro Alif Rakhman, Achmad Wahid Kurniawan</p>	<p>Implementasi Algoritma Kriptografi Rivest Shamir Adleman (Rsa) Dan Vigenere Cipher Pada Gambar Bitmap 8 Bit</p>	<p>Jurnal Teknologi Informasi (Techno.Com)</p>	<p>Pada Penelitian Ini, Menggunakan Perpaduan Algoritma Rivest Shamir Adleman (Rsa) Dan Vigenere Cipher Untuk Melakukan Pengamanan Citra. Citra Yang Akan Digunakan Yaitu File Bitmap Dengan Kedalaman Piksel 8 Bit. Citra Akan Diolah Dengan Cara Mengenkripsi Nilai Indeks Warna Rgb Pada Masing-Masing Piksel Dengan Menggunakan Algoritma Kriptografi Rsa Terlebih Dahulu Kemudian Dilanjutkan Dengan Menggunakan Algoritma Vigenere Cipher. Sedangkan Untuk Tahap Pendekripsiannya Dilakukan Dengan Menggunakan Algoritma Vigenere Cipher Terlebih Dahulu Kemudian Menggunakan</p>

				<p>Algoritma Kriptografi Rsa. Selanjutnya Dilakukan Analisis Pengaruh Penerapan Algoritma Rivest Shamir Adleman (Rsa) Dan Vigenere Cipher Pada Citra Yang Akan Diamankan, Meliputi Analisis Ruang Kunci, Analisis Perubahan Indeks Warna, Dan Analisis Waktu Proses Enkripsi Dan Deskripsi. Pengujian Yang Dilakukan Untuk Analisis Tersebut, Menggunakan Citra Berdimensi 3840 X 2160 Piksel Dan Ukuran File 7,91 Mb Dan Citra Berdimensi 5012 X 2819 Piksel Dan Ukuran File 13,4 Mb. Analisis Ruang Kunci Menunjukkan Bahwa Citra Telah Berhasil Didekripsikan Dan Secara Visual Pola Citra Kembali Ke Bentuk Semula Tanpa Mengalami Cacat Sedikitpun. Analisis Perubahan Indeks Warna, Dilihat Secara Visual Pada Hasil Palette Warna</p>
--	--	--	--	--

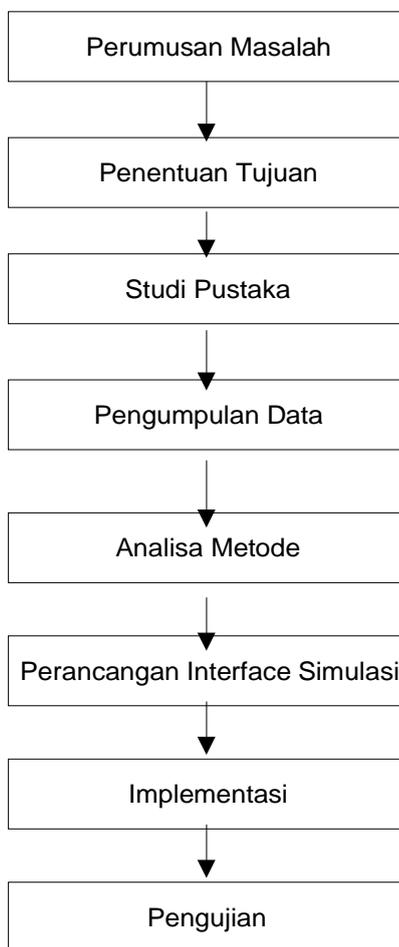
				<p>Membuktikan Bahwa Metode Enkripsi Yang Dirancang Telah Berhasil Digunakan Untuk Memperbarui Nilai Indeks Warna Citra Asli. Sedangkan Dari Analisis Waktu Proses Enkripsi Dan Deskripsi Dapat Disimpulkan Rata-Rata Lama Waktu Yang Dibutuhkan Untuk Proses Dekripsi Lebih Lama Dibandingkan Dengan Lama Waktu Proses Enkripsi.</p>
--	--	--	--	---

BAB III

METODE PENELITIAN

3.1 Tahapan Penelitian

Adapun tahapan penelitian yang dilakukan oleh penulis ini dengan judul Simulasi Pengamanan Text Dalam Proses Enkripsi Dan Deskripsi adalah sebagai berikut:



Gambar 3.1 Tahapan Penelitian

3.2 Metode Pengumpulan Data

Pengumpulan data adalah pencarian terhadap sesuatu karena ada perhatian dan keinginan terhadap hasil suatu aktivitas. Metode pengumpulan data dalam penulisan ini dibagi menjadi 3, yaitu :

1. Wawancara (*Interview*).

Wawancara ini dilakukan dengan cara mengadakan komunikasi langsung dengan dosen pengampu mata kuliah keamanan data di Universitas Pembangunan Pancabudi Medan yang dapat memberikan informasi dan data-data yang diperoleh mengenai keamanan data dan *Vigenere chipper*.

2. Pengamatan (*Observation*)

Penulis melakukan pengamatan langsung pada setiap penggunaan aplikasi chatting yang sudah ada seperti WA, BBM dan Line untuk mengamati proses keamanan yang sudah dibuat sebelumnya.

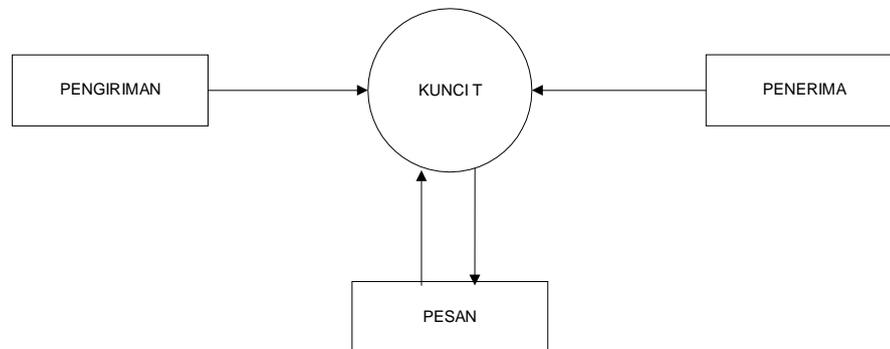
3. Penelitian Kepustakaan (*Library Research*)

Merupakan cara untuk mencari referensi dengan mengumpulkan bahan-bahan pustaka yang dilakukan di perpustakaan kampus, maupun perpustakaan umum, juga melakukan pencarian lewat internet, dengan mengunjungi situs-situs seperti *google Book online* yang dapat membantu pembahasan materi.

