PENGAMANAN INFORMASI PADA KRIPTOGRAFI SIMETRIS MENGGUNAKAN TEKNIK ONE TIME PAD CIPHER

Disusun dan Diajukan untuk Memenuhi Persyaratan Ujian Akhir Memperoleh
Gelar Sarjana Komputer pada Fakultas Sains dan Teknologi
Universitas Pembangunan Panca Budi
Medan

SKRIPSI

OLEH:

NAMA	:	EDWIN ARIFSYAH SIDABUTAR
NPM	:	1614370329
PROGRAM STUDI	:	SISTEM KOMPUTER

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2020

LEMBAR PENGESAHAN

PENGAMANAN INFORMASI PADA KRIPTOGRAFI SIMETRIS MENGGUNAKAN TEKNIK ONE TIME PAD CIPHER

Disusun Oleh:

NAMA	:	EDWIN ARIFSYAH SIDABUTAR
NPM	:	1614370529
PROGRAM STUDI	:	SISTEM KOMPUTER

Skripsi Telah Disetujui oleh Dosen Pembimbing Skripsi
Pada Tanggal :

Dosen Pembimbing I	Dosen Pembimbing II
Muhammad Iqbal, S.Kom., M.Kom.	A. P. U. Siahaan, S.Kom., M.Kom.

Mengetahui:

Dekan Fakultas Sains dan Teknologi	Ketua Program Studi Sistem Komputer
Hamdani, S.T., M.T.	Eko Hariyanto, S.Kom., M.Kom.

SURAT PERNYATAAN

Saya yang bertandatangan di bawah ini :

Nama : Juanda Arifsyah Sidabutar

NPM : 1614370329

Prodi : Sistem Komputer

Konsentrasi : Keamanan Jaringan Komputer

Judul Skripsi : Pengamanan Informasi Pada Kriptografi Simetris Menggunakan Teknik One Time Pad Chiper

Dengan ini menyatakan bahwa :

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

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

Medan, 07 Oktober 2020

Yang membuat pernyataan

Edwin Arifsyah Sidabutar

SURAT PERNYATAAN

Saya Yang Bertanda Tangan Dibawah Ini :

Nama	:	EDWIN ARIFSYAH SIDABUTAR
N. P. M	:	1614370329
Tempat/Tgl. Lahir	:	SIDOARJO / 28 FEBRUARI 1999
Alamat	:	Jln.Gatot Subroto km 4,5 Medan
No. HP	:	081262851413
Nama Orang Tua	:	martin sidabutar/erika simatupang
Fakultas	:	SAINS & TEKNOLOGI
Program Studi	:	Sistem Komputer
Judul	:	PENGAMANAN INFORMASI PADA KRIPTOGRAFI SIMETRIS MENGGUNAKAN TEKNIK ONE TIME PAD CIPHER

Bersama dengan surat ini menyatakan dengan sebenar - benarnya bahwa data yang tertera diatas adalah sudah benar sesuai dengan ijazah pada pendidikan terakhir yang saya jalani. Maka dengan ini saya tidak akan melakukan penuntutan kepada UNPAB. Apabila ada kesalahan data pada ijazah saya.

Demiktianlah surat pernyataan ini saya buat dengan sebenar - benarnya, tanpa ada paksaan dari pihak manapun dan dibuat dalam keadaan sadar. Jika terjadi kesalahan, Maka saya bersedia bertanggung jawab atas kelalaian saya.

Agustus 2020
Surat Pernyataan

EDWIN ARIFSYAH SIDABUTAR
1614370329

FM-BPAA-2012-041

Hal : Permohonan Meja Hijau

Medan, 04 Agustus 2020
Kepada Yth : Bapak/Ibu Dekan
Fakultas SAINS & TEKNOLOGI
UNPAB Medan
Di -
Tempat

Dengan hormat, saya yang bertanda tangan di bawah ini :

Nama	: EDWIN ARIFSYAH SIDABUTAR
Tempat/Tgl. Lahir	: SIDOMUJO / 28 FEBRUARI 1999
Nama Orang Tua	: marlin sidabutar
N. P. M	: 1614370329
Fakultas	: SAINS & TEKNOLOGI
Program Studi	: Sistem Komputer
No. HP	: 0812e7851413
Alamat	: Jln.Gatot Subroto km 4,5 Medan

Dateng bermohon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul **PENGAMANAN INFORMASI PADA KRIPTOGRAFI SIMETRIS MENGGUNAKAN TEKNIK ONE TIME PAD CIPHER**, Selanjutnya saya menyatakan :

1. Melampirkan KRM yang telah disahkan oleh Ka. Prodi dan Dekan
2. Tidak akan mengikuti ujian perbaikan nilai mata kuliah untuk perbaikan indek prestasi (IP), dan ijazah diterbitkan ijazahnya setelah lulus ujian meja hijau.
3. Telah tercap keterangan bebas pustaka
4. Terlampir surat keterangan bebas laboratorium
5. Terlampir pas photo untuk ijazah ukuran 4x6 = 5 lembar dan 3x4 = 5 lembar Hitam Putih
6. Terlampir foto copy STTB SLTA dilegalisir 1 (satu) lembar dan bagi mahasiswa yang lanjutan D3 ke S1 lampirkan ijazah dan transkipnya sebanyak 1 lembar.
7. Terlampir pelunasan kwitansi pembayaran uang kuliah berjalan dan wisuda sebanyak 1 lembar
8. Skripsi sudah dijilid lux 2 examplar (1 untuk perpustakaan, 1 untuk mahasiswa) dan jilid kertas jenuk 5 examplar untuk penguji (bentuk dan warna penjilidan diserahkan berdasarkan keuentuan fakultas yang berlaku) dan lembar persetujuan sudah di tandatangani dosen pembimbing, prodi dan dekan
9. Soft Copy Serfpsi dimpan di CD sebanyak 2 disc (Sesuai dengan Judul Skripsinya)
10. Terlampir surat keterangan BKKOL (para saat pengambilan ijazah)
11. Setelah menyelesaikan persyaratan point point diatas berkas di masukan kedalam MAP
12. Bersedia melunasakan biaya biaya yang dibebankan untuk memproses pelaksanaan ujian dimaksud, dengan perincian sbb :

1.	[102] Ujian Meja Hijau	: Rp.	0
2.	[270] Administrasi Wisuda	: Rp.	1,500,000
3.	[202] Bebas Pustaka	: Rp.	100,000
4.	[221] Bebas LAB	: Rp.	5,000
	Total Biaya	: Rp.	1,605,000

Periode Wisuda Ke : 65

Ukuran Toga : M

Diketahui/Disetujui oleh :

Hormat saya

Hamdani, ST., MT
Dekan Fakultas SAINS & TEKNOLOGI

EDWIN ARIFSYAH SIDABUTAR
1614370329

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

YAYASAN PROF. DR. H. KADIRUN YAHYA

UNIVERSITAS PEMBANGUNAN PANCA BUDI

Jl. Jend. Gatot Subroto KM 4,5 PO. BOX 1099 Telp. 061-30108057 Fax. (061) 4514808
MEDAN - INDONESIA
Website : www.pancabudi.ac.id - Email : admin@pancabudi.ac.id

LEMBAR BUKTI BIMBINGAN SKRIPSI

Nama Mahasiswa	:	EDWIN ARIFSYAH SIDABUTAR
NPM	:	1614370329
Program Studi	:	Sistem Komputer
Jenjang Pendidikan	:	Strata Satu
Dosen Pembimbing	:	Muhammad Iqbal, S.Kom., M.Kom.
Judul Skripsi	:	PENGAMANAN INFORMASI PADA KRIPTOGRAFI SIMETRIS MENGGUNAKAN TEKNIK ONE TIME PAD CIPHER0

Tanggal	Pembahasan Materi	Status	Keterangan
05 Mei 2020	Acc Seminar Hasil	Diacc ujui	
24 Juli 2020	Acc sidang meja hijau	Disetujui	
26 Agustus 2020	Acc jilid	Disetujui	

Medan, 25 September 2020
Dosen Pembimbing,

Muhammad Iqbal, S.Kom., M.Kom.

YAYASAN PROF. DR. H. KADIRUN YAHYA

UNIVERSITAS PEMBANGUNAN PANCA BUDI

JL. Jend. Gatot Subroto KM 4,5 PO. BOX 1099 Telp. 061-30106057 Fax. (061) 4514808
MEDAN - INDONESIA
Website : www.pancabudi.ac.id - Email : admin@pancabudi.ac.id

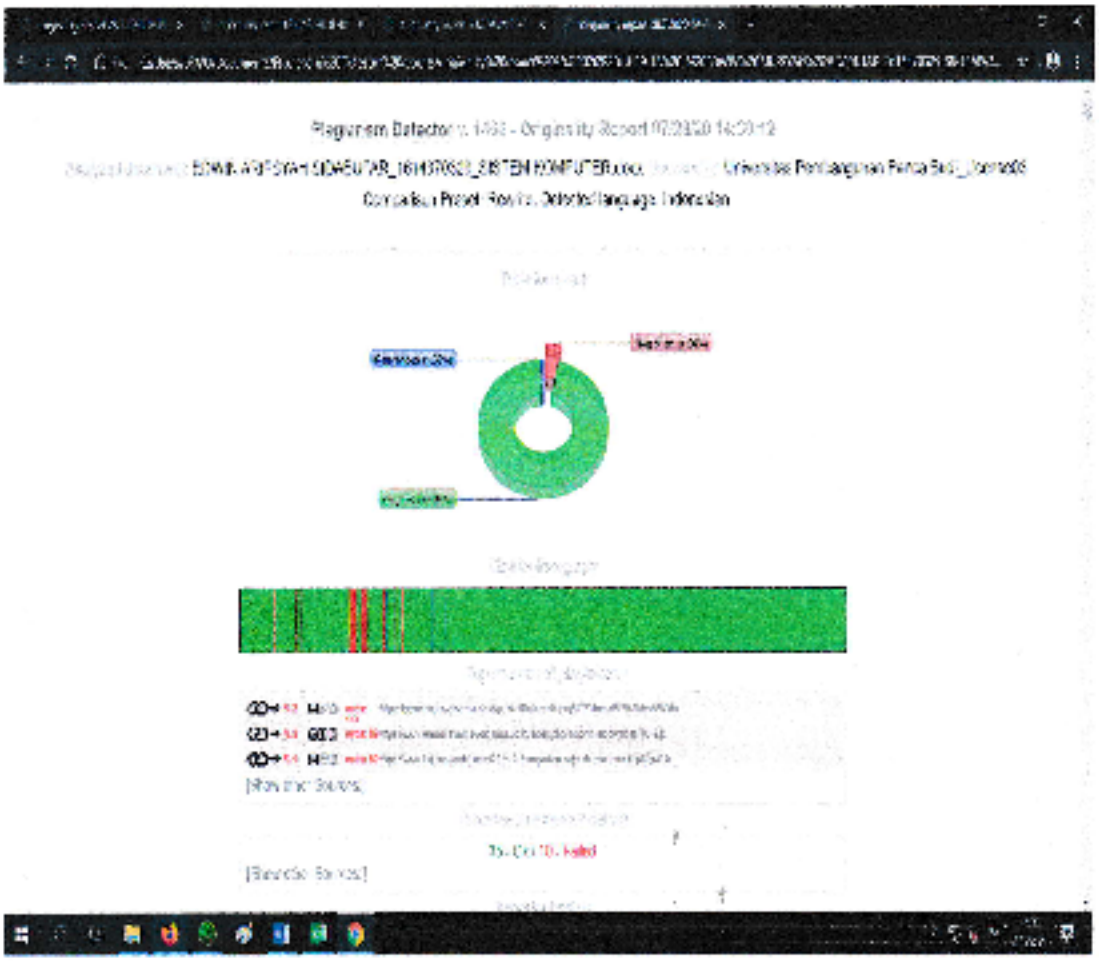
LEMBAR BUKTI BIMBINGAN SKRIPSI

Nama Mahasiswa	:	EDWIN ARIFSYAH SIDABUTAR
NPM	:	1614370329
Program Studi	:	Sistem Komputer
Jenjang Pendidikan	:	Strata Satu
Dosen Pembimbing	:	Andysah Putera Utama Siahaan, S.Kom.,M.Kom
Judul Skripsi	:	PENGAMANAN INFORMASI PADA KRIPTOGRAFI SIMETRIS MENGGUNAKAN TEKNIK ONE TIME PAD CIPHER0

Tanggal	Pembahasan Materi	Status	Keterangan
25 April 2020	ACC Seminar Hasil	Disetujui	
03 Mei 2020	ACC Revisi Skripsi. Lanjut ke pendaftaran seminar hasil.	Disetujui	
13 Juli 2020	ACC Sidang Meja Hijau	Disetujui	
19 Agustus 2020	ACC Jilid	Disetujui	

Medan, 25 September 2020
Dosen Pembimbing,

Andysah Putera Utama Siahaan, S.Kom.,M.Kom



SURAT KETERANGAN PLAGIAT CHECKER

Dengan ini saya Ka.LPMU UNPAB menerangkan bahwa saurat ini adalah bukti pengesahan dari LPMU sebagi pengesah proses plagiat checker Tugas Akhir/ Skripsi/Tesis selama masa pandemi ***Covid-19*** sesuai dengan edaran rektor Nomor : 7594/13/R/2020 Tentang Pemberitahuan Perpanjangan PBM Online.

