



**IMPLEMENTASI KRIPTOGRAFI GRONSFELD CIPHER  
DALAM MENGAMANKAN FILE SPREADSHEET  
PADA DATA KEUANGAN**

**Disusun dan Diajukan Untuk Memenuhi Persyaratan Ujian Akhir  
Meny peroleh Gelar Sarjana Komputer Pada Fakultas Sains Dan Teknologi  
Universitas Pembangunan Panca Budi  
Medan**

---

**SKRIPSI**

---

**OLEH**

**NAMA : MAYA SARI  
N.P.M : 1514370456  
PROGRAM STUDI : SISTEM KOMPUTER**

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

## ABSTRAK

MAYA SARI

### Implementasi Kriptografi Gronsfeld Cipher Dalam Mengamankan File Spreadsheet Pada Data Keuangan 2019

Untuk menjaga keamanan file-file penting biasanya digunakan teknik *enkripsi* agar kerahasiaan data tersebut terjamin, salah satunya dengan menggunakan algoritma kriptografi. *Spreadsheet* adalah sebuah program aplikasi komputer interaktif untuk organisasi, mensimulasikan kertas, akutansi *worksheet*, dan analisis data dalam bentuk tabel. Mengamanan sebuah file *spreadsheet* yang bersifat rahasia terutama pada data keuangan dengan menggunakan kriptografi Gronsfeld Cipher. *Gronsfeld Cipher* merupakan algoritma klasik untuk menyandikan sebuah *plaintext* dengan cara substitusi sehingga dalam memecahkan pesan tersebut akan terasa susah. Penelitian ini menggunakan pemrograman *Visual Basic 2010* dan *Microsoft Excel 2010* dalam membuat aplikasi keamanan ini.

**Kata Kunci :** *Enkripsi, Gronfeld, Keamanan, Spreadsheet, Visual Basic.*

## DAFTAR ISI

<b>KATA PENGANTAR</b> .....	i
<b>DAFTAR ISI</b> .....	ii
<b>DAFTAR GAMBAR</b> .....	iv
<b>DAFTAR TABEL</b> .....	v
<b>DAFTAR ISTILAH</b> .....	vi
<b>BAB I PENDAHULUAN</b>	
1.1 Latar Belakang Masalah .....	1
1.2 Rumusan Masalah .....	2
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	3
<b>BAB II LANDASAN TEORI</b>	
2.1 Keamanan Data .....	4
2.2 Kriptografi.....	5
2.2.1 Enkripsi .....	5
2.2.2 Deskripsi .....	6
2.2.3 Kunci ( <i>Key</i> ) .....	6
2.3 Gronsfeld Cipher .....	6
2.4 File Spreadsheet .....	7
2.5 Data Keuangan .....	9
2.6 Informasi .....	10
2.7 <i>Flowchart</i> .....	11
2.7.1 Jenis-Jenis Flowchart/Bagan Alir.....	11
2.7.2 Simbol - Simbol Flowchart / Bagan Alir .....	14
2.8 <i>Unified Modeling Language (UML)</i> .....	14
2.8.1 <i>Use Case Diagram</i> .....	15
2.8.2 <i>Activity Diagram</i> .....	17
2.8.3 <i>Sequence Diagram</i> .....	18
2.9 <i>Visual Basic 2010</i> .....	19
2.10 Tabel ASCII .....	22
<b>BAB III METODE PENELITIAN</b>	
3.1 Tahapan Penelitian .....	24
3.2 Metode Pengumpulan Data .....	25
3.2.1 Penelitian Kepustakaan ( <i>Library Research</i> ) .....	25
3.2.2 Pengamatan ( <i>Observation</i> ) .....	25
3.3 Analisis Sistem Sedang Berjalan.....	25
3.3.1 Proses Pemasukkan Data .....	26
3.3.2 Proses Transaksi Data .....	27
3.3.3 Proses Laporan .....	27

3.3.4	Kelemahan-Kelemahan Proses Sistem Sedang Berjalan .....	28
3.3.5	Analisis Kebutuhan Sistem .....	29
3.4	Rancangan Penelitian .....	30
3.4.1	Perancangan Berorientasi Objek .....	30
3.4.2	Perancangan Antar Muka .....	33

#### **BAB IV ANALISA DAN PEMBAHASAN**

4.1	Kebutuhan Spesifikasi <i>Minimum Hardware</i> dan <i>Software</i> .....	40
4.2	Pengujian Aplikasi Dan Pembahasan.....	41
4.2.1	Implementasi Sistem .....	41
4.3	Pengujian Sistem .....	46
4.3.1	Enkripsi .....	46
4.3.2	Deskripsi .....	48
4.4	Pengujian Aplikasi .....	49

#### **BAB V KESIMPULAN DAN SARAN**

5.1	Kesimpulan.....	51
5.2	Saran.....	51

#### **DAFTAR PUSTAKA BIOGRAFI PENULIS**

## DAFTAR GAMBAR

	<b>Halaman</b>
Gambar 2.1	Proses <i>Enkripsi</i> dan <i>Deskripsi</i> ..... 6
Gambar 2.2	Rumus Pada <i>Excel</i> ..... 8
Gambar 2.3	Simbol-Simbol Flowchart ..... 14
Gambar 2.4	Simbol Activity Diagram ..... 18
Gambar 2.5	Tampilan VB 2010 ..... 20
Gambar 2.6	Tampilan Toolbox ..... 21
Gambar 2.7	Tampilan Windows Project ..... 21
Gambar 2.8	Tampilan Windows Properties ..... 22
Gambar 3.1	Tahapan Penelitian ..... 24
Gambar 3.2	Analisis Permasalahan Yang Berjalan ..... 26
Gambar 3.3	Pembuatan File <i>Excel</i> ..... 26
Gambar 3.4	Transaksi Pengambilan Data ..... 27
Gambar 3.5	Laporan ..... 28
Gambar 3.6	Keterangan Hasil <i>Enkripsi</i> ..... 28
Gambar 3.7	Hasil <i>Enkripsi</i> ..... 29
Gambar 3.8	Keterangan Hasil Akhir ..... 29
Gambar 3.9	<i>Use Case Diagram</i> ..... 30
Gambar 3.10	<i>Activity Diagram</i> ..... 31
Gambar 3.11	<i>Sequence Diagram</i> ..... 32
Gambar 3.12	Rancangan Halaman Judul ..... 33
Gambar 3.13	Rancangan Halaman Menu Utama ..... 34
Gambar 3.14	Rancangan Halaman Materi ..... 35
Gambar 3.15	Rancangan Halaman <i>Enkripsi</i> ..... 36
Gambar 3.16	Rancangan Halaman <i>Deskripsi</i> ..... 37
Gambar 3.17	Rancangan Halaman Tentang ..... 38
Gambar 4.1	Tampilan Halaman Judul ..... 41
Gambar 4.2	Tampilan Halaman Utama ..... 42
Gambar 4.3	Tampilan Materi ..... 43
Gambar 4.4	Tampilan <i>Enkripsi</i> ..... 43
Gambar 4.5	Tampilan <i>Deskripsi</i> ..... 44
Gambar 4.6	Tampilan Tentang ..... 45

## DAFTAR TABEL

	<b>Halaman</b>
Tabel 2.1 Simbol <i>Use Case Diagram</i> .....	15
Tabel 2.2 Simbol <i>Squence Diagram</i> .....	19
Tabel 2.3 Tabel <i>ASCII</i> .....	23
Tabel 4.1 Pengujian Aplikasi .....	49

## DAFTAR ISTILAH

- ASCII**      *ASCII (American Standard Code for Information Interchange)* atau kode Standar Amerika untuk Pertukaran Informasi. Merupakan suatu standar internasional dalam kode huruf dan lumeri seperti *Hex* dan *Unicode* tetapi *ASCII* lebih bersifat *universal*, contohnya 124 adalah untuk karakter “|”.
- UML**      *Unified Modeling Language (UML)* adalah bahasa spesifikasi standar yang dipergunakan untuk mendokumentasikan, menspesifikasikan dan membanngun perangkat lunak. *UML* merupakan metodologi dalam mengembangkan sistem berorientasi objek dan juga merupakan alat untuk mendukung pengembangan sistem.

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Keamanan dan kerahasiaan data merupakan suatu aspek yang sangat penting dalam proses pertukaran pesan atau informasi. Suatu pesan yang sifatnya rahasia membutuhkan suatu sistem penyimpanan dan pengiriman data atau *file* agar tidak mudah terbaca dan diketahui semua orang. Ada berbagai macam cara untuk mengamankan data atau *file*, salah satunya adalah menggunakan metode kriptografi.

Saat ini *kriptografi* terbagi menjadi dua yaitu kriptografi klasik dan kriptografi modern. Pada *kriptografi* klasik terdapat algoritma *Gronsfeld Cipher*. *Gronsfeld Cipher* merupakan algoritma klasik untuk menyandikan sebuah *plaintext* dengan cara substitusi sehingga dalam memecahkan pesan tersebut akan terasa susah. Penelitian ini menggunakan pemrograman *Visual Basic 2010* dan *Microsoft Excel 2010*.

Pengertian *spreadsheet* ialah dokumen yang menyimpan data dalam *grid* baris (*rows*) horizontal dan kolom (*columns*) vertikal. Pada baris, umumnya akan diberi label menggunakan nomor 1, 2, 3 dst, sementara pada kolom umumnya diberi label menggunakan huruf A, B, C dst.

Lokasi baris atau kolom individu seperti C2 atau D15 biasa disebut dengan sel (*cell*). Dengan memasukkan data kedalam *spreadsheet*, informasi dapat disimpan dengan cara lebih terstruktur dari pada menggunakan teks biasa. struktur

pada baris atau kolom juga memungkinkan data yang akan dianalisis menggunakan formula.

Proses pengamanan pesan tersebut hanya berupa text yang dikirim, dan penerima harus memiliki kunci untuk membuka pesan asli. Dengan adanya *Gronsfeld cipher* 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.

Berdasarkan latar belakang yang telah penulis uraikan di atas, maka penulis tertarik untuk memilih judul **“Implementasi Kriptografi *Gronsfeld Cipher* Dalam Mengamankan File *Spreadsheet* Pada Data Keuangan”**.

## **1.2 Rumusan Masalah**

Berdasarkan latar belakang masalah di atas dapat penulis simpulkan bahwa yang menjadi pokok permasalahan dalam pembahasan ini adalah sebagai berikut:

1. Apa yang harus diamankan dalam file *spreadsheet* ?
2. Bagaimana merancang sebuah keamanan file *spreadsheet* pada data keuangan?
3. Bagaimana menerapkan metode algoritma *Gronsfeld Cipher* dalam proses keamanan file *spreadsheet* pada data keuangan?

### **1.3 Batasan Masalah**

Berdasarkan perumusan masalah diatas maka penulis melakukan pembatasan masalah yang akan dibahas sebagai berikut:

1. Implementasi *enkripsi* dan *dekripsi* menggunakan file *spreadsheet* yang ada didalam *Microsoft Excel 2010*.
2. Program yang dibahas menggunakan pemrograman *Visual Basic 2010*.
3. Mengkaitkan proses *enkripsi* dan *deskripsi* dengan tabel *ASCII*.

### **1.4 Tujuan Penelitian**

Adapun tujuan dari penelitian dengan menggunakan algoritma *Gronsfeld Cipher* ini yang ingin dicapai adalah sebagai berikut:

1. Mengamankan data sebuah file *spreadsheet* yang bersifat rahasia terutama data keuangan.
2. Merancang sistem aplikasi keamanan data dengan algoritma *Gronsfeld Cipher* pada file *spreadsheet*.
3. Menerapkan *Gronsfeld Cipher* dengan pemrograman *Visual Basic 2010*.

### **1.5 Manfaat Penelitian**

Adapun manfaat dalam penelitian ini yang diperoleh dari penerapan dengan algoritma *Gronsfeld Cipher* dalam proses keamanan file *spreadsheet* adalah sebagai berikut:

1. Kerahasiaan data yang dikirim dan diterima lebih aman.
2. Melindungi file *spreadsheet* yang terdapat data-data penting.

