



**IMPLEMENTASI PENINGKATAN KEAMANAN PADA  
ALGORITMA VIGENERE CHIPER DENGAN  
TEKNIK XOR**

Disusun dan Diajukan Sebagai Salah Satu Syarat Untuk Menempuh Ujian Akhir  
Memperoleh Gelar Sarjana Komputer pada Fakultas Sains dan Teknologi  
Universitas Pembangunan Panca Budi  
Medan

**SKRIPSI**

**OLEH**

**NAMA : Satria Haryadi Siswantoro**

**NPM : 1414370047**

**PROGRAM STUDI : SISTEM KOMPUTER**

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

**LEMBAR PENGESAHAN**

**IMPLEMENTASI PENINGKATAN KEAMANAN PADA  
ALGORITMA VIGENERE CHIPER DENGAN  
TEKNIK XOR**

Disusun dan Diajukan Sebagai Salah Satu Syarat Untuk Menempuh Ujian Akhir  
Memperoleh Gelar Sarjana Komputer Pada Fakultas Sains dan Teknologi  
Universitas Pembangunan Panca Budi  
Medan

**SKRIPSI**

**OLEH**

**NAMA : SATRIA HARYADI SISWANTORO**  
**N.P.M : 1414370047**  
**PROGRAM STUDI : SISTEM KOMPUTER**

**Diketahui Dan Disetujui Oleh**

**Dosen Pembimbing I**

**Andysah Putera Utama, S.Kom., M.Kom., Ph.D**

**Dosen Pembimbing II**

**Zulham Sitorus, S.Kom., M.Kom**

**Mengetahui,**

**Dekan Fakultas Sains dan Teknologi**

**Sri Shindi Indira, S.T., M.S.C**

**Ketua Program Studi**

**Dr. Muhanamad Iqbal, S.Kom., M.Kom**

## ISURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama : Satria Haryadi Siswantoro  
NPM : 1414370047  
Prodi : Sistem Komputer  
Konsentrasi : Keamanan Jaringan Komputer  
Judul Skripsi : IMPLEMENTASI PENINGKATAN KEAMANAN PADA ALGORITA VIGENERE CHIPPER DENGAN TEKNIK XOR

Dengan ini menyatakan bahwa :

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

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

Medan,

Yang membuat pernyataan



Satria Haryadi Siswanto

Hal : Permohonan Meja Hijau

Medan, 20 Maret 2019  
 Kepada Yth : Bapak/Ibu Dekan  
 Fakultas SAINS & TEKNOLOGI  
 UNPAB Medan  
 Di -  
 Tempat

Telah di terima  
 berkas persyaratan  
 dapat di proses  
 Medan. 28 MAR 2019  
 an KA...  
 NOZAK  
**TEGUH WAHYONO, SE., MM.**

Dengan hormat, saya yang bertanda tangan di bawah ini :

Nama : SATRIA HARYADI SISWANTORO  
 Tempat/Tgl. Lahir : Sei Semayang Dusun 6 Sridadi / 19 Juni 1993  
 Nama Orang Tua : ER SUPARLAN  
 N. P. M : 1414370047  
 Fakultas : SAINS & TEKNOLOGI  
 Program Studi : Sistem Komputer  
 No. HP : 081396374239  
 Alamat : Diski

Datang bermohon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul IMPLEMENTASI PENINGKATAN KEAMANAN PADA ALGORITMA VIGENERE CIPHER DENGAN TEKNIK XOR, Selanjutnya saya menyatakan :

- Melampirkan KKM yang telah disahkan oleh Ka. Prodi dan Dekan
- Tidak akan menuntut ujian perbaikan nilai mata kuliah untuk perbaikan indek prestasi (IP), dan mohon diterbitkan ijazahnya setelah lulus ujian meja hijau.
- Telah tercap 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 dilegalisir 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 lux 2 examplar (1 untuk perpustakaan, 1 untuk mahasiswa) dan jilid kertas jeruk 5 examplar untuk penguji (bentuk dan warna penjilidan diserahkan berdasarkan ketentuan fakultas yang berlaku) dan lembar persetujuan sudah di tandatangani dosen pembimbing, prodi dan dekan
- 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 uang dibebankan untuk memproses pelaksanaan ujian dimaksud, dengan perincian 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. 1.895,000

UK - 50%

20/03/2019  
 Rp. 3.000.000  
 Rp. 1.895.000  
 Ukuran Toga : XL


Diketahui/Ditutupi oleh :  
  
 Sri Shindi Indira, S. P. M. Sc.  
 Dekan Fakultas SAINS & TEKNOLOGI

Hormat saya

  
 SATRIA HARYADI SISWANTORO  
 1414370047

Catatan :

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

Telah Diperiksa oleh LPMU  
 dengan Plagiat % 57  
 20 Maret 2019  
 KAJIPUS  
  
 Cahyo Pramono, SE., MM

ANDA BEBAS PUSTAKA  
 No. 2025/Perp/Bp/2019  
 Dinyatakan tidak ada sangkut  
 paut dengan UPT. Perpustakaan  
 Medan, 28 MAR 2019  
 UPT PERPUSTAKAAN  
  
 Sri Shindi Indira, S. P. M. Sc.

### Plagiarism Detector v. 1079 - Originality Report:

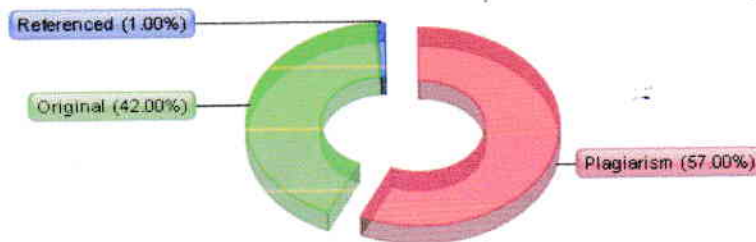
Analyzed document: 2/27/2019 8:41:09 AM

# "SATRIA HARYADI SISWANTORO\_1414370047\_SISTEM KOMPUTER.docx"

Licensed to: Universitas Pembangunan Panca Budi\_License3



Relation chart:



Distribution graph:

Comparison Preset: Rewrite. Detected language: Indonesian

Top sources of plagiarism:

|      |            |   |
|------|------------|---|
| % 27 | wrds: 1666 | <a href="http://repository.usu.ac.id/bitstream/handle/123456789/20100/Chapter%20II.pdf?sequence=4&amp;a...">http://repository.usu.ac.id/bitstream/handle/123456789/20100/Chapter%20II.pdf?sequence=4&amp;a...</a> |
| % 20 | wrds: 1243 | <a href="https://amindadewisutiasih.blogspot.com/2011/04/kryptography-classik-dan-vigenere.html">https://amindadewisutiasih.blogspot.com/2011/04/kryptography-classik-dan-vigenere.html</a>                       |
| % 20 | wrds: 1243 | <a href="http://amindadewisutiasih.blogspot.com/2011/04/kryptography-classik-dan-vigenere.html">http://amindadewisutiasih.blogspot.com/2011/04/kryptography-classik-dan-vigenere.html</a>                         |

Show other Sources:]

Processed resources details:

248 - Ok / 36 - Failed

Show other Sources:]

Important notes:

| Wikipedia: | Google Books: | Ghostwriting services: | Anti-cheating: |
|------------|---------------|------------------------|----------------|
|            |               |                        |                |



# 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 TEKNIK ARSITEKTUR | (TERAKREDITASI) |
| PROGRAM STUDI SISTEM KOMPUTER   | (TERAKREDITASI) |
| PROGRAM STUDI TEKNIK KOMPUTER   | (TERAKREDITASI) |
| PROGRAM STUDI AGROTEKNOLOGI     | (TERAKREDITASI) |
| PROGRAM STUDI PETERNAKAN        | (TERAKREDITASI) |

## PERMOHONAN MENGAJUKAN JUDUL SKRIPSI

Saya yang bertanda tangan di bawah ini :

Nama Lengkap

: SATRIA HARYADI SISWANTORO

Tempat/Tgl. Lahir

: Sei Semayang Dusun 6 Sridadi / 19 Juni 1993

Nomor Pokok Mahasiswa

: 1414370047

Program Studi

: Sistem Komputer

Konsentrasi

: Keamanan Jaringan Komputer

Jumlah Kredit yang telah dicapai

: 139 SKS, IPK 3.18

Dengan ini mengajukan judul skripsi sesuai dengan bidang ilmu, dengan judul:

| No. | Judul SKRIPSI   | Persetujuan                                  |
|-----|---|--|
| 1.  | ANALISIS PERANCANGAN APLIKASI ABSENSI PEGAWAI DI BRITISH LEARNING CENTERE MEDAN BERBASIS LAN  | <input type="checkbox"/>                     |
| 2.  | IMPLEMENTASI PENINGKATAN KEAMANAN PADA ALGORITMA VIGENERE CIPHER DENGAN TEKNIK XOR DAN KUNCI ACAK 1024-BITS DENGAN ALGORITMA BLUM BLUM SHUB | <input checked="" type="checkbox"/> 13/10/18 |
| 3.  | IMPLEMENTASI ALGORITMA ELGAMA UNTUK PENINGKATAN KEAMANAN DATA DENGAN ALGORITMA BLUM BLUM SHUB SEBAGAI PEMBANGKIT BILANGAN ACAK              | <input type="checkbox"/>                     |

3: Judul yang disetujui oleh Kepala Program Studi diberikan tanda



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

Medan, 29 Oktober 2018

Pemohon,  
  
( Satria Haryadi Siswanto )

Nomor : .....  
Tanggal : .....  
Disetujui oleh:  
Dekan  
  
( Sri Shindi Indira, S.T., M.Sc. )

Tanggal : .....  
Disetujui oleh:  
Dosen Pembimbing I :  
  
( Anelysah P. U. Satrio )

Tanggal : 13/03/2018  
Disetujui oleh:  
Ka. Prodi Sistem Komputer  
  
( MUHAMMAD IQBAL, S.Kom., M.Kom. )

Tanggal : .....  
Disetujui oleh:  
Dosen Pembimbing II :



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

: Universitas Pembangunan Panca Budi  
: SAINS & TEKNOLOGI  
bimbing I : ANDISYAH PUTERA Utama S.Kom. M.Kom  
bimbing II : ZULHAM SITOPUS S.Kom. M.Kom  
Pasiswa : SATRIA HARYADI SISWANTORO  
Program Studi : Sistem Komputer  
Nomor Mahasiswa : 1414370047  
Pendidikan : SI  
Jenis Akhir/Skripsi : IMPLEMENTASI PENINGKATAN KEAMANAN PADA ALGORITMA Vigenere Cipher dengan teknik XOR

| BAGAL | PEMBAHASAN MATERI     | PARAF | KETERANGAN |
|-------|-----------------------|-------|------------|
|       | Rusi Judul            |       |            |
|       | Acc Serien Judul      |       |            |
| 1     | Revisi Bab I          |       |            |
| 1     | Rusi Bab II           |       |            |
| k     | Revisi Bab III, IV    |       |            |
| 1/2   | Revisi Bab III, IV, V |       |            |
| 1/2   | Acc Serien            |       |            |
| 1/3   | Acc Judul             |       |            |
| 1     | Acc Judul             |       |            |

Medan, 06 Desember 2018  
Diketahui/Dijetujui oleh :  
Dekan,



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



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

itas : Universitas Pembangunan Panca Budi  
 s : SAINS & TEKNOLOGI  
 Pembimbing I : ANDY SYAH PUTERA UTAMA S.Kom M.Kom  
 Pembimbing II : ZULHAM SITORUS S.Kom M.Kom  
 Mahasiswa : SATRIA HARYADI SISWANTORO  
 Program Studi : Sistem Komputer  
 Pokok Mahasiswa : 1414370047  
 Pendidikan : SI  
 Tugas Akhir/Skripsi : IMPLEMENTASI PENINGKATAN KEAMANAN PADA ALGORITMA VIGENERE CHIPER DENGAN TEKNIK XOR

| NO  | PEMBAHASAN MATERI     | PARAF | KETERANGAN |
|-----|-----------------------|-------|------------|
| 1   | Acc. Revisi Proposal  |       |            |
| 1   | Revisi I, II, III     |       |            |
| 1/1 | Analisa di pergelar   |       |            |
| 1/1 | Pemilihan seni daya   |       |            |
| 1/2 | pendua                |       |            |
| 1/2 | Acc. I, II, III       |       |            |
| 5/2 | Format belu di senile |       |            |
|     | Acc. Revisi           |       |            |

2/3 19. Acc. Sidang muf-lyu

Medan, 06 Desember 2018  
 Diketahui/Disetujui oleh :  
 Dekan,

19. Dec. iild lua







YAYASAN PROF. DR. H. KADIRUN YAHYA  
UNIVERSITAS PEMBANGUNAN PANCA BUDI  
**LABORATORIUM KOMPUTER**

Jl. Jend. Gatot Subroto Km 4,5 Sei Sikambing Telp. 061-8455571  
Medan - 20122

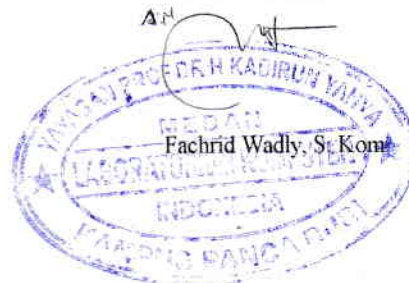
KARTU BEBAS PRAKTIKUM

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

Nama : Satria Haryadi Siswantoro  
N.P.M. : 1414370047  
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, 28 Maret 2019  
Ka. Laboratorium