3.3 Analisa Permasalahan yang Berjalan

Pertukaran data dalam hal ini pesan rahasia berbentuk teks dengan menggunakan metode tradisional yaitu dengan cara bertukar kata kunci tunggal.

Diagram dibawah adalah penggambaran bagaimana pertukaran pesan rahasia menggunakan kunci tunggal terjadi.



Gambar 3.2 Skema Pengiriman Pesan

Pemberitahuan kata kunci dari pengirim ke penerima menggunakan media yang umum digunakan oleh banyak orang.

3.4 Analisa Kelemahan yang Berjalan

1. 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.
2. Pemberitahuan atau pertukaran kata kunci yang dikirimkan oleh pengirim ke penerima memiliki potensi dapat diketahui oleh orang lain sehingga pesan rahasia dapat terbongkar.

3.5 Solusi Pemecahan Masalah

Pemecahan masalah yang penulis lakukan adalah dengan melakukan penerapan metode ini yang didalamnya terdapat Algoritma *Vigenere Cipher*. Penggunaan metode ini dapat digunakan sebagai solusi agar pengirim dan

penerima tidak lagi harus bertukar kunci tunggal untuk membuka pesan melainkan dapat memiliki kata kunci masing-masing.

Tabel 3.1 Tabel Perencanaan Rancangan

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 Kebutuhan Sistem

Analisis kebutuhan sistem merupakan analisis yang dibutuhkan untuk menentukan spesifikasi kebutuhan sistem. Spesifikasi ini juga meliputi elemen atau komponen – komponen apa saja yang dibutuhkan untuk sistem yang akan dibangun sampai dengan sistem tersebut diimplementasikan. Analisis kebutuhan ini juga menentukan spesifikasi masukan yang diperlukan sistem, keluaran yang akan dihasilkan sistem dan proses yang dibutuhkan untuk mengolah masukan sehingga menghasilkan suatu keluaran yang diinginkan.

3.6.1. Analisis Perangkat Keras (Hardware)

Perangkat keras minimum yang digunakan untuk membangun Sistem Informasi Penjualan ini adalah

1. Processor berkecepatan 2.0 Ghz
2. RAM 2 Gb
3. Hardisk minimal 10 Gb untuk menyimpan data
4. LAN Card
5. Keyboard dan Mouse
6. Monitor 14.

3.6.2. Analisis Perangkat Lunak (Software)

Untuk mendukung dalam penyimpanan informasi, dibutuhkan suatu fasilitas yang memadai. Yaitu berupa perangkat lunak (software) yang dirancang untuk memudahkan dalam pembangunan dan menjalankan sistem nantinya. Adapun perangkat lunak yang digunakan adalah sebagai berikut :

1. Microsoft Windows 7 , Windows XP sebagai sistem operasi
2. Mozilla Firefox version 3.5 sebagai browser
4. Dreamweaver CS 3 Server 10 sebagai Web Server

3.7 Analisa Proses Sistem Yang Berjalan

Visual basic 2010 akan menjadi sarana untuk menciptakan perangkat lunak ini. Pada analisa proses ini penggunaan digunakan sebagai metode yang didalamnya terdapat kombinasi dari algoritma *Vigenere Cipher*. Algoritma *Vigenere Cipher* digunakan oleh pengirim untuk mengenkripsi pesan yang akan dikirimkan..

Perhitungan secara matematis dilakukan sebagai penggambaran proses yang akan terjadi pada metode ini yang didalamnya terdapat algoritma *Vigenere Cipher*. Berikut tahapannya:

1. Proses Enkripsi Pesan Asli oleh Pengirim

Tahap ini dilakukan dengan menggunakan Algoritma *Vigenere Cipher* yang akan digunakan untuk meng-enkripsi pesan asli (*plaintext*) pengirim.

Diketahui Plaintext “SELAMAT DATANG” dengan kunci “KAMPUS”.

Maka untuk mendapatkan ciphertextnya harus menggunakan penghitungan seperti di bawah ini:

Langkah Pertama membuat tabel konversi ASCII.

Ciphertext : SELAMAT DATANG

Kunci : KAMPUS

Penerima memilih kata KAMPUS sebagai kunci yang akan ia gunakan untuk melakukan proses enkripsi menggunakan Algoritma Vigenere Cipher, sehingga pada prosesnya kata KAMPUS akan mengikuti banyak karakter ciphertext 1 yang didapat.

Ciphertext : SELAMAT DATANG

Kunci : KAMPUS

Selanjutnya akan di enkripsi dengan formula Algoritma Vigenere Cipher yaitu:

$$C = P + K \text{ mod } 255$$

Dalam hal ini plaintext adalah ciphertext 1 yang didapat.

$$\begin{aligned} C1 &= S + K \text{ mod } 255 \\ &= 83 + 75 \text{ mod } 255 \\ &= 158 = \text{ž} \end{aligned}$$

$$\begin{aligned} C2 &= E + A \text{ mod } 255 \\ &= 69 + 65 \text{ mod } 255 \\ &= 134 = \text{†} \end{aligned}$$

$$\begin{aligned} C3 &= L + M \text{ mod } 255 \\ &= 76 + 77 \text{ mod } 255 \\ &= \text{TM} \end{aligned}$$

$$\begin{aligned} C4 &= A + P \text{ mod } 255 \\ &= 65 + 80 \text{ mod } 255 \\ &= 145 = \text{‘} \end{aligned}$$

$$C5 = M + U \text{ mod } 255$$

$$= 77 + 85 \pmod{255}$$

$$= 162 = \text{¢}$$

$$C6 = A + S \pmod{255}$$

$$= 65 + 83 \pmod{255}$$

$$= 148 = \text{”}$$

$$C7 = T + K \pmod{255}$$

$$= 84 + 75 \pmod{255}$$

$$= 159 = \text{ÿ}$$

$$C8 = D + A \pmod{255}$$

$$= 68 + 65 \pmod{255}$$

$$= 133 = \text{a}$$

$$C9 = A + M \pmod{255}$$

$$= 65 + 77 \pmod{255}$$

$$= 142 = \text{‘}$$

$$C10 = T + P \pmod{255}$$

$$= 84 + 80 \pmod{255}$$

$$= 164 = \text{‘}$$

$$C11 = A + U \pmod{255}$$

$$= 65 + 85 \pmod{255}$$

$$= 150 = \text{©}$$

$$C12 = N + S \pmod{255}$$

$$= 78 + 83 \pmod{255}$$

$$= 161 = \text{”}$$

$$\begin{aligned}
 C_{13} &= G + K \text{ mod } 255 \\
 &= 71 + 74 \text{ mod } 255 \\
 &= 145 = \text{TM}
 \end{aligned}$$