## **BAB II**

### **LANDASAN TEORI**

#### **2.1 Keamanan Data**

Seiring dengan kemajuan teknologi informasi maka sangat di perlukan sebuah keamanan data terhadap kerahasiaan informasi yang saling di pertukarkan melalui jaringan internet, apa lagi jika data tersebut dalam suatu jaringan komputer yang terhubung/terkoneksi dengan jaringan lain. Informasi yang terkandung di dalamnya pun bisa saja berubah sehingga menyebabkan salah penafsiran oleh penerima pesan. Selain itu data yang dibajak kemungkinan rusak atau hilang yang menimbulkan kerugian material yang besar (Angga & Desi, 2018). Dalam keamanan data ada beberapa aspek yang berkaitan dengan persyaratan keamanan yaitu :

1. *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.

2. *Integrity*

Berhubungan dengan akses merubah data dan informasi. Data dan informasi di dalam suatu sistem komputer hanya dapat diubah oleh orang yang berhak

### 3. *Availability*

Berhubungan dengan ketersediaan data dan informasi. Data dan informasi yang berada dalam suatu sistem komputer tersedia dan dapat dimanfaatkan oleh orang yang berhak.

## 2.2 *Kriptografi*

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Dalam ilmu *kriptografi*, terdapat dua buah proses yaitu melakukan *enkripsi* dan *dekripsi*. Pesan yang akan dienkripsi disebut sebagai *plaintext* (teks biasa). Algoritma yang dipakai untuk *mengenkripsi* dan *mendekripsi* sebuah *plaintext* melibatkan penggunaan suatu bentuk kunci. Pesan *plaintext* yang telah dienkripsi (atau dikodekan) dikenal sebagai *ciphertext* (teks sandi) ( Fresly, Indah & Awang, 2015).

### 2.2.1 *Enkripsi*

*Enkripsi (Encryption)* adalah sebuah proses menjadikan pesan yang dapat dibaca (*plaintext*) menjadi pesan acak yang tidak dapat dibaca (*ciphertext*).

### 2.2.2 Dekripsi

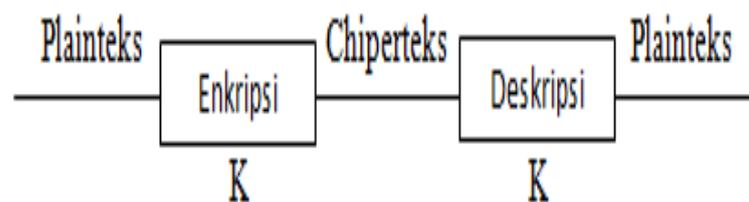
*Deskripsi* merupakan proses kebalikan dari enkripsi dimana proses ini akan mengubah *ciphertext* menjadi *plaintext* dengan menggunakan algoritma "pembalik" dan *key* yang sama.

### 2.2.3 Kunci (*key*)

parameter yang digunakan untuk transformasi *enkripsi* dan *dekripsi*.

Kunci biasanya berupa *string* atau deretan bilangan.

Dengan menggunakan kunci *K*, maka fungsi *enkripsi* dan *dekripsi* dapat ditulis sebagai skema diperlihatkan pada Gambar berikut:



**Gambar 2.1** proses *Enkripsi & Deskripsi*

Sumber : Ms. Word 2010 (2019)

## 2.3 Gronsfeld Cipher

*Gronsfeld* adalah satu *cipher* substitusi sederhana *polyalphabetic*. *Gaspar Schot* adalah seorang *kriptografer* abad ke 17 di Jerman, yang belajar *cipher* ini selama perjalanan antara Mainz dan Frankfurt dengan menghitung *Gronsfeld*,

maka terciptalah nama dari *chiper* tersebut yaitu *Gronsfeld*. System *Gronsfeld* menggunakan suatu kunci numerik yang biasanya cukup pendek misalnya 7341, kunci ini diulang secara priodik, sesuai dengan jumlah kata *plaintext* (Azanudin, 2013).

*Gronsfeld Cipher* tanpa menggunakan Tabel *Gronsfeld*, dengan menggunakan metode ' Huruf hasil *Gronsfeld* = (Huruf Asli dalam bentuk angka) + (Kata Kunci dalam bentuk angka) ' untuk mengetahui teks hasil *Gronsfeld* nya. jika hasil *Gronsfeld* dalam bentuk angkamu lebih besar dari pada 26, maka kurangilah hasil tersebut dengan 26 .

contoh :

Huruf Asli : S = 19

Angka Kunci : 1

Huruf hasil *Gronsfeld*:  $19 + 1 = 20$  ( 20 = huruf T )

Huruf Asli : T = 20

Angka Kunci : 7

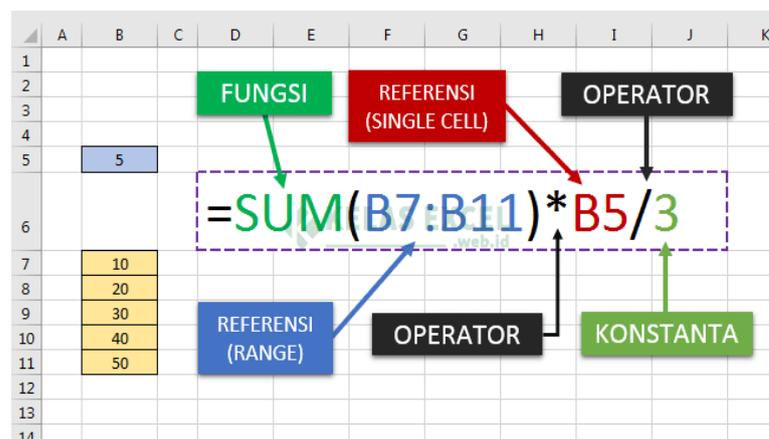
Huruf hasil *Gronsfeld* :  $20 + 7 = 27$  (  $27 - 26 = 1$  = huruf A )

berarti, huruf hasil pengubahan dalam bentuk *Gronsfeld* adalah T dan A.

## 2.4 File Spreadsheet

*Spreadsheet* adalah sebuah program aplikasi komputer interaktif untuk organisasi, mensimulasikan kertas, akutansi *worksheet*, dan analisis data dalam bentuk tabel ( Harminal, Hidayat & Herdhiana, 2016).

Cara menggunakan rumus atau formula *excel* selalu diawali dengan tanda sama dengan (=). Selain itu dalam sebuah rumus atau formula *excel* dapat terdiri atas satu atau semua dari beberapa hal berikut:



**Gambar 2.2** Rumus pada Excel

Sumber : [www.Kelasexcel.id](http://www.Kelasexcel.id) (2014)

1. SAMA DENGAN(=) : Tanda sama dengan atau "=" merupakan tanda awal dari penulisan formula atau rumus *excel* yang harus dituliskan jika kita hendak membuat atau menggunakan formula apapun.
2. FUNGSI : Fungsi merupakan sebuah kode tertentu yang melakukan kalkulasi tertentu di *excel* berdasarkan susunan argumen yang telah di

tetapkan pada Microsoft *excel*. Fungsi bisa digunakan untuk menjalankan perhitungan sederhana atau kompleks. Misalnya fungsi *SUM* yang merupakan sebuah Fungsi *excel* yang digunakan untuk menjumlahkan data.

3. REFERENSI : Referensi adalah acuan pada sebuah sel atau range pada lembar kerja, baik pada *sheet* yang sama maupun *sheet* yang berbeda. pada contoh di atas misalnya B2:B5 merupakan referensi dalam bentuk *Range* (Kumpulan *Cell*) sedangkan C2 Merupakan Referensi dalam bentuk sel tunggal.
4. KONSTANTA : Konstanta merupakan nilai yang bukan hasil dari sebuah kalkulasi perhitungan, karena itu nilainya selalu sama atau tidak berubah. Konstanta dapat berbentuk teks maupun angka yang dimasukkan langsung ke rumus, misalnya angka 3
5. OPERATOR : Operator merupakan simbol karakter yang menentukan tipe perhitungan yang ingin anda jalankan pada sebuah rumus *excel*. Pada contoh diatas yang termasuk operator adalah tanda \* (perkalian) dan / (pembagian). Untuk lebih jelas tentang operator silahkan baca artikel tentang Operator Perhitungan dalam Rumus *Excel*

## **2.5 Data Keuangan**

Pengertian laporan keuangan menurut Zaki Baridwan menyatakan bahwa :  
“Laporan keuangan merupakan ringkasan dari suatu proses pencatatan,

merupakan suatu ringkasan transaksi-transaksi keuangan yang terjadi selama tahun buku yang bersangkutan” (Sarjana, Budi & Dwi, 2013).

laporan keuangan merupakan hasil akhir dari proses pencatatan transaksi keuangan suatu perusahaan yang menunjukkan kondisi keuangan perusahaan tersebut pada satu periode akuntansi dan merupakan gambaran umum mengenai kinerja suatu perusahaan

suatu perubahan diperlukan dalam berbagai aspek misalkan bentuk penyajian informasi, sehingga informasi dapat efektif dan mudah dipahami sumber informasi dari sebuah laporan keuangan banyak dijadikan pedoman dalam pengambilan sebuah keputusan bagi para kreditur, pengamat ekonomi, pemegang saham, dan pemerintah sesuai dengan kepentingan yang ada, serta merupakan pedoman perincian pada setiap prestasi operasional suatu perusahaan ketika Analisa Rasio Keuangan dilakukan. Dengan adanya laporan keuangan maka akan diperoleh gambaran mengenai bagaimana perkembangan perusahaan, sehingga yang berkepentingan terhadap perkembangan perusahaan dapat mengadakan analisis terhadap semua data keuangan yang terdapat dalam laporan keuangan.

## **2.6 Informasi**

Informasi adalah data yang telah diolah menjadi bentuk yang memiliki arti bagi si penerima dan bermanfaat bagi pengambilan keputusan saat ini atau mendatang. Secara umum Informasi adalah hasil pemrosesan data yang diperoleh dari setiap elemen sistem menjadi bentuk yang mudah dipahami dan merupakan pengetahuan yang relevan dan berguna.

Adapun fungsi-fungsi informasi adalah sebagai berikut:

- 1) Untuk meningkatkan pengetahuan bagi si pemakai.
- 2) Untuk mengurangi ketidak pastian 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.

## **2.7 Flowchart**

Flowchart merupakan penyajian yang sistematis tentang proses dan logika dari kegiatan penanganan informasi atau penggambaran secara grafik dari langkah-langkah dan urutan prosedur dari suatu program. Bagan alir (*flowchart*) adalah bagan (*chart*) yang menunjukkan alir (*flow*) di dalam program atau prosedur sistem secara logika (Muslim & Ali, 2013).

### **2.7.1 Jenis Jenis Flowchart / Bagan Alir**

Ada beberapa jenis - Jenis *flowchart* diantaranya:

- a) Bagan alir sistem (*systems flowchart*).
- b) Bagan alir dokumen (*document flowchart*).
- c) Bagan alir skematik (*schematic flowchart*).
- d) Bagan alir program (*program flowchart*).
- e) Bagan alir proses (*process flowchart*).

a. *System Flowchart*

*System flowchart* dapat didefinisikan sebagai bagan yang menunjukkan arus pekerjaan secara keseluruhan dari sistem. Bagan ini menjelaskan urutan-urutan dari prosedur-prosedur yang ada di dalam sistem. Bagan alir sistem menunjukkan apa yang dikerjakan di sistem.

b. *Document Flowchart*

Bagan alir dokumen (*document flowchart*) atau disebut juga bagan alir formulir (*form flowchart*) atau *paperwork flowchart* merupakan bagan alir yang menunjukkan arus dari laporan dan formulir termasuk tembusan-tembusannya.

c. *Schematic Flowchart*

Bagan alir skematik (*schematic flowchart*) merupakan bagan alir yang mirip dengan bagan alir sistem, yaitu untuk menggambarkan prosedur di dalam sistem. Perbedaannya adalah, bagan alir skematik selain menggunakan simbol-simbol bagan alir sistem, juga menggunakan gambar-gambar komputer dan peralatan lainnya yang

digunakan. Maksud penggunaan gambar-gambar ini adalah untuk memudahkan komunikasi kepada orang yang kurang paham dengan simbol-simbol bagan alir. Penggunaan gambar-gambar ini memudahkan untuk dipahami, tetapi sulit dan lama menggambarinya.