## **ABSTRAK**

**SATRIA HARYADI SISWANTORO**

### **IMPLEMENTASI PENINGKATAN KEAMANAN PADA ALGORITMA VIGENERE CHIPER DENGAN TEKNIK XOR**

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     |
|--|-------------|
| <b>COVER .....</b>                     |             |
| <b>LEMBAR PENGESAHAN .....</b>         |             |
| <b>ABSTRAK .....</b>                   |             |
| <b>KATA PENGANTAR.....</b>             | <b>i</b>    |
| <b>DAFTAR ISI.....</b>                 | <b>iii</b>  |
| <b>DAFTAR GAMBAR.....</b>              | <b>vi</b>   |
| <b>DAFTAR TABEL.....</b>               | <b>viii</b> |
| <b>BAB I PENDAHULUAN.....</b>          | <b>1</b>    |
| 1. Latar Belakang.....                 | 1           |
| 2. Perumusan Masalah.....              | 3           |
| 3. Batasan Masalah .....               | 3           |
| 4. Tujuan Dan Manfaat Penulisan .....  | 3           |
| 5. Metodologipenelitian.....           | 4           |
| 6. Sistematika Penulisan .....         | 5           |
| <b>BAB II LANDASAN TEORI.....</b>      | <b>6</b>    |
| 1. Aplikasi.....                       | 6           |
| 2. Kriptografi .....                   | 6           |
| 3. Serangan Terhadap Kriptografi ..... | 14          |
| 4. Keamanan Algoritma Kriptografi..... | 19          |

|                |  |           |
|----------------|--|-----------|
| 5.             | Algoritma Kriptografi Klasik .....             | 19        |
| 6.             | UML.....                                       | 21        |
| 7.             | Microsoft Visual Studi .....                   | 27        |
| <b>BAB III</b> | <b>ANALISIS PERANCANGAN SISTEM.....</b>        | <b>30</b> |
| 1.             | Analisis Permasalahan yang pernah ada.....     | 30        |
| 2.             | Analisis Permasalahan.....                     | 31        |
| 3.             | Perancangan Berorientasi Objek .....           | 36        |
| 4.             | Struktur Program .....                         | 40        |
| 5.             | Perancangan Antarmuka.....                     | 40        |
| a.             | Rancangan Halaman Menu Utama.....              | 40        |
| b.             | Rancangan Halaman Materi.....                  | 41        |
| c.             | Rancangan Halaman Enkripsi.....                | 42        |
| d.             | Rancangan Halaman Deskripsi .....              | 43        |
| e.             | Rancangan Halaman About.....                   | 44        |
| <b>BAB IV</b>  | <b>IMPLEMENTASI DAN PENGUJIAN SISTEM .....</b> | <b>45</b> |
| 1.             | Implementasi Sistem .....                      | 45        |
| a.             | Tampilan Menu Utama .....                      | 45        |
| b.             | Tampilan Materi .....                          | 46        |
| c.             | Tampilan Enkripsi.....                         | 46        |
| d.             | Tampilan Deskripsi .....                       | 47        |
| d.             | Tampilan Tentang.....                          | 48        |
| 2.             | Pengujian Sistem.....                          | 48        |

|              |                      |           |
|--------------|----------------------|-----------|
| <b>BAB V</b> | <b>PENUTUP .....</b> | <b>50</b> |
|              | 1. Kesimpulan .....  | 50        |
|              | 2. Saran .....       | 50        |

**DAFTAR PUSTAKA**

**LAMPIRAN**

## DAFTAR GAMBAR

| No  | Judul   | Hal |
|-----|---|-----|
| 1.  | Skema Enkripsi dan Deskripsi Menggunakan Kunci..... | 10  |
| 2.  | Tabel Vigenere.....                                 | 15  |
| 3.  | Actor.....  | 24  |
| 4.  | Use Case Symbol.....                                | 24  |
| 5.  | Asosiasi.....                                       | 24  |
| 6.  | Sistem.....   | 25  |
| 7.  | Objek .....   | 26  |
| 8.  | Lifeline.....                                       | 27  |
| 9.  | Activation.....                                     | 27  |
| 10. | Message.....  | 28  |
| 11. | Sistem Yang Pernah Ada.....                         | 30  |
| 11. | Flowchat Vigenere Chiper.....                       | 31  |
| 12. | Use Case Diagram.....                               | 37  |
| 13. | Activity Diagram.....                               | 38  |
| 14. | Sequence Diagram.....                               | 39  |
| 15. | Struktur Navigasi Enkripsi.....                     | 40  |
| 16. | Rancangan Halaman Menu Utama.....                   | 41  |
| 17. | Rancangan Halaman Materi.....                       | 42  |
| 18. | Rancangan Halaman Enkripsi.....                     | 42  |

|           |                                  |            |
|-----------|----------------------------------|------------|
| 19.       | Rancangan Halaman Deskripsi..... | 43         |
| 21.       | Rancangan Halaman Tentang.....   | 44         |
| <b>No</b> | <b>Judul</b>                     | <b>Hal</b> |
| <hr/>     |                                  |            |
| 22.       | Tampilan Menu Utama.....         | 45         |
| 23.       | Tampilan Materi.....             | 46         |
| 24.       | Tampilan Enkripsi.....           | 47         |
| 25.       | Tampilan Deskripsi.....          | 47         |
| 26.       | Tampilan Tentang.....            | 48         |

## DAFTAR TABEL

| <b>No</b> | <b>Judul</b>  | <b>Hal</b> |
|-----------|---|------------|
| 1.        | Konversi Vigenere Cipher ke Angka .....             | 13         |
| 2.        | Konversi Vigenere Cipher Contoh Ke Angka .....      | 14         |
| 3.        | Tabel konversi Vigenere Cipher Huruf Ke Angka ..... | 34         |



# **BAB I**

## **PENDAHULUAN**

### **1.1 Latar Belakang**

Keamanan data dan informasi merupakan hal yang sangat penting di era informasi saat ini. Umumnya, setiap institusi memiliki dokumen-dokumen penting dan bersifat rahasia yang hanya boleh diakses oleh orang tertentu. Sistem informasi yang dikembangkan harus menjamin keamanan dan kerahasiaan dokumen-dokumen tersebut. Namun kendalanya bahwa media-media yang digunakan sering kali dapat disadap oleh pihak lain. Oleh karena itu, diperlukan metode untuk mengamankannya, salah satunya dengan menggunakan metode *kriptografi*.

Dalam *kriptografi*, penulis ini membuat keamanan pesan menggunakan metode algoritma *vigenere cipher*. Proses pengamanan pesan tersebut hanya berupa text yang dikirim, dan penerima harus memiliki kunci untuk membuka pesan asli. Dengan adanya vigenere ini pesan teks yang muncul berupa hasil dari algoritma tersebut. Saat ini, ilmu kriptografi semakin banyak digunakan dan mulai berubah menjadi kebutuhan. Dengan maraknya perkembangan ilmu dan teknologi, informasi-informasi penting pun tidak lagi hanya berada pada media tulis saja.

Teknik XOR adalah Dalam kriptografi, pembuatan chiper (teks hasil enkripsi) melalui operasi XOR merupakan suatu algoritma enkripsi yang relatif sederhana. Teknik ini beroperasi sesuai dengan prinsip:

$$A \text{ XOR } 0 = A,$$

$$A \text{ XOR } A = 0,$$

$$(B \text{ XOR } A) \text{ XOR } A = B \text{ XOR } 0 = B,$$

Dengan logika ini, suatu string teks dapat diekripsi dengan menerapkan operasi XOR berbasis bit (binary digit) terhadap setiap karakter menggunakan key tertentu. Bagaimana mendekripsi outputnya untuk mendapatkan plaintext kembali? Dengan menerapkan operasi XOR terhadap chiper.

Penulis akan membuat suatu aplikasi penerapan algoritma *vigenere* dengan menggunakan sistem yang berbasiskan desktop. Aplikasi yang akan penulis rancang adalah sebagai penerapan *algoritma vigenere* agar dapat memahami cara teknik enkripsi dan dekripsi data teks yang digunakan kepada pengguna yang masih awam dalam teknik manipulasi data tersebut. Berdasarkan latar belakang diatas maka penulis tertarik untuk memilih judul “**Implementasi Peningkatan Keamanan Pada Algoritma Vigenere Chiper Dengan Teknik XOR**”.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas maka rumusan masalah adalah sebagai berikut :

1. Bagaimana merancang sebuah keamaan menggunakan kriptografi *vigenere chiper* dengan teknik XOR sebagai pengaman informasi teks?
2. Bagaimana membuat aplikasi dengan menerapkan kriptografi sebagai pengamanan aplikasi berbasis *desktop* ?

### **1.3 Batasan Masalah**

Dalam perancangan aplikasi pengamanan informasi ini penulis membatasi masalah sebagai berikut :

1. Aplikasi yang dibangun hanya menampilkan proses melakukan enkripsi dan dekripsi informasi.
2. Perancangan aplikasi merupakan simulasi pengamanan aplikasi.
3. Program yang digunakan dalam perancangan aplikasi ini adalah *visual basic .net 2010* menggunakan algoritma *vigenere cipher* dalam proses pengamanan aplikasi.

### **1.4 Tujuan Penelitian**

Tujuan yang ingin dicapai penulis dalam perancangan aplikasi pengamanan aplikasi adalah :

1. Merancang keamanan aplikasi dengan menerapkan kriptografi dengan menggunakan algoritma *vigenere chiper* dengan teknik XOR.

2. Merancang sistem pengamanan informasi dengan proses enkripsi dan dekripsi menggunakan metode algoritma *vigenere chiper* dengan teknik XOR.

### **1.5 Manfaat Penelitian**

Perancangan aplikasi penerapan *algoritma vigenere* ini bermanfaat bagi masyarakat luas antara lain :

1. Dengan menggunakan aplikasi ini seseorang dapat mengamankan suatu informasi tanpa takut diketahuin oleh orang lain.
2. Dapat digunakan dalam proses kerahasiaan data.
3. Proses pertukaran data atau informasi menjadi aman.

### **1.6 Metodologi Penelitian**

Metode Pengumpulan Data yang digunakan dalam penelitian ini adalah metode deskriptif. Adapun teknik pengumpulan data dilakukan dengan cara sebagai berikut:

1. Studi literature

Pengumpulan data dengan cara mengumpulkan *literature*, jurnal, *paper* dan bacaan-bacaan yang ada kaitannya dengan judul penelitian.

2. Studi Pustaka

Pengumpulan data dengan menggunakan atau mengumpulkan sumber-sumber tertulis, dengan cara membaca, mempelajari dan mencatat hal-hal penting

yang berhubungan dengan masalah yang sedang dibahas guna memperoleh gambaran secara teoritis.

## **1.7 Sistematika Penulisan**

Adapun struktur penulisan pada masing-masing bab dalam laporan tugas akhir ini adalah sebagai berikut:

### **BAB I PENDAHULUAN**

Pada bab ini memaparkan mengenai latar belakang masalah, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, metodologi penelitian dan sistematika penulisan.

### **BAB II LANDASAN TEORI**

Bab ini mengaji teori-teori yang didapat dari sumber-sumber yang relevan untuk digunakan sebagai panduan dalam penelitian serta alat perancangan yang digunakan dalam penyusunan skripsi.

### **BAB III PERANCANGAN SISTEM**

Bab ini membahas perancangan tentang gambaran sistem serta deskripsi dari hasil analisis sistem yang akan dijadikan sebagai petunjuk untuk perancangan sistem selanjutnya.

### **BAB IV IMPLEMENTASI SISTEM**

Bab ini menguraikan langkah-langkah dalam implementasi sistem, disertai dengan komponen-komponen kebutuhan sistem.

## BAB V PENUTUP

Merupakan bab yang memaparkan kesimpulan beserta saran-saran atas penelitian yang dibuat.

## **BAB II**

### **LANDASAN TEORI**

#### **2.1 Aplikasi**

Aplikasi adalah alat bantu untuk mempermudah dan mempercepat proses pekerjaan dan bukan merupakan beban bagi para penggunanya, atau aplikasi adalah satu unit perangkat lunak yang dibuat untuk melayani kebutuhan akan beberapa aktivitas seperti sistem perniagaan, *game*, pelayanan masyarakat, periklanan, atau semua proses yang hampir dilakukan manusia. Aplikasi berguna untuk melakukan pengolahan data maupun kegiatan-kegiatan seperti pembuatan dokumen atau pengolahan data. Aplikasi adalah bagian PC yang berinteraksi langsung dengan *user*. Aplikasi berjalan di atas sistem operasi, sehingga agar aplikasi bisa diaktifkan perlu melakukan instalasi sistem operasi terlebih dahulu.