Sehingga ciphertext kedua yang didapat adalah:

$$\text{Ciphertext} = \text{z}^{\text{TM}} \text{c}^{\text{TM}} \text{Y}^{\text{TM}} \text{a}^{\text{TM}} \text{c}^{\text{TM}}$$

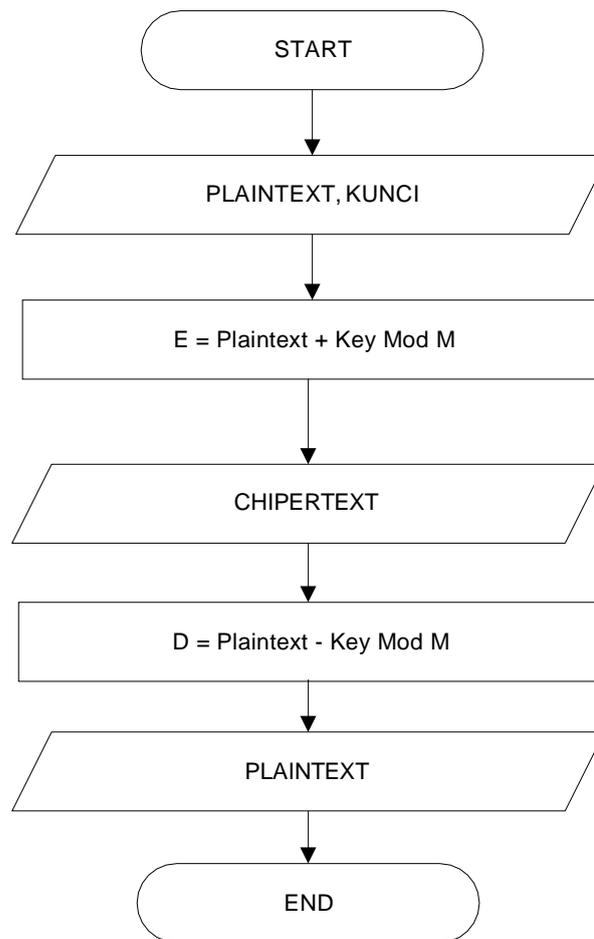
3.8 Flowchart Sistem

Flowchart merupakan langkah awal pembuatan program. Dengan adanya flowchart urutan proses kegiatan menjadi lebih jelas. Bila terdapat penambahan proses maka dapat dilakukan lebih mudah. Setelah flowchart selesai disusun, selanjutnya pemrogram (programmer) menerjemahkannya ke bentuk program dengan bahasa pemrograman.

Flowchart merupakan urutan-urutan langkah kerja suatu proses yang digambarkan dengan menggunakan simbol - simbol yang disusun secara sistematis. (Iswandy, 2015)

3.9 Flowchart Vigenere Cipher

Flowchart Vigenere Cipher yang digunakan oleh pengirim untuk mengenkripsi dan mendeskripsi plaintext hingga mendapatkan ciphertext digambarkan sebagai berikut:

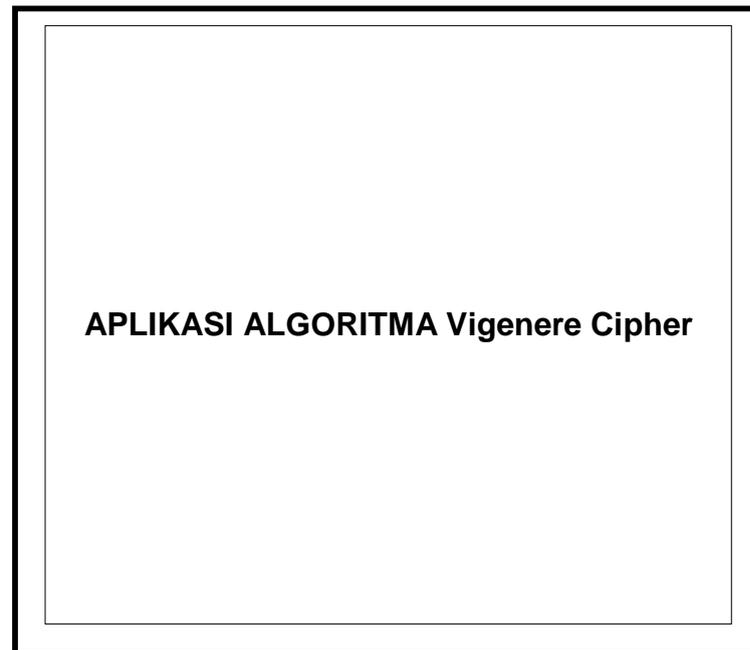


Gambar 3.3 Flowchart Vigenere Cipher

3.10 Perancangan Antarmuka

1. Rancangan Halaman Judul

Halaman judul merupakan halaman yang pertama muncul pada saat program dijalankan

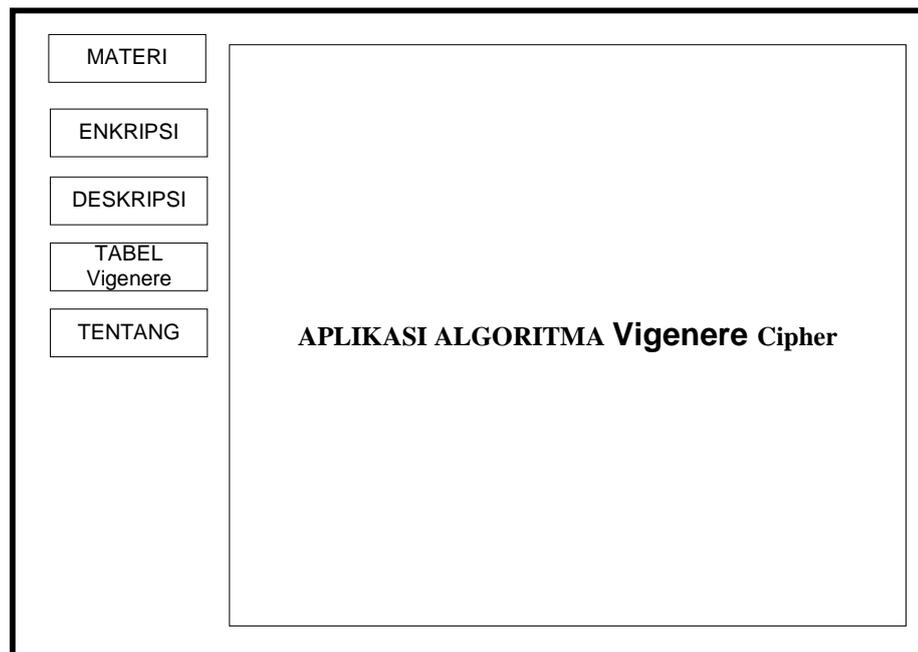


Gambar 3.4 Rancangan Halaman Judul

Pada rancangan di atas akan menampilkan judul yang kemudian akan pindah ke form menu utama dengan menggunakan timer.