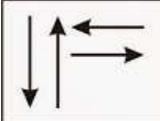
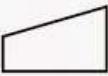
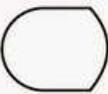
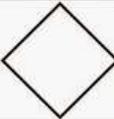
#### d. Program *Flowchart*

Bagan alir program (*program flowchart*) merupakan bagan yang menjelaskan secara rinci langkah-langkah dari proses program. Bagan alir program dibuat dari derivikasi bagan alir sistem. Bagan alir program dapat terdiri dari dua macam, yaitu bagan alir logika program (*program logic flowchart*) dan bagan alir program komputer terinci (*detailed computer program flowchart*). Bagan alir logika program digunakan untuk menggambarkan tiap-tiap langkah di dalam program komputer secara logika. Bagan alat- logika program ini dipersiapkan oleh analis sistem. Gambar berikut menunjukkan bagan alir logika program. Bagan alir program komputer terinci (*detailed computer program flow-chart*) digunakan untuk menggambarkan instruksi-instruksi program komputer secara terinci. Bagan alir ini dipersiapkan oleh pemrogram.

e. *Process Flowchart*

Bagan alir proses (*process flowchart*) merupakan bagan alir yang banyak digunakan di teknik industri. Bagan alir ini juga berguna bagi analisis sistem untuk menggambarkan proses dalam suatu prosedur.

### 2.7.2 Simbol - Simbol Flowchart / Bagan Alir

	<b>Flow Direction symbol</b> Yaitu simbol yang digunakan untuk menghubungkan antara simbol yang satu dengan simbol yang lain. Simbol ini disebut juga connecting line.		<b>Simbol Manual Input</b> Simbol untuk pemasukan data secara manual on-line keyboard
	<b>Terminator Symbol</b> Yaitu simbol untuk permulaan (start) atau akhir (stop) dari suatu kegiatan		<b>Simbol Preparation</b> Simbol untuk mempersiapkan penyimpanan yang akan digunakan sebagai tempat pengolahan di dalam storage.
	<b>Connector Symbol</b> Yaitu simbol untuk keluar - masuk atau penyambungan proses dalam lembar / halaman yang sama.		<b>Simbol Predefine Proses</b> Simbol untuk pelaksanaan suatu bagian (sub-program)/prosedure
	<b>Connector Symbol</b> Yaitu simbol untuk keluar - masuk atau penyambungan proses pada lembar / halaman yang berbeda.		<b>Simbol Display</b> Simbol yang menyatakan peralatan output yang digunakan yaitu layar, plotter, printer dan sebagainya.
	<b>Processing Symbol</b> Simbol yang menunjukkan pengolahan yang dilakukan oleh komputer		<b>Simbol disk and On-line Storage</b> Simbol yang menyatakan input yang berasal dari disk atau disimpan ke disk.
	<b>Simbol Manual Operation</b> Simbol yang menunjukkan pengolahan yang tidak dilakukan oleh computer		<b>Simbol magnetik tape Unit</b> Simbol yang menyatakan input berasal dari pita magnetik atau output disimpan ke pita magnetik.
	<b>Simbol Decision</b> Simbol pemilihan proses berdasarkan kondisi yang ada.		<b>Simbol Punch Card</b> Simbol yang menyatakan bahwa input berasal dari kartu atau output ditulis ke kartu
	<b>Simbol Input-Output</b> Simbol yang menyatakan proses input dan output tanpa tergantung dengan jenis peralatannya		<b>Simbol Dokumen</b> Simbol yang menyatakan input berasal dari dokumen dalam bentuk kertas atau output dicetak ke kertas.

**Gambar 2.3** Simbol-Simbol *Flowchart*

Sumber : <https://fahmilatiefmunir.blogspot.com> (2016)

## 2.8 Unified Modeling Language (UML)

*Unified Modeling Language (UML)* adalah bahasa spesifikasi standar yang dipergunakan untuk mendokumentasikan, menspesifikasikan dan membangun perangkat lunak. *UML* merupakan metodologi dalam mengembangkan sistem berorientasi objek dan juga merupakan alat untuk mendukung pengembangan sistem.

*UML* sendiri juga memberikan standar penulisan sebuah sistem *blue print*, yang meliputi konsep bisnis proses, penulisan kelas-kelas dalam bahasa program yang spesifik, skema *database*, dan komponen-komponen yang diperlukan dalam sistem software (Suendri, 2018).

Diagram *Unified Modelling Language (UML)* antara lain sebagai berikut:

### 2.8.1 Use Case Diagram

menggambarkan *external view* dari sistem yang akan kita buat modelnya, Model *use case* dapat dijabarkan dalam diagram *use case*, tetapi perlu diingat, diagram tidak identik dengan model karena model lebih luas dari diagram. *Use case* harus mampu menggambarkan urutan aktor yang menghasilkan nilai terukur.

**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> .

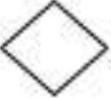
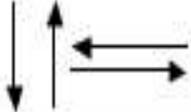
2		<i>Dependency</i>	Hubungan dimana perubahan yang terjadi pada suatu elemen mandiri ( <i>independent</i> ) akan mempengaruhi elemen yang bergantung padanya elemen yang tidak mandiri ( <i>independent</i> ).
3		<i>Generalization</i>	Hubungan dimana objek anak ( <i>descendent</i> ) berbagi perilaku dan 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 actor
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)

### 2.8.2 *Activity Diagram*

menunjukkan aktivitas sistem dalam bentuk kumpulan aksi-aksi, bagaimana masing-masing aksi tersebut dimulai, keputusan yang mungkin terjadi hingga berakhirnya aksi. *Activity* diagram juga dapat menggambarkan proses lebih dari satu aksi dalam waktu bersamaan. “Diagram *activity* adalah aktifitas-aktifitas, objek, *state*, *transisi state* dan *event*. Dengan kata lain kegiatan diagram alur kerja menggambarkan perilaku sistem untuk aktivitas”.

NO	GAMBAR	NAMA	KETERANGAN
1		Activity	Memperlihatkan bagaimana masing-masing kelas antarmuka saling berinteraksi satu sama lain
2		Action	State dari sistem yang mencerminkan eksekusi dari suatu aksi
3		Initial Node	Bagaimana objek dibentuk atau diawali.
4		Activity Final Node	Bagaimana objek dibentuk dan diakhiri
5		Decision	Digunakan untuk menggambarkan suatu keputusan / tindakan yang harus diambil pada kondisi tertentu
6		Line Connector	Digunakan untuk menghubungkan satu simbol dengan simbol lainnya

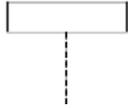
**Gambar 2.4** simbol *activity diagram*

Sumber : Gellysa Urva (2015)

### 2.8.3 *Sequence Diagram*

Secara mudahnya *sequence diagram* adalah gambaran tahap demi tahap, termasuk kronologi (urutan) perubahan secara logis yang seharusnya dilakukan untuk menghasilkan sesuatu sesuai dengan *use case diagram*.

Tabel 2.3 Simbol *Sequence Diagram*

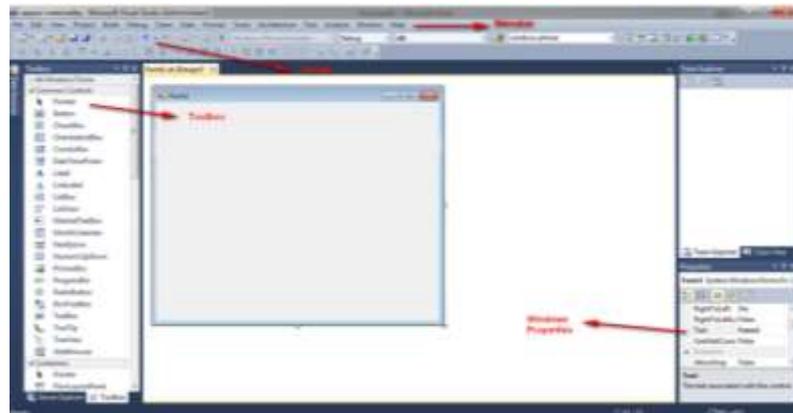
NO	GAMBAR	NAMA	KETERANGAN
1		<i>LifeLine</i>	Objek <i>entity</i> , antarmuka yang saling berinteraksi.
2		<i>Message</i>	Spesifikasi dari komunikasi antar objek yang memuat informasi-informasi tentang aktifitas yang terjadi
3		<i>Message</i>	Spesifikasi dari komunikasi antar objek yang memuat informasi-informasi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

Sumber : Gellysa Urva (2015)

## 2.9 *Visual Basic 2010*

*Visual Studio 2010* pada dasarnya adalah sebuah bahasa pemrograman komputer. Dimana pengertian dari bahasa pemrograman itu adalah perintah-perintah atau instruksi yang dimengerti oleh komputer untuk melakukan tugas-tugas tertentu. *Visual basic* adalah sebuah bahasa pemrograman yang berpusat pada object (*Object Oriented Programming*) digunakan dalam pembuatan aplikasi *Windows* yang berbasis *Graphical User Interface*, hal ini menjadikan *Visual Basic* menjadi bahasa pemrograman yang wajib diketahui dan dikuasai oleh setiap *programmer*. (Ninuk & Syadid, 2017).

*Toolbox* ditempatkan disebelah kiri jendela kerja. Dibawah ini adalah *screenshot* tampilan *Visual Basic 2010* :

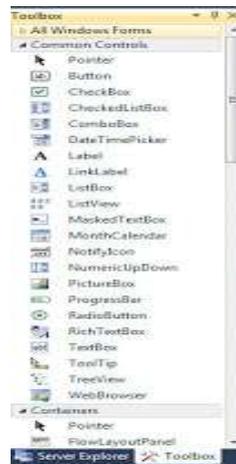


**Gambar 2.5 Tampilan VB 2010**

Sumber : [blogspot.com](http://blogspot.com) (2016)

### ***Toolbox***

*Toolbox* merupakan komponen lingkungan kerja VB yang berisikan *tool-tool* untuk ditempatkan di *form*. Jika kita membuat sebuah aplikasi, maka komponen-komponen tersebut akan kita tempatkan di *form* dan menjadi komponen jendela program.

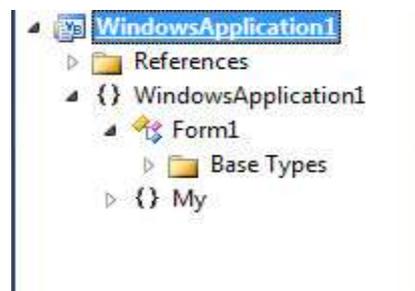


**Gambar 2.6 Tampilan Toolbox**

Sumber : [blogspot.com](http://blogspot.com) (2016)

### ***Windows Project***

*Window Project* berfungsi untuk menampilkan daftar *form* dan *modul* yang terdapat di *project* aplikasi yang sedang dikerjakan.



**Gambar 2.7 Tampilan windows project**

Sumber : [blogspot.com](http://blogspot.com) (2016)

### ***Windows Properties***

*Windows Properties* berfungsi untuk menampilkan daftar properti dari sebuah komponen yang sedang aktif. Kita dapat mengubah properti dari sebuah komponen dengan cara mengaktifkan (mengklik/memilih) komponen tersebut, kemudian mengubah nilai propertinya di *Window Properties*.



**Gambar 2.8** Tampilan *Windows properties*

Sumber : [blogspot.com](http://blogspot.com) (2016)

## 2.10 Tabel *ASCII*

*ASCII* (*American Standard Code for Information Interchange*) atau kode Standar Amerika untuk Pertukaran Informasi. Merupakan suatu standar internasional dalam kode huruf dan lumeri seperti *Hex* dan *Unicode* tetapi *ASCII* lebih bersifat *universal*, contohnya 124 adalah untuk karakter “|”. Dalam *kriptografi*, kode *ASCII* ini merupakan urutan bit yang akan mewakili teks asli yang kemudian *dienkripsi* untuk mendapatkan teks kode dalam bentuk urutan bit. *ASCII* memerlukan 8 bit untuk mendapatkan satu karakter dan blok kode mempunyai 64 bit untuk satu blok (Rizky & Muhammad, 2017).