#### **2.2 Kriptografi**

##### **a. Pengertian Kriptografi**

*Kriptografi* berasal dari bahasa Yunani, *crypto* dan *graphia*. *Crypto* berarti secret (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut terminologinya, *Kriptografi* adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. Dalam perkembangannya, *Kriptografi* juga digunakan untuk mengidentifikasi

pengiriman pesan dan tanda tangan digital dan keaslian pesan dengan sidik jari digital. (*Dony Ariyus, 2005*)

Di dalam *Kriptografi* kita akan sering menemukan berbagai istilah atau terminology. Beberapa istilah yang harus diketahui yaitu :

1) Pesan, *Plaintext*, dan *Cipherteks*

Pesan (*message*) adalah data atau inFormasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah (*Plaintext*) atau teks jelas (*cleartext*). Agar pesan tidak dapat dimengerti maknanya oleh pihak lain yang tidak berkepentingan, maka pesan perlu disandikan ke bentuk lain yang tidak dapat dipahami. Bentuk pesan yang tersandi disebut *Cipherteks* atau kriptogram. *Cipherteks* harus dapat ditransFormasikan kembali menjadi *Plaintext* semula agar dapat diterima dan bisa dibaca.

2) Pengirim dan penerima

Komunikasi data melibatkan pertukaran pesan antara dua *entitas*. Pengirim (*sender*) adalah *entitas* yang mengirim pesan kepada *entitas* lainnya. Penerima (*receiver*) adalah *entitas* yang menerima pesan. Pengirim tentu menginginkan pesan dapat dikirim secara aman, yaitu pengirim yakin bahwa pihak lain tidak dapat membaca isi pesan yang dikirim. Solusinya adalah dengan cara menyandikan pesan menjadi *Cipherteks*.

3) Enkripsi dan dekripsi



Proses menyandikan *Plainteks* menjadi *Cipherteks* disebut enkripsi (*encryption*) atau *enCiphering*. Sedangkan proses mengembalikan *Cipherteks* menjadi *Plainteks* disebut dekripsi (*decryption*) atau *deCiphering*.

#### 4) *Cipher* dan kunci

Algoritma kriptografi disebut juga *Cipher*, yaitu aturan untuk enkripsi dan dekripsi, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Beberapa *Cipher* memerlukan algoritma yang berbeda untuk *enCiphering* dan *deCiphering*.

Konsep matematis yang mendasari algoritma *Kriptografi* adalah relasi antara dua buah himpunan yang berisi elemen – elemen *Plainteks* dan himpunan yang berisi *Cipherteks*. Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen- elemen antara dua himpunan tersebut. Misalkan  $P$  menyatakan *Plainteks* dan  $C$  menyatakan *Cipherteks*, maka fungsi enkripsi  $E$  memetakan  $P$  ke  $C$ .

$$E(P) = C$$

Dan fungsi dekripsi  $D$  memetakan  $C$  ke  $P$

$$D(C) = P$$

Karena proses enkripsi kemudian dekripsi mengembalikan pesan ke pesan semula, maka kesamaan berikut harus benar,

$$D(E(P)) = P$$

*Kriptografi* mengatasi masalah keamanan data dengan menggunakan kunci, yang dalam hal ini algoritma tidak dirahasiakan lagi, tetapi kunci harus tetap dijaga kerahasiaannya. Kunci (*key*) adalah parameter yang digunakan untuk transformasi *enCiphering* dan *deCiphering*. Kunci biasanya berupa string atau deretan bilangan. Dengan menggunakan  $K$ , maka fungsi enkripsi dan dekripsi dapat ditulis sebagai :

$$E_K(P)=C \text{ dan } D_K(C)=P$$

Dan kedua fungsi ini memenuhi

$$D_K(E_K(P))=P$$

Keterangan :

$P = \text{Plainteks}$

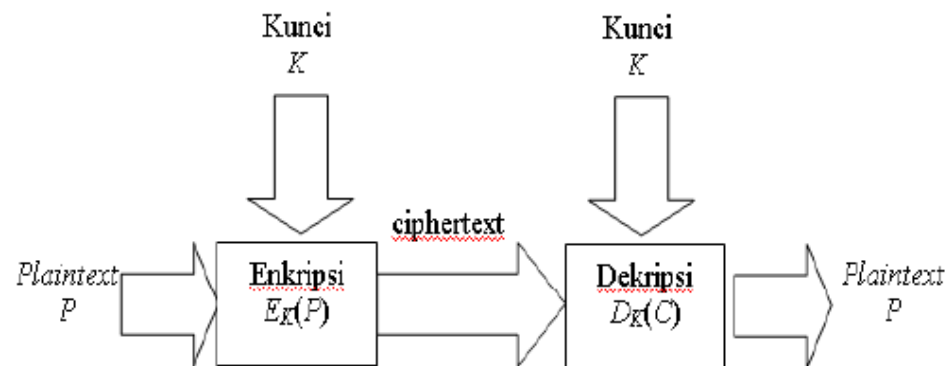
$C = \text{Cipherteks}$

$K = \text{kunci}$

$EK = \text{proses enkripsi menggunakan kunci } K$

$DK = \text{proses dekripsi menggunakan kunci } K$

Skema enkripsi dengan menggunakan kunci diperlihatkan pada gambar dibawah ini :



**Gambar 2.1** Skema enkripsi dan dekripsi dengan menggunakan kunci

Gambar di atas menjelaskan bahwa *Plaintext* (tulisan asli) disandikan menggunakan kunci sehingga muncul sebagai *Ciphertext*. Kemudian tulisan dideskripsikan untuk mendapatkan tulisan asli atau *Plaintext*.

#### 5) Sistem Kriptografi

*Kriptografi* membentuk sebuah sistem yang dinamakan sistem *Kriptografi*. *Sistem Kriptografi* (*cryptosystem*) adalah kumpulan yang terdiri dari algoritma *Kriptografi*, semua *Plainteks* dan *Cipherteks* yang mungkin, dan kunci. Di dalam *Kriptografi*, *Cipher* hanyalah salah satu komponen saja.

#### 6) Penyadap

penyadap (*eavesdropper*) adalah orang yang mencoba menangkap pesan selama ditransmisikan. Tujuan penyadap adalah untuk mendapatkan informasi sebanyak - banyaknya mengenai sistem *Kriptografi* yang digunakan untuk berkomunikasi dengan maksud untuk memecahkan

*Cipherteks*. Nama lain penyadap : *enemy, adversary, intruder, interceptor, bad guy*.

#### 7) Kriptanalisis dan kriptologi

*Kriptografi* berkembang sedemikian rupa sehingga melahirkan bidang yang berlawanan yaitu kriptanalisis. *Kriptanalisis ( cryptanalysis)* adalah ilmu dan seni untuk memecahkan *Cipherteks* menjadi *Plainteks* tanpa mengetahui kunci yang digunakan. Pelakunya disebut kriptanalisis. Jika seorang kriptografer (*cryptographer*) mentransFormasikan *Plainteks* menjadi *Cipherteks* dengan suatu algoritma dan kunci maka sebaliknya seorang kriptanalisis berusaha untuk memecahkan *Cipherteks* tersebut untuk menemukan *Plainteks* atau kunci. Kriptologi (*cryptology*) adalah studi mengenai *Kriptografi* dan kriptanalisis.

#### b. Tujuan *Kriptografi*

Dari paparan awal dapat dirangkumkan bahwa *Kriptografi* bertujuan untuk memberi layanan keamanan. Yang dinamakan aspek – aspek keamanan sebagai berikut :

##### 1. Kerahasiaan (*confidentiality*)

Adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak – pihak yang tidak berhak. Di dalam *Kriptografi* layanan ini direalisasikan dengan menyandikan *Plainteks* menjadi *Cipherteks*. Misalnya pesan “harap datang pukul 8” disandikan menjadi

“trxC#45motyptre!%”. istilah lain yang senada dengan confidentiality adalah *secrecy* dan *privacy*.

2. Integritas data (*data integrity*)

Adalah layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman. Dengan kata lain, aspek keamanan ini dapat diungkapkan sebagai pertanyaan: “ apakah pesan yang diterima masih asli atau tidak mengalami perubahan (modifikasi)?”.

3. Otentikasi (*authentication*)

Adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak – pihak yang berkomunikasi ( *user autehentication*). Dua pihak yang saling berkomunikasi harus dapat mengotentikasi satu sama lain sehingga ia dapat memastikan sumber pesan.

4. *Non-Repudiation*

Adalah layanan untuk menjaga *entitas* yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

c. *Vigenere Cipher*

Teknik dari substitusi *Vigenere* dapat dilakukan dengan dua cara:

1. Angka

Teknik substitusi *Vigenere* dilakukan menggunakan angka dengan menukarkan huruf dengan angka.

**Tabel 2.1** Konversi *Vigenere* ke Angka

|   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 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 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Algoritma *Vigenere* dengan teknik angka menggunakan tabel pemindahan huruf ke angka dimana huruf yang dimulai dari huruf A akan dipindahkan menjadi angka 0. Sementara huruf B menjadi angka 1 dan selanjutnya akan berakhir pada angka 25.

Contoh :

*Plaintext* : *This cyptosystem is not secure*

Kunci : *Cipher*

Maka untuk mendapatkan *Ciphertextnya* adalah tulisan *Plaintext* diubah ke dalam bentuk angka seperti pada tabel konversi di bawah ini

**Tabel 2.2** Konversi *Vigenere* Contoh Ke Angka

|    |    |    |    |   |    |    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|---|----|----|----|----|----|----|----|----|----|----|----|
| T  | H  | I  | S  | C | R  | Y  | P  | T  | O  | S  | Y  | S  | T  | E  | M  |
| 19 | 7  | 8  | 18 | 2 | 17 | 24 | 25 | 19 | 14 | 18 | 24 | 18 | 19 | 4  | 12 |
| 2  | 8  | 15 | 7  | 4 | 17 | 2  | 8  | 15 | 7  | 4  | 17 | 2  | 8  | 15 | 7  |
| 21 | 15 | 23 | 25 | 6 | 8  | 0  | 23 | 8  | 21 | 22 | 15 | 20 | 1  | 19 | 19 |

|    |    |    |    |    |    |   |    |    |    |    |
|----|----|----|----|----|----|---|----|----|----|----|
| I  | S  | N  | O  | T  | S  | E | C  | U  | R  | E  |
| 8  | 18 | 13 | 14 | 19 | 18 | 4 | 2  | 20 | 17 | 4  |
| 4  | 17 | 2  | 8  | 15 | 7  | 4 | 17 | 2  | 8  | 15 |
| 12 | 9  | 15 | 22 | 8  | 25 | 8 | 19 | 22 | 25 | 19 |

Pada baris kedua merupakan hasil konversi *Plaintext* ke dalam bentuk angka. Untuk baris ketiga didapat dari konversi kunci yang diulang sampai tulisan *Plaintext* berakhir. Pada baris keempat merupakan hasil penjumlahan antara baris kedua dan ketiga. Jika hasil penjumlahan berada di atas 26 maka akan diulang kembali ke huruf A. setelah hasil penjumlahan didapat, maka angka kembali dikonversi ke huruf sehingga didapat *Ciphertext*nya adalah:

VPXZGIAXIVWPUBTTMJPWIZITWZT

## 2. Huruf

Teknik substitusi *Vigenere* dengan menggunakan huruf dapat dilakukan dengan pada gambar tabel di bawah ini

Tabel 2.3 *Vigenere Cipher*

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

## 1. Serangan Terhadap *Kriptografi*

### 1. Jenis – jenis Serangan

Serangan (“serangan kriptanalisis”) terhadap *Kriptografi* dapat dikelompokkan dengan beberapa cara:

- 1) Berdasarkan keterlibatan penyerang dalam komunikasi, serangan dapat dibagi atas dua macam, yaitu:
  - a. Serangan pasif (*passive attack*)



Pada serangan ini, penyerang tidak terlibat dalam komunikasi antara pengirim dan penerima, namun penyerang menyadap semua pertukaran pesan antara kedua *entitas* tersebut. Tujuannya adalah untuk mendapatkan sebanyak mungkin *inFormasi* yang digunakan untuk kriptanalisis. Beberapa metode penyadapan antara lain :

- *Wiretapping* : penyadap mencegat data yang ditransmisikan pada saluran kabel komunikasi dengan menggunakan sambunganperangkat keras.
- *Electromagnetic Eavesdropping* : penyadap mencegat data yang ditrasnmisikan melalui saluran wireless, misalnya radio dan microwave.
- *Acoustic Eavesdropping* : menangkap gelombang suara yang dihasilkan oleh suara manusia.

b. Serangan aktif (*active attack*)

Pada jenis serangan ini, penyerang mengintervensi komunikasi dan ikut mempengaruhi sistem untuk keuntungan dirinya. Misalnya penyerang mengubah aliran pesan seperti menghapus sebagian *Cipherteks*, mengubah *Cipherteks*, menyisipkan potongan *Cipherteks* palsu, me-replay pesan lama, mengubah *inFormasi* yang tersimpan, dan sebagainya.