Demikian disampaikan.

NB: Segala penyalahgunaan/pelanggaran atas surat ini akan di proses sesuai ketentuan yang berlaku UNPAB.

Ka.LPMU

Cahyo Pramono, SE.,MM

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI

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

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

PERMOHONAN JUDUL TESIS / SKRIPSI / TUGAS AKHIR*

Saya yang bertanda tangan di bawah ini :

Nama Lengkap	: EDWIN ARIFSYAH SIDABUTAR
Tempat/Tgl. Lahir	: SIDOARJO / 28 Februari 1999
Nomor Pokok Mahasiswa	: 1614370329
Program Studi	: Sistem Komputer
Konsentrasi	: Keamanan Jaringan Komputer
Jumlah Kredit yang telah dicapai	: 124 SKS, IPK 3.62
Nomor Hp	: 085371176383
Dengan ini mengajukan judul sesuai bidang ilmu sebagai berikut	:

No.	Judul
1.	PENGAMANAN INFORMASI PADA KRIPTOGRAFI SIMETRIS MENGGUNAKAN TEKNIK ONE TIME PAD CIPHERD

Catatan : Diisi Oleh Dosen Jika Ada Perubahan Judul

*Coret Yang Tidak Perlu

Rektor I,

Cahyo Prayogo, SE., MM

Medan, 12 Mei 2020
Pemohon,

(Edwin Arifsyah Sidabutar)

Tanggal : ..... Disahkan oleh : Dekan (Hamdani, ST., MT)	Tanggal : ..... Disetujui oleh : Dosen Pembimbing I : (Muhammad Iqbal, S.Kom., M.Kom.)
Tanggal : ..... Disetujui oleh: Ka. Prodi Sistem Komputer	Tanggal : ..... Disetujui oleh: Dosen Pembimbing II:

YAYASAN PROF. DR. H. KADIRUN YAHYA
PERPUSTAKAAN UNIVERSITAS PEMBANGUNAN PANCA BUDI
Jl. Jend. Gatot Subroto KM. 4,5 Medan Sunggal, Kota Medan Kode Pos 20122

SURAT BEBAS PUSTAKA
NOMOR: 2587/PERP/BP/2020

Perpustakaan Universitas Pembangunan Panca Budi menerangkan bahwa berdasarkan data pengguna perpustakaan ... sandaran

: EDWIN ARIFSYAH SIDABUTAR
: 1614370329
Semester : Akhir
: SAINS & TEKNOLOGI
Prodi : Sistem Komputer

...nya terhitung sejak tanggal 29 Juli 2020, dinyatakan tidak memiliki tanggungan dan atau pinjaman buku sekaligus ... terdaftar sebagai anggota Perpustakaan Universitas Pembangunan Panca Budi Medan.

Medan, 29 Juli 2020
Diketahui oleh,
Kepala Perpustakaan,

Sugiarjo, S.Sos., S.Pd.I

YAYASAN PROF. DR. H. KADIRUN YAHYA
UNIVERSITAS PEMBANGUNAN PANCA BUDI
LABORATORIUM KOMPUTER
Jl. Jend. Gatot Subroto Km 4.5 Sei Sikambing Telp. 061-8456673
Medan - 20122

KARTU BEBAS PRAKTIKUM
Nomor. 13442/BL/LAKO/2020

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

Nama	: EDWIN ARIFSYAH SIDABUTAR
NIM	: 1514370329
Jenjang/Semester	: Akhir
Fakultas	: SAINS & TEKNOLOGI
Jurusan/Prodi	: Sistem Komputer

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

Medan, 04 Agustus 2020
Ka. Laboratorium

Fachrid Wadly, S.Kom., M.Kom.

Dokumen : FM-LAKO-06-01	Revisi : 01	Tgl. Efektif : 04 Juni 2015

ABSTRAK

EDWIN ARIFSYAH SIDABUTAR
Pengamanan Informasi Pada Kriptografi Simetris Menggunakan Teknik One Time Pad Cipher
2020

Informasi merupakan berita penting yang harus dijaga. Berita ini tidak boleh jatuh ke tangan orang yang tidak bertanggung jawab. Informasi tersebut merupakan data pribadi yang harus dijaga kerahasiaannya. Kelalaian sering terjadi dalam menjaga informasi agar tidak jatuh kepada orang lain. Diperlukan suatu teknik kriptografi dalam usaha mengamankan informasi tersebut. Pencurian data tidak dapat dihindari, tetapi keamanan data dapat ditingkatkan agar tidak terjadi penyalahgunaan data.Teknik One Time Pad dapat digunakan untuk membantu pengguna dalam mengamankan informasi. One Time Pad bekerja dengan cara melakukan konversi karakter plaintext menjadi bentuk ASCII sehingga akhirnya dibentuk nilai biner dari ASCII tersebut. Bit-bit tersebut akan mengalami proses XNOR terhadap kunci yang diberikan. Teknik ini bekerja dengan cepat dan baik sehingga keamanan informasi dapat dijaga dengan baik.

Kata Kunci: *algoritma, enkripsi, kriptografi, One Tipe Pad*

KATA PENGANTAR

Puji syukur ke hadiratTuhan Yang Maha Kuasa, karena dengan berkat dan rahmat-Nya penulis masih diberikan kesempatan untuk menyelesaikan skripsi ini sebagaimana mestinya. Judul skripsi yang penulis paparkan adalah ”**PENGAMANAN INFORMASI PADA KRIPTOGRAFI SIMETRIS MENGGUNAKAN TEKNIK ONE TIME PAD CIPHER**”.Dalam kesempatan ini, penulis mengucapkan rasa terima kasih yang tak terhingga kepada pihak-pihak yang telah membantu dalam penyelesaian skripsi ini. Penulis ingin mengucapkan terima kasih kepada :

1. Orang tua saya yang selalu memberikan semangat, dukungan dan motivasi dalam penyusunan skripsi ini.
2. Bapak Dr. H. Muhammad Isa Indrawan, S.E., M.M., selaku Rektor Universitas Pembangunanan Panca Budi Medan.
3. Rektor I Bapak Ir. Bhakti Alamsyah, M.T., Ph.D.
4. Bapak Hamdani, S.T., M.T., selaku Dekan Fakultas Sains dan Teknologi Universitas Pembangunan Panca Budi Medan.
5. Bapak Eko Hariyanto, S.Kom., M.Kom, selaku Ketua Program Studi Sistem Komputer Universitas Pembangunan Panca Budi Medan.
6. Bapak Muhammad Iqbal, S.Kom., M.Kom., selaku Dosen Pembimbing I yang telah memberikan arahan dan membimbing dalam penyelesaian skripsi ini.
7. Bapak Andysah Putera Utama Siahaan,S.Kom., M.Kom., selaku Dosen Pembimbing II yang telah memberikan ilmu pengetahuan, serta bimbingan dalam penyelesaian skripsi ini.
8. Dosen-dosen pada Program Studi Sistem Komputer Fakultas Sains dan Teknologi Universitas Pembangunan Panca Budi Medan.
9. Staff dan karyawan pada Universitas Pembangunan Panca Budi Medan.
10. Seluruh teman-teman penulis dari program studi Sistem Komputer, Fakultas Sains dan Teknologi, Universitas Pembangunan Panca Budi, Medan

Penulis juga menyadari bahwa penyusunan skripsi ini belum mendapatkan kesempurnaandalam segi penulisan ataupun isi. Hal ini disebabkan pengetahuan penulis yang sangat terbatas. Penulis sangat mengharapkan adanya kritik dan saran dari pembaca untuk dapat memperbaiki isi skripsi.

Medan, 02 Mei 2020
Penulis

Edwin Arifsyah Sidabutar
1614370329

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Informasi ini juga tidak terlepas dari keamanan data, beberapa informasi ini umumnya hanya ditujukan bagi sekelompok orang tertentu, jadi oleh karena itu keamanan data ini sangat diperlukan untuk mencegah informasi agar supaya tidak sampai kepada pihak-pihak lain yang tidak berkepentingan sehingga kemungkinan terjadinya kebocoran dapat dihindari dengan merancang suatu sistem keamanan yang berfungsi untuk melindungi sistem informasi tersebut.

Dalam keamanan informasi ditemukan berbagai macam masalah yang sering ditemukan antara lain penyadapan pasif, penyadapan aktif, penipuan dan lain-lain. Dalam prakteknya, pencurian data dapat berwujud dalam pembacaan suatu data file teks oleh pihak yang tidak berwenang, memanipulasi data file teks, kerusakan data akibat buruknya konektivitas fisik ataupun keamanan dari data tersebut.

Salah satu cara yang digunakan untuk pengamanan data adalah menggunakan sistem kriptografi. Kriptografi berasal dari bahasa Yunani, yaitu kryptos yang artinya yang tersembunyi dan graphein yang artinya tulisan(Cokro, 2016). Awal mula kriptografi dipahami sebagai ilmu tentang menyembunyikan,tetapi seiring perkembangan zaman hingga saat ini pengertian kriptografi berkembang menjadi ilmu tentang teknik matematis yang digunakan untuk menyelesaikan persoalan keamanan berupa privasi dan otentikasi. Dalam

perkembangannya kriptografi dikenal menjadi kriptografi klasik dan kriptografi modern, kriptografi klasik contohnya caesar cipher, vigenere cipher dan lainnya sedangkan kriptografi modern contohnya ada md5, rc4, dan lain sebagainya

Kriptografibekerja dengan menyandikan isi informasi (plaintext) tersebut menjadi isi yang tidak dipahami melalui proses encryption dan untuk memperoleh kembali informasi yang asli, dilakukan proses decryption, disertai dengan menggunakan kunci yang benar. Namun, sejalan dengan perkembangan ilmu penyandian atau kriptografi, usaha-usaha untuk memperoleh kunci tersebut dapat dilakukan oleh siapa saja, termasuk pihak yang tidak sah untuk memiliki informasi tersebut.

Kelemahan dari algoritma klasik adalah kunci yang dapat dipecahkan dengan gampang. Hal ini dapat dilihat pada algoritma yang sederhana seperti algoritma Caesar Cipher dan Vigenere Cipher. Algoritma Caesar Cipher melakukan proses enkripsi hanya dengan menggeser plaintext dengan angka saja (Siahaan, 2016). Pergeseran angka tersebut dilakukan untuk tiap karakter pada plaintext dengan menggunakan nilai kunci yang sama, sehingga apabila satu karakter terpecahkan, ini akan membongkar keseluruhan karakter sehingga ciphertext dapat dipecahkan. Akibatnya algoritma ini rentan terhadap penyerangan.

Kelemahan ini harus dapat diselesaikan dengan teknik kriptografi lainnya. Teknik One Time Pad adalah salah satu cara yang dapat digunakan dalam menyelesaikan kelemahan yang ditimbukan oleh algoritma lama tersebut. Teknik ini tergolong dalam kriptografi *Stream Cipher*. Algoritma ini melakukan operasi

Exclusive-OR pada bit-bit untuk tiap karakter plaintext sehingga kerentanan dapat diatasi.

Oleh karena itu, penelitian tentang kriptografi akan selalu berkembang untuk memperoleh algoritma kriptografi yang makin kuat, sehingga usaha-usaha untuk memecah kode kriptografi secara tidak sah menjadi lebih sulit. Berdasarkan penelitian ini penulis ingin membahas tentang**"PENGAMANAN INFORMASI PADA KRIPTOGRAFI SIMETRIS MENGGUNAKAN TEKNIK ONE TIME PAD CIPHER".**

1.2 Rumusan Masalah

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

1. Bagaimana melakukan proses enkripsi dan dekripsi dengan teknik *OneTime Pad Cipher*?
2. Bagaimana melakukan operasi *Xnor* pada *One Time Pad Cipher*?
3. Bagaimana menentukan modulo pada algoritma *One Time Pad Cipher*?

1.3 Batasan Masalah

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

1. Program aplikasi berbasis desktop dan tidak online.
2. Panjang enkripsi digunakan adalah sebanyak 1000 karakter.
3. Pesan yang akan dienkripsi adalah pesan berbasis teks.
4. Program aplikasi menggunakan Microsoft Visual Basic.Net 2010.

1.4 Tujuan Penelitian

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

1. Untuk melakukan proses enkripsi dan dekripsi dengan teknik *One Time Pad Cipher*.
2. Untuk melakukan operasi exclusive-OR pada *One Time Pad Cipher*.
3. Untuk menentukan modulo pada algoritma *On Time Pad Cipher*.

1.5 Manfaat Penelitian

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

1. Mengamankan pesan dengan cara mengirimkan pesan terenkripsi.
2. Pesanterenkripsi dikirimkan tidak dapat dipecahkan sehingga terjadi penyalahgunaan data.
3. Memberikan kenyamanan pada pengirim dan penerima pesan.