Tabel 2.4 Tabel ASCII

The ASCII code

American Standard Code for Information Interchange

www.theasciicode.com.ar

ASCII control characters				ASCII printable characters				Extended ASCII characters								
DEC	HEX	Simbolo ASCII		DEC	HEX	Simbolo		DEC	HEX	Simbolo		DEC	HEX	Simbolo		
00	00h	NULL	(carácter nulo)	32	20h	espacio		128	80h	Ç	160	A0h	à	192	C0h	À
01	01h	SOH	(inicio encabezado)	33	21h	!		129	81h	ü	161	A1h	í	193	C1h	Á
02	02h	STX	(inicio texto)	34	22h	"		130	82h	é	162	A2h	ò	194	C2h	Â
03	03h	ETX	(fin de texto)	35	23h	#		131	83h	à	163	A3h	ó	195	C3h	Ã
04	04h	EOT	(fin transmisión)	36	24h	\$		132	84h	ä	164	A4h	ô	196	C4h	Ä
05	05h	ENQ	(enquiry)	37	25h	%		133	85h	å	165	A5h	ñ	197	C5h	Å
06	06h	ACK	(acknowledgement)	38	26h	&		134	86h	ä	166	A6h	°	198	C6h	Ä
07	07h	BEL	(timbre)	39	27h	'		135	87h	ç	167	A7h	°	199	C7h	Å
08	08h	BS	(retroceso)	40	28h	(		136	88h	è	168	A8h	°	200	C8h	Ä
09	09h	HT	(tab horizontal)	41	29h	)		137	89h	é	169	A9h	°	201	C9h	Ä
10	0Ah	LF	(salto de línea)	42	2Ah	+		138	8Ah	è	170	AAh	°	202	CAh	Ä
11	0Bh	VT	(tab vertical)	43	2Bh	*		139	8Bh	í	171	ABh	½	203	CBh	Ä
12	0Ch	FF	(form feed)	44	2Ch	,		140	8Ch	ì	172	ACH	¼	204	CAh	Ä
13	0Dh	CR	(retorno de carro)	45	2Dh	.		141	8Dh	í	173	ADh	½	205	CDh	Ä
14	0Eh	SO	(shift Out)	46	2Eh	.		142	8Eh	Ā	174	Aeh	°	206	CEh	Ä
15	0Fh	SI	(shift In)	47	2Fh	/		143	8Fh	Ā	175	Afh	°	207	CFh	Ä
16	10h	DLE	(data link escape)	48	30h	0		144	90h	Ē	176	B0h	°	208	DOh	Ä
17	11h	DC1	(device control 1)	49	31h	1		145	91h	æ	177	B1h	°	209	D1h	Ä
18	12h	DC2	(device control 2)	50	32h	2		146	92h	Æ	178	B2h	°	210	D2h	Ä
19	13h	DC3	(device control 3)	51	33h	3		147	93h	ø	179	B3h	°	211	D3h	Ä
20	14h	DC4	(device control 4)	52	34h	4		148	94h	ø	180	B4h	°	212	D4h	Ä
21	15h	NAK	(negative acknowle.)	53	35h	5		149	95h	ø	181	B5h	°	213	D5h	Ä
22	16h	SYN	(synchronous idle)	54	36h	6		150	96h	ü	182	B6h	°	214	D6h	Ä
23	17h	ETB	(end of trans. block)	55	37h	7		151	97h	ü	183	B7h	°	215	D7h	Ä
24	18h	CAN	(cancel)	56	38h	8		152	98h	y	184	B8h	°	216	D8h	Ä
25	19h	EM	(end of medium)	57	39h	9		153	99h	O	185	B9h	°	217	D9h	Ä
26	1Ah	SUB	(substitute)	58	3Ah	:		154	9Ah	U	186	BAh	°	218	DAh	Ä
27	1Bh	ESC	(escape)	59	3Bh	;		155	9Bh	ø	187	BBh	°	219	DBh	Ä
28	1Ch	FS	(file separator)	60	3Ch	<		156	9Ch	£	188	BCh	°	220	DCh	Ä
29	1Dh	GS	(group separator)	61	3Dh	>		157	9Dh	∅	189	BDh	°	221	DDh	Ä
30	1Eh	RS	(record separator)	62	3Eh	>		158	9Eh	x	190	BEh	°	222	DEh	Ä
31	1Fh	US	(unit separator)	63	3Fh	?		159	9Fh	f	191	BFh	°	223	DFh	Ä
127	20h	DEL	(delete)													

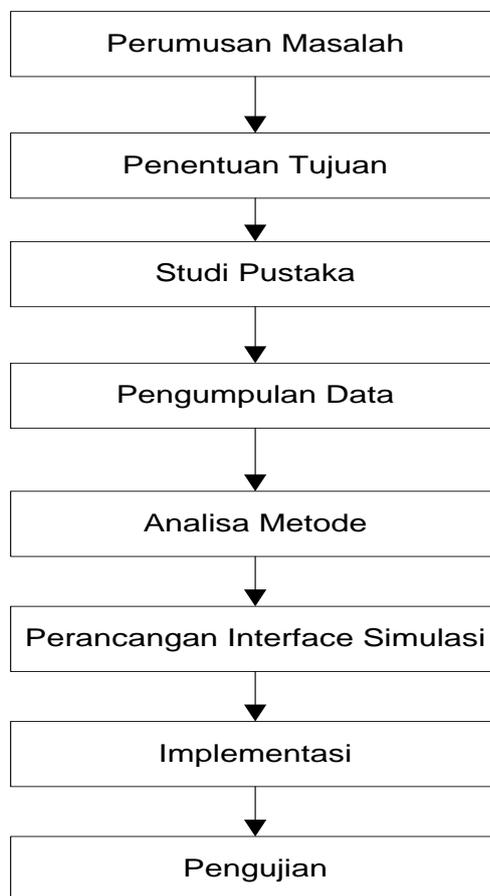
Sumber : <https://theasciicode.com.ar/> (2012)

## BAB III

### METODE PENELITIAN

#### 3.1 Tahapan Penelitian

Adapun tahapan penelitian yang dilakukan oleh penulis ini dengan judul implementasi *kriptografi gronsfeld chiper* dalam mengamankan file *spreadsheet* pada data keuangan adalah sebagai berikut :



**Gambar 3.1** Tahapan Penelitian

Sumber : *Ms. Word* 2010 (2019)

## **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 yaitu :

### **3.2.1 Penelitian Kepustakaan (*Library Research*)**

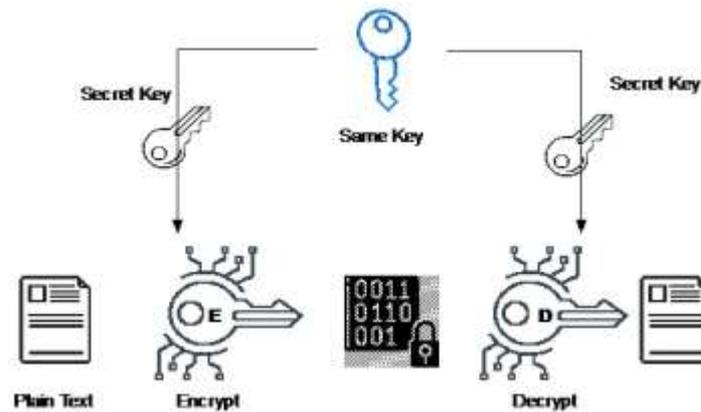
Merupakan cara untuk mencari referensi dengan mengumpulkan bahan-bahan pustaka yang dilakukan di perpustakaan kampus, maupun perpustakaan umum, juga melakukan pencarian lewat internet, dengan mengunjungi situs-situs seperti *google Book online* yang dapat membantu pembahasan materi.

### **3.2.2 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.

## **3.3 Analisis Sistem Sedang 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** Analisis Permasalahan yang Berjalan

Sumber : <https://socs.binus.ac.id> (2018)

### 3.3.1 Proses Pemasukkan Data

Pada tahap ini penulis membuat data keuangan pada file *excel* yang akan digunakan pada *gronsfeld cipher* untuk proses enkripsi dan deskripsi

The screenshot shows a Microsoft Excel spreadsheet titled "LAPORAN GAJI KARYAWAN". The spreadsheet has the following data:

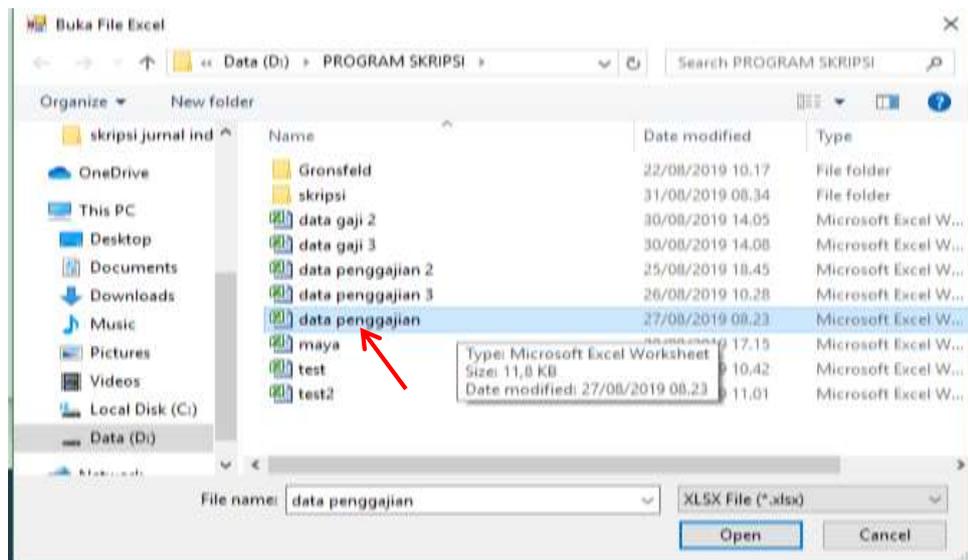
No	Nama Karyawan	Jabatan	Gaji Pokok	Tunjangan	Pajak	Total Gaji
1	Andiansyah	Pimpinan	3.500.000	175.000	367.500	3.307.500
2	Heandrik	Marketing	2.000.000	100.000	210.000	1.890.000
3	Yuni	Sekretaris	1.800.000	90.000	189.000	1.701.000
4	Mimi	Keuangan	1.700.000	85.000	178.500	1.606.500
5	Lukman	Admin	1.500.000	75.000	157.500	1.417.500
6	Mukait	Programmer	2.000.000	100.000	210.000	1.890.000
7	Adi	Telesi	1.800.000	90.000	189.000	1.701.000
8	Maya	Analisa	2.500.000	125.000	262.500	2.362.500
9	Sukardi	Kepala Bag	3.000.000	150.000	315.000	2.835.000
10	Heindra	Security	1.800.000	90.000	189.000	1.701.000

**Gambar 3.3** Pembuatan File Excel

Sumber : *Ms. Excel* 2010 (2019)

### 3.3.2 Proses Transaksi Data

Pada saat program dijalankan pengambilan data untuk proses *enkripsi* dan *deskripsi* akan langsung mengarah pada penyimpanan *local disk* komputer dimana data file tersebut tersimpan.

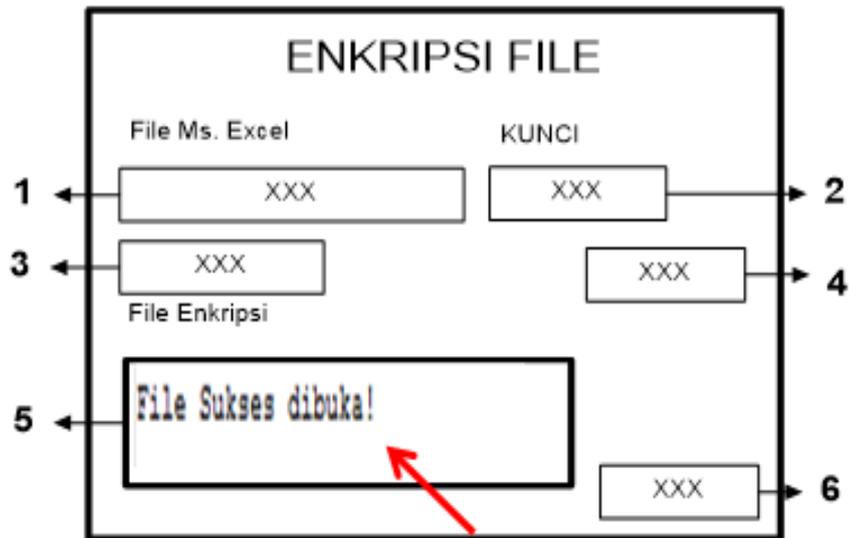


**Gambar 3.4** Transaksi Pengambilan Data

Sumber : *Local Disk D* (2019)

### 3.3.3 Proses Laporan

Pada saat proses pengambilan file di *local disk* maka akan muncul laporan di form bahwa proses pengambilan file tersebut berhasil.