2) Berdasarkan banyaknya inFormasi yang diketahui oleh kriptanalis, maka serangan dapat dikelompokkan menjadi lima jenis, yaitu:

1. *Ciphertext-only attack*

Ini adalah jenis serangan yang paling umum namun paling sulit, karena inFormasi yang tersedia hanyalah *Cipherteks* saja. Kriptanalis memiliki beberapa *Cipherteks* dari beberapa pesan, semuanya dienkripsi dengan algoritma yang sama. Untuk itu kriptanalis menggunakan beberapa cara, seperti mencoba semua kemungkinan kunci secara *exhaustive search*. Menggunakan analisis frekuensi, membuat terkaan berdasarkan inFormasi yang diketahui, dan sebagainya.

2. *Known-Plaintext attack*

Ini adalah jenis serangan dimana kriptanalis memiliki pasangan *Plainteks* dan *Cipherteks* yang berkoresponden.

3. *Chosen-Plaintext attack*

Serangan jenis ini lebih hebat dari pada *known-Plaintext attack*, karena kriptanalis dapat memilih *Plainteks* yang dimilikinya untuk dienkripsikan, yaitu *Plainteks-Plainteks* yang lebih mengarahkan penemuan kunci.

4. *Chosen-Ciphertext attack*

Ini adalah jenis serangan dimana kriptanalis memilih *Ciphertext* untuk dideskripsikan dan memiliki akses ke *Plaintext* hasil deskripsi.

### 5. *Chosen text attack*

Ini adalah jenis serangan yang merupakan kombinasi *chosen-Plaintext attack* dan *chosen-chiphertext attack*.

3) Berdasarkan teknik yang digunakan dalam menemukan kunci, maka serangan dapat dibagi menjadi dua, yaitu :

#### a) *Exhaustive attack* atau *brute force attack*

Ini adalah serangan untuk mengungkap *Plainteks* atau kunci dengan menggunakan semua kemungkinan kunci. Diasumsikan kriptanalis mengetahui algoritma *Kriptografi* yang digunakan oleh pengirim pesan. Selain itu kriptanalis memiliki sejumlah *Cipherteks* dan *Plainteks* yang bersesuaian.

#### b) *Analytical attack*

Pada jenis serangan ini, kriptanalis tidak mencoba-coba semua kemungkinan kunci tetapi menganalisis kelemahan algoritma *Kriptografi* untuk mengurangi kemungkinan kunci yang tidak ada. Diasumsikan kriptanalis mengetahui algoritma *Kriptografi* yang digunakan oleh pengirim pesan. Analisis dapat menggunakan pendekatan matematik dan statistik dalam rangka menemukan kunci.

#### c) *Related-key attack*

Kriptanalis memiliki *Cipherteks* yang dienkripsi dengan dua kunci berbeda. Kriptanalis tidak mengetahui kedua kunci tersebut namun ia

mengetahui hubungan antara kedua kunci, misalnya mengetahui kedua kunci hanya berbeda 1 bit.

d) *Rubber-hose cryptanalysis*

Ini mungkin jenis serangan yang paling ekstrim dan paling efektif.

Penyerang mengancam, mengirim surat gelap, atau melakukan penyiksaan sampai orang yang memegang kunci memberinya kunci untuk mendekripsi pesan.

4) Kompleksitas serangan

Kompleksitas serangan dapat diukur dengan beberapa cara, yaitu :

a) Kompleksitas data (*data complexity*)

Jumlah data (*Plainteks* dan *Cipherteks*) yang dibutuhkan sebagai masukan untuk serangan. Semakin banyak data yang dibutuhkan untuk melakukan serangan, semakin kompleks serangan tersebut, yang berarti semakin bagus sistem *Kriptografi* tersebut.

b) Kompleksitas waktu (*time complexity*)

Waktu yang dibutuhkan untuk melakukan serangan. Semakin lama waktu yang dibutuhkan untuk melakukan serangan, berarti semakin bagus *Kriptografi* tersebut.

c) Kompleksitas ruang memori (*space/storage complexity*)

Jumlah memori yang dibutuhkan untuk melakukan serangan. Semakin banyak memori yang dibutuhkan untuk melakukan serangan, berarti semakin bagus sistem *Kriptografi* tersebut.

### 2.3 Keamanan Algoritma Kriptografi

Doni Ariyus (2005) Menuliskan Lard Knudsen mengelompokkan hasil kriptanalisis ke dalam beberapa kategori berdasarkan jumlah dan kualitas *inFormasi* yang berhasil ditemukan :

- Pemecahan total (*total break*). Kriptanalisis menemukan kunci  $K$
- Deduksi (*penarikan kesimpulan*) global (*global deduction*). Kriptanalisis menemukan algoritma alternatif,  $A$ , yang ekuivalen dengan tetapi tidak mengetahui kunci  $K$ . )
- Deduksi lokal (*instance/local deduction*). Kriptanalisis menemukan *Plainteks* dari *Cipherteks* yang disadap.

Deduksi *inFormasi* (*inFormation deduction*). Kriptanalisis menemukan beberapa *inFormasi* perihal kunci atau *Plainteks*. Misalnya kriptanalisis mengetahui beberapa kunci, kriptanalisis mengetahui bahasa yang digunakan untuk menulis *Plainteks*, kriptanalisis mengetahui *Format Plainteks*, dan sebagainya. Sebuah algoritma dikatakan aman mutlak tanpa syarat (*unconditionally secure*) bila *Cipherteks* yang dihasilkan oleh algoritma tersebut tidak mengandung cukup *inFormasi* untuk menentukan *Plainteks*.

## 2.4 Algoritma Kriptografi Klasik

Sebelum komputer ada, *Kriptografi* dilakukan dengan menggunakan pensil dan kertas. Algoritma *Kriptografi* (*Cipher*) yang digunakan saat itu, dinamakan juga algoritma klasik, adalah berbasis karakter, yaitu enkripsi dan dekripsi dilakukan pada setiap karakter pesan. Semua algoritma klasik termasuk ke dalam sistem *Kriptografi* simetris dan digunakan jauh sebelum *Kriptografi* kunci publik ditemukan.

Kriptografi klasik memiliki beberapa ciri :

1. Berbasis karakter
2. Menggunakan pena dan kertas saja, belum ada komputer
3. Termasuk ke dalam *Kriptografi* kunci simetris.

Tiga alasan mempelajari algoritma klasik :

1. Memahami konsep dasar *Kriptografi*
2. Dasar algoritma *Kriptografi* modern
3. Memahami kelemahan sistem kode.

(Ariyus, Dony. 2005)

Pada dasarnya, algoritma *Kriptografi* klasik dapat dikelompokkan ke dalam dua macam *Cipher*, yaitu :

### 1) *Cipher* substitusi (*substitution Cipher*)

Di dalam *Cipher* substitusi setiap unit *Plainteks* diganti dengan satu unit *Cipherteks*. Satu “unit” di isini berarti satu huruf, pasangan huruf, atau dikelompokkan lebih dari dua huruf. Algoritma substitusi tertua yang diketahui adalah *Caesar Cipher* yang digunakan oleh kaisar Romawi , Julius

Caesar (sehingga dinamakan juga *caesar Cipher*), untuk mengirimkan pesan yang dikirimkan kepada gubernurnya.

2) *Cipher* transposisi (*transposition Cipher*)

Pada *Cipher* transposisi, huruf-huruf di dalam *Plainteks* tetap saja, hanya saja urutannya diubah. Dengan kata lain algoritma ini melakukan transpose terhadap rangkaian karakter di dalam teks. Nama lain untuk metode ini adalah permutasi atau pengacakan (*scrambling*) karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut.

## 2.5 *Visual Basic Net 2010*

Merupakan sebuah bahasa pemrograman dan sebagai sarana (*tool*) untuk menghasilkan program-program aplikasi berbasis windows. Beberapa kemampuan atau manfaat dari *Visual Basic* diantaranya:

- a. Untuk membuat program aplikasi berbasis windows.
- b. Untuk membuat obyek-obyek pembantu program, seperti Control Active X, File Help, Aplikasi Internet dan sebagainya.
- c. Menguji program (debugging) dan menghasilkan program akhir berakhiran "EXE" yang bersifat executable atau dapat langsung dijalankan.

Keistimewaan utama dari *Visual Basic* adalah:

- d. Menggunakan platform pembuatan program yang diberi nama *developer studio*, yang memiliki tampilan seperti C++ dan visual J++.

- e. Memiliki kompilator handal yang dapat menghasilkan *File Executable* yang lebih cepat dan efisien.
- f. Memiliki tambahan saran wizard yang baru. Tambahan kontrol-kontrol baru dan lebih canggih serta peningkatan kaidah struktur bahasa *Visual Basic*.
- g. Kemampuan membuat Active X dan fasilitas internet yang lebih banyak.
- h. Sarana akses yang lebih cepat dan andal untuk membuat aplikasi database yang berkemampuan tinggi.
- i. *Visual Basic.net* memiliki beberapa versi baru edisi yang disesuaikan dengan kebutuhan pemakainya.

Dalam pemrograman berbasis OOP (*Object Oriented Programming*), sebuah program dibagi menjadi bagian-bagian kecil yang disebut dengan obyek. Setiap obyek memiliki entiti terpisah dengan entiti-entiti lain dalam lingkungannya. Obyek-obyek yang terpisah ini dapat diolah sendiri-sendiri, dan setiap obyek memiliki sekumpulan sifat dan metode yang melakukan fungsi tertentu sesuai dengan yang telah diprogramkan kepadanya.

Adapun obyek-obyek yang dipergunakan dalam program ini adalah:

1. *Project*

*Project* adalah sekumpulan modul. Jadi *Project* merupakan aplikasi itu sendiri. *Project* disimpan dalam file yang berakhiran VBP. Jika kita akan melaksanakan pembuatan program aplikasi, akan terdapat jendela *Project* yang berisi semua file yang dibutuhkan menjalankan program aplikasi *Visual Basic.net* pada saat pembuatan program aplikasi baru maka jendela *Project*



otomatis akan berisi object *Form1*. Pada jendela *Project* terdapat tiga icon yaitu View Code, View Object, dan Toggle Folders. Icon View Code dipakai untuk menampilkan jendela editor kode program. Icon View Object dipakai untuk menampilkan bentuk *Formulir (Form)* dan icon Toggle Folders digunakan untuk menampilkan folder

## 2. *Form*

*Form* adalah jendela yang dipakai untuk membuat user interface/tampilan. Secara otomatis akan tersedia *Form* yang baru jika membuat suatu program aplikasi yang baru, dengan nama *Form1*. pada umumnya dalam suatu *Form* terdapat garis titik-titik yang disebut dengan Grid. Untuk lebih memahami *Form* ini maka di bawah ini terdapat gambar jendela *Form*.

## 3. Toolbox

Toolbox adalah kumpulan dari obyek yang digunakan untuk membuat user interface (tampilan) serta control bagi program aplikasi. Untuk menempatkan control pada suatu *Form* dapat dilakukan dengan klik ganda control dalam toolbox, kemudian mengubah besar dan ukurannya serta memindahkannya dengan metode Drag and Drop atau dengan cara mengklik kontrol toolbox, kemudian pindahkan pointer mouse jendela *Form*. Kursor berubah menjadi Crosshair lalu tempatkan pada sudut kiri atas dimana kita inginkan kontrol tersebut diletakkan, tekan tombol mouse kiri dan tahan ketika menyeret kursor ke arah sudut kanan bawah.

## 4. Properties

Properties berisikan daftar struktur setting properti yang digunakan pada sebuah object terpilih. Kotak drop-down pada bagian atas jendela berisi daftar semua object pada *Form* yang aktif. Ada tab tampilan, yaitu alphabetic (urut abjad) dan categorized (urut berdasarkan kelompok).

#### 5. Kode Program

Kode program adalah serangkaian tulisan perintah yang akan dilaksanakan jika suatu obyek dijalankan. Kode program ini mengontrol dan menentukan jalannya suatu obyek.

#### 6. Event

Event adalah peristiwa atau kejadian yang diterima suatu obyek, misalnya klik, seret, tunjuk, dan lain sebagainya.

#### 7. Metode (Methods)

Metode adalah serangkaian perintah yang sudah tersedia pada suatu obyek yang dapat diminta untuk mengerjakan tugas khusus.

#### 8. Module

Module dapat disejajarkan dengan *Form*, tetapi module tidak mengandung obyek. Module berisikan prosedur umum, deklarasi variabel dan definisi konstanta yang digunakan oleh aplikasi.