2. Rancangan Halaman Menu Utama

Form ini berisi tombol-tombol seperti menu Materi, Enkripsi, Deskripsi, tentang, dan Keluar.



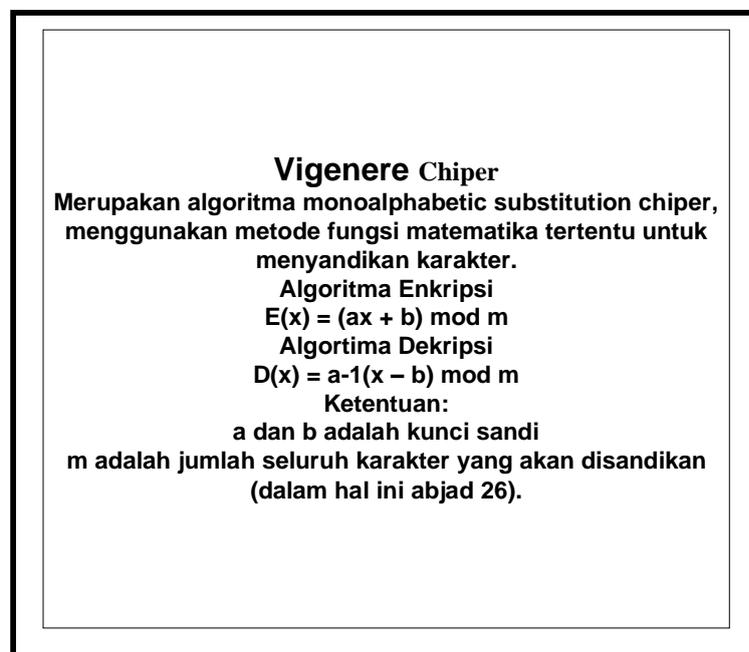
Gambar 3.5 Rancangan Halaman Menu Utama

Pada tampilan di atas terdapat 5 tombol yaitu Materi, Enkripsi, Deskripsi, Tabel Vigenere, Tentang dan keluar.

- Tombol Materi berfungsi untuk menghubungkan pengguna ke form materi.
- Tombol Enkripsi berfungsi untuk menghubungkan pengguna ke form Enkripsi.
- Tombol Deskripsi berfungsi untuk menampilkan form Deskripsi.
- Tombol Tentang berfungsi untuk menghubungkan pengguna ke form tentang.
- Tombol Keluar berfungsi untuk keluar dari program.

3. Rancangan Halaman Materi

Form ini digunakan untuk menjelaskan cara kerja penyandian, dimulai dari plaintext kemudian kunci yang dikonversikan dalam bentuk angka. Setelah itu dilakukan proses penjumlahan dan jika hasil penjumlahan maka akan dikurangi 6 lalu hasilnya akan dikembalikan lagi ke dalam bentuk huruf.



Gambar 3.6 Rancangan Halaman Materi

4. Rancangan Halaman Enkripsi

Berisi penjelasan mengenai Enkripsi. Pengguna memasukkan tulisan asli atau *plaintext* ke dalam tombol masukan *plaintext* kemudian dimasukkan juga kunci. Setelah itu, ditekan tombol Proses Enkripsi yang kemudian akan menampilkan ciphertext atau tulisan yang telah disandikan.

The wireframe shows a rectangular box with a black border. At the top left, the title 'ENKRIPSI' is written. Below it, there are two input fields: 'PLAIN TEXT' on the left and 'KUNCI' on the right. Below the 'PLAIN TEXT' field is a large rectangular area labeled 'CHIPER TEXT'. To the right of this area is a button labeled 'PROSES'.

Gambar 3.7 Rancangan Halaman Enkripsi

5. Rancangan Halaman Deskripsi

Berisi penjelasan mengenai Enkripsi. Pengguna memasukkan tulisan asli atau *plaintext* ke dalam tombol masukan *plaintext* kemudian dimasukkan juga kunci. Setelah itu, ditekan tombol Proses Enkripsi yang kemudian akan menampilkan ciphertext atau tulisan yang telah disandikan.

The wireframe shows a rectangular box with a black border. At the top left, the title 'DESKRIPSI' is written. Below it, there are two input fields: 'CHIPER TEXT' on the left and 'KUNCI' on the right. Below the 'KUNCI' field is a large rectangular area labeled 'PLAIN TEXT'. To the right of this area is a button labeled 'PROSES'.

Gambar 3.8 Rancangan Halaman Deskripsi

Pada gambar di atas terdapat kotak input Deskripsi berfungsi untuk memasukkan tulisan yang telah disandikan. Kemudian terdapat tombol Proses Deskripsi untuk mengembalikan ke tulisan asli jika kunci yang dimasukkan sama dengan kunci pada saat penggunaan plaintext.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Implementasi Sistem

Tahap implementasi sistem merupakan tahap dimana aplikasi yang telah dirancang dijalankan. Tahap ini menunjukkan apakah setiap proses dapat berjalan dengan baik dan mampu memberikan hasil yang diharapkan. Proses perancangan aplikasi menggunakan *visual basic NET 2010* ditampilkan dalam bentuk form-form yang menjadi sarana bagi pengguna untuk melakukan proses implementasi.

4.2 Pengujian Sistem

Pengujian sistem dilakukan untuk menunjukkan apakah sistem yang telah dirancang dapat berjalan sesuai harapan. Selain itu tujuan pengujian adalah untuk dapat menemukan kesalahan fungsi pada aplikasi yang dibangun dan memperbaikinya.

Pengujian dilakukan dengan memasukkan karakter atau huruf dari file berformat .txt selanjutnya diproses oleh aplikasi apakah aplikasi tersebut dapat memberikan hasil yang sesuai. Proses yang akan dilakukan pengujian dalam aplikasi ini adalah simulasi pengiriman pesan dengan menggunakan metode algoritma vigenere antara pengirim kepada penerima dengan kunci yang dimiliki masing-masing pihak tanpa perlu bertukar kunci tunggal hingga pada akhirnya pesan asli yang dikirimkan oleh pengirim dapat dibaca oleh penerima .