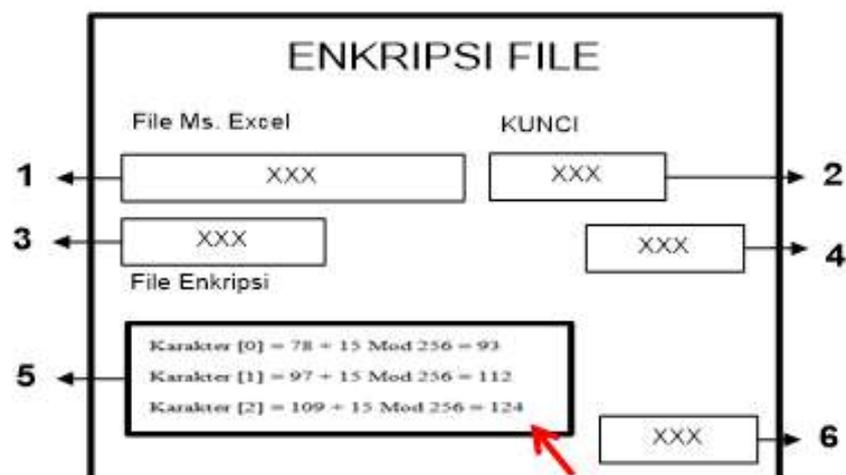


Gambar 3.5 Laporan

Sumber : Ms. Word 2010 (2019)

### 3.3.4 Kelemahan-Kelemahan Proses Sistem Sedang Berjalan

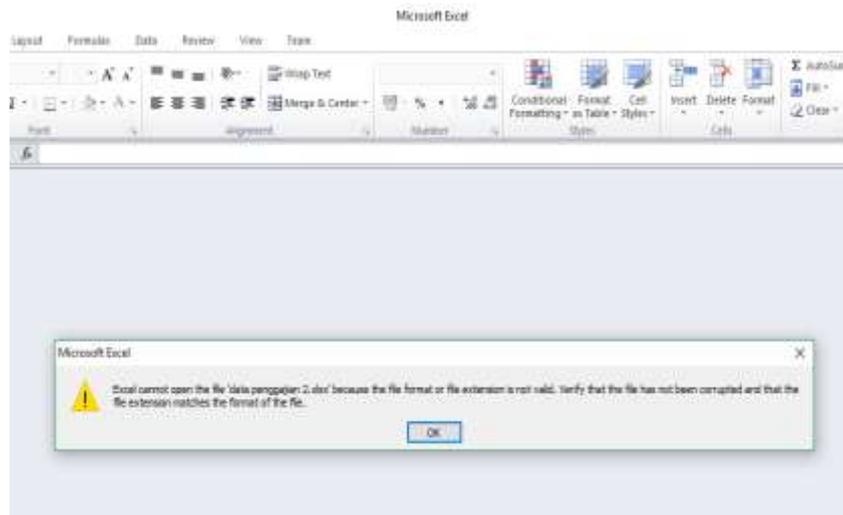
- Sulit untuk mengetahui hasil dari *enkripsi* dan *deskripsi* yang telah di berikan kunci pada saat keterangan hasil dari *enkripsi* dan *deskripsi* muncul pada form keterangan



Gambar 3.6 Keterangan Hasil Enkripsi

Sumber : Ms. Excel 2010 (2019)

- Pada saat file yang telah di enkripsi dan telah di simpan kembali pada *local disk*, file tersebut tidak akan bisa di buka.

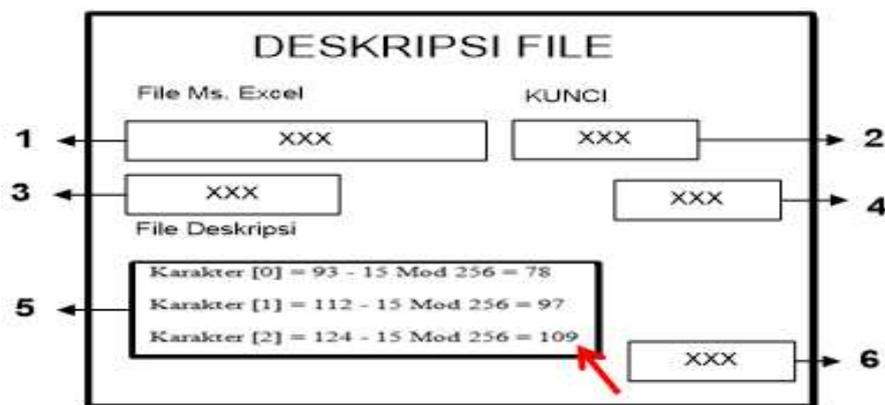


**Gambar 3.7** Hasil *Enkripsi*

Sumber : *Ms. Excel* 2010 (2019)

### 3.3.5 Analisis Kebutuhan Sistem

Pada saat file enkripsi ingin dikembalikan ke file aslinya maka file harus di deskripsikan agar file tersebut bisa dibuka kembali.



**Gambar 3.8** Keterangan Hasil Akhir

Sumber : *Ms. Word* 2010 (2019)

### 3.4 Rancangan Penelitian

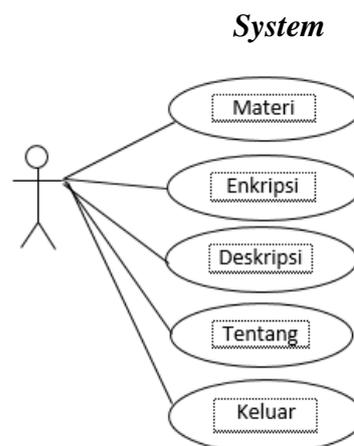
Analisis kebutuhan sistem merupakan analisis yang dibutuhkan untuk menentukan spesifikasi kebutuhan sistem. Spesifikasi ini juga meliputi elemen atau komponen – komponen apa saja yang dibutuhkan untuk sistem yang akan dibangun sampai dengan sistem tersebut diimplementasikan. Analisis kebutuhan ini juga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

#### 3.4.1 Perancangan Berorientasi Objek

Perancangan atau p emodelan berorientasi objek merupakan proses mendapatkan informasi dari model dan menampilkannya secara grafik dengan menggunakan sebuah standar elemen grafik.

##### 1. *Use case Diagram*

Berikut adalah *use case diagram* yang menggambarkan kegiatan.



**Gambar 3.9** *Use Case Diagram*

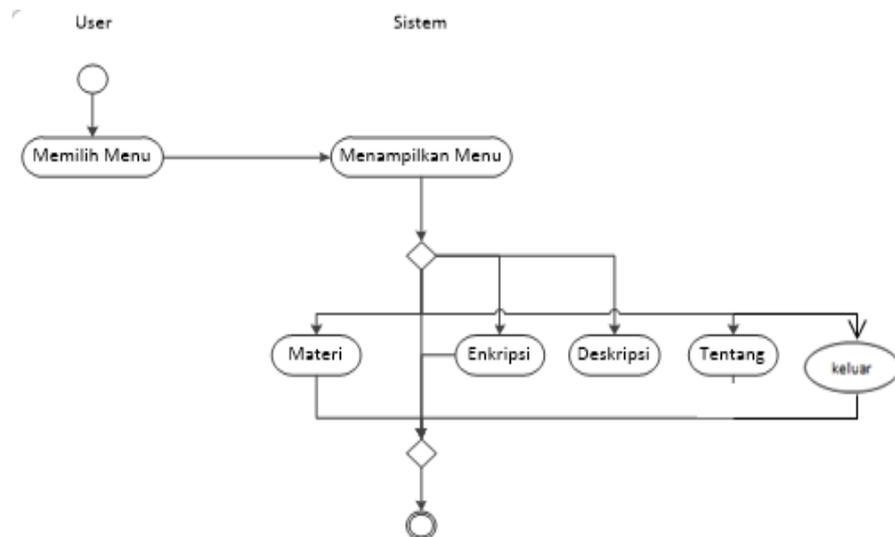
Sumber : *Ms. Word 2010 (2019)*

Keterangan :

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

## 2. Activity Diagram

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

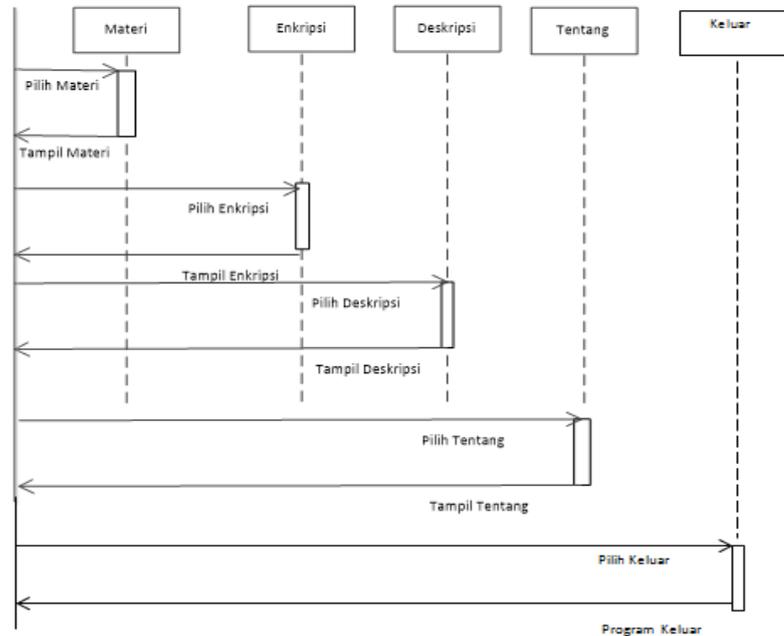


**Gambar 3.10** Activity Diagram

Sumber : Ms. Word 2010 (2019)

## 3. Sequence Diagram

*Sequence Diagram* menggambarkan tahap-tahap proses berjalannya program sesuai dengan *Use Case*.



**Gambar 3.11** *Sequence Diagram*

Sumber : *Ms. Word 2010 (2019)*

Keterangan :

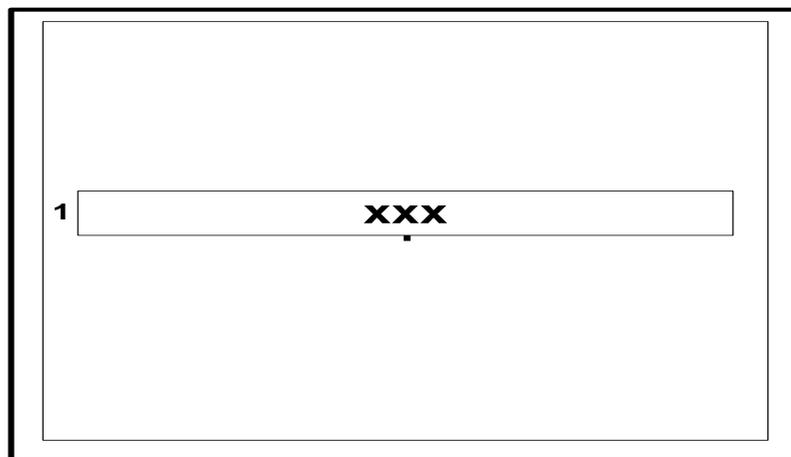
1. Dalam diagram di atas menjelaskan bahwa *user* memilih materi kemudian sistem menampilkan materi yang berkaitan dengan materi
2. *User* *merequest enkripsi* kemudian sistem menampilkan menu *enkripsi*
3. *User* *merequest deskripsi* kemudian sistem menampilkan menu *deskripsi*
4. *User* *merequest* menu tentang kemudian sistem menampilkan form tentang.
5. *User* *merequest* menu keluar kemudian sistem akan keluar dari program

### 3.4.2 Perancangan Antarmuka

Perancangan ini dibuat sebelum program yang asli berhasil di buat, agar dapat mempermudah dalam hal mendesain program.

#### 1. Rancangan Halaman Judul

Halaman judul merupakan halaman yang pertama muncul pada saat program dijalankan.