## 2.6 Pengertian UML

*Unified Modelling Language* (UML) adalah sebuah bahasa yang telah menjadi standar dalam industri untuk visualisasi, merancang dan

mendokumentasikan sistem piranti lunak. UML menawarkan sebuah standar untuk merancang model sebuah sistem. Dengan menggunakan UML dapat dibuat model untuk semua jenis aplikasi piranti lunak, di mana aplikasi tersebut dapat berjalan pada piranti keras, sistem operasi dan jaringan apapun, serta ditulis dalam bahasa pemrograman apapun. Tetapi karena UML juga menggunakan *class* dan *operation* dalam konsep dasarnya, maka lebih cocok untuk penulisan piranti lunak dalam bahasa berorientasi objek seperti C++, Java, atau VB. NET (Prastuti Sulistyorini, 2012).

*Unified Modeling Language* (UML) adalah kumpulan notasi grafis yang didukung oleh sebuah model tunggal, yang membantu dalam menjelaskan dan merancang sistem perangkat lunak, khususnya sistem perangkat lunak dibangun menggunakan gaya berorientasi objek. UML terdiri atas banyak elemen-elemen grafis yang digabungkan membentuk diagram. Tujuan representasi elemen-elemen grafis ke dalam diagram adalah untuk menyajikan beragam sudut pandang dari sebuah sistem berdasarkan fungsi masing-masing diagram tersebut. Kumpulan dari beragam sudut pandang inilah yang kita sebut sebuah model (Andy Prasetyo Utomo, 2013).

Dengan menggunakan model ini diharapkan pengembangan piranti lunak dapat memenuhi semua kebutuhan pengguna dengan lengkap dan tepat, termasuk faktor-faktor seperti *scalability*, *robustness*, *security*, dan sebagainya. Untuk melakukan pemodelan sistem perangkat lunak secara visual digunakan UML (*Unified Modelling Language*) yang digambarkan secara elektronik lewat sarana

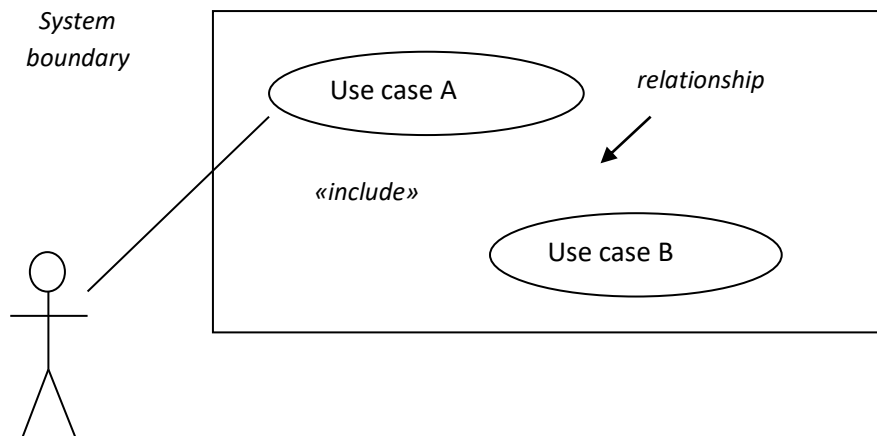
perangkat lunak *Rational Rose*. Sebagai mana telah diterapkan oleh Gufran (2012) di mana UML diterapkan untuk mengukur kinerja mahasiswa menggunakan pendekatan berorientasi objek. Kemudian UML diterapkan juga oleh Sunguk (2012) untuk menerapkan sistem *database* dan aplikasi komputer. Selanjutnya Jakimi dan Koutbi (2009) menerapkan pendekatan UML untuk sekenario rekayasa dan kode generasi.

### **1. Use Case Diagram**

*Use case* merupakan teknik menangkap kebutuhan-kebutuhan fungsional dari sistem baru atau sistem yang diubah. Setiap *use case* terdiri dari satu atau lebih skenario yang menerangkan bagaimana sistem berinteraksi dengan pengguna atau sistem yang lain untuk mencapai suatu sasaran bisnis tertentu. Dalam tehnik ini tidak diterangkan cara kerja sistem secara internal maupun implementasinya. Yang ditunjukkan adalah langkah-langkah yang dilakukan pengguna dalam menggunakan perangkat lunak (Nyimas Artina, 2006).

Diagram *Use Case* merupakan diagram yang menggambarkan fungsi berupa komponen, kelas, atau kejadian yang ada dalam *system* (Ade Sutedi *et al*, 2015). *Use case* atau diagram *use case* merupakan pemodelan untuk kelakuan (*behavior*) sistem *inFormasi* yang akan dibuat. *Use case* mendeskripsikan sebuah interaksi antara satu atau lebih aktor dengan sistem *inFormasi* yang akan dibuat. Secara kasar, *use case* digunakan untuk mengetahui fungsi apa saja yang ada di dalam sebuah sistem *inFormasi* dan siapa saja yang berhak menggunakan fungsi-fungsi itu (Rosa A.S dan M. Shalahuddin, 2014).

Syarat penamaan pada *use case* adalah nama didefinisikan sesimpel mungkin dan dapat dipahami. Ada dua hal utama pada *use case* yaitu pendefinisian apa yang disebut aktor dan *use case*.

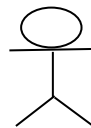


**Gambar 2.1** Use Case Diagram

Terdapat 2 bagian utama dalam *use case modeling* sebagaimana dijelaskan sebagai berikut:

- Aktor

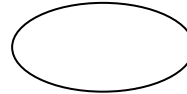
Aktor merupakan orang, proses, atau sistem lain yang berinteraksi dengan sistem inFormasi yang akan dibuat di luar sistem inFormasi yang akan dibuat itu sendiri, jadi walaupun simbol dari aktor adalah gambar orang, tapi aktor belum tentu merupakan orang.



**Gambar 2.2** Aktor

- *Use Case*

*Use case* merupakan fungsional yang disediakan sistem sebagai unit-unit yang saling bertukar pesan antar unit atau aktor.



**Gambar 2.3** *Use Case*

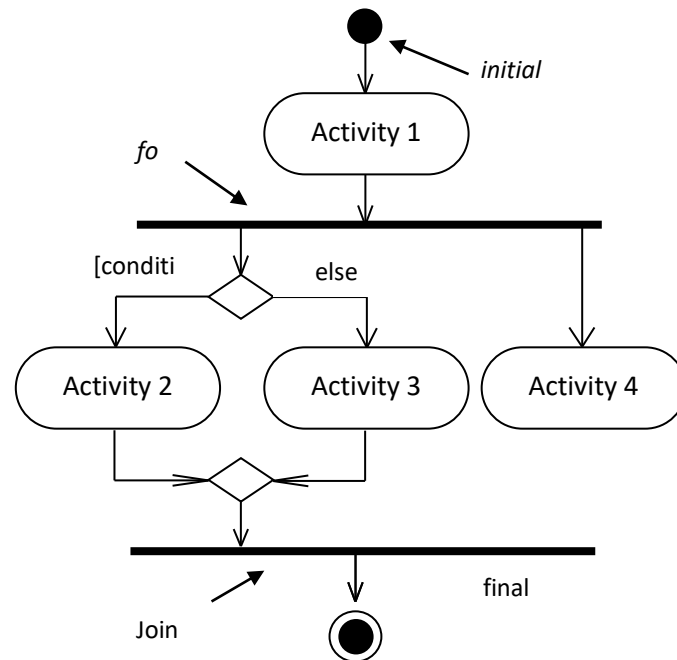
## 2. Activity Diagram

*Activity diagrams* menggambarkan *workflow* (aliran kerja) atau aktivitas sari sebuah sistem atau proses bisnis. Yang perlu diperhatikan di sini adalah bahwa diagram aktivitas menggambarkan aktivitas sistem bukan apa yang dilakukan aktor, jadi aktivitas yang dapat dilakukan oleh sistem (Rosa A.S dan M. Shalahuddin, 2014).

Diagram aktivitas juga banyak digunakan untuk mendefinisikan hal-hal berikut :

1. Rancangan proses bisnis dimana setiap urutan aktivitas yang digambarkan merupakan proses bisnis sistem yang didefinisikan.
2. Urutan atau pengelompokkan tampilan dari sistem/*user interface* di mana setiap aktivitas dianggap memiliki antarmuka tampilan.

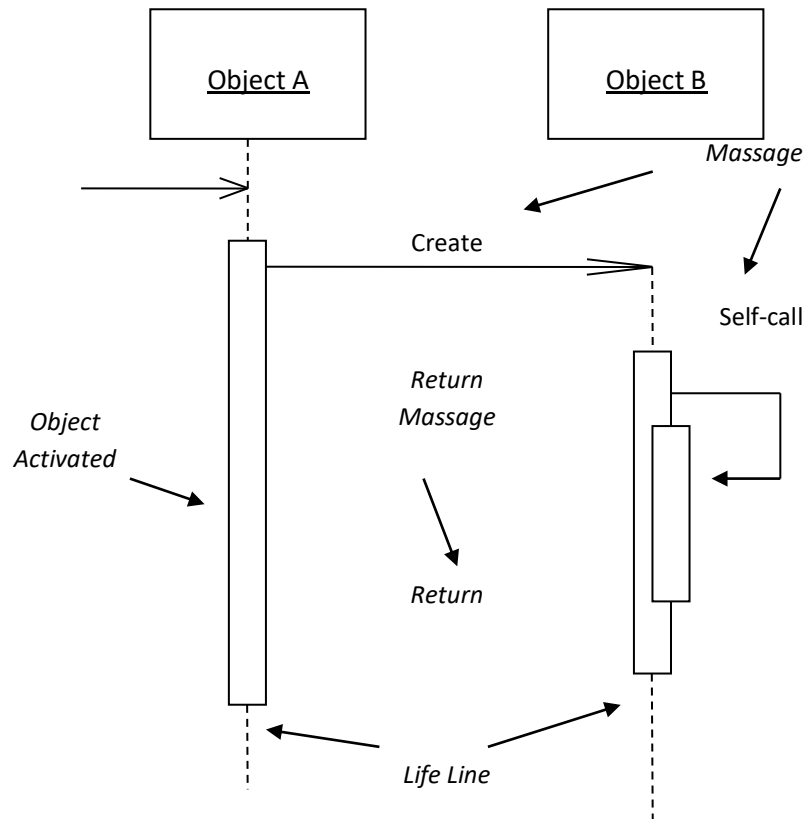
3. Rancangan pengujian di mana setiap aktivitas dianggap memerlukan sebuah pengujian yang perlu didefinisikan kasus ujinya.



**Gambar 2.4** Activity Diagram

### 3. Sequence Diagram

*Sequence diagram* menggambarkan kelakuan objek pada *use case* dengan mendeskripsikan waktu hidup objek dan *message* yang dikirimkan dan diterima antar objek. Oleh karena itu untuk menggambarkan diagram sekuen maka harus diketahui objek-objek yang terlibat dalam sebuah *use case* beserta metode-metode yang dimiliki kelas yang diinstansiasi menjadi objek itu (Rosa A.S dan M. Shalahuddin, 2014).



**Gambar 2.5** *Sequence Diagram*

## 2.7 Pengertian Flowchat

Menurut (Sariadin Siallagan, 2013), Flowchart adalah suatu diagram alir yang mempergunakan simbol atau tanda untuk menyelesaikan masalah. Dalam hal ini, penyelesaian masalah menggunakan simbol-simbol yang telah disepakati.

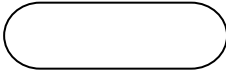


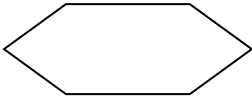

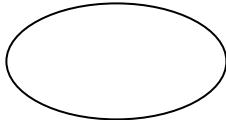
Menurut (Abdillah Baraja, 2012) Flowchart adalah representasi grafik yang menggambarkan setiap langkah yang akan dilakukan dalam suatu proses, yang

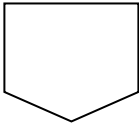

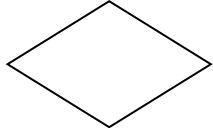
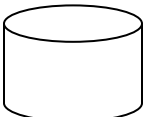
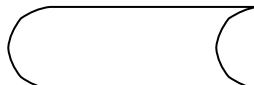
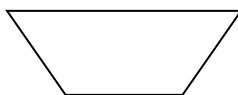

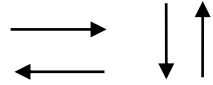




merupakan alat bantu yang banyak digunakan untuk menggambarkan sistem secara pisikal.

Bagan alir (flowchart) adalah bagan (chart) yang menunjukkan alir (flow) di dalam program atau prosedur system secara logika. Digunakan terutama untuk alat bantu komunikasi dan untuk dokumentasi.