BAB II

LANDASAN TEORI

2.1 Data

Data, dalam konteks komputasi, mengacu pada bagian informasi digital yang berbeda. Data biasanya diformat dengan cara tertentu dan dapat ada dalam berbagai bentuk, seperti angka, teks, dll. Ketika digunakan dalam konteks media transmisi, data merujuk ke informasi dalam format digital biner. Data adalah istilah luas dalam teknologi komputer, tetapi sering digunakan untuk mengidentifikasi dan memisahkan informasi dari bit belaka. Dalam telekomunikasi, data sering merujuk pada informasi digital, bukan analog. Tidak seperti transmisi analog, yang memerlukan koneksi garis keras selama durasi transmisi, data digital dikirim dalam paket(Sun et al., 2014).

Dalam komputasi, data adalah informasi yang telah diterjemahkan ke dalam bentuk yang efisien untuk pergerakan atau pemrosesan. Relatif terhadap komputer dan media transmisi saat ini, data adalah informasi yang diubah menjadi bentuk digital biner. Data dapat diterima untuk digunakan sebagai subjek tunggal atau subjek jamak. Data mentah adalah istilah yang digunakan untuk menggambarkan data dalam format digital paling dasar.

Konsep data dalam konteks komputasi berakar pada karya Claude Shannon, seorang yang dikenal sebagai bapak teori informasi. Dia mengantarkan konsep digital biner berdasarkan penerapan logika Boolean dua nilai ke sirkuit elektronik. Dengan Format digit biner mendasari CPU, memori semikonduktor

dan disk drive, serta banyak perangkat periferal yang umum dalam komputasi saat ini. Input komputer awal untuk kontrol dan data berupa kartu punch, diikuti oleh pita magnetik dan hard disk.

Pada awalnya, pentingnya data dalam komputasi bisnis menjadi jelas dengan popularitas istilah "pemrosesan data" dan "pemrosesan data elektronik," yang, untuk beberapa waktu, datang untuk mencakup keseluruhan dari apa yang sekarang dikenal sebagai teknologi informasi. Selama sejarah komputasi perusahaan, spesialisasi terjadi, dan profesi data yang berbeda muncul seiring dengan pertumbuhan pemrosesan data perusahaan.

2.1.1 Bagaimana Data Disimpan

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

Unit-unit pengukuran data terus bertambah seiring dengan meningkatnya jumlah data yang dikumpulkan dan disimpan. Istilah "brontobyte" yang relatif baru, misalnya, adalah penyimpanan data yang setara dengan 10 hingga 27 byte.Data dapat disimpan dalam format file, seperti pada sistem mainframe menggunakan ISAM dan VSAM. Format file lain untuk penyimpanan, konversi, dan pemrosesan data termasuk nilai yang dipisah koma. Format ini terus di berbagai jenis mesin, bahkan ketika pendekatan yang lebih berorientasi data terstruktur memperoleh pijakan dalam komputasi perusahaan. Spesialisasi yang

lebih besar dikembangkan sebagai basis data, sistem manajemen basis data, dan kemudian teknologi basis data relasional muncul untuk mengatur informasi(Zhang et al., 2009).

2.1.2 Jenis data

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

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

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

2.1.3 Pengelolaan dan Penggunaan Data

Dengan semakin banyaknya data dalam organisasi, penekanan tambahan telah ditempatkan pada memastikan kualitas data dengan mengurangi duplikasi dan menjamin yang paling akurat, catatan saat ini digunakan. Banyak langkah yang terlibat dengan manajemen data modern termasuk pembersihan data, serta mengekstrak, mengubah dan memuat (ETL) proses untuk mengintegrasikan data. Data untuk diproses telah dilengkapi dengan metadata, kadang-kadang disebut sebagai "data tentang data," yang membantu administrator dan pengguna memahami database dan data lainnya.

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

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

2.2 Keamanan Data

Keamanan data adalah seperangkat standar dan teknologi yang melindungi data dari kehancuran, modifikasi, atau pengungkapan yang disengaja atau tidak disengaja. Keamanan data dapat diterapkan dengan menggunakan berbagai teknik dan teknologi, termasuk kontrol administratif, keamanan fisik, kontrol logis, standar organisasi, dan teknik perlindungan lainnya yang membatasi akses ke pengguna atau proses yang tidak sah atau berbahaya(Rao & Selvamani, 2015).

Keamanan data mengacu pada langkah-langkah privasi digital pelindung yang diterapkan untuk mencegah akses tidak sah ke komputer, database, dan situs web. Keamanan data juga melindungi data dari korupsi. Keamanan data adalah aspek penting dari TI untuk organisasi dari berbagai ukuran dan tipe. Keamanan data juga dikenal sebagai keamanan informasi atau keamanan komputer.

Contoh teknologi keamanan data termasuk backup, masking data dan penghapusan data. Ukuran teknologi keamanan data utama adalah enkripsi, di mana data digital, perangkat lunak / perangkat keras, dan hard drive dienkripsi dan karenanya tidak dapat dibaca oleh pengguna dan peretas yang tidak sah. Salah satu metode yang paling umum dijumpai dalam mempraktikkan keamanan data adalah penggunaan otentikasi. Dengan otentikasi, pengguna harus memberikan kata sandi, kode, data biometrik, atau bentuk data lainnya untuk memverifikasi identitas sebelum akses ke sistem atau data diberikan. Keamanan data juga sangat penting untuk catatan dari perawatan kesehatan, sehingga pendukung sistem pada sebuah yang daapat bentuk data kesehatan dan praktisi medis di AS dan dari sebuh negara-negara lain juga berupaya menerapkan privasi rekam medis

elektronik dengan menciptakan kesadaran tentang hak-hak pasien terkait dengan pelepasan data ke laboratorium, dokter, rumah sakit dan fasilitas medis lainnya.

2.2.1 Pentingnya Keamanan Data

Semua bisnis saat ini menangani data hingga taraf tertentu. Dari raksasa perbankan yang menangani data pribadi dan keuangan dalam volume besar hingga bisnis satu orang yang menyimpan detail kontak pelanggannya di ponsel, data berperan di perusahaan baik besar maupun kecil.

Tujuan utama keamanan data adalah untuk melindungi data yang dikumpulkan, disimpan, diterima, atau ditransmisikan oleh suatu organisasi. Kepatuhan juga merupakan pertimbangan utama. Tidak masalah perangkat, teknologi, atau proses mana yang digunakan untuk mengelola, menyimpan, atau mengumpulkan data, itu harus dilindungi. Pelanggaran data dapat menyebabkan kasus litigasi dan denda yang sangat besar, belum lagi kerusakan reputasi organisasi. Pentingnya melindungi data dari ancaman keamanan lebih penting saat ini daripada sebelumnya.

Keamanan data mengacu pada proses melindungi data dari akses yang tidak sah dan korupsi data sepanjang siklus hidupnya. Keamanan data termasuk enkripsi data, tokenization, dan praktik kunci yang melindungi data di semua aplikasi dan platform.Organisasi di seluruh dunia banyak berinvestasi dalam kemampuan pertahanan cyber teknologi informasi untuk melindungi aset penting mereka. Apakah suatu perusahaan perlu melindungi merek, modal intelektual, dan informasi pelanggan atau menyediakan kontrol untuk infrastruktur penting, sarana

untuk mendeteksi insiden dan merespons melindungi kepentingan organisasi memiliki tiga elemen umum: orang, proses, dan teknologi.

2.2.2 Solusi Keamanan Data

Data membutuhkan enkripsi dalam mengamankan informasi yang ada dalam data tersebut. Dengan enkripsi data canggih, tokenization, dan manajemen utama untuk melindungi data di seluruh aplikasi, transaksi, penyimpanan, dan platform big data, Teknik ini menyederhanakan perlindungan data sensitif bahkan dalam kasus penggunaan yang paling kompleks sekalipun. Beberapa model keamanan data antara lain:

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

- Keamanan Pembayaran - Solusi menyediakan enkripsi dan tokenisasi point-to-point lengkap untuk transaksi pembayaran ritel, memungkinkan pengurangan lingkup PCI.
- Big Data, Hadoop, dan perlindungan data IofT - Solusi yang melindungi data sensitif di Danau Data - termasuk Hadoop, Teradata, Micro Focus Vertica, dan platform Big Data lainnya.
- Keamanan Aplikasi Seluler - Melindungi data sensitif di aplikasi seluler asli sembari menjaga data dari ujung ke ujung.
- Keamanan Peramban Web - Melindungi data sensitif yang diambil di peramban, dari titik pelanggan memasukkan pemegang kartu atau data pribadi dan menjaganya agar tetap terlindungi melalui ekosistem ke tujuan tuan rumah tepercaya.
- eMail Security - Solusi yang menyediakan enkripsi ujung ke ujung untuk email dan olahpesan seluler, menjaga informasi pribadi dan informasi kesehatan pribadi tetap aman dan pribadi.

2.2.3 Kerahasiaan

Kerahasiaan mengacu pada melindungi informasi agar tidak diakses oleh pihak yang tidak berwenang. Dengan kata lain, hanya orang yang diberi wewenang untuk melakukannya yang dapat akses ke data sensitif. Bayangkan catatan bank harus dapat diakses, tentu saja, dan karyawan di bank yang membantu transaksi harus dapat mengaksesnya, tetapi tidak ada orang lain untuk yang seharusnya. Kegagalan untuk menjaga kerahasiaan berarti bahwa seseorang

yang seharusnya tidak memiliki akses telah berhasil mendapatkannya, melalui perilaku yang disengaja atau karena kecelakaan. Kegagalan kerahasiaan seperti itu, umumnya dikenal sebagai pelanggaran, biasanya tidak dapat diperbaiki. Setelah rahasia itu terungkap, tidak ada cara untuk mengetahuinya. Jika catatan bank diposting di situs web publik, semua orang dapat mengetahui nomor rekening bank, saldo, dll., Informasi itu tidak dapat dihapus dari pikiran, kertas, komputer, dan tempat lain mereka. Hampir semua insiden keamanan utama yang dilaporkan di media saat ini melibatkan kerugian besar kerahasiaan. Jadi, secara ringkas, pelanggaran kerahasiaan berarti bahwa seseorang memperoleh akses ke informasi yang seharusnya tidak memiliki akses ke sana.

2.2.4 Integritas

Integritas mengacu pada memastikan keaslian informasi — bahwa informasi tidak diubah, dan bahwa sumber informasi itu asli. Bayangkan jika seseorang memiliki situs web dan Anda menjual produk di situs itu. Sekarang bayangkan penyerang dapat berbelanja di situs web dan dengan jahat mengubah harga produk Anda sehingga mereka dapat membeli apa pun dengan harga berapa pun yang mereka pilih. Itu akan menjadi kegagalan integritas karena informasi dalam hal ini, harga suatu produk telah diubah dan perubahan ini tidak dapat digagalkan. Contoh lain dari kegagalan integritas adalah ketika sesorang mencoba terhubung ke situs web dan penyerang jahat antara Anda dan situs web mengalihkan lalu lintas ke situs web yang berbeda. Dalam hal ini, situs yang dituju tidak asli.

2.2.5 Ketersediaan

Ketersediaan berarti informasi dapat diakses oleh pengguna yang berwenang. Jika penyerang tidak dapat mengkompromikan dua elemen pertama dari keamanan informasi (lihat di atas) mereka dapat mencoba melakukan serangan seperti penolakan layanan yang akan menurunkan server, membuat situs web tidak tersedia untuk pengguna yang sah karena kurangnya ketersediaan.

2.2.6 Kontrol Akses

Kesalahan terbesar yang bisa dilakukan oleh perancang aplikasi adalah mengabaikan kontrol akses sebagai bagian dari fungsionalitas yang diperlukan. Jarang bahwa setiap pengguna atau sistem yang berinteraksi dengan suatu aplikasi harus memiliki hak yang sama di seluruh aplikasi itu. Beberapa pengguna mungkin memerlukan akses ke data tertentu dan bukan yang lain; beberapa sistem harus atau tidak dapat mengakses aplikasi. Akses ke komponen, fungsi, atau modul tertentu dalam aplikasi juga harus dikontrol. Kontrol akses juga penting untuk kepatuhan audit dan peraturan. Beberapa cara umum mengelola kontrol akses adalah:

- Baca, tulis, dan jalankan hak istimewa: File
- Kontrol akses berbasis peran: administrator, pengguna
- Alamat IP akses berbasis host, nama mesin
- Objek kode kontrol akses tingkat objek, banyak pembaca / penulis tunggal

2.3 Algoritma

Untuk membuat komputer melakukan apa pun, sesorang harus menulis program komputer. Untuk menulis program komputer, sesorang harus memberi tahu komputer, langkah demi langkah, persis apa yang sesorang inginkan. Komputer kemudian "mengeksekusi" program, mengikuti setiap langkah secara mekanis, untuk mencapai tujuan akhir. Ketika sesorang memberi tahu komputer apa yang harus dilakukan, sesorang juga harus memilih bagaimana melakukannya. Di situlah algoritma komputer masuk. Algoritma adalah teknik dasar yang digunakan untuk menyelesaikan pekerjaan(Gurevich, 2012). Mari kita ikuti contoh untuk membantu mendapatkan pemahaman tentang konsep algoritma. Katakanlah sesorang memiliki seorang teman yang tiba di bandara, dan teman sesorang perlu pergi dari bandara ke rumah. Berikut adalah empat algoritma berbeda yang mungkin akan diberikan kepada orang lain untuk sampai ke rumah:

- Algoritma taksi:
    - Pergi ke tempat taksi.
    - Naik taksi.
    - Berikan alamat saya pada pengemudi.