**Gambar 3.12** Rancangan Halaman Judul

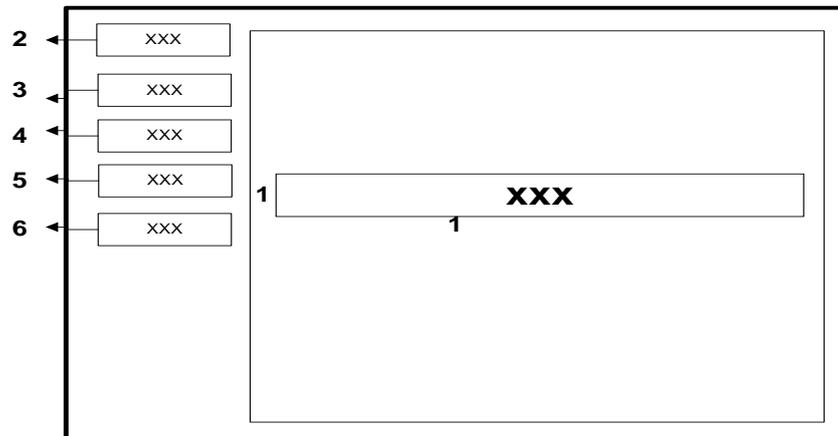
Sumber : *Ms. Word* 2010 (2019)

Keterangan:

1. Berfungsi untuk menampilkan judul program.

#### 2. Rancangan Halaman Menu Utama

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



**Gambar 3.13** Rancangan Halaman Menu Utama

Sumber : *Ms. Word* 2010 (2019)

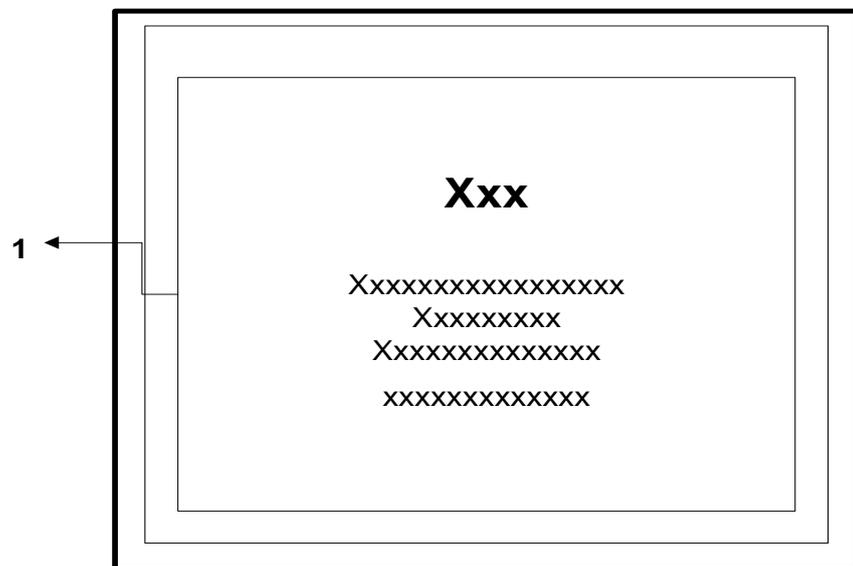
Pada tampilan di atas terdapat 5 tombol yaitu Judul, Materi, *Enkripsi*, *Deskripsi*, Tentang dan keluar.

Keterangan:

1. Tombol Berfungsi untuk menampilkan judul
2. Tombol Materi berfungsi untuk menghubungkan pengguna ke form materi.
3. Tombol *Enkripsi* berfungsi untuk menghubungkan pengguna ke form *Enkripsi*.
4. Tombol *Deskripsi* berfungsi untuk menampilkan form *Deskripsi*.
5. Tombol Tentang berfungsi untuk menghubungkan pengguna ke form tentang.
6. 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 3.14** Rancangan Halaman Materi

Sumber : *Ms. Word* 2010 (2019)

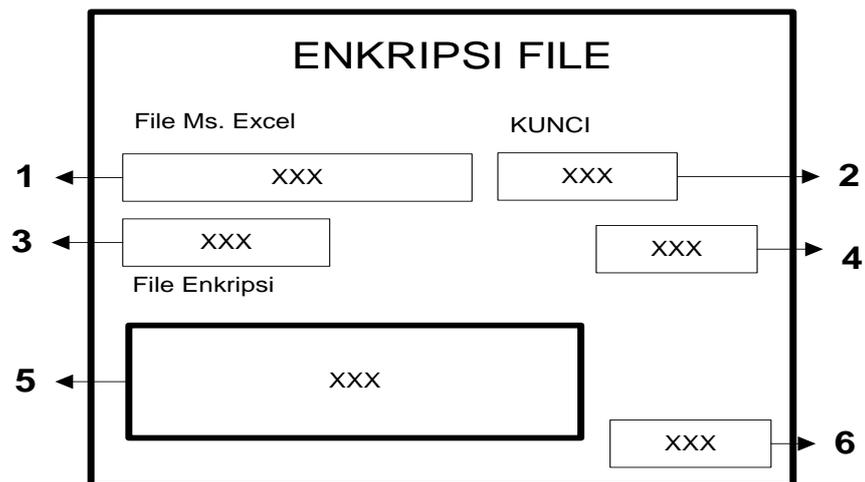
Keterangan:

1. Tombol Materi Berfungsi untuk menampilkan Materi tentang penggunaan kunci pada *Kriptografi Gronsfeld Cipher*

### 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.



**Gambar 3.15** Rancangan Halaman Enkripsi

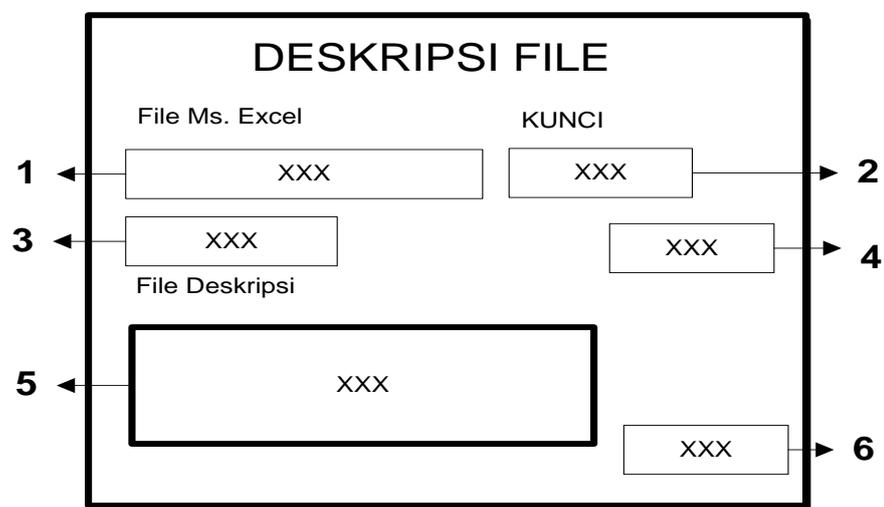
Sumber : *Ms. Word 2010 (2019)*

Keterangan:

1. Berfungsi untuk menampilkan nama *Ms. Excel* yang sudah di upload.
2. Berfungsi untuk menginputkan kunci untuk mengenkripsi *Ms. Excel*.
3. Tombol yang berfungsi untuk mencari *Ms. Excel* yang ingin di *enkripsi*.
4. Tombol yang berfungsi untuk melakukan proses *enkripsi* pada *Ms. Excel* menggunakan *Gronsfeld*.
5. Berfungsi untuk menampilkan hasil dari proses *enkripsi* dari sebuah *Ms. Excel*.
6. Tombol untuk menyimpan hasil dari *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.



**Gambar 3.16** Rancangan Halaman Deskripsi

Sumber : *Ms. Word 2010 (2019)*

Keterangan:

1. Berfungsi untuk menampilkan nama *Ms. Excel* yang sudah di upload.
2. Berfungsi untuk menginputkan kunci untuk *mendeskripsi Ms. Excel*.
3. Tombol yang berfungsi untuk mencari *Ms. Excel* yang ingin di *deskripsi*.

4. Tombol yang berfungsi untuk melakukan proses *deskripsi* pada *Ms. Excel* menggunakan *Gronsfeld*.
5. Berfungsi untuk menampilkan hasil dari proses deskripsi dari sebuah *Ms. Excel*.
6. Tombol untuk menyimpan hasil *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 Tentang

Pada form ini membahas tentang sejarah munculnya gronsfeld.



**Gambar 3.17** Tampilan Halaman Tentang

Sumber : *Ms. Word* 2010 (2019)

Keterangan :

1. Tombol Tentang Berfungsi untuk menampilkan tentang sejarah munculnya *gronsfeld*.

## **7. Rancangan Halaman Keluar**

form keluar digunakan untuk memerintahkan pengguna keluar dari program.

## BAB IV

### HASIL DAN PEMBAHASAN

#### 4.1 **Kebutuhan Spesifikasi *Minimum Hardware dan Software***

Dalam membuat program ini di butuhkan *hardware* dan *software* yang dapat membantu dalam menyelesaikan program tersebut :

##### 1. Perangkat Keras (*Hardware*)

Perangkat keras minimum yang digunakan untuk membangun keamanan *kriptografi gronsfeld cipher* ini adalah

- a. Processor
- b. RAM 2 Gb
- c. *Keyboard* dan *Mouse*
- d. Monitor atau Laptop

##### 2. Analisis Perangkat Lunak (*Software*)

Untuk mendukung membangun suatu fasilitas yang memadai. Yaitu berupa perangkat lunak (*software*) yang dirancang untuk memudahkan dalam pembangunan dan menjalankan sisten nantinya. Adapun perangkat lunak yang digunakan adalah sebagai berikut :

- a. *Microsoft Windows 10*
- b. *Microsoft Visual Studio 2010*
- c. *Microsoft Office 2010*

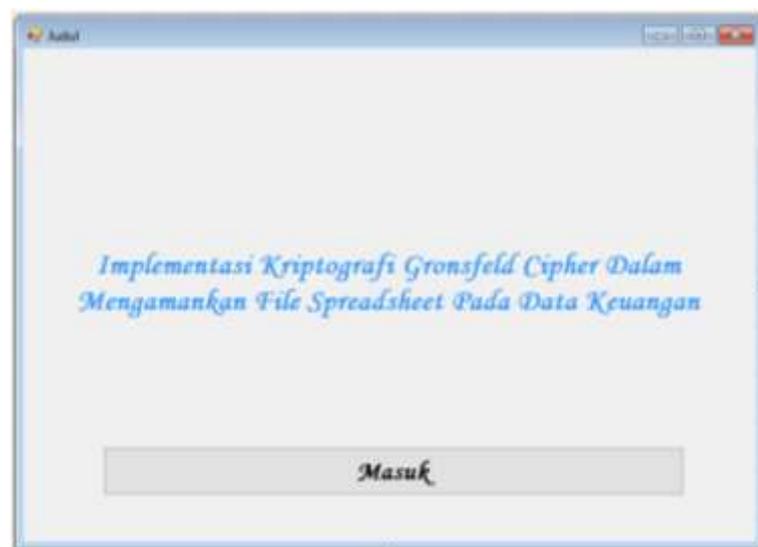
## 4.2 Pengujian Aplikasi dan Pembahasan

### 4.2.1 Implementasi Sistem

Tahap implementasi merupakan lanjutan dari tahap perancangan sistem. Pada tahap ini dilakukan implementasi sistem ke dalam bahasa pemrograman berdasarkan hasil analisa dan perancangan sistem. Pada tahap implementasi ini digunakan perangkat lunak dan perangkat keras, sehingga sistem yang dibangun dapat diselesaikan dengan baik.