**Tabel 2.4** Simbol-Simbol Flowchart

| NO | SIMBOL  | FUNGSI   |
|----|---|--|
| 1. |    | Terminal menyatakan awal atau akhir dari suatu logaritma.        |
| 2. |  | Menyatakan proses.   |
| 3. |  | Proses yang terdefenisi atau sub program.                        |
| 4. |  | Persiapan yang digunakan untuk memberi nilai awal suatu besaran. |
| 5. |  | Menyatakan masukan dan keluaran (input/output).                  |
| 6. |  | Menyatakan penyambung ke simbol lain dalam satu halaman.         |

|     |   |   |
|-----|---|---|
| 7.  |    | Menyatakan penyambung ke halaman lainnya.   |
| 8.  |    | Menyatakan pencetakan (dokumen) pada kertas.  |
| 9.  |    | Menyatakan <i>decision</i> (keputusan) yang digunakan untuk penyeleksian kondisi didalam program. |
| 10. |    | Menyatakan media prnyimpanan drum magnetik.   |
| 11. |   | Menyatakan input/output menggunakan disket.   |
| 12. |  | Menyatakan operasi yang dilakakukan secara manual.  |
| 13. |  | Menyatakan input/output dari kartu plong.   |
| 14. |  | Menyatakan aliran pekerjaan (proses).   |
| 15. |  | Multidocument (banyak dokumen).   |

|     |   |                                    |
|-----|---|------------------------------------|
| 16. |  | Delay (penundaan atau kelambatan). |
|-----|---|------------------------------------|

Sumber : Abdillah Baraja, 2012

## BAB III

### ANALISA DAN PERANCANGAN SISTEM

#### 3.1 Analisa Permasalahan

##### 1. Analisa sistem yang berjalan

Dalam materi perkuliahan Keamanan komputer terdapat bab mengenai enkripsi. Salah satu bentuk enkripsi adalah menggunakan metode vigenere. Untuk mendapatkan hasil teks yang diubah (*ciphertext*), menggunakan angka dan tabel untuk konversi. Penggunaan angka jauh lebih sulit dibandingkan dengan menggunakan tabel.

Contoh soal:

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:

$$C = P + K \text{ mod } 255 - 1$$

Dalam hal ini plaintext adalah ciphertext 1 yang didapat.

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

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

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

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

$$\begin{aligned} C5 &= M + U \text{ mod } 255 \\ &= 77 + 85 \text{ mod } 255 \\ &= 162 = \text{¢} \end{aligned}$$

$$\begin{aligned} C6 &= A + S \text{ mod } 255 \\ &= 65 + 83 \text{ mod } 255 \\ &= 148 = \text{'"} \end{aligned}$$

$$\begin{aligned}
 C7 &= T + K \text{ mod } 255 \\
 &= 84 + 75 \text{ mod } 255 \\
 &= 159 = \ddot{Y}
 \end{aligned}$$

$$\begin{aligned}
 C8 &= D + A \text{ mod } 255 \\
 &= 68 + 65 \text{ mod } 255 \\
 &= 133 = a
 \end{aligned}$$

$$\begin{aligned}
 C9 &= A + M \text{ mod } 255 \\
 &= 65 + 77 \text{ mod } 255 \\
 &= 142 = '
 \end{aligned}$$

$$\begin{aligned}
 C10 &= T + P \text{ mod } 255 \\
 &= 84 + 80 \text{ mod } 255 \\
 &= 164 = '
 \end{aligned}$$

$$\begin{aligned}
 C11 &= A + U \text{ mod } 255 \\
 &= 65 + 85 \text{ mod } 255 \\
 &= 150 = \textcircled{C}
 \end{aligned}$$

$$\begin{aligned}
 C12 &= N + S \text{ mod } 255 \\
 &= 78 + 83 \text{ mod } 255 \\
 &= 161 = ''
 \end{aligned}$$

$$\begin{aligned}
 C13 &= G + K \text{ mod } 255 \\
 &= 71 + 74 \text{ mod } 255 \\
 &= 145 = \text{TM}
 \end{aligned}$$

Sehingga ciphertext kedua yang didapat adalah:

$$\text{Ciphertext} = \text{ Plaintext} \oplus \text{Key}$$

## 2. Kelemahan sistem yang berjalan

Berdasarkan hasil dari analisa yang diperoleh penulis dapat menguraikan beberapa kelemahan pada sistem yang sedang berjalan, diantaranya :

- 1) Harus melihat tabel untuk proses penyandian teks
- 2) Jika tulisan terlalu banyak, menambah kesulitan pada proses penyandian.
- 3) Memungkinkan kesalahan pada proses penyandian

## 3. Analisa Sistem yang Dibangun

Perancangan sistem yang akan dibangun dilakukan setelah menganalisa permasalahan yang ada dari sistem berjalan. Sistem baru yang akan dibangun ini merupakan perubahan dari sistem yang dilakukan secara manual yang akan dijadikan secara komputerisasi dengan menggunakan aplikasi visual studio.

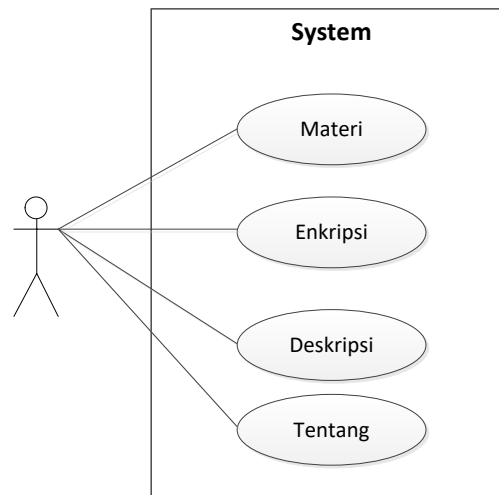
### 3.2 Perancangan Berorientasi Objek

Perancangan atau Pemodelan Berorientasi Ojek merupakan proses mendapatkan informasi dari model dan menampilkannya secara grafik dengan menggunakan sebuah standar elemen grafik. Tujuan dari perancangan berorientasi ojbek ini memungkinkan adanya komunikasi yang lebih berkualitas antara

pengguna, pengembang penganalisis, tetster, manajer dan siapapun yang terlibat dalam proyek pengembangan sistem informasi.

a. Use case Diagram

Berikut adalah *use case diagram* yang menggambarkan kegiatan.



Gambar 3.1 Use Case Diagram

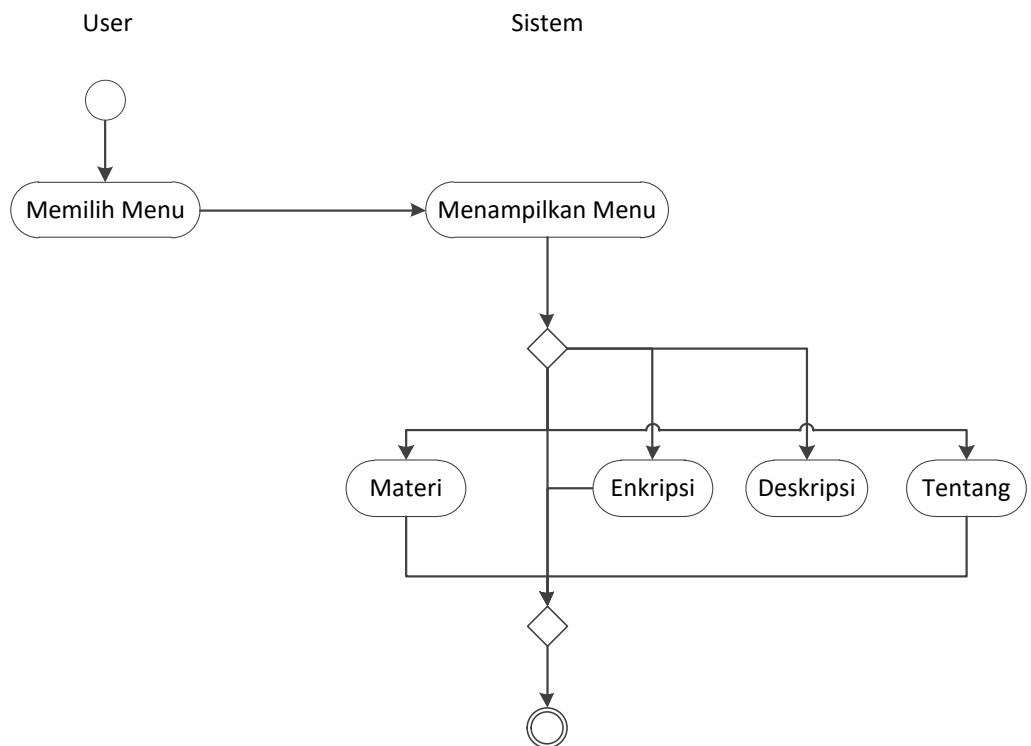
Keterangan :

Dalam *use case* diagram di atas, *user/pengguna* sebagai *actor* yang mempunyai *use case* Materi, Enkripsi dan Tentang.

b. Pembuatan Activity Diagram

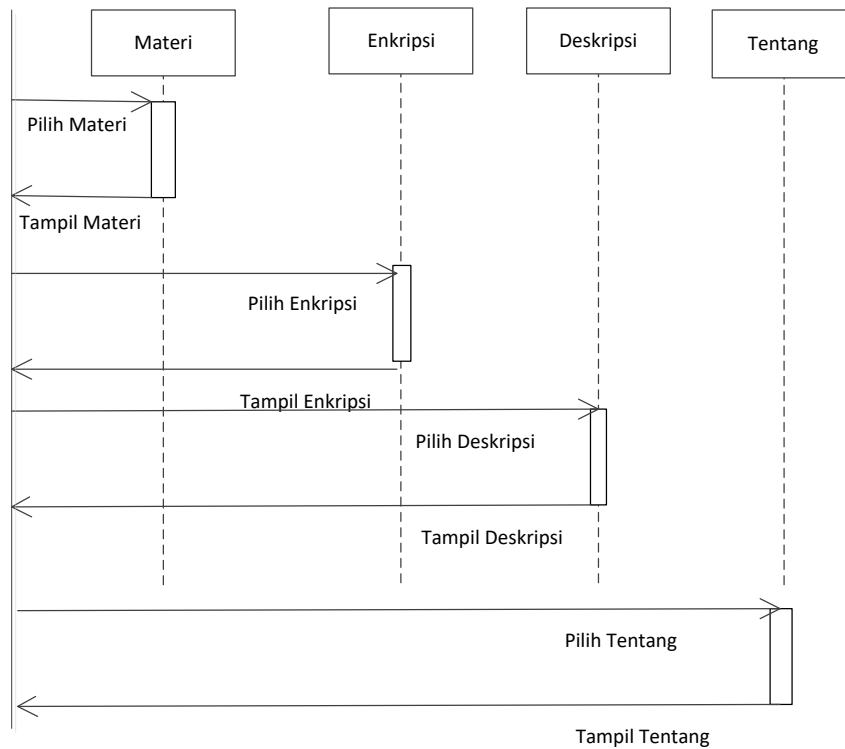
Activity diagram menggambarkan aktifitas-aktifitas yang terjadi dalam aplikasi dari aktivitas dimulai sampai aktivitas berhenti.





Gambar 3.2 Activity Diagram

## c. Sequence Diagram



**Gambar 3.4** *Sequence Diagram*

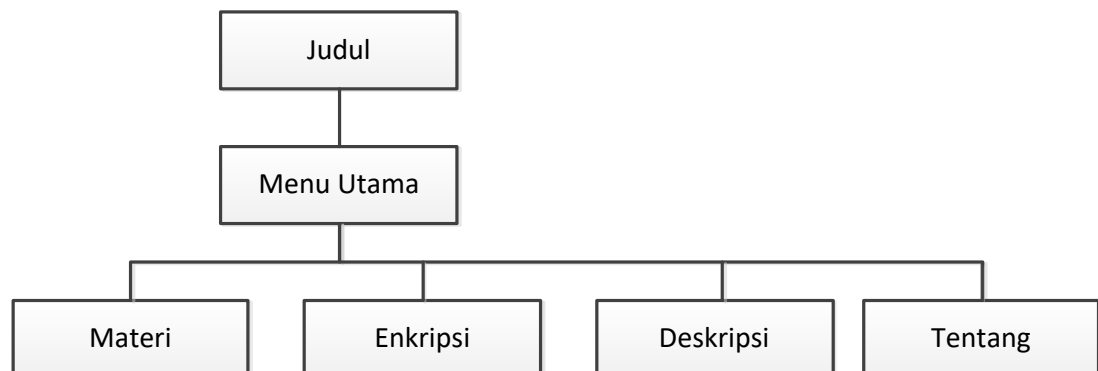
Keterangan Gambar :

1. Dalam diagram di atas menjelaskan bahwa user memilih materi kemudian Sistem menampilkan materi yang berkaitan dengan materi
2. User merequest Enkripsi kemudian Sistem menampilkan menu Enkripsi
3. User merequest Deskripsi kemudian Sistem menampilkan menu Deskripsi

4. User merequest Menu Tentang kemudian Sistem menampilkan Form Tentang.

### 3.3 Struktur Program

Struktur program mempresentasikan organisasi komponen program (modul) serta mengimplementasikan suatu hirarki kontrol. Hirarki kontrol tidak mengimplementasikan aspek prosedural dari perangkat lunak seperti urutan proses, kejadian atau urutan dari keputusan atau perulangan operasi.