4.2.1 Tampilan Awal/ Home

Tampilan pada gambar dibawah merupakan tampilan awal ketika aplikasi dijalankan. Pada form ini pengguna dapat memilih untuk membuka beberapa form lainnya seperti tombol tentang yang akan mengarahkan pengguna menuju form yang menjelaskan profil aplikasi ini, tombol materi dan tombol pengaturan yang akan mengarahkan pengguna ke form yang menjelaskan tata cara penggunaan dari aplikasi ini.



Gambar 4.1. Tampilan Awal/ Home

4.2.2 Tampilan Halaman Judul

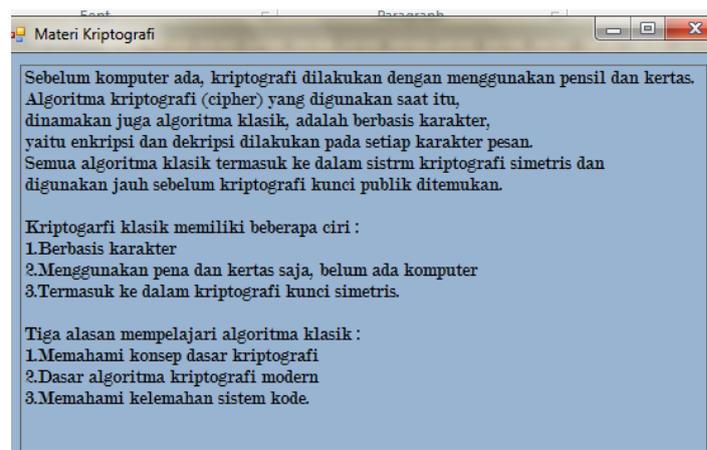
Tampilan berikut ini menampilkan halaman atau form yang berisi tentang profil dari aplikasi ini. Di dalamnya terdapat judul dari aplikasi beserta maksud dari pembuatannya beserta nama dan nomor pokok mahasiswa penulis.



Gambar 4.2. Tampilan Halaman Judul

4.2.3 Tampilan Materi

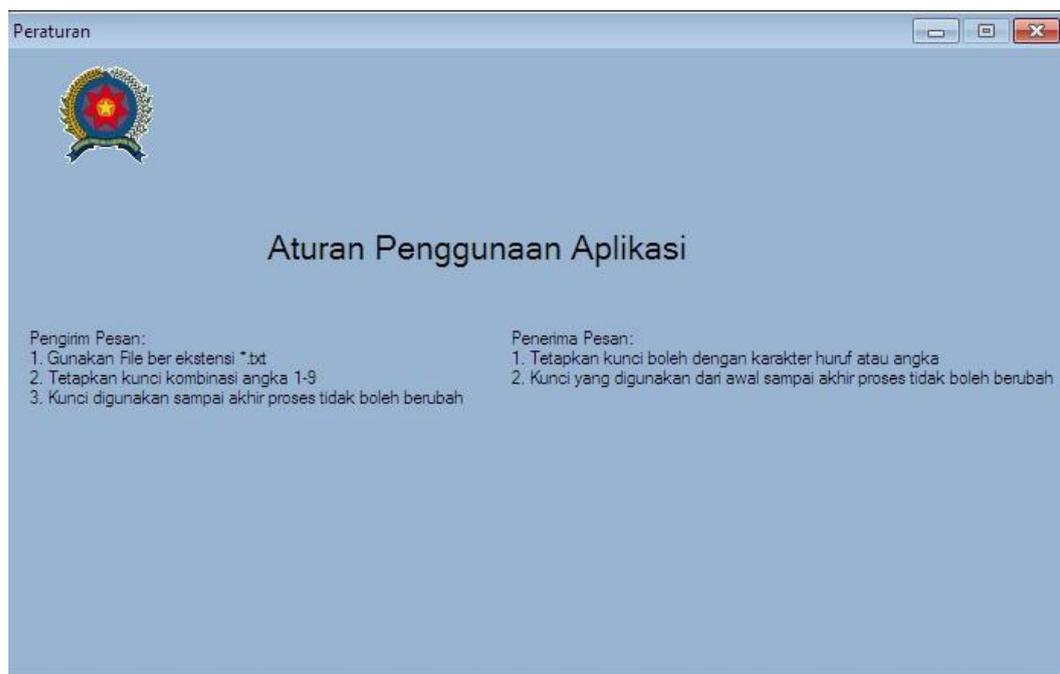
Tampilan materi merupakan tampilan halaman atau form yang berisi tentang materi yang dijalankan. Pada halaman tersebut dijelaskan apa-apa saja yang menjadi kewajiban bagi pengirim dan penerima saat menjalankan simulasi algoritma vigenere.



Gambar 4.3. Tampilan Materi

4.2.4 Tampilan Aturan Penggunaan Aplikasi

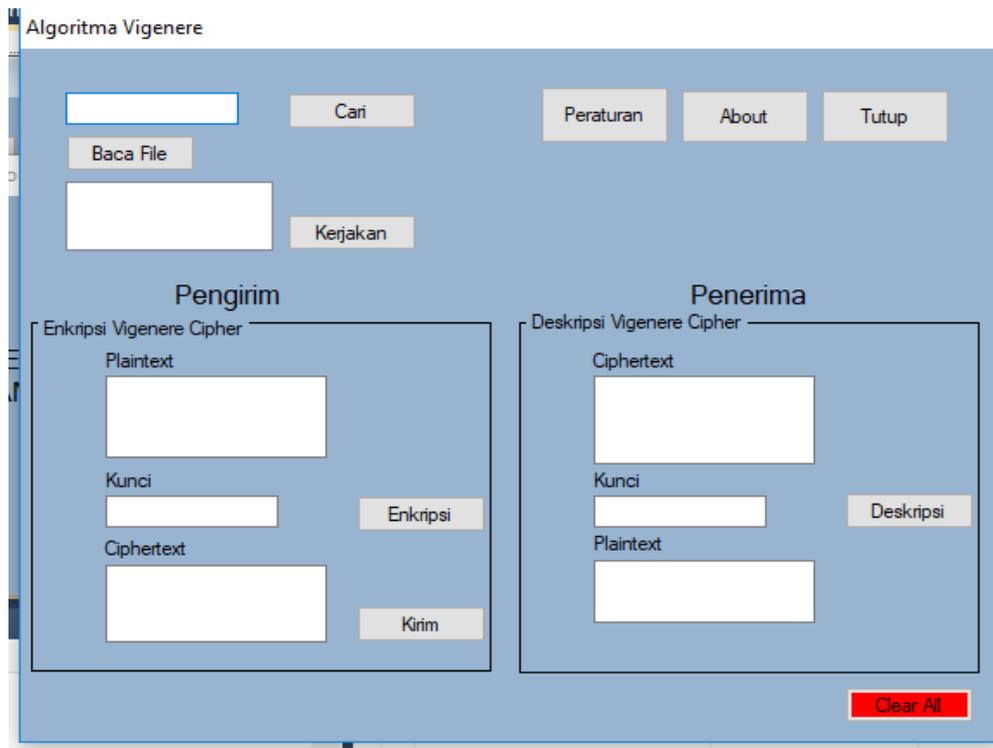
Tampilan aturan penggunaan aplikasi merupakan tampilan halaman atau form yang berisi tentang tata cara penggunaan aplikasi yang dijalankan. Pada halaman tersebut dijelaskan apa-apa saja yang menjadi kewajiban bagi pengirim dan penerima saat menjalankan simulasi algoritma vigenere.