#### 1. Tampilan Halaman Judul

Halaman ini merupakan halaman yang muncul pertama sekali pada saat sistem dijalankan. Tampilan halaman judul dapat dilihat pada gambar berikut :



**Gambar 4.1** Tampilan Halaman Judul

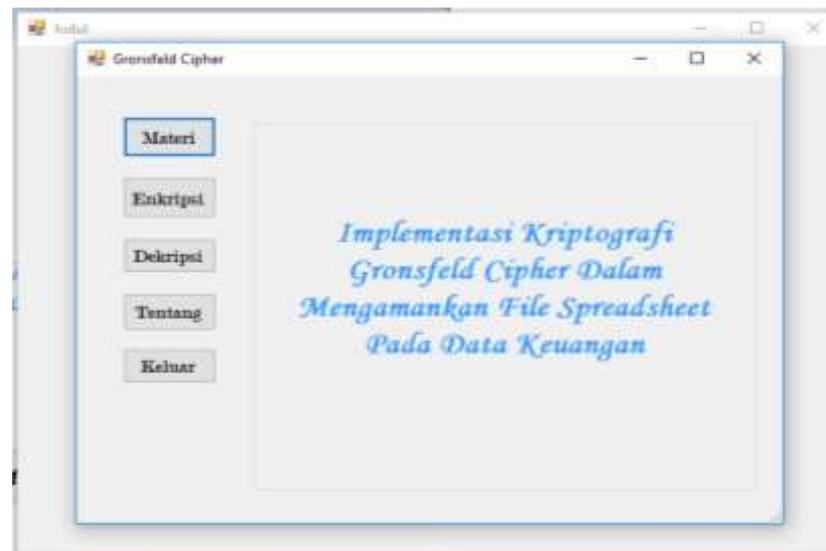
Sumber : *Visual Basic 2010* (2019)

Keterangan:

1. Klik tombol masuk, untuk masuk kehalaman Utama

## 2. Tampilan Halaman Utama

Halaman ini merupakan halaman yang muncul pada saat tombol masuk di klik. Tampilan halaman utama dapat dilihat pada gambar berikut :



**Gambar 4.2** Tampilan Halaman Utama

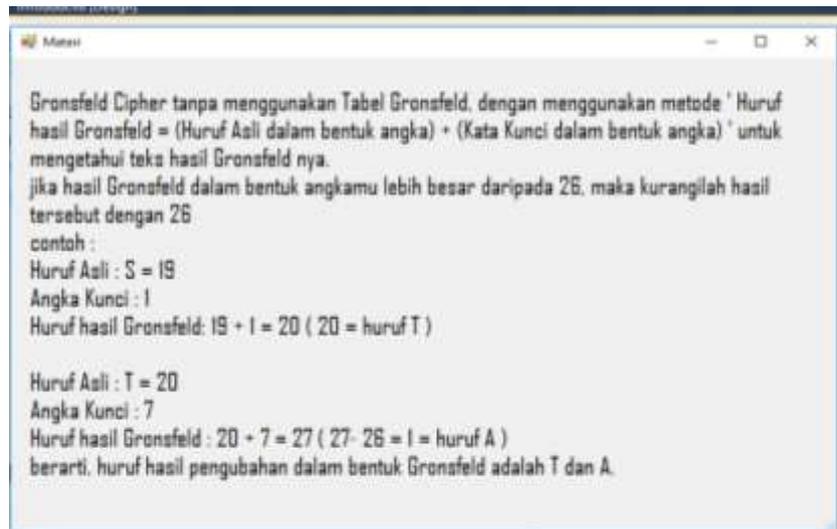
Sumber : *Visual Basic 2010* (2019)

Keterangan:

Pada halaman utama terdapat beberapa menu yang dapat dipilih.

## 3. Tampilan Halaman Materi

Ketika materi di klik maka akan muncul petunjuk tentang penggunaan kunci *gronfeld* seperti pada gambar berikut :

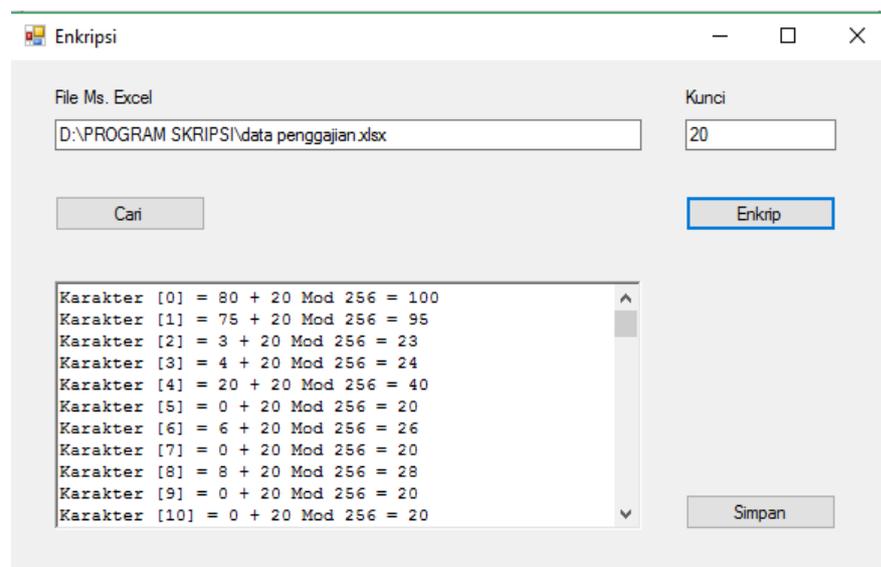


**Gambar 4.3** Tampilan Materi

Sumber : *Visual Basic 2010 (2019)*

#### 4. Tampilan Halaman Enkripsi

Ketika menu *enkripsi* di klik maka akan muncul tampilan form untuk mengenkripsi file *excel* seperti pada gambar berikut :



**Gambar 4.4** Tampilan Enkripsi

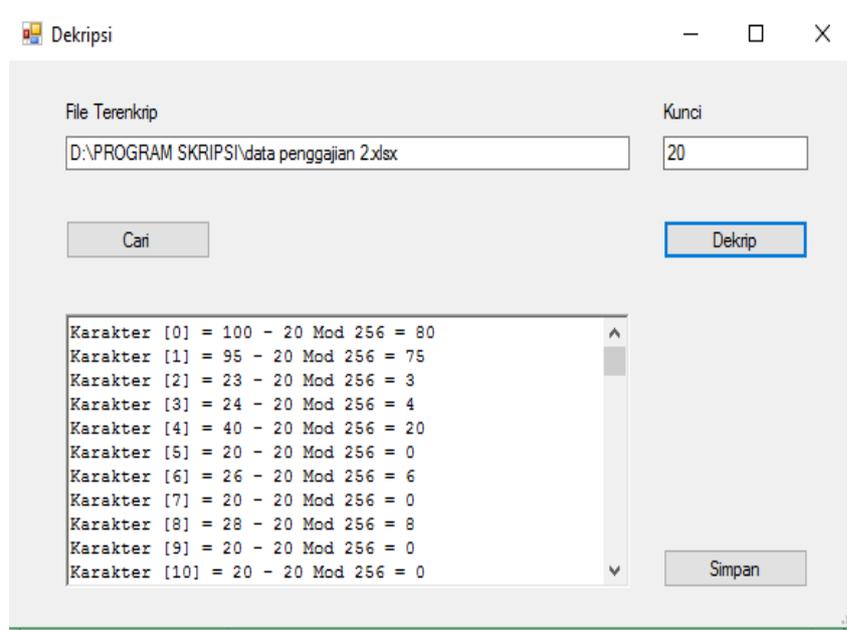
Sumber : *Visual Basic 2010 (2019)*

Keterangan :

1. Klik tombol cari, untuk mencari file yang akan di *enkripsi*
2. Setelah file ditemukan, ketikkan kunci di form kunci
3. Lalu klik tombol *enkripsi*
4. Maka akan muncul keterangan hasil *enkripsi* pada form hasil
5. Lalu klik tombol simpan, untuk menyimpan hasil *enkripsi*

## 5. Tampilan Halaman Deskripsi

Ketika menu *deskripsi* di klik maka akan muncul tampilan form untuk mendeskripsikan file *excel* seperti pada gambar berikut :



**Gambar 4.5** Tampilan *Deskripsi*

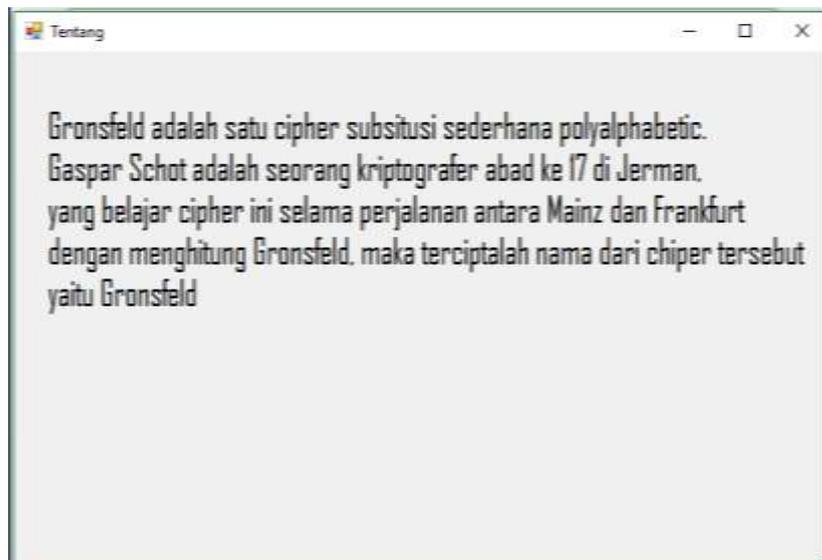
Sumber : *Visual Basic* 2010 (2019)

Keterangan :

1. Klik tombol cari untuk mencari file *excel* yang sudah di *enkripsi*
2. Lalu ketikkan kunci yang sama pada saat mengenkripsi file tersebut
3. Klik tombol *deskripsi*
4. Maka akan muncul keterangan hasil *deskripsi* di form hasil
5. Klik tombol simpan untuk menyimpan file hasil *deskripsi*

## 6. Tampilan Halaman Tentang

Ketika menu Tentang di klik maka akan muncul tampilan form yang berisi tentang sejarah munculnya *gronsfeld* seperti pada gambar berikut :



**Gambar 4.6** Tampilan Tentang

Sumber : *Visual Basic* 2010 (2019)

## 7. Tampilan Halaman Keluar

Pada saat klik tombol keluar, maka pengguna akan keluar dari program

### 4.3 Pengujian Sistem

Perangkat lunak adalah elemen kritis dari jaminan kualitas perangkat lunak dan merepresentasikan kajian pokok dari spesifikasi, perancangan, dan pengkodean. Pengujian yang digunakan untuk menguji secara manual perhitungan *enkripsi* dan *dekripsi* menggunakan algoritma *Gronsfeld*.

#### 4.3.1 Enkripsi

Bagian ini akan dilakukan pengujian terhadap file Spreadsheet yang berisi kalimat “Nama saya adalah Maya Sari” dengan *key* “15” dan Mod 255.

Contoh :

- Karakter dimulai [0] = 78 (N, dilihat dari tabel ASCII) + 15 (*Key*) Mod 255  
= 93 (hasil)

Hasil perhitungan *Gronsfeld cipher* dapat dilihat pada kalkulasi berikut ini:

$$\text{Karakter [0]} = 78 + 15 \text{ Mod } 255 = 93$$

$$\text{Karakter [1]} = 97 + 15 \text{ Mod } 255 = 112$$

$$\text{Karakter [2]} = 109 + 15 \text{ Mod } 255 = 124$$

$$\text{Karakter [3]} = 97 + 15 \text{ Mod } 255 = 112$$

$$\text{Karakter [4]} = 32 + 15 \text{ Mod } 255 = 47$$

$$\text{Karakter [5]} = 115 + 15 \text{ Mod } 255 = 130$$

$$\text{Karakter [6]} = 97 + 15 \text{ Mod } 255 = 112$$

$$\text{Karakter [7]} = 121 + 15 \text{ Mod } 255 = 136$$

$$\text{Karakter [8]} = 97 + 15 \text{ Mod } 255 = 112$$

$$\text{Karakter [9]} = 32 + 15 \text{ Mod } 255 = 47$$

$$\text{Karakter [10]} = 97 + 15 \text{ Mod } 255 = 112$$

$$\text{Karakter [11]} = 100 + 15 \text{ Mod } 255 = 115$$

$$\text{Karakter [12]} = 97 + 15 \text{ Mod } 255 = 112$$

$$\text{Karakter [13]} = 108 + 15 \text{ Mod } 255 = 123$$

$$\text{Karakter [14]} = 97 + 15 \text{ Mod } 255 = 112$$

$$\text{Karakter [15]} = 104 + 15 \text{ Mod } 255 = 119$$

$$\text{Karakter [16]} = 32 + 15 \text{ Mod } 255 = 47$$

$$\text{Karakter [17]} = 77 + 15 \text{ Mod } 255 = 92$$

$$\text{Karakter [18]} = 97 + 15 \text{ Mod } 255 = 112$$

$$\text{Karakter [19]} = 121 + 15 \text{ Mod } 255 = 136$$

$$\text{Karakter [20]} = 97 + 15 \text{ Mod } 255 = 112$$

$$\text{Karakter [21]} = 32 + 15 \text{ Mod } 255 = 47$$

$$\text{Karakter [22]} = 83 + 15 \text{ Mod } 255 = 98$$

$$\text{Karakter [23]} = 97 + 15 \text{ Mod } 255 = 112$$

$$\text{Karakter [24]} = 114 + 15 \text{ Mod } 255 = 129$$

$$\text{Karakter [25]} = 105 + 15 \text{ Mod } 255 = 120$$

### 4.3.2 Dekripsi

Bagian ini akan dilakukan pengembalian hasil *enkripsi* menjadi *plaintext* awal.