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

- Algoritma rent-a-car:
    - Naik shuttle ke tempat rental mobil.
    - Menyewa mobil.
    - Ikuti petunjuk untuk sampai ke rumah saya.

- Algoritma bus:
    - Di luar klaim bagasi, naik bus nomor 70.
    - Transfer ke bus 14 di Main Street.
    - Turun di Elm street.
    - Berjalanlah dua blok ke utara ke rumah saya.

Keempat algoritma ini mencapai tujuan yang persis sama, tetapi masing-masing algoritma melakukannya dengan cara yang sama sekali berbeda. Setiap algoritma juga memiliki biaya dan waktu perjalanan yang berbeda. Naik taksi, misalnya, mungkin adalah cara tercepat, tetapi juga yang paling mahal. Naik bus jelas lebih murah, tetapi jauh lebih lambat. Anda memilih algoritma berdasarkan keadaan.

Dalam pemrograman komputer, seringkali ada banyak cara berbeda - algoritma - untuk menyelesaikan tugas yang diberikan. Setiap algoritma memiliki kelebihan dan kekurangan dalam situasi yang berbeda. Penyortiran adalah satu tempat di mana banyak penelitian telah dilakukan karena komputer menghabiskan banyak daftar penyortiran waktu. Berikut adalah lima algoritma berbeda yang digunakan dalam penyortiran:

- Bin sort
- Gabungkan semacam
- Semacam gelembung
- Semacam shell
- Quicksort

Jika ada sejuta nilai integer antara 1 dan 10 dan perlu diurutkan, jenis bin sort adalah algoritma yang tepat untuk digunakan. Jika Anda memiliki sejuta judul buku, quicksort mungkin merupakan algoritma terbaik. Dengan mengetahui kekuatan dan kelemahan dari berbagai algoritma, Anda memilih yang terbaik untuk tugas yang ada.

2.3.1 Desain Konseptual

Algoritma adalah serangkaian instruksi, sering disebut sebagai "proses," yang harus diikuti ketika memecahkan masalah tertentu. Meskipun secara teknis tidak dibatasi oleh definisi, kata itu hampir selalu terkait dengan komputer, karena algoritma yang diproses komputer dapat mengatasi masalah yang jauh lebih besar daripada manusia, jauh lebih cepat. Karena komputasi modern menggunakan algoritma jauh lebih sering daripada pada titik lain dalam sejarah manusia, bidang telah tumbuh di sekitar desain, analisis, dan penyempurnaan. Bidang desain algoritma membutuhkan latar belakang matematika yang kuat, dengan gelar ilmu komputer yang sangat dicari kualifikasi. Ini menawarkan semakin banyak pilihan

karir yang sangat dikompensasi, karena kebutuhan akan lebih banyak (dan juga lebih canggih) algoritma terus meningkat.

Pada tingkat yang paling sederhana, algoritma pada dasarnya hanya seperangkat instruksi yang diperlukan untuk menyelesaikan tugas. Pengembangan algoritma, meskipun umumnya tidak disebut demikian, telah menjadi kebiasaan yang populer dan pengejaran profesional untuk semua catatan sejarah. Jauh sebelum fajar era komputer modern, orang menetapkan rutinitas yang telah ditentukan untuk bagaimana mereka akan melakukan tugas sehari-hari, sering menuliskan daftar langkah-langkah yang harus diambil untuk mencapai tujuan penting, mengurangi risiko melupakan sesuatu yang penting. Ini, pada dasarnya, adalah apa itu algoritma. Desainer mengambil pendekatan yang mirip dengan pengembangan algoritma untuk tujuan komputasi: pertama, mereka melihat masalah. Kemudian, mereka menguraikan langkah-langkah yang akan diperlukan untuk menyelesaikannya. Akhirnya, mereka mengembangkan serangkaian operasi matematika untuk mencapai langkah-langkah tersebut.

2.3.2 Tugas Algoritma

Tugas sederhana dapat diselesaikan dengan algoritma yang dihasilkan dengan beberapa menit, atau paling banyak pekerjaan pagi. Tingkat kompleksitas menjalankan tantangan yang panjang, namun, sampai pada masalah yang sangat rumit sehingga mereka telah menghalangi matematikawan yang tak terhitung jumlahnya selama bertahun-tahun - atau bahkan berabad-abad. Komputer modern menghadapi masalah pada tingkat ini di bidang-bidang seperti keamanan dunia

maya, serta penanganan data besar - penyortiran set data yang efisien dan menyeluruh sedemikian besar sehingga bahkan komputer standar tidak dapat memprosesnya secara tepat waktu. Contoh data besar mungkin termasuk "setiap artikel di Wikipedia," "setiap halaman web yang diindeks dan diarsipkan akan kembali ke tahun 1998," atau "enam bulan terakhir pembelian online yang dilakukan di Amerika."

2.3.3 Rekayasa Algoritma

Ketika desain algoritma baru diterapkan dalam istilah praktis, disiplin terkait dikenal sebagai rekayasa algoritma. Kedua fungsi tersebut sering dilakukan oleh orang yang sama, meskipun organisasi yang lebih besar (seperti Amazon dan Google) mempekerjakan desainer dan insinyur khusus, mengingat tingkat kebutuhan mereka akan algoritma baru dan khusus. Seperti proses desain, rekayasa algoritma sering kali melibatkan akreditasi sains komputer, dengan latar belakang yang kuat dalam matematika: di mana mereka ada sebagai profesi yang terpisah dan terspesialisasi, insinyur algoritma mengambil ide-ide konseptual dari desainer dan proses kreatif dari mereka yang akan dipahami oleh komputer. Dengan kemajuan teknologi digital yang mantap, para insinyur yang berdedikasi akan terus menjadi semakin umum.

2.4 Kriptografi

Kriptografi adalah teknik mengubah dan mentransmisikan data rahasia dengan cara disandikan sehingga hanya pengguna yang berwenang dan

dimaksudkan dapat memperoleh atau bekerja di dalamnya. Ini adalah kata asal Yunani di mana "crypto" berarti tersembunyi dan "graphy" berarti menulis, jadi kriptografi berarti tulisan tersembunyi atau rahasia. Ini memperkenalkan triad seperti kerahasiaan, non-penolakan, integritas dan keaslian dalam komunikasi data yang sedang berlangsung.

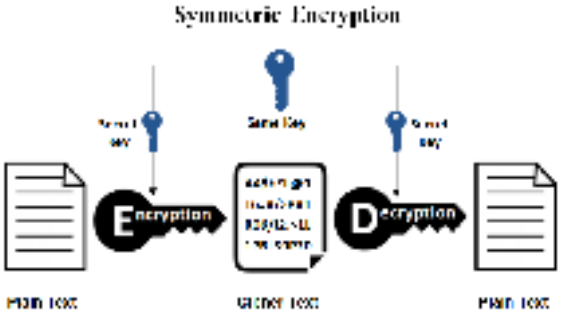
Kriptografi adalah disiplin atau teknik yang digunakan dalam melindungi integritas atau kerahasiaan pesan elektronik dengan mengubahnya menjadi bentuk (ciphertext) yang tidak dapat dibaca. Hanya penggunaan kunci rahasia yang dapat mengubah teks sandi menjadi bentuk yang dapat dibaca manusia (teks jelas). Perangkat lunak kriptografi dan / atau perangkat keras menggunakan rumus matematika (algoritma) untuk mengubah teks dari satu bentuk ke bentuk lainnya.

Komunikasi yang aman dapat disediakan menggunakan teknik, di hadapan konten pihak ketiga berbahaya yang disebut musuh. Teknik-teknik ini dapat disebut sebagai Kriptografi. Pesan pribadi apa pun dapat disembunyikan dari publik atau pihak ketiga, menggunakan seperangkat protokol. Protokol-protokol ini perlu dianalisis dan dibangun dengan cara yang efisien untuk menjaga kerahasiaan pesan yang dikirim. Kriptografi modern memiliki aspek tertentu yang merupakan pusatnya seperti integritas data, otentikasi, kerahasiaan dll. Di dunia modern, kriptografi sangat bergantung pada mata pelajaran seperti matematika dan ilmu komputer. Algoritma untuk Kriptografi dirancang sedemikian rupa sehingga sulit untuk praktik oleh pihak ketiga jahat yang juga dikenal sebagai musuh. Pendekatan praktis terhadap pemecahan algoritma semacam itu akan gagal, namun, pendekatan teoritis mungkin memecahkan sistem tersebut. Dengan

demikian, algoritma apa pun dapat disebut sebagai aman, jika sifat kuncinya tidak dapat disimpulkan, dengan ciphertext yang diberikan. Kriptografi dapat dikategorikan menjadi dua cabang: Symmetric dan Asymmetric. Dengan pendekatan simetris, satu kunci digunakan untuk proses enkripsi dan dekripsi yaitu pengirim dan penerima harus memiliki kunci bersama. Namun, dengan pendekatan ini, distribusi kunci adalah tautan yang lemah, yang memunculkan pendekatan baru.

2.4.1 Kriptografi Simetris

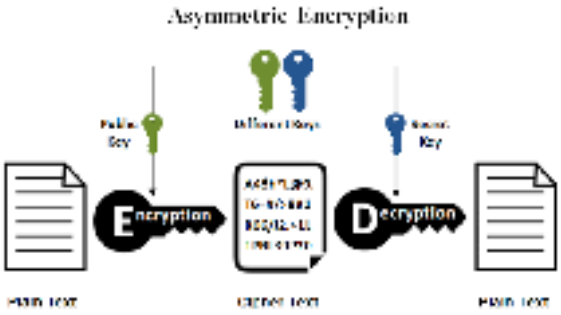
Kriptografi kunci simetris adalah setiap algoritma kriptografi yang didasarkan pada kunci bersama yang digunakan untuk mengenkripsi atau mendekripsi teks / cyphertext, dalam kontrak dengan kriptografi kunci asimetris, di mana kunci enkripsi dan dekripsi dihubungkan oleh berbeda. Enkripsi simetris umumnya lebih efisien daripada enkripsi asimetris dan karenanya lebih disukai ketika sejumlah besar data perlu dipertukarkan. Membuat kunci bersama sulit menggunakan hanya algoritma enkripsi simetris, sehingga dalam banyak kasus, enkripsi asimetris digunakan untuk membuat kunci bersama antara dua pihak. Contoh untuk kriptografi kunci simetris termasuk AES, DES, dan 3DES. Protokol pertukaran kunci yang digunakan untuk membangun kunci enkripsi bersama termasuk Diffie-Hellman (DH), Eliptic Curve (EC) dan RSA. Berikut ini skema dari kriptografi simetris(Ayushi, 2010).



Gambar 2.1Skema kriptografi simetris
Sumber: (Ayushi, 2010)

2.4.2 Kriptografi Asimetris

Dalam versi kriptografi asimetris, pengirim dan penerima memiliki dua kunci, publik dan pribadi. Kunci pribadi dirahasiakan sedangkan kunci publik terbuka ke dunia luar. Set data apa pun, yang dienkripsi dengan kunci publik hanya dapat didekripsi menggunakan kunci pribadi yang sesuai. Ketika datang ke perbandingan, pendekatan simetris lebih cepat daripada yang asimetris. Contoh - tanda tangan digital menggunakan kriptografi asimetris untuk mengenkripsi pesan dalam hash alih-alih pesan lengkap. Berikut ini skema kriptografi asimetris(S. et al., 2012).



Gambar 2.2 Skema kriptografi asimetris
Sumber: (Ayushi, 2010)

2.5 One Time Pad

Dalam kriptografi, OneTime Pad (OTP) adalah teknik enkripsi yang tidak dapat dipecahkan, tetapi membutuhkan penggunaan kunci pra-bagi-pakai satu kali dengan ukuran yang sama dengan, atau lebih lama dari, pesan yang dikirim. Dalam teknik ini, plaintext dipasangkan dengan kunci rahasia acak (juga disebut sebagai OneTime Pad). Kemudian, setiap bit atau karakter dari plaintext dienkripsi dengan menggabungkannya dengan bit atau karakter yang sesuai dari pad menggunakan penambahan modular. Jika kuncinya adalah (1) benar-benar acak, (2) setidaknya selama plaintext, (3) tidak pernah digunakan kembali secara keseluruhan atau sebagian, dan (4) dirahasiakan sepenuhnya, maka ciphertext yang dihasilkan tidak akan dapat mendekripsi atau istirahat. Juga telah terbukti bahwa sandi apa pun dengan properti kerahasiaan sempurna harus menggunakan kunci dengan persyaratan yang sama efektifnya dengan kunci OTP. [3] Versi digital dari cipher pad satu kali telah digunakan oleh negara-negara untuk komunikasi diplomatik dan militer yang kritis, tetapi masalah distribusi kunci yang aman telah membuatnya tidak praktis untuk sebagian besar aplikasi.