Gambar 4.4. Tampilan Aturan Penggunaan Aplikasi

4.2.5 Tampilan Halaman Utama Algoritma Vigenere

Tampilan berikut merupakan tampilan utama pada aplikasi ini. Algoritma vigenere merupakan protokol yang menjamin tidak adanya pertukaran kunci antara pihak-pihak yang melakukan enkripsi dan dekripsi. Kedua belah pihak menggunakan kunci mereka masing-masing untuk mengenkripsi pesan dan kemudian untuk mendekripsi pesan tanpa perlu mengetahui kunci yang lainnya



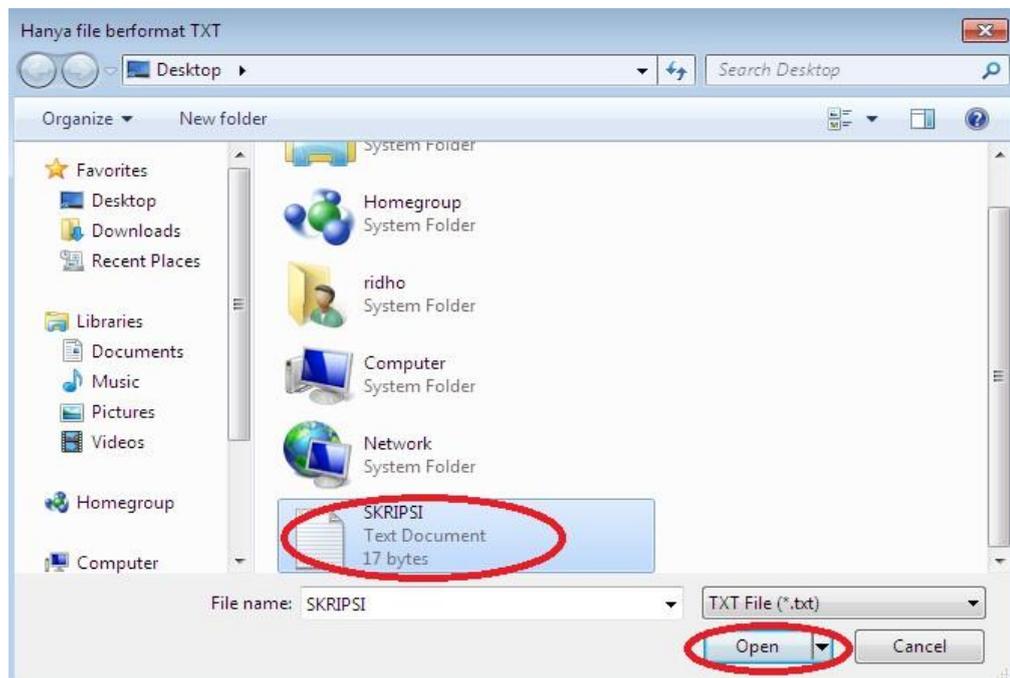
Gambar 4.5. Tampilan Halaman Utama Algoritma Vigenere

Uji coba pada system aplikasi ini dilakukan dengan memasukkan input teks yang bersumber dari file berekstensi *.txt ,dengan menggunakan tombol pencarian yang berada disisi kanan atas.



Gambar 4.6. Tombol Pencarian Data

Pengguna kemudian akan diarahkan menuju direktori file berekstensi *.txt tersebut berada.



Gambar 4.7. Tampilan Memilih File

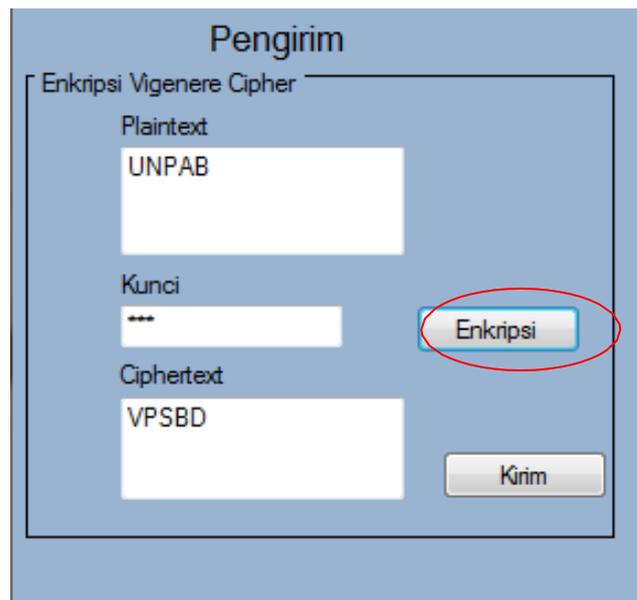
Setelah mendapatkan file berekstensi *.txt yang diinginkan pengguna akan diarahkan kembali ke halaman algoritma vigenere. Kemudian pengguna dapat menekan tombol buka file untuk menampilkan isi dari file *.txt tersebut kedalam listbox yang tersedia.