Gambar 3.5 Struktur Navigasi Enkripsi

### 3.4 Perancangan Antarmuka

1. Rancangan Halaman Judul

Halaman judul merupakan halaman yang pertama muncul pada saat program dijalankan

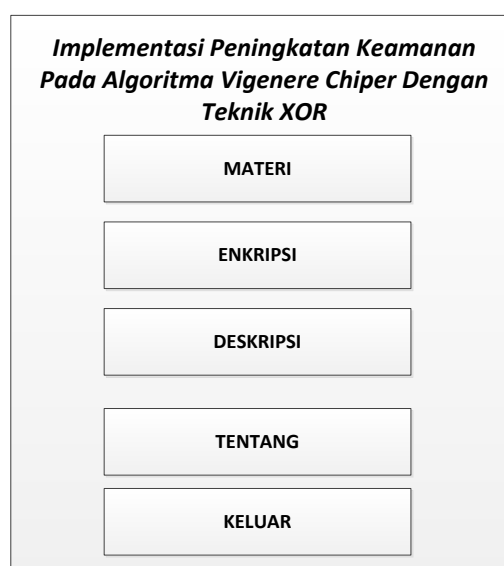


Gambar 3.6 Rancangan Halaman Judul

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 3.7 Rancangan Halaman Menu Utama

Pada tampilan di atas terdapat 5 tombol yaitu Materi, Enkripsi, Deskripsi, 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

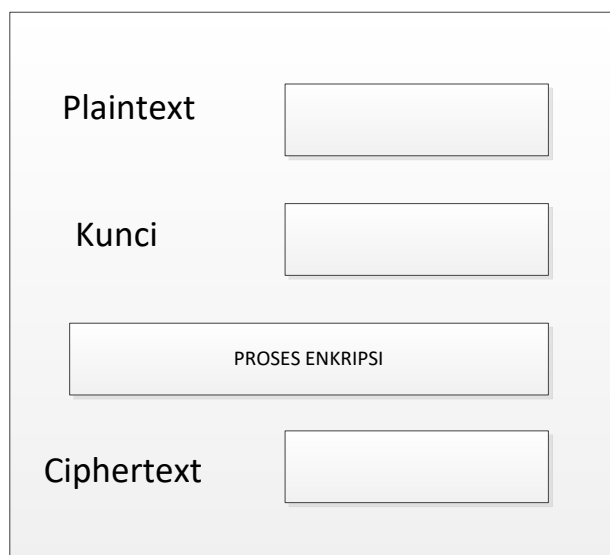
Form ini digunakan untuk menjelaskan cara kerja penyandian, dimulai dari plaintext kemudian kunci yang dikonversikan dalam bentuk angka. Setelah itu dilakukan proses penjumlahan dan jika hasil penjumlahan maka akan dikurangi 6 lalu hasilnya akan dikembalikan lagi ke dalam bentuk huruf.



Gambar 3.8. 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.



Plaintext

Kunci

Ciphertext

Gambar 3.9 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.



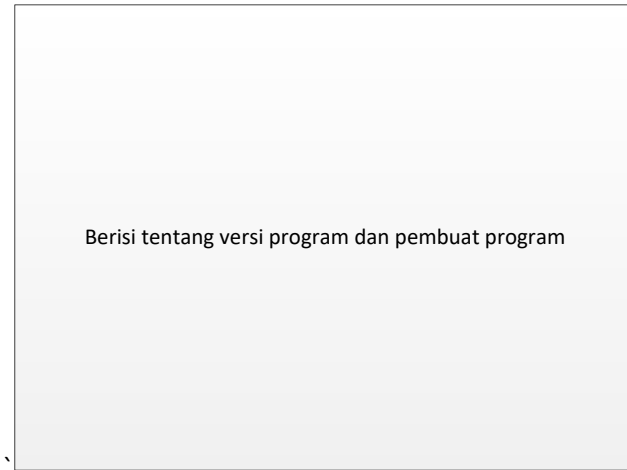
The image shows a user interface for a description page. It features four input fields and one button. The fields are labeled 'Deskripsi', 'Kunci', and 'Tulisan Asli'. The button is labeled 'Proses Deskripsi'. The fields are arranged vertically, with 'Deskripsi' at the top, followed by 'Kunci', then 'Proses Deskripsi', and finally 'Tulisan Asli' at the bottom.

Gambar 3.10 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.

### 6. Rancangan Halaman About

Berisi mengenai versi program dan pembuat program.



**Gambar 3.11 Menu About**



## **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.

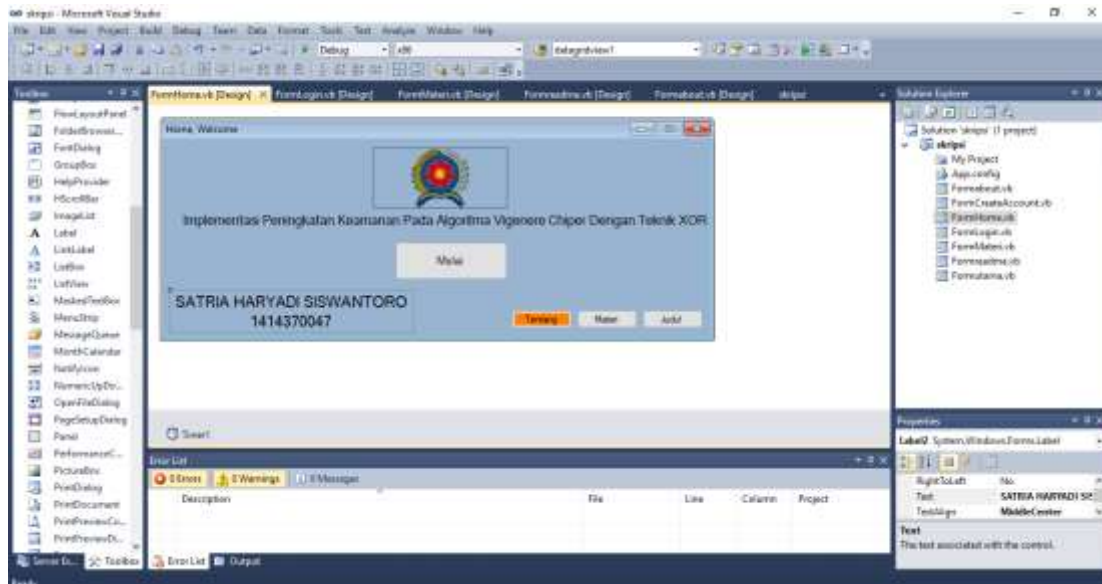
#### **4.2 Pengujian Sistem**

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 .

## 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**

## 2. Tampilan Halaman Judul

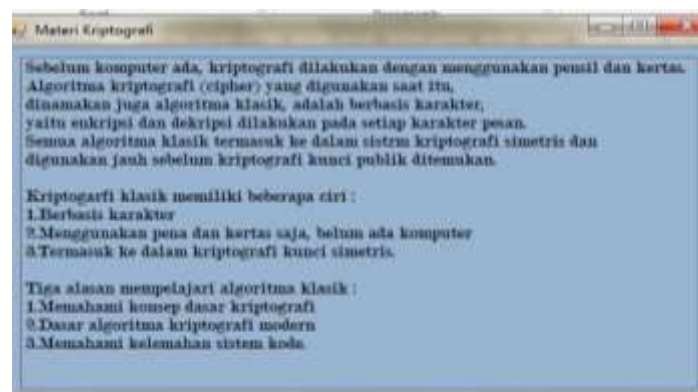
Tampilan berikut ini menampilkan halaman atau form yang berisi tentang profil dari aplikasi ini. Di dalamnya terdapat judul dari aplikasi beserta maksud dari pembuatannya beserta nama dan nomor pokok mahasiswa penulis.



**Gambar 4.2 Tampilan Halaman Judul**

### 3. Tampilan Materi

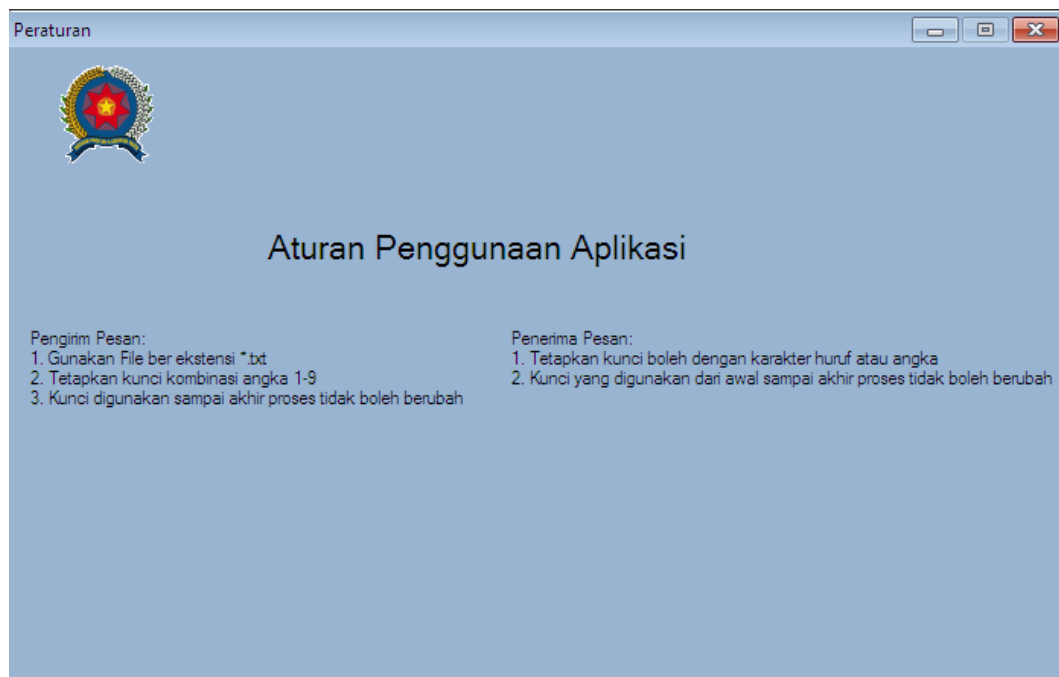
Tampilan materi merupakan tampilan halaman atau form yang berisi tentang materi yang dijalankan. Pada halaman tersebut dijelaskan apa-apa saja yang menjadi kewajiban bagi pengirim dan penerima saat menjalankan simulasi algoritma vigenere.



**Gambar 4.3 Tampilan Materi**

#### 4. Tampilan Aturan Penggunaan Aplikasi

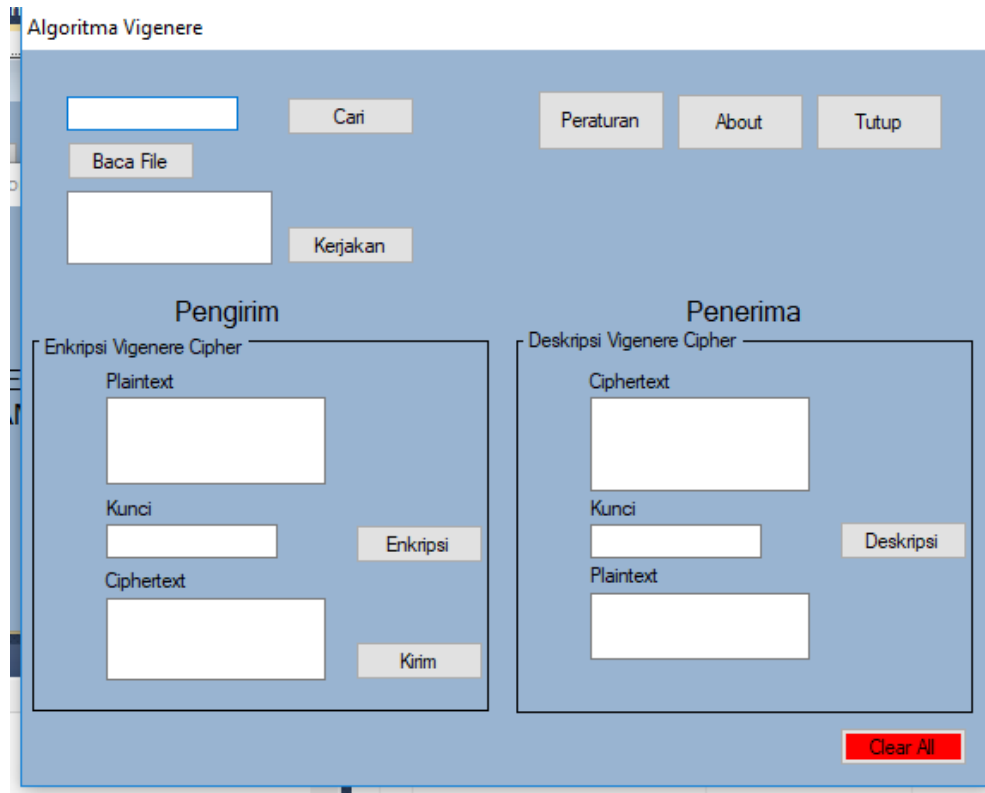
Tampilan aturan penggunaan aplikasi merupakan tampilan halaman atau form yang berisi tentang tata cara penggunaan aplikasi yang dijalankan. Pada halaman tersebut dijelaskan apa-apa saja yang menjadi kewajiban bagi pengirim dan penerima saat menjalankan simulasi algoritma vigenere.