Pertama kali dijelaskan oleh Frank Miller pada tahun 1882, OneTime Pad ditemukan kembali pada tahun 1917. Pada 22 Juli 1919, Paten A.1010191 dikeluarkan untuk Gilbert Vernam untuk operasi XOR yang digunakan untuk enkripsi OneTime Pad. Berasal dari sandi Vernam-nya, sistem itu adalah sandi yang menggabungkan pesan dengan kunci yang dibaca dari kaset yang dilubangi. Dalam bentuk aslinya, sistem Vernam rentan karena pita kunci adalah loop, yang digunakan kembali setiap kali loop membuat siklus penuh. Penggunaan satu kali

datang kemudian, ketika Joseph Mauborgne mengakui bahwa jika pita kunci itu benar-benar acak, maka kriptanalisis akan menjadi mustahil.

Bagian "pad" dari nama tersebut berasal dari implementasi awal di mana bahan utama didistribusikan sebagai pad kertas, memungkinkan lembaran atas saat ini dirobek dan dihancurkan setelah digunakan. Untuk penyembunyian, pad terkadang sangat kecil sehingga diperlukan kaca pembesar yang kuat untuk menggunakannya. KGB menggunakan pembalut dengan ukuran sedemikian rupa sehingga bisa muat di telapak tangan, atau di kulit kenari. Untuk meningkatkan keamanan, bantalan sekali pakai kadang-kadang dicetak pada lembaran nitroselulosa yang sangat mudah terbakar, sehingga mudah terbakar setelah digunakan.

Ada beberapa ambiguitas untuk istilah "sandi Vernam" karena beberapa sumber menggunakan "sandi Vernam" dan "bantalan satu kali" secara sinonim, sementara yang lain merujuk pada sembarang aliran aditif sebagai "sandi Vernam", termasuk yang didasarkan pada keamanan kriptografi. pseudorandom number generator (CSPRNG).

2.6 Unified Modelling Language (UML)

Unified Modeling Language (UML) adalah bahasa pemodelan standar yang memungkinkan pengembang menentukan, memvisualisasikan, membuat, mendokumentasikan perangkat lunak(Technopedia, 2019). Dengan demikian, UML membuat artefak ini dapat diskalakan, aman, dan kuat dalam eksekusi. UML adalah aspek yang penting yang terlibat dalam pengembangan perangkat

lunak berorientasi objek. Ini menggunakan notasi grafis untuk membuat model visual dari sistem perangkat lunak. Arsitektur UML didasarkan pada fasilitas meta-objek, yang mendefinisikan dasar untuk membuat bahasa pemodelan. Mereka cukup tepat untuk menghasilkan seluruh aplikasi. UML yang sepenuhnya dapat dieksekusi dapat digunakan untuk berbagai platform menggunakan teknologi yang berbeda dan dapat digunakan dengan semua proses sepanjang siklus pengembangan perangkat lunak. UML dirancang untuk memungkinkan pengguna mengembangkan bahasa pemodelan visual yang ekspresif, siap pakai. Selain itu, mendukung konsep pengembangan tingkat tinggi seperti kerangka kerja, pola, dan kolaborasi(Wasserkrug et al., 2019).

Penggunaan model ini bertujuan untuk mengidentifikasikan bagian-bagian yang termasuk dalam lingkup sistem yang dibahas dan bagaimana hubungan antara sistem dengan subsistem maupun sistem lain diluarnya(Sukmawati & Priyadi, 2019).

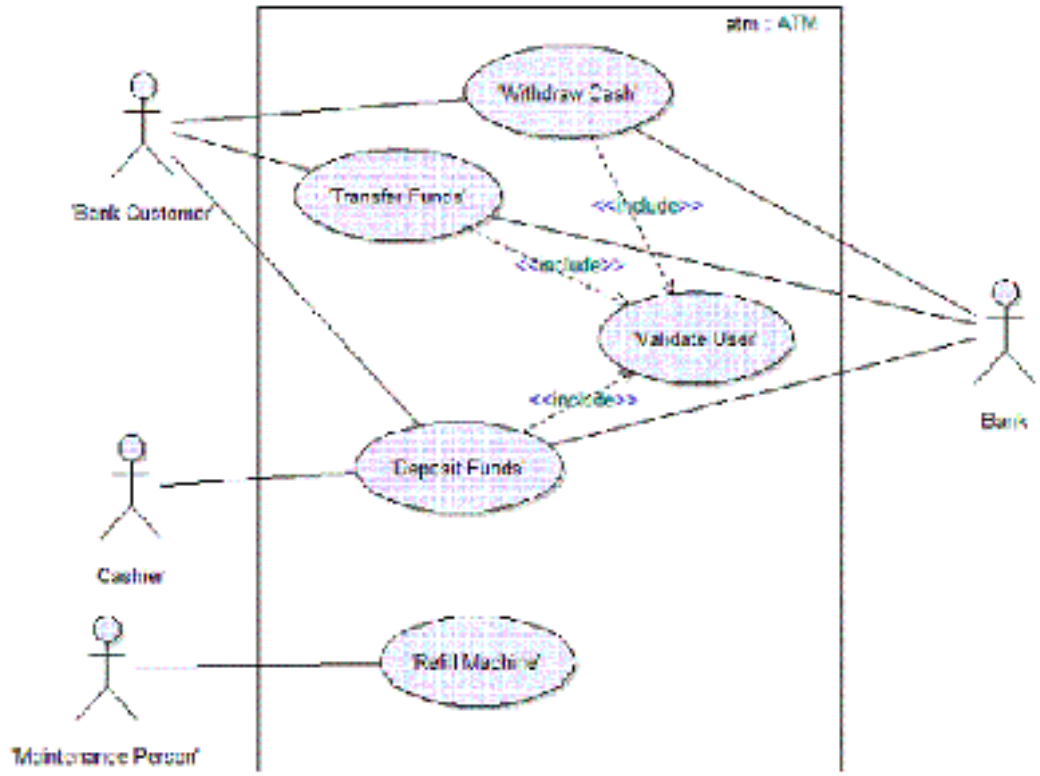
2.6.1 UseCase Diagram

Use Case Diagram adalah model tentang bagaimana berbagai jenis pengguna berinteraksi dengan sistem untuk memecahkan masalah. Dengan demikian, ini menggambarkan tujuan pengguna, interaksi antara pengguna dan sistem, dan perilaku sistem yang diperlukan dalam memenuhi tujuan-tujuan ini. Model use-case terdiri dari sejumlah elemen model. Elemen model yang paling penting adalah kasus penggunaan, aktor dan hubungan di antara mereka. Diagram use-case digunakan untuk menggambarkan secara grafis subset dari model untuk

menyederhanakan komunikasi. Biasanya akan ada beberapa diagram kasus penggunaan yang terkait dengan model yang diberikan, masing-masing menunjukkan subset elemen model yang relevan untuk tujuan tertentu. Elemen model yang sama dapat ditampilkan pada beberapa diagram use-case, tetapi setiap instance harus konsisten. Jika alat digunakan untuk mempertahankan model use-case, kendala konsistensi ini otomatis sehingga setiap perubahan pada elemen model (mengubah nama misalnya) akan secara otomatis tercermin dalam setiap diagram use-case yang menunjukkan elemen itu(UTM, 2019).

Model use-case dapat berisi paket yang digunakan untuk menyusun model untuk menyederhanakan analisis, komunikasi, navigasi, pengembangan, pemeliharaan, dan perencanaan. Faktanya, sebagian besar model use-case adalah tekstual, dengan teks yang ditangkap dalam Spesifikasi Use-Case yang terkait dengan setiap elemen model use-case. Spesifikasi ini menjelaskan alur peristiwa use case. Model use-case berfungsi sebagai utas pemersatu sepanjang pengembangan sistem. Ini digunakan sebagai spesifikasi utama dari persyaratan fungsional untuk sistem, sebagai dasar untuk analisis dan desain, sebagai input untuk perencanaan iterasi, sebagai dasar mendefinisikan kasus uji dan sebagai dasar untuk dokumentasi pengguna.(Kurniawan, 2018).

Use case diagram merupakan suatu diagram yang berisi *use case, actor*, serta *relationship* diantaranya. *Use Case Diagram* dapat digunakan untuk kebutuhan apa saja yang diperlukan dalam suatu sistem, sehingga sistem dapat digambarkan dengan jelas bagaimana proses dari sistem tersebut, bagaimana cara aktor menggunakan sistem, serta apa saja yang dapat dilakukan pada suatu sistem.

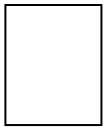


Gambar 2.3 Use-case Diagram ATM
Sumber: (Uml-diagrams.org, 2019)

Gambar di atas adalah contoh dari penggunaan use-case diagram pada mesin ATM. Use-case memiliki beberapa simbol untuk menyatakan kegiatan dari use-case tersebut. Adapun simbol dari *use case* adalah sebagai berikut:

Tabel 2.1 Simbol Use Case Diagram

No	Gambar	Nama	Keterangan

1		*Actor*	Menspesifikasikan himpuan peran yang pengguna mainkan ketika berinteraksi dengan *use case*.
2		*Dependency*	Hubungan dimana perubahan yang terjadi pada suatu elemen mandiri *(independent)* akan mempengaruhi elemen yang bergantung padanya elemen yang tidak mandiri.
3		*Generalization*	Hubungan dimana objek anak berbagi perilaku dan struktur data dari objek yang ada diatasnya .
4		*Include*	Menspesifikasikan bahwa *use case* sumber secara *eksplisit*.
5		*Extend*	Menspesifikasikan bahwa *use case* target memperluas perilaku dari *use case* sumber pada suatu titik yang diberikan.
6		*Association*	Apa yang menghubungkan antara objek satu dengan objek lainnya.
7		*System*	Menspesifikasikan paket yang menampilkan sistem secara terbatas.

8		*Use Case*	Deskripsi dari urutan aksi-aksi yang ditampilkan sistem yang menghasilkan suatu hasil yang terukur bagi suatu actor
9		*Collaboration*	Interaksi aturan-aturan dan elemen lain yang bekerja sama untuk menyediakan prilaku yang lebih besar dari jumlah dan elemen-elemennya (sinergi).
10		*Note*	Elemen fisik yang eksis saat aplikasi dijalankan dan mencerminkan suatu sumber daya komputasi

Sumber: (Kurniawan, 2018)

2.6.2 Activity Diagram

Activity Diagram (Diagram Aktifitas) menggambarkan berbagai alir aktifitas dalam sistem yang sedang dirancang, bagaimana masing-masing alir berawal, *decision* yang mungkin terjadi, dan bagaimana mereka berakhir (Ladjamudin, 2017).

Activity diagram menurut adalah salah satu cara untuk memodelkan *event-event* yang terjadi dalam suatu *use case*. Diagram ini juga dapat digantikan dengan sejumlah teks.

Tabel 2.2Simbol ActivityDiagram

No	Gambar	Nama	Keterangan
1		*Actifity*	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 /diawali.
4		*Actifity Final Node*	Bagaimana objek dibentuk dan dihancurkan
5		*Fork Node*	Satu aliran yang pada tahap tertentu berubah menjadi beberapa aliran

Sumber: (Kurniawan, 2018)

2.6.3 Flowchart

Flowchart digunakan dalam mendesain dan mendokumentasikan proses atau program sederhana. Seperti jenis diagram lainnya, diagram membantu memvisualisasikan apa yang sedang terjadi dan dengan demikian membantu memahami suatu proses, dan mungkin juga menemukan fitur-fitur yang kurang jelas dalam proses tersebut, seperti kekurangan dan hambatan. Ada berbagai jenis diagram alur: masing-masing jenis memiliki set kotak dan notasi sendiri. Dua jenis kotak yang paling umum dalam diagram alur adalah:

- langkah pemrosesan, biasanya disebut aktivitas dan dilambangkan sebagai kotak persegi panjang.
- keputusan biasanya dilambangkan sebagai berlian.

Diagram alir digambarkan sebagai "lintas fungsional" ketika bagan dibagi menjadi bagian vertikal atau horizontal yang berbeda, untuk menggambarkan kontrol unit organisasi yang berbeda. Simbol yang muncul di bagian tertentu berada dalam kendali unit organisasi itu. Flowchart lintas fungsional memungkinkan penulis untuk menemukan tanggung jawab untuk melakukan suatu tindakan atau membuat keputusan dengan benar, dan untuk menunjukkan tanggung jawab masing-masing unit organisasi untuk bagian berbeda dari satu proses tunggal.

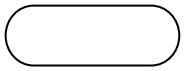
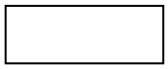
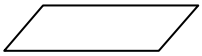
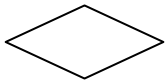
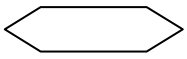
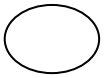
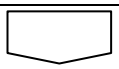
Diagram alir menggambarkan aspek-aspek tertentu dari proses dan biasanya dilengkapi dengan jenis diagram lainnya. Misalnya, Kaoru Ishikawa, mendefinisikan diagram alir sebagai salah satu dari tujuh alat dasar kendali mutu, di sebelah histogram, diagram Pareto, lembar periksa, diagram kontrol, diagram sebab-akibat, dan diagram sebaran. Demikian pula, di UML, notasi pemodelan konsep standar yang digunakan dalam pengembangan perangkat lunak, diagram aktivitas, yang merupakan jenis diagram alur, hanyalah salah satu dari banyak jenis diagram yang berbeda.