Gambar 4.8. Tampilan Tombol Baca File

Otomatis rangkaian karakter tersebut akan berpindah ke textbox yang berada dibawahnya. Pada tahap awal rangkaian karakter akan berada di sisi bagian

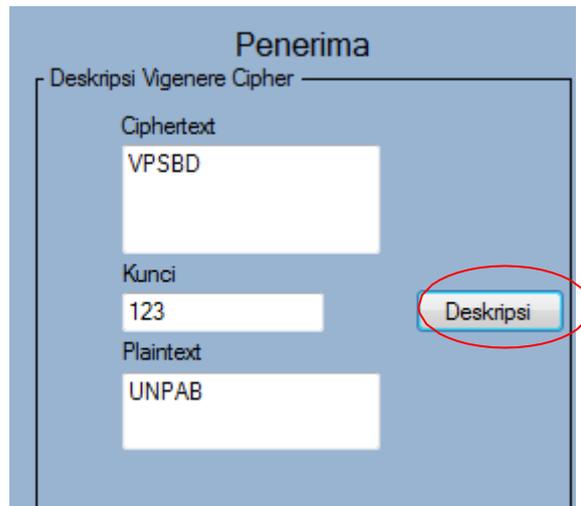
pengirim yang akan mengeksekusi rangkaian karakter tersebut untuk diubah menjadi ciphertext menggunakan Algoritma Vigenere Cipher. Untuk dapat mengeksekusi dibutuhkan kunci yang hanya dapat diisi karakter angka dari 0 sampai 9.



The image shows a software interface for Vigenere Cipher encryption. The title is 'Pengirim'. Below the title is a section titled 'Enkripsi Vigenere Cipher'. Inside this section, there are three text input fields: 'Plaintext' containing 'UNPAB', 'Kunci' containing '***', and 'Ciphertext' containing 'VPSBD'. To the right of the 'Kunci' field is a button labeled 'Enkripsi', which is circled in red. Below the 'Ciphertext' field is a button labeled 'Kirim'.

Gambar 4.9. Tampilan Enkripsi dengan Algoritma Vigenere

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 dibawahnya. Tombol kirim yang ditekan oleh penerima berfungsi untuk meneruskan pesan kembali pada pengirim. Selanjutnya ciphertext yang merupakan enkripsi dari ciphertext yang diterima dari pengirim akan diteruskan ke pengirim.



Gambar 4.10. Tampilan Deskripsi Vigenere Cipher

Aplikasi ditutup dengan menekan tombol tutup yang terdapat disisi kanan atas. Tombol tutup tersebut akan mengarahkan pengguna untuk kembali pada form awal.



Gambar 4.11. Tampilan Tombol Tutup

Selanjutnya setelah pengguna kembali ke halaman awal dari aplikasi ini. Pengguna dapat mengakhiri aplikasi dengan menekan tombol keluar yang terdapat pada pojok kanan atas.

4.3 Validasi Sistem

- a. Hasil Perhitungan Manual Proses Enkripsi.

Tabel 4.1. Tabel Konversi Huruf Ke Angka

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Pada tabel diatas berfungsi untuk memindahkan huruf dalam bentuk angka. Langkah kedua membuat sebuah tabel yang bertujuan memindahkan huruf ke dalam bentuk angka.

Plaintext	U	N	P	A	B
	20	13	15	0	1

Langkah selanjutnya, masukan kunci "1 2 3"

Plaintext	U	N	P	A	B
	20	13	15	0	1
Key	1	2	3	1	2

Pada baris tabel yang ketiga, kunci dimasukan berulang sampai cell pada tabel terpenuhi. Pada langkah selanjutnya dilakukan penjumlahan antara baris

kedua dan ketiga. Jika hasil penjumlahan melebihi 25, maka hasil penjumlahan dikurangi 26 dimana jumlah alfabet ada 26.

Plaintext	U	N	P	A	B
	20	13	15	0	1
Key	1	2	3	1	2
Kode CT	21	15	18	1	3

Setelah dilakukan penjumlahan maka langkah terakhir adalah mengembalikan hasil nilai angka ke dalam bentuk huruf.

Perhitungan aplikasi

The image shows a software application window titled "Pengirim" (Sender) for "Enkripsi Vigenere Cipher". It contains three text input fields: "Plaintext" with the value "UNPAB", "Kunci" (Key) with the value "***", and "Ciphertext" with the value "VPSBD". To the right of the "Kunci" field is a blue button labeled "Enkripsi". Below the "Ciphertext" field is a grey button labeled "Kirim".

Perhitungan manual

ENKRIPSI	Plaintext	U	N	P	A	B
		20	13	15	0	1
	Key	1	2	3	1	2
	Kode CT	21	15	18	1	3
	Chipertext	V	P	S	B	D

Maka diketahui ciphertext dari plaintext "UNPAB" dengan kunci "BCD" adalah VPSBD.

Kesimpulan : Berdasarkan proses enkripsi menggunakan aplikasi dan proses perhitungan manual, hasil yang didapat yaitu: proses yang diaplikasi sama dengan hasil yang ada pada perhitungan manual.

- b. Hasil perhitungan manual proses deskripsi.

Setelah dienkripsi, maka *plaintext* "UNPAB" akan berubah menjadi "VPSBD" berdasarkan kunci yang telah ditetapkan.

Chipertext	V	P	S	B	D
	21	15	17	1	3

Kunci yang diinputkan adalah sebagai berikut.

Chipertext	V	P	S	B	D
	21	15	17	1	3
Key	1	2	3	1	2

Berdasarkan langkah diatas maka diperoleh hasil sebagai berikut.

Chipertext	V	P	S	B	D
	21	15	17	1	3
Key	1	2	3	1	2
Kode PT	20	13	14	0	1

Setelah dilakukan perjumlahan dari enkripsi ke dekripsi maka hasil akhirnya adalah sebagai berikut.

Perhitungan aplikasi

Penerima

Deskripsi Vigenere Cipher

Ciphertext
VPSBD

Kunci
123

Plaintext
UNPAB

Perhitungan manual

DEKRIPSI	Chipertext	V	P	S	B	D
		21	15	17	1	3
	Key	1	2	3	1	2
	Kode PT	20	13	14	0	1
	Plaintext	U	N	P	A	B

Kesimpulan:

Berdasarkan proses deskripsi menggunakan aplikasi dan proses perhitungan manual, hasil yang didapat yaitu: proses yang diaplikasi sama dengan hasil yang ada pada perhitungan manual.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan pembahasan dalam perancangan Penerapan Algoritma *Vigenere Cipher* dalam Meningkatkan Keamanan Data, maka dapat diambil kesimpulan sebagai berikut :

1. Perangkat lunak ini dirancang untuk menampilkan simulasi pengiriman pesan berekstensi yang diinputkan kedalam textbox antara pengirim dan penerima.
2. Pengirim mengirimkan pesan menggunakan dua kunci yang ditentukan sendiri oleh pengirim.
3. Penerima pesan menggunakan kunci yang diberikan oleh pengirim pesan, agar bisa membuka pesan asli yang dikirimkan oleh pengirim.