Contoh :

- Karakter dimulai [0] = 93 ( ), dilihat dari tabel ASCII) - 15 (*Key*) Mod 255  
= 78 (hasil)

Hasil perhitungan *dekripsi* menggunakan *Gronsfeld cipher* dapat dilihat pada kalkulasi berikut ini:

$$\text{Karakter [0]} = 93 - 15 \text{ Mod } 255 = 78$$

$$\text{Karakter [1]} = 112 - 15 \text{ Mod } 255 = 97$$

$$\text{Karakter [2]} = 124 - 15 \text{ Mod } 255 = 109$$

$$\text{Karakter [3]} = 112 - 15 \text{ Mod } 255 = 97$$

$$\text{Karakter [4]} = 47 - 15 \text{ Mod } 255 = 32$$

$$\text{Karakter [5]} = 130 - 15 \text{ Mod } 255 = 115$$

$$\text{Karakter [6]} = 112 - 15 \text{ Mod } 255 = 97$$

$$\text{Karakter [7]} = 136 - 15 \text{ Mod } 255 = 121$$

$$\text{Karakter [8]} = 112 - 15 \text{ Mod } 255 = 97$$

$$\text{Karakter [9]} = 47 - 15 \text{ Mod } 255 = 32$$

$$\text{Karakter [10]} = 112 - 15 \text{ Mod } 255 = 97$$

$$\text{Karakter [11]} = 115 - 15 \text{ Mod } 255 = 100$$

$$\text{Karakter [12]} = 112 - 15 \text{ Mod } 255 = 97$$

$$\text{Karakter [13]} = 123 - 15 \text{ Mod } 255 = 108$$

$$\text{Karakter [14]} = 112 - 15 \text{ Mod } 255 = 97$$

$$\text{Karakter [15]} = 119 - 15 \text{ Mod } 255 = 104$$

$$\text{Karakter [16]} = 47 - 15 \text{ Mod } 255 = 32$$

$$\text{Karakter [17]} = 92 - 15 \text{ Mod } 255 = 77$$

$$\text{Karakter [18]} = 112 - 15 \text{ Mod } 255 = 97$$

$$\text{Karakter [19]} = 136 - 15 \text{ Mod } 255 = 121$$

$$\text{Karakter [20]} = 112 - 15 \text{ Mod } 255 = 97$$

$$\text{Karakter [21]} = 47 - 15 \text{ Mod } 255 = 32$$

$$\text{Karakter [22]} = 98 - 15 \text{ Mod } 255 = 83$$

$$\text{Karakter [23]} = 112 - 15 \text{ Mod } 255 = 97$$

$$\text{Karakter [24]} = 129 - 15 \text{ Mod } 255 = 114$$

$$\text{Karakter [25]} = 120 - 15 \text{ Mod } 255 = 105$$

Hasil *dekripsi* kembali seperti awal yaitu “Nama saya adalah Maya Sari”.

#### 4.4 Pengujian Aplikasi

Pengujian aplikasi perlu di lakukan untuk mengetahui bahwa aplikasi tersebut berjalan sesuai keinginan atau tidak.

**Tabel 4.1** Pengujian Aplikasi

No.	Pengujian Forum	Pengujian Botton	Hasil
1.	Halaman Judul	Masuk	<input checked="" type="checkbox"/> Berhasil <input type="checkbox"/> Tidak
2.	Halaman Utama	Materi	<input checked="" type="checkbox"/> Berhasil <input type="checkbox"/> Tidak
		Enkripsi	<input checked="" type="checkbox"/> Berhasil <input type="checkbox"/> Tidak

		Deskripsi	<input checked="" type="checkbox"/> Berhasil	<input type="checkbox"/> Tidak
		Tentang	<input checked="" type="checkbox"/> Berhasil	<input type="checkbox"/> Tidak
		Keluar	<input checked="" type="checkbox"/> Berhasil	<input type="checkbox"/> Tidak
3.	Materi	-	<input checked="" type="checkbox"/> Berhasil	<input type="checkbox"/> Tidak
4.	Enkripsi	Cari	<input checked="" type="checkbox"/> Berhasil	<input type="checkbox"/> Tidak
		Enkripsi	<input checked="" type="checkbox"/> Berhasil	<input type="checkbox"/> Tidak
		Simpan	<input checked="" type="checkbox"/> Berhasil	<input type="checkbox"/> Tidak
5.	Deskripsi	Cari	<input checked="" type="checkbox"/> Berhasil	<input type="checkbox"/> Tidak
		Deskripsi	<input checked="" type="checkbox"/> Berhasil	<input type="checkbox"/> Tidak
		Simpan	<input checked="" type="checkbox"/> Berhasil	<input type="checkbox"/> Tidak
6.	Tentang	-	<input checked="" type="checkbox"/> Berhasil	<input type="checkbox"/> Tidak

Sumber : Ms. Word 2010 (2019)

## **BAB V**

### **PENUTUP**

#### **5.1 Kesimpulan**

Setelah keseluruhan proses dilakukan, yaitu dari perancangan hingga pengujian perangkat lunak, maka dapat diambil kesimpulan sebagai berikut:

1. *Algoritma kriptografi Gronsfeld cipher* dilakukan di file *spreadsheet* dengan menambahkan kunci kepada pesan asli sehingga pesan rahasia didapatkan.
2. Setelah dilakukan pengujian dengan file *spreadsheet*, sulit untuk membaca hasil dari *gronsfeld cipher*.
3. Ukuran file *spreadsheet* tidak berubah karena setiap hasil karakter pesan rahasia selalu di mod 255.
4. Kecepatan waktu proses bergantung pada besarnya file *spreadsheet* dan kecepatan prosessor komputer yang digunakan.

#### **5.2 Saran**

Adapun saran-saran yang dapat penulis berikan untuk pengembangan dan perbaikan sistem ini adalah sebagai berikut :

1. Penelitian tentang file *spreadsheet* ini dapat dikembangkan lagi dengan mencoba memperbaiki dalam proses penyimpanan file hasil *enkripsi* dan *deskripsi*.

2. Metode *enkripsi* dan *deskripsi* yang diterapkan pada file *spreadsheet* ini dapat di perbaiki lagi dalam kecepatan memproses hasil, agar untuk file *spreadsheet* yang memiliki kapasitas besar tidak memakan waktu yang lama.

## DAFTAR PUSTAKA

- Angga Aditya Permana, Desi Nurnaningsih. (2018). Rancangan Aplikasi Pengamanan Data Dengan Algoritma *Advanced Encryption Standard (Aes)*. Teknik Informatika. 11 (2). 177-186. Diakses dari <http://journal.uinjkt.ac.id>.
- Azanuddin. (2013). Penyandian Short Message Service (Sms) Pada Telepon Selular Dengan Menggunakan Algoritma Gronsfeld. *Pelita Informatika Budi Darma*. IV (1). 47-59. Diakses dari <https://ejurnal.stmik-budidarma.ac.id>.
- Fresly Nandar Pabokory, Indah Fitri Astuti, Awang Harsa Kridalaksana. (2015). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma *Advanced EncryptionStandard*. *Informatika Mulawarman*. 10 (1). 20-31. Diakses dari <http://e-journals.unmul.ac.id>.
- I M. Sarjana, K. Budi Susrusa, Dwi Putra Darmawan. (2013). Analisis Kinerja Keuangan Pada Koperasi Serba Usaha Di Kabupaten Buleleng. *Sarjana Manajemen Agribisnis*. I (2). 16-18. Diakses dari <https://ojs.unud.ac.id>
- Kiki Yulansari, Sukadi. (2013). Sistem Informasi Pengolahan Data Iuran Badan Pembantu Penyelenggaraan Pendidikan Sekolah Menengah Kejuruan Negeri 2 Donorojo. *Seruni - Seminar Riset Unggulan Nasional Informatika dan Komputer FTI UNSA*. 2 (1). 5-13. Diakses dari <https://ijns.org>.
- Muslim Setyo Rejeki, Ali Tarmuji. (2013). Membangun Aplikasi Autogenerate Script Ke Flowchart Untuk Mendukung Business Process Reengineering. *Sarjana Teknik Informatika*. 1 (2). 448-456. Diakses dari <https://www.neliti.com>.
- Ninuk Wiliani, Syadid Zambi. (2017). Rancang Bangun Aplikasi Kasir Tiket Nonton Bola Bareng Pada X Kasir Di Suatu Lokasi X Dengan Visual Basic 2010 Dan Mysql. *Rekayasa Informasi*. 6 (2). 77-83. Diakses dari <https://ejournal.istn.ac.id>.
- Perwitasari, I. D. (2018). Teknik Marker Based Tracking Augmented Reality untuk Visualisasi Anatomi Organ Tubuh Manusia Berbasis Android. *INTECOMS: Journal of Information Technology and Computer Science*, 1(1), 8-18.
- Puspita, Khairani, and Purwa Hasan Putra. "Penerapan Metode Simple Additive Weighting (SAW) Dalam Menentukan Pendirian Lokasi Gramedia Di Sumatera Utara." *Seminar Nasional Teknologi Informasi Dan Multimedia*, ISSN. 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.
- Putri, R. E., & Siahaan, A. (2017). Examination of document similarity using Rabin-Karp algorithm. *International Journal of Recent Trends in Engineering & Research*, 3(8), 196-201.
- 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).
- Rhady Dzulfanaldy Harminal, Asep Hidayat, Ria Herdhiana. (2016). Penerapan Pembelajaran Modular Berbasis Komputer Untuk Meningkatkan Keterampilan Siswa Dalam Membuat Paket Program Spreadsheet. Harminal, Hidayat & Herdhiana. 2 (1). 1-10. Diakses dari <http://jurnal.fkip.unla.ac.id>.
- Rizqi Sukma Kharisma, Muhammad Aziz Fatchu Rachman. (2017) Pembuatan Aplikasi Notes Menggunakan Algoritma Kriptografi Polyalphabetic Substitution Cipher Kombinasi Kode Ascii Dan Operasi Xor Berbasis Android. *Teknologi Informasi*. XII (35). 1-7. Diakses dari <https://jti.respati.ac.id>.
- Rizal, Chairul. "Pengaruh Varietas dan Pupuk Petroganik Terhadap Pertumbuhan, Produksi dan Viabilitas Benih Jagung (*Zea mays L.*)."  
*ETD Unsyiah* (2013).
- Ruwaida, D., & Kurnia, D. (2018). Rancang Bangun File Transfer Protocol (FTP) dengan Pengamanan Open SSL pada Jaringan VPN Mikrotik di SMK Dwiwarna. *CESS (Journal of Computer Engineering, System and Science)*, 3(1), 45-49.
- kbar, A. (2018). Pembangunan Model Electronic Government Pemerintahan Desa Menuju Smart Desa. *Jurnal Teknik dan Informatika*, 5(1), 1-5.
- 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.
- Sarif, M. I. (2017). Penemuan Aturan yang Berkaitan dengan Pola dalam Deret Berkala (Time Series).
- 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.
- Sitorus, Z. (2018). Kebutuhan Web Service untuk Sinkronisasi Data Antar Sistem Informasi dalam Universitas. *Jurnal Teknik dan Informatika*, 5(2), 87-90.

- Sumartono, I., Siahaan, A. P. U., & Mayasari, N. (2016). An overview of the RC4 algorithm. *IOSR J. Comput. Eng*, 18(6), 67-73.
- Supiyandi, S., Hermansyah, H., & Sembiring, K. A. (2020). Implementasi dan Penggunaan Algoritma Base64 dalam Pengamanan File Video. *Jurnal media informatika budidarma*, 4(2), 340-346.
- Suendri. (2018). Implementasi Diagram UML (Unified Modelling Language) Pada Perancangan Sistem Informasi Remunerasi Dosen Dengan Database Oracle (Studi Kasus: UIN Sumatera Utara Medan). *Ilmu Komputer dan Informatika*. 3 (1). 1-9. Diakses dari <https://jurnal.uinsu.ac.id>.