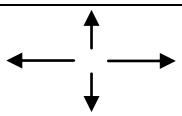
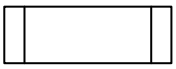
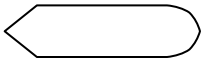
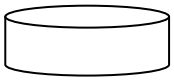
Diagram Nassi-Shneiderman dan Drakon-chart adalah diagram alir, alur proses, diagram alur fungsional, peta proses, diagram proses, diagram proses fungsional, model proses bisnis, model proses, diagram alir proses, diagram alur

kerja, diagram alir bisnis. Istilah "diagram alur" dan "diagram alir" digunakan secara bergantian(Nakatsu, 2019).

Struktur grafik yang mendasari diagram alur adalah grafik aliran, yang mengabstraksi jenis simpul, isinya, dan informasi tambahan lainnya. Adapun simbol-simbol flowchart lihat pada tabel sebagai berikut :

Tabel 2.3 SimbolFlowchart

NO	SIMBOL	FUNGSI
1.		**Terminal**, untuk memulai atau mengakhiri suatu program
2.		**Proses**, suatu simbol yang menunjukkan setiap pengolahan yang dilakukan.
3.		**Input-Output**, untuk memasukkan menunjukkan hasil dari suatu proses
4.		**Decision**, suatu kondisi yang akan menghasilkan beberapa kemungkinan jawaban atau pilihan
5.		**Preparation,** suatu symbol yang menyediakan tempat pengolahan
6.		**Connector**, suatu prosedur penghubung yang akan masuk atau keluar melalui symbol ini dalam lembar yang sama
7.		**Off-Page Connector**, merupakan symbol masuk atau keluarannya suatu prosedur pada lembaran kertas lainnya

8.		**Arus/Flow**, dari pada prosedur yang dapat dilakukan atas ke bawah dari bawah ke atas, ke atas dari kiri ke kanan ataupun dari kanan ke kiri
9.		**Predefined Process**, untuk menyatakan sekumpulan langkah proses yang ditulis sebagai prosedur
10.		Simbol untuk output, yang ditunjukkan ke suatu device, seperti printer, dan sebagainya
11		Penyimpanan file secara sementara
12		Menunjukkan input / Output Hardisk (media penyimpanan)

Sumber: (Kurniawan, 2018)

2.7 Visual Basic

Visual Basic (VB) adalah bahasa pemrograman yang digerakkan oleh peristiwa dan lingkungan dari Microsoft yang menyediakan antarmuka pengguna grafis (GUI) yang memungkinkan programmer untuk memodifikasi kode hanya dengan menyeret dan menjatuhkan objek dan menentukan perilaku dan penampilan mereka. VB berasal dari bahasa pemrograman BASIC dan dianggap event-driven dan berorientasi objek.VB dimaksudkan agar mudah dipelajari dan cepat untuk menulis kode; Akibatnya, kadang-kadang disebut sistem pengembangan aplikasi cepat (RAD) dan digunakan untuk prototipe aplikasi yang nantinya akan ditulis dalam bahasa yang lebih sulit tetapi efisien(Lee, 2014).

Versi terakhir VB, Visual Basic 6, dirilis pada tahun 1998, tetapi sejak itu telah digantikan oleh VB. NET, Visual Basic for Applications (VBA) dan Visual Studio .NET. VBA dan Visual Studio adalah dua kerangka kerja yang paling umum digunakan saat ini. VB adalah alat pengembangan berbasis GUI yang menawarkan RAD lebih cepat daripada kebanyakan bahasa pemrograman lainnya. VB juga memiliki fitur sintaksis yang lebih mudah daripada bahasa lain, lingkungan visual yang mudah dipahami dan konektivitas basis data yang tinggi.

2.7.1 Visual Basic.NET

Microsoft Visual Studio adalah salah satu bahasa pemrograman yang dikeluarkan dan dikembangkan oleh Microsoft. Metode pemrograman yang diterapkan dalam Visual Basic 2010 berorientasi kepada objek atau lebih sering dikenal dengan istilah OOP (*Object Oriented Programming*) sehingga mempermudah pengembangan program.

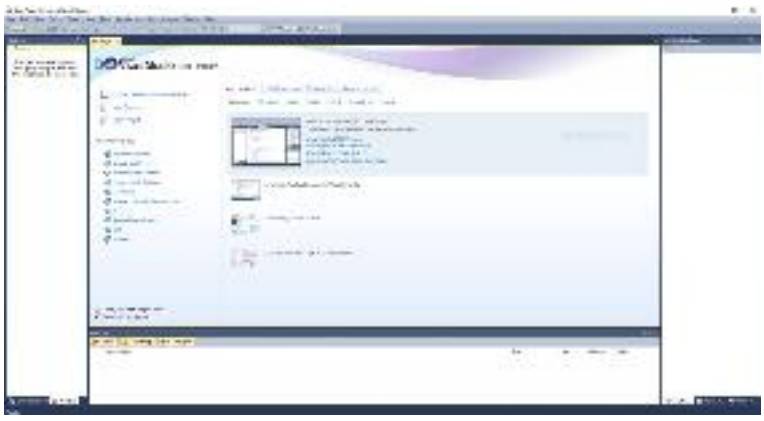
Visual Basic 2010 merupakan program *event-driven*, artinya program menunggu pengguna melakukan sesuatu ("*event*"), seperti klik pada ikon, dan kemudian program akan merespons ("*driven*"). Karena penggunaannya mudah, Visual BASIC memungkinkan programmer pemula untuk menciptakan aplikasi-aplikasi berbasis windows yang menarik.

Microsoft Visual Studio dapat digunakan untuk mengembangkan aplikasi dalam native code (dalam bentuk bahasa mesin yang berjalan di atas Windows) ataupun managed code (dalam bentuk Microsoft Intermediate Language di atas .NET Framework). Selain itu, Visual Studio juga dapat digunakan untuk

mengembangkan aplikasi Silverlight, aplikasi Windows Mobile (yang berjalan di atas .NET Compact Framework).

2.7.2 Antarmuka Visual Basic.NET

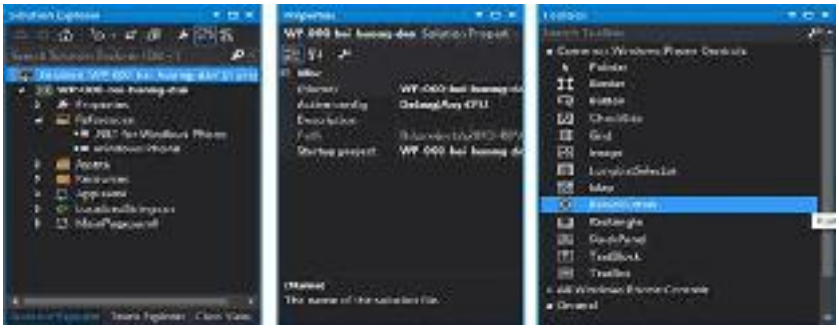
Visual Basic.Net memiliki beberapa versi. Gambar 2.2. adalah tampilan dari Visual Basic.Net versi 2010.



Gambar 2.4 Antarmuka Visual Basic.NET 2010
Sumber: (Rahmel, 2018)

2.7.3 Toolbox

Toolbox adalah sebuah panel yang menampung tombol-tombol yang berguna untuk membuat suatu desain mulai dari tombol *label*, *pointer*, *button*, dan lain-lain. Berikut ini adalah tampilan*toolbox* pada *visualbasic* 2010.



Gambar 2.5Tampilan Toolbox
Sumber : (Lee, 2014)

Tabel 2.7adalah daftar berisi nama tombol yang terdapat didalam *toolbox* beserta fungsinya.

Tabel 2.4Toolbox Visual Basic

Nama tombol	Fungsi
Pointer	Memilih, mengatur ukuran dan memindahkan posisi yang terpasang di bagian *form*.
Bindingsources	Untuk mengkoneksikan program ke *database.*
Label	Menampilkan teks, dimana pengguna program tidak bisa mengubah teks tersebut.
Groupbox	Untuk mengelompokkan *item* yang ada di *form.*
Checkbox	Membuat kotak periksa, dimana pengguna program dapat memilih sekaligus.
Listbox	Membuat daftar pilihan.
Timer	Membuat kontrol waktu dan interval yang diperlukan.
Image	Menampilkan gambar pada *form* dalam format *bitmap, icone*, atau *metafile*.
Picturebox	Menampilkan gambar dari sebuah *file.*

Textbox	Membuat teks, dimana teks tersebut dapat diubah oleh pembuat program.
Button	Membuat tombol perintah.
Combobox	Menambahkan kontrol kotak *combo* yang merupakan kontrol gabungan antara *textbox* dan *listbox.*

Sumber : (Lee, 2014)

2.7.4 Kelebihan Visual Basic

Berikut ini adalah beberapa kelebihan Visual Basic dibandingkan bahasa pemrograman lainnya:

1 VB.NET mengatasi semua masalah yang sulit disekitar pengembangan aplikasi berbasis windows.

2 VB.NET mempunyai fasilitas penanganan Bug yang hebat dan Real Time Background Compiler.

3 Windows Form designer memungkinkan develover memperoleh aplikasi dekstop dalam waktu singkat.

4 VB.NET menyediakan bagi Develover pemrograman data akses ActiveX Data Object(ADO).

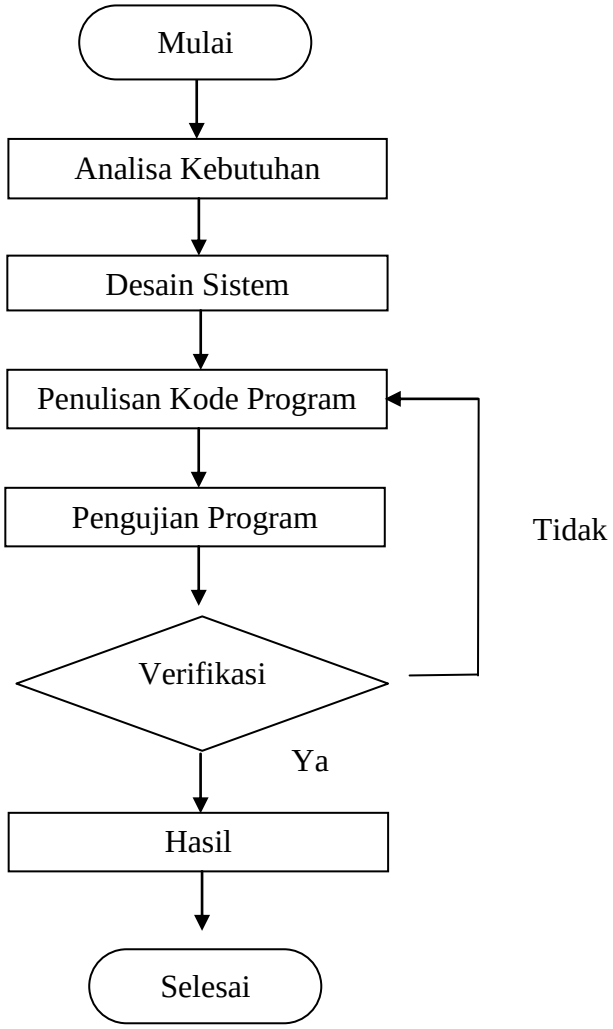
5 VB.NET menghasilkan “Visual Basic untuk Web”. Menggunakan form web yang baru,dapat dengan mudah membangun Thin-Client aplikasi berbasiskan web yang secara cerdas dapat berjalan di browser dan Platform manapun.

BAB III

METODE PENELITIAN

3.1 Tahapan Penelitian

Tahapan penelitian digunakan untuk membuat penelitian lebih terstruktur. Tahapan ini dikerjakan dari cara memperoleh data untuk kebutuhan penelitian sampai penyelesaian penelitian digambarkan dalam bentuk flowchart pada gambar 3.1.



Gambar 3.1Tahapan Penelitian

Berikut adalah tahapan penelitian yang dilakukan:

- Studi Literatur

  Studi literatur dilakukan untuk mendapatkan teori-teori tentang ilmu kriptografi khususnya teknik One Time Pad. Studi ini dapat dilaksanakan dengan membaca buku dan informasi yang ada di internet sehingga menambah wawasan daeri penulis.

- Analisa Kebutuhan

  Bagian ini menjelaskan proses analisa permasalahan dan bagaimana permasalahan dapat diselesaikan dengan baik. Analisa akan memeriksa kebenaran dari rancangan yang akan dibuat.

- Desain Sistem

  Bagian ini merancang tampilan dari program aplikasi yang akan dibuat. Setiap perancangan dilakukan tahap demi tahap untuk setiap menu-menu yang ada.

- Penulisan Kode Program

  Kode program dilakukan dan dibuat dengan menggunakan bahasa pemograman Microsoft Visual Basic.Net 2010. Program ini berada pada naungan Microsoft Visual Studio 2010.

- Verifikasi

  Bagian ini dilakukan pengujian kebenaran output yang dihasilkan oleh program aplikasi Microsoft Visual Basic.Net 2010.

- Hasil

Hasil akan ditampilkan apabila sudah menjalani verifikasi dan menyatakan keberhasilannya.