**Gambar 4.4 Tampilan Aturan Penggunaan Aplikasi**

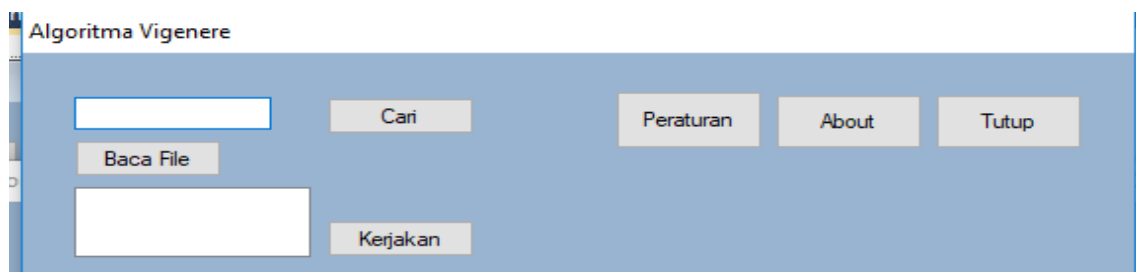
#### 5. Tampilan Halaman Utama Algoritma Vigenere

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



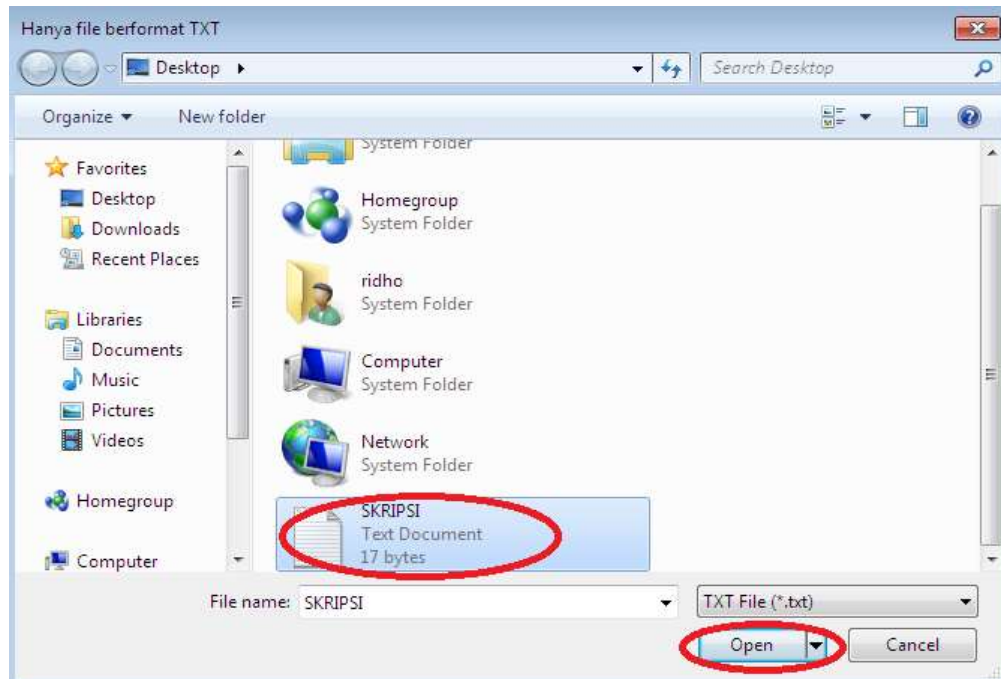
**Gambar 4.5 Tampilan Halaman Utama Algoritma Vigenere**

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.



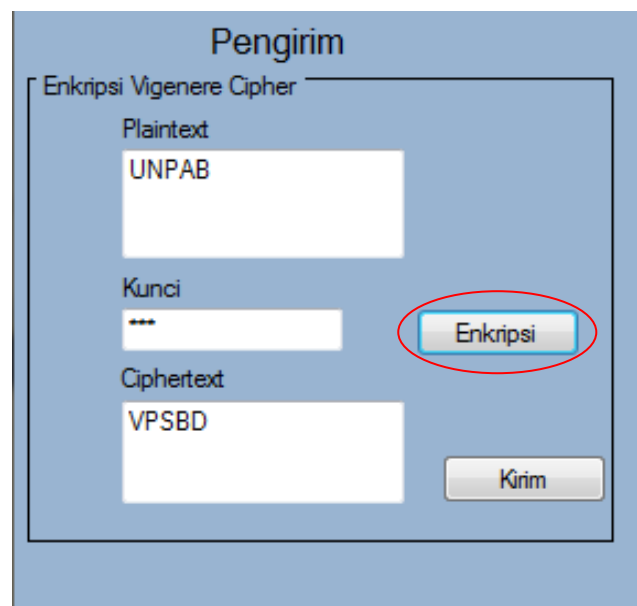
**Gambar 4.7 Tampilan Memilih File**

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**

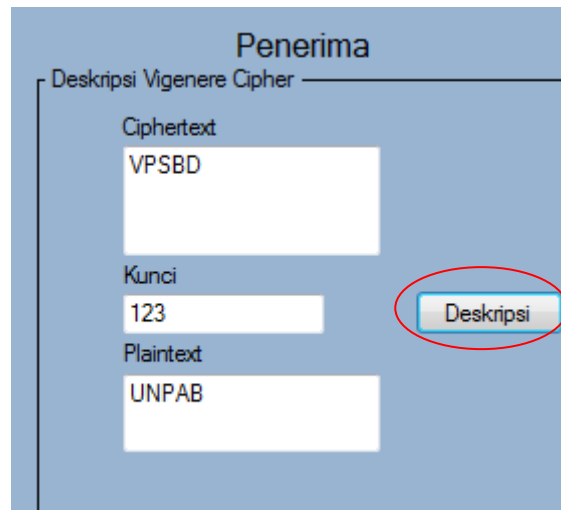
Otomatis rangkaian karakter tersebut akan berpindah ke textbox yang berada dibawahnya. Pada tahap awal rangkaian karakter akan berada di sisi bagian pengirim yang akan mengeksekusi rangkaian karakter tersebut untuk diubah menjadi ciphertext menggunakan Algoritma Vigenere Cipher. Untuk dapat mengeksekusi dibutuhkan kunci yang hanya dapat diisi karakter angka dari 0 sampai 9.



The image shows a software interface 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 button labeled "Enkripsi" (Encrypt), which is circled in red. Below the "Ciphertext" field is a button labeled "Kirim" (Send).

**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 Gronsfeld 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 dimasukkan 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 perjumlahan maka langkah terakhir adalah mengembalikan hasil nilai angka ke dalam bentuk huruf.

Perhitungan aplikasi

Perhitungan manual

|          |            |    |    |    |   |   |
|----------|------------|----|----|----|---|---|
|          | Plaintext  | U  | N  | P  | A | B |
|          |            | 20 | 13 | 15 | 0 | 1 |
| ENKRIPSI | 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 |
| <b>Key</b> | <b>1</b> | <b>2</b> | <b>3</b> | 1 | 2 |

Berdasarkan langkah diatas maka diperoleh hasil sebagai berikut.

|            |          |          |          |   |   |
|------------|----------|----------|----------|---|---|
| Chipertext | V        | P        | S        | B | D |
|            | 21       | 15       | 17       | 1 | 3 |
| <b>Key</b> | <b>1</b> | <b>2</b> | <b>3</b> | 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

Deskripsi

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 Penerapan Kriptografi Sebagai Alternatif Pengamanan Pada Aplikasi, maka dapat diambil kesimpulan sebagai berikut :

1. Perangkat lunak ini dirancang untuk menampilkan simulasi pengamanan aplikasi menggunakan kriptografi.
2. Penggunaan Algoritma Vigenere memiliki manfaat bagi pengguna aplikasi.
3. Pengamanan aplikasi menggunakan kriptografi dengan algoritma vigenere chiper ini sangat berguna dikarenakan proses enkripsi dan deskripsinya sulit untuk ditebak dan di bobol.

#### **5.2 Saran**

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

1. Perangkat lunak ini dapat dikembangkan dengan menggunakan kombinasi metode-metode lain.
2. Perangkat lunak ini dapat dikembangkan dan terhubung ke jaringan sehingga dapat dijalankan di lebih dari satu computer.
3. Perangkat lunak ini dapat dikembangkan menggunakan algoritma-algoritma lain yang lebih kompleks.

## DAFTAR PUSTAKA

- Abdul Kadir., 2014, Membuat Aplikasi Web Dengan PHP Dan Database MySQL.
- Al-Bahra Bin Ladjamuddin B., 2014, Konsep Sistem Basis Data Dan Implementasinya.  
Yogyakarta : Andi
- Andri Kristanto., 2015, Kupas Tuntas PHP Dan MySQL. Klaten : Cable Book
- Angga Wibowo., 2016, 16 (Enam Belas) Aplikasi PHP Gratis Untuk Pembangunan  
Situs Web. Yogyakarta : Andi
- Badawi, A. (2018). Evaluasi Pengaruh Modifikasi Three Pass Protocol Terhadap Transmisi  
Kunci Enkripsi.
- Budi Sutedjo Dharma Oetomo., 2016, Perencanaan Dan Pembangunan Sistem  
Informasi. Yogyakarta : Andi
- Dhany, H. W., Izhari, F., Fahmi, H., Tulus, M., & Sutarman, M. (2017, October).  
Encryption and decryption using password based encryption, MD5, and DES. In  
International Conference on Public Policy, Social Computing and Development 2017  
(ICOPOSDev 2017) (pp. 278-283). Atlantis Press.
- Eddy Prahasta., 2016, Sistem Informasi Geografis Konsep-Konsep Dasar Perspektif  
Geodasi dan Geomatika. Bandung : Informatika
- Eko Budiyanto., 2014, Sistem Informasi Geografis Menggunakan MapInfo.  
Yogyakarta : Andi
- Faisal, 2015, Aplikasi Berbasis Web Dengan PHP dan MySQL. Jakarta : Ram Media
- Fuad, R. N., & Winata, H. N. (2017). Aplikasi Keamanan File Audio Wav (Waveform)  
Dengan Terapan Algoritma Rsa. Infotekjar: Jurnal Nasional Informatika Dan  
Teknologi Jaringan, 1(2), 113-119.
- Hariyanto, E., Lubis, S. A., & Sitorus, Z. (2017). Perancangan prototipe helm pengukur  
kualitas udara. KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer),  
1(1).

- Hendrawan, J. (2018). Rancang Bangun Aplikasi Mobile Learning Tuntunan Shalat. INTECOMS: Journal of Information Technology and Computer Science, 1(1), 44-59.
- Iqbal, M., Siahaan, A. P. U., Purba, N. E., & Purwanto, D. (2017). Prim's Algorithm for Optimizing Fiber Optic Trajectory Planning. Int. J. Sci. Res. Sci. Technol, 3(6), 504-509.
- Jogianto Hartono., 2012 Pengenalan Komputer, Dasar Ilmu Komputer, Pemrograman, Sistem Informasi dan Intelegensi Buatan. Yogyakarta : Andi
- Madcoms., 2014, Aplikasi Program PHP dan MySQL Untuk Membuat Website Interaktif. Madiun : Andi
- Mariance, U. C. (2018). Analisa dan Perancangan Media Promosi dan Pemasaran Berbasis Web Menggunakan Work System Framework (Studi Kasus di Toko Mandiri Prabot Kota Medan). Jurnal Ilmiah Core IT: Community Research Information Technology, 6(1).
- Pemrograman Terstruktur, Yogyakarta : Andi
- Putri, N. A. (2018). Sistem Pakar untuk Mengidentifikasi Kepribadian Siswa Menggunakan Metode Certainty Factor dalam Mendukung Pendekatan Guru. INTECOMS: Journal of Information Technology and Computer Science, 1(1), 78-90.
- Rahim, R. (2018, October). A Novelty Once Methode Power System Policies Based On SCS (Solar Cell System). In International Conference of ASEAN Prespective and Policy (ICAP) (Vol. 1, No. 1, pp. 195-198).
- Sarif, M. I. (2017). Penemuan Aturan yang Berkaitan dengan Pola dalam Deret Berkala (Time Series).
- Sarif, M. I. Classification Of Feasibility Of Basic Food Recipients In Kelurahan Tanjung Morawa A, Tanjung Morawa Sub-District Using Naïve Bayes Classifier Algorithm.
- Sitorus, Z. (2018). Kebutuhan Web Service untuk Sinkronisasi Data Antar Sistem Informasi dalam Universitas. Jurnal Teknik dan Informatika, 5(2), 87-90.
- Sitorus, Z., Saputra, K, S., Sulistianingsih, I. (2018) C4.5 Algorithm Modeling For Decision Tree Classification Process Against Status UKM.
- Sumartono, I., Siahaan, A. P. U., & Mayasari, N. (2016). An overview of the RC4 algorithm. IOSR J. Comput. Eng, 18(6), 67-73.



Tata Surbakti., 2014, Analisa Sistem Informasi. Yogyakarta : Andi,2014,  
Yogyakarta : Andi.