5.2 Saran

Adapun saran-saran yang dapat dilakukan penelitian ataupun pengembangan selanjutnya adalah sebagai berikut:

1. Diharapkan adanya kombinasi algoritma keamanan data lainnya.
2. Proses pengamanan data yang dilakukan oleh penulis masih menggunakan visual studio, diharapkan ada yang menggunakan diandroid agar bisa digunakan pada mobile.

DAFTAR PUSTAKA

- Anonim, E. H. Rachmawanto and C. A. Sari, "Keamanan File Menggunakan Teknik Kriptografi Shift Cipher," Jurnal Techno. Com, vol. 14, no. 2, pp. 329-335, 2014.
- Barus, S., Sitorus, V. M., Napitupulu, D., Mesran, M., & Supiyandi, S. (2018). Sistem Pendukung Keputusan Pengangkatan Guru Tetap Menerapkan Metode Weight Aggregated Sum Product Assesment (WASPAS). Jurnal Media Informatika Budidarma, 2(2).
- Batubara, Supina. "Analisis perbandingan metode fuzzy mamdani dan fuzzy sugeno untuk penentuan kualitas cor beton instan." IT Journal Research and Development 2.1 (2017): 1-11
- Bishop, Rosdiana, "Sekuritas Sistem Dengan Kriptografi," in Prosiding Sendi_U 2013, Semarang, 2013.
- FACHRI, Barany. Perancangan Sistem Informasi Iklan Produk Halal Mui Berbasis Mobile Web Menggunakan Multimedia Interaktif. Jurasik (Jurnal Riset Sistem Informasi dan Teknik Informatika), 2018, 3: 98-102.
- Fresly, Faizal Zuli1, Ari Irawan, "Implementasi Kriptografi Dengan Algoritma Blowfish dan Riverst Shamir Adleman (RSA) Untuk Proteksi File," Jurnal Format Volume 6 nomor 2 Tahun 2016.
- Gede Angga Pradipta " Penerepan Kombinasi metode Enkripsi Vigenere Cipher Dan Trasposisi Pada Aplikasi Client Server Chatting, " Jurnal Sistem Dan Informatika Vol. 10, Nomor 2, 2016.
- Ginting, G., Fadlina, M., Siahaan, A. P. U., & Rahim, R. (2017). Technical approach of TOPSIS in decision making. Int. J. Recent Trends Eng. Res, 3(8), 58-64.

- Khairul, K., IlhamiArsyah, U., Wijaya, R. F., & Utomo, R. B. (2018, September). Implementasi Augmented Reality Sebagai Media Promosi Penjualan Rumah. In Seminar Nasional Royal (Senar) (Vol. 1, No. 1, pp. 429-434).
- Kurniawan, H. (2018). Pengenalan Struktur Baru untuk Web Mining dan Personalisasi Halaman Web. *Jurnal Teknik dan Informatika*, 5(2), 13-19
- Mayasari, Nova. "Comparison of Support Vector Machine and Decision Tree in Predicting On-Time Graduation (Case Study: Universitas Pembangunan Panca Budi)." *Int. J. Recent Trends Eng. Res* 2.12 (2016): 140-151.
- Nandar Pabokory, Indah Fitri Astuti, Awang Harsa Kridalaksana, " Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *Jurnal Informatika Mulawarman* Vol. 10. Nomor 1, 2015.
- Putera, A., Siahaan, U., & Rahim, R. (2016). Dynamic key matrix of hill cipher using genetic algorithm. *Int. J. Secur. Its Appl*, 10(8), 173-180.
- Putra, Randi Rian, and Cendra Wadisman. "Implementasi Data Mining Pemilihan Pelanggan Potensial Menggunakan Algoritma K Means." *INTECOMS: Journal of Information Technology and Computer Science* 1.1 (2018): 72-77.
- Rahim, R., Supiyandi, S., Siahaan, A. P. U., Listyorini, T., Utomo, A. P., Triyanto, W. A., ... & Khairunnisa, K. (2018, June). TOPSIS Method Application for Decision Support System in Internal Control for Selecting Best Employees. In *Journal of Physics: Conference Series* (Vol. 1028, No. 1, p. 012052). IOP Publishing.
- Ramadhan, A., & Mohd. Awal Hakimi. (2006). *Pemrograman Web Database dengan PHP dan MySQL*. Synergy Media.
- Ramadhan, M., & Nugroho, N. B. (2009). Desain web dengan php. *Jurnal Saintikom*, 6(1).
- Renddy, Teady Matius, Surya Mulyana, Fresly, " Steganografi Dengan Deret Untuk Mengacak Pola Penempatan Pada Rgb," *Jurnal Teknologi Informasi*, 2015.

- Rhee, C. A. Sari, E. H. Rachmawanto, Y. P. Astuti and L. Umaroh, "Optimasi Penyandian File Kriptografi Shift Cipher," in Prosiding Sendi_U 2013, Semarang, 2013.
- Sari, R. D., Supiyandi, A. P. U., Siahaan, M. M., & Ginting, R. B. (2017). A Review of IP and MAC Address Filtering in Wireless Network Security. *Int. J. Sci. Res. Sci. Technol*, 3(6), 470-473.
- Siahaan, A. P. U., Aryza, S., Nasution, M. D. T. P., Napitupulu, D., Wijaya, R. F., & Arisandi, D. (2018). Effect of matrix size in affecting noise reduction level of filtering.
- Siahaan, MD Lesmana, Melva Sari Panjaitan, and Andysah Putera Utama Siahaan. "MikroTik bandwidth management to gain the users prosperity prevalent." *Int. J. Eng. Trends Technol* 42.5 (2016): 218-222.
- Sidik, A. P. (2018). Algoritma RSA dan Elgamal sebagai Algoritma Tambahan untuk Mengatasi Kelemahan Algoritma One Time Pad pada Skema Three Pass Protocol.
- Suriski Sitingjak, Yuli Fauziah, Juwairiah, " Aplikasi Kriptografi File Menggunakan Algoritma Blowfish," *Jurnal Informatika Mulawarman* Vol. 10. Nomor 1, 2015.
- Tasril, V. (2018). Sistem Pendukung Keputusan Pemilihan Penerimaan Beasiswa Berprestasi Menggunakan Metode Elimination Et Choix Traduisant La Realite. *INTECOMS: Journal of Information Technology and Computer Science*, 1(1), 100-109.