3.2 Metode Pengumpulan Data

Metode pengumpulan data yang dilakukan bertujuan untuk mendapatkan hasil berdasarkan perancangan algoritma yang sudah dipaparkan sebelumnya. Ada beberapa tahap yang dilakukan dalam melakukan pengumpulan data yaitu :

1. Studi Kepustakaan

   Pada tahap ini dilakukan dengan mengumpulkan data, mempelajari, dan membaca berbagai referensi baik itu buku, jurnal, makalah, internet, dan berbagai sumber lainnya untuk memperoleh informasi.

2. Wawancara

   Wawancara dilakukan dengan mendapatkan informasi secara tatap muka terhadap orang yang memiliki pengetahuan kriptografi tentang One Time Pad. Hasil wawancara akan digunakan untuk menambah pengetahuan dalam membuat program aplikasi.

3. Pengamatan

   Pengamatan dilakukan dengan cara melihat hasil yang dikeluarkan oleh program aplikasi dan perhitungan manual. Uji coba dilakukan untuk mendapatkan nilai yang konsisten antara perhitungan manual dan hasil program aplikasi.

3.3 Analisa Sistem Yang Sudah Ada

Pengiriman pesan hanya dilakukan dengan hanya menggunakan kunci angka seperti pada Beaufort Cipher. Pengiriman ini sungguh tidak aman karena begitu kunci atau angka diketahui maka seluruh isi ciphertext dapat dibongkar dengan menggunakan kunci tersebut. Hal ini akan mengakitbatkan kerugian bagi pemilik pesan tersebut. Sistem seperti ini banyak memiliki kekurangan dari segi pengamanan, untuk itu diperlukan sistem yang lebih baik.

3.4 Analisa Sistem Yang Diusulkan

Dalam pengiriman pesan, peningkatan keamanan sangat dibutuhkan agar terhindar dari pencurian datal. Sistem yang diusulkan yaitu menggunakan One Time Pad. Pengamanan jenis ini akan memiliki kunci yang panjang sehingga susah untuk ditebak oleh orang yang ingin membongkar pesan tersebut. Teknik kriptografi ini juga menggunakan proses bit sehingga hasil enkripsi untuk karakter yang sama belum tentu menghasilkan ciphertext yang sama karena melakukan operasi bit yang berbeda.Pada penelitian ini, plaintext akan dienkripsi menggunakan kunci yang akan diubah menjadi deretan bit. Plaintext juga akan diubah menjadi deretan bit. ciphertext baru.

3.5 Rancangan Penelitian

Rancangan penelitian menggambarkan bagaimana alur kerja dari penelitian dilakukan. Rancangan ini akan digambarkan menggunakan diagram dan flowchart.Ada dua buah diagram yang akan digunakan pada penelitian antara lain:

1. Use case diagram
2. Activity Diagram

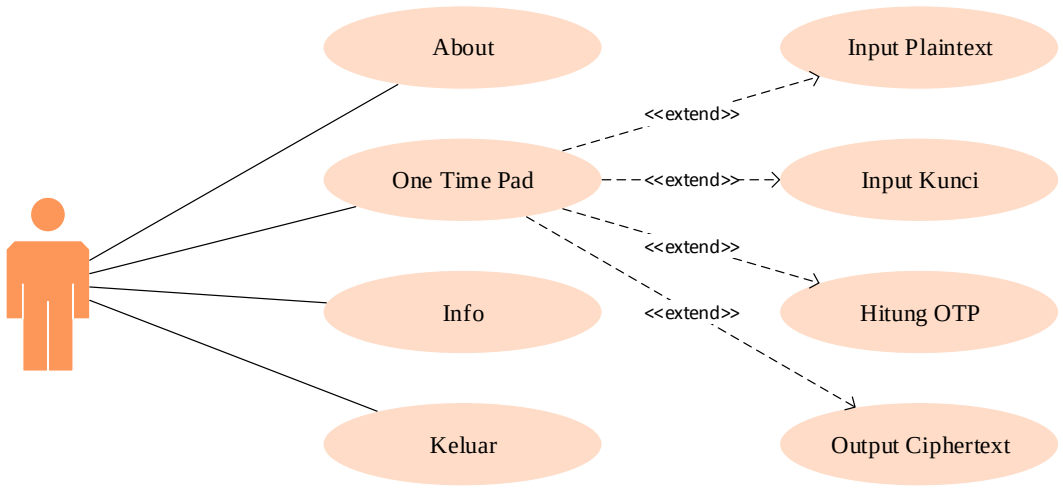
Penelitian ini juga menggunakan sebuah flowchart yang akan menunjukkan alur dan tahapan yang dilakukan dalam pembuatan program aplikasi. Flowchart terdiri dari dua, antara lain:

1. Flowchart Enkripsi
2. Flowchart Dekripsi

Bagian ini akan menerapkan perancangan penelitian dalam menggambarkan setiap model dan bagian yang berfungsi untuk melengkapi kegiatan pengguna tentang gambaran yang jelas tentang perancangan sistem yang akan dibuat serta diimplementasikan.

3.5.1 Use Case Diagram

Use Case adalah deskripsi fungsi dari sebuah sistem dari perspektif pengguna. *Use Case* bekerja dengan cara mendeskripsikan tipikal interaksi antara *User* (pengguna) sebuah sistem dengan sistemnya sendiri melalui sebuah cerita bagaimana sebuah sistem dipakai. Gambar 3.2 adalah perancangan *Use Case* untuk kriptografi dengan teknik One Time pad.



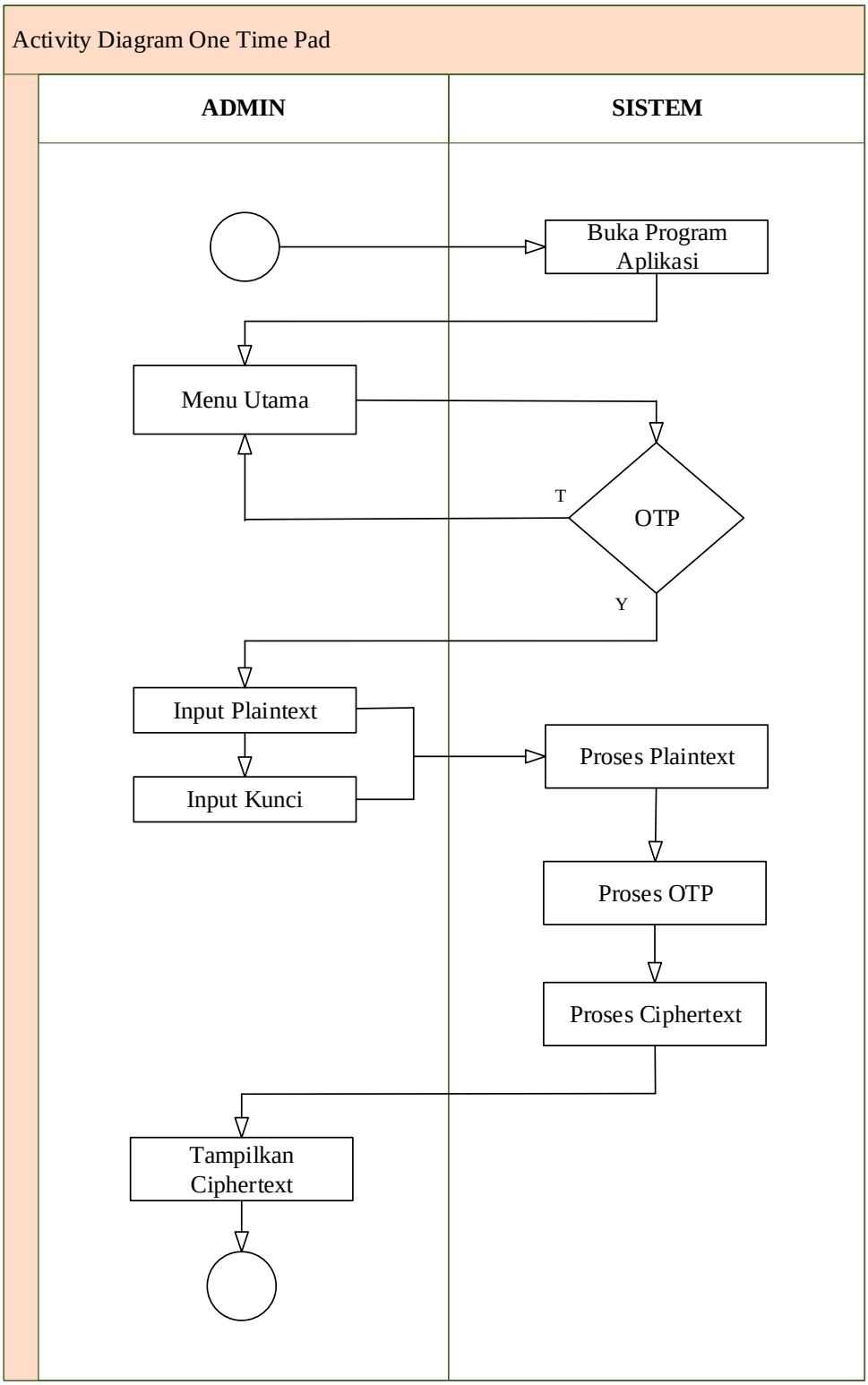
Gambar 3.2 Use Case Diagram

Use case pada gambar 3.2 menjelaskan bahwa aktor memiliki empat buah menu yang dapat dipilih pada program aplikasi. Menu kriptografi terletak pada One Time Pad. Pada saat One Time Pad dibuka, maka akan mengerjakan empat buah tahapan, antara lain:

1. Input Plaintext
2. Input Kunci
3. Hitung One Time Pad
4. Output Ciphertext

3.5.2 Activity Diagram

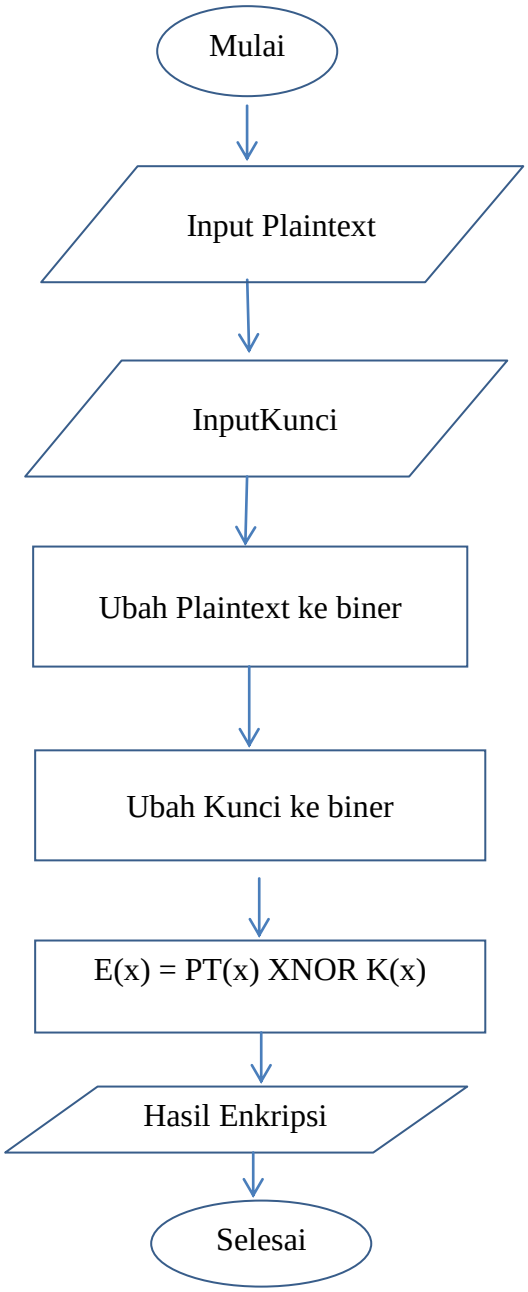
*Activity diagram*akan menggambarkan alur aktifitas dari sistem, untuk *Activity diagram* dari kriptrografi simetris dengan menggunakan teknik One Time Pad. Gambar3.3 menjelaskan activity diagram tersebut.



Gambar 3.3 Activity Diagram

3.5.3 Flowchart Enkripsi

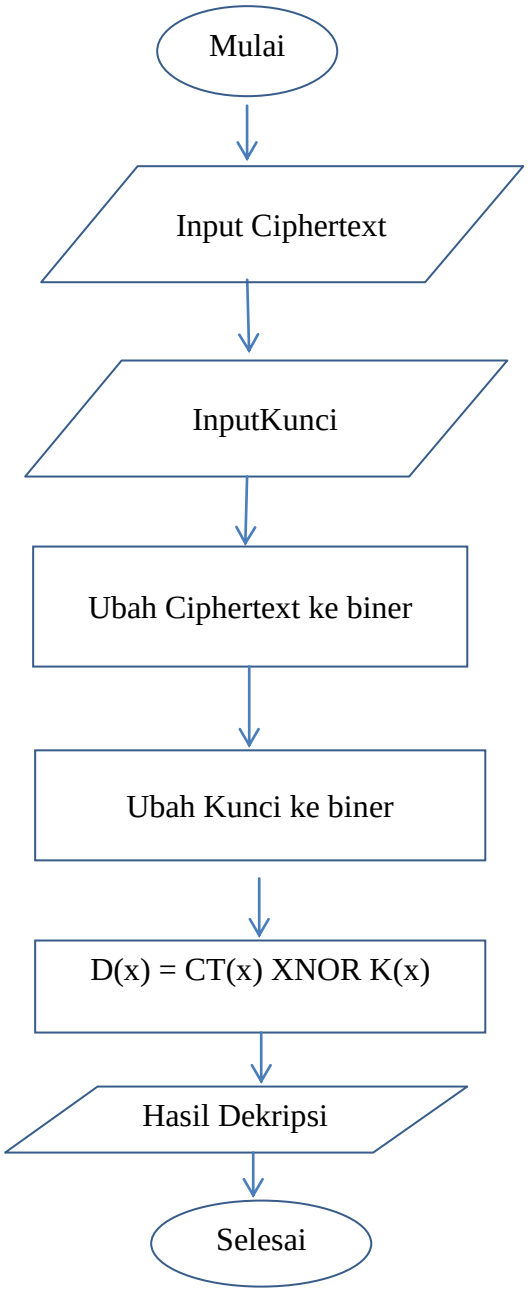
Flowchart akan menjelaskan alur dari proses enkripsi dengan metode stream cipher dengan teknik One Time Pad. Rancangan flowchar tenkripsi dapat dilihat pada gambar 3.4.



Gambar 3.4Flowchart EnkripsiOTP

3.5.4 Flowchart Dekripsi

Flowchartberikut akan menjelaskan alur dari proses dekripsi dengan metode stream cipher dengan teknik One Time Pad. Rancangan flowchartdekripsi dapat dilihat pada gambar 3.5.



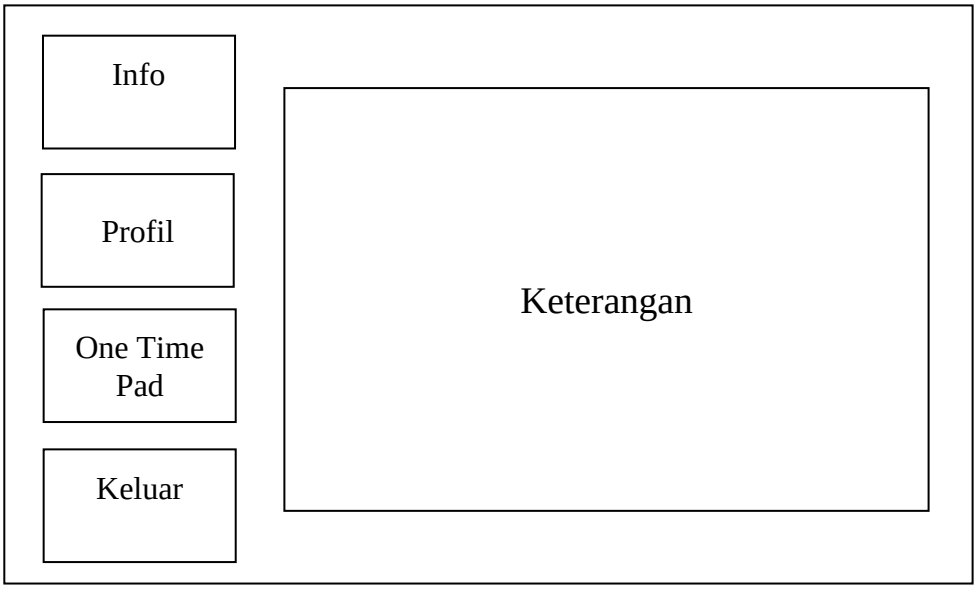
Gambar 3.5Flowchart Dekripsi OTP

3.6 Desain Antarmuka

Perancangan desain tampilan atau desain antarmuka merupakan perancangan bagaimana suatu program aplikasi akan ditampilkan. Perancangan ini bertujuan untuk memudahkan pengguna dalam menentukan dan melakukan proses enkripsi dan dekripsi dengan teknik One Time Pad. Perancangan ini kemudian akan diprogram dengan bahasa pemograman Microsoft Visual Basic.Net 2010. Desain antarmuka ini terbagi menjadi beberapa tahap yang memiliki satu buah menu utama yang berfungsi sebagai pembuka menu yang ada didalamnya. Berikut ini akan dijelaskan tahap-tahap desain antarmuka yang akan penulis lakukan.

3.6.1 Menu Utama

Menu utama akan ditampilkan pada saat progam aplikasi dijalankan. Gambar 3.6 adalah perancangan menu utama yang terdiri dari tiga buah sub-menu.



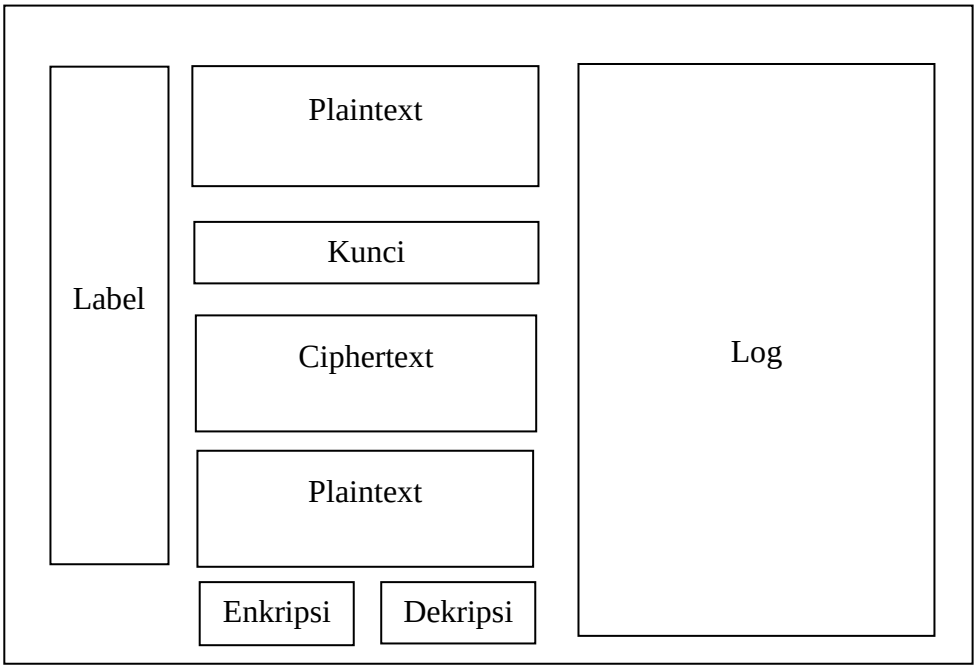
Gambar 3.6Perancangan Menu Utama

Menu ini memiliki berapa sub-menu antara lain:

1. Info
2. Profil
3. One Time Pad
4. Keluar

3.6.2 Menu One Time Pad

Menu ini adalah bagian penting dari program aplikasi yang akan mengerjakan proses enkripsi dan dekripsi dengan teknik One Time Pad. Pada menu ini terdapat beberapa bagian yang menjadi input, proses, output dan riwayat perhitungan lengkap dari plaintext ke ciphertext dan juga ciphertext ke plaintext kembali. Gambar 3.7menjelaskan perancangan menu One Time Pad.



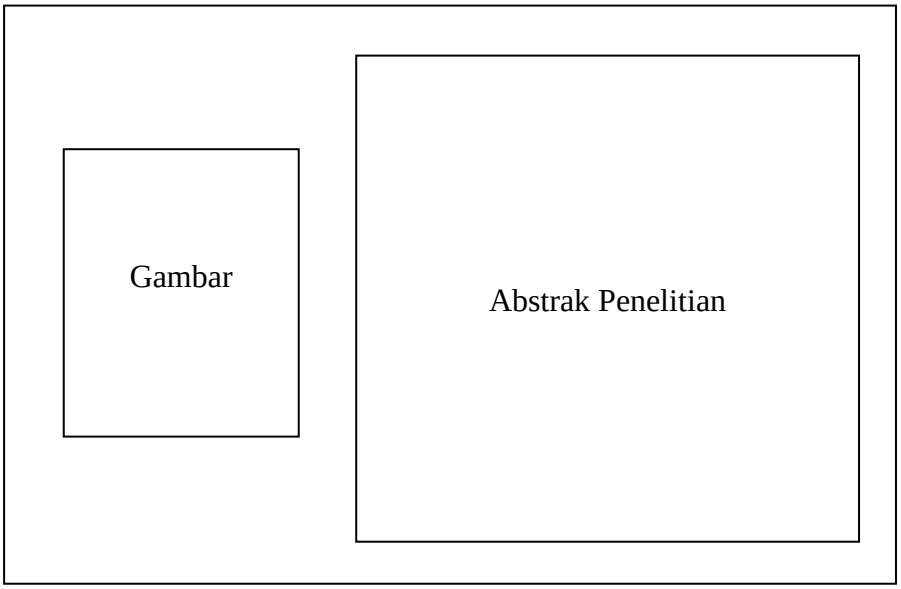
Gambar 3.7Perancangan Menu One Time Pad

Menu One Time Pad memiliki beberapa bagian antara lain:

1. Plaintext
2. Kunci
3. Ciphertext
4. Label
5. Tombol Enkripsi
6. Tombol Dekripsi

3.6.3 Menu Info

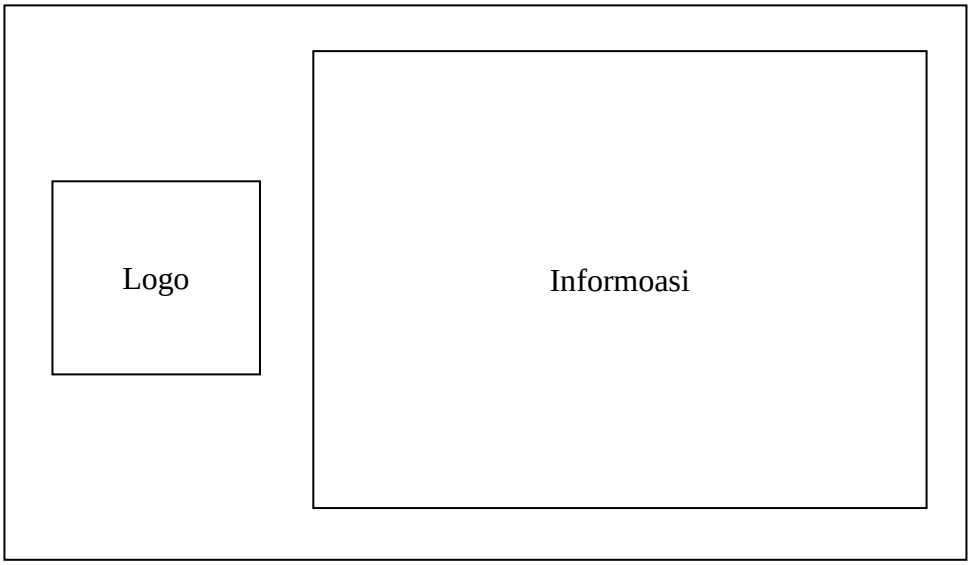
Menu ini menampilkan abtrak dari penelitian yang telah penuis lakukan. Menu ini akan menjelaskan rumusan masalah, tujuan dan manfaat serta hasil penelitian yang diperoleh. Gambar 3.8 adalah perancangan menu Info.



Gambar 3.8Perancangan Menu Info

3.6.4 Menu Profil

Menu ini akan menampilkan biodata singkat tentang penulis. Pada menu ini akan ditampilkan logo dari Universitas Pembangunan Panca Budi. Menu ini terdiri dari dua objek, yaitu logo dan informasi. Gambar berikut ini adalah hasil tampilan dari menu About.



Gambar 3.9Perancangan Menu Profil

BAB IV

HASIL DAN PEMBAHASAN

Hasil dan pembahasan akan membahas hasilperancangan danpembuatan program kriptografi dengan teknik One Time Pad.Hasil dan pembahasan merupakan implementasi dari program aplikasi yang sudah dibuat sebelumnya dengan menggunakan Microsoft Visual Basic.Net 2010. Pada bagian implementasi dibedakan kepada dua jenis yaitu implementasi algoritma dan implementasi antarmuka.

4.1 Spesifikasi Sistem

Penelitian ini merupakan penelitian yang mengambil topik ilmu kriptografi, yaitu teknik One Time Pad. Selain membutuhkan datapenelitian yang bersumber dari internet,dibutuhkan juga perangkat pendukung agar penelitian ini dapat diterapkan denganbaik dan benar. Perangkat pendukung yang dibutuhkan dibagi menjadi dua yaituperangkat keras dan perangkat lunak. Adapun spesifikasi perangkat keras perangkat lunak tersebut dapat dilihat pada bagian selanjutnya.

4.1.1 Spesifikasi Perangkat Keras

Penerapan teknik One Time Pad pada metode kriptografi stream cipher sudah pasti akan membutuhkan perangkat keras sebagai media fisiksebagai sarana pendukung utama. Berikut ini adalah spesifikasi perangkat keras yang digunakan pada penelitian ini.

Tabel 4.1Spesifikasi perangkat keras

No.	Nama Komponen	Spesifikasi
1	Processor	Intel Core i5 2.4 GHz
2	RAM	8192 MB
3	Storage	500 GB
4	Display	14inch

4.1.2 Spesifikasi Perangkat Lunak

Perangkat lunak juga harus wajib ada untuk mendukung kerja dari perangkat keras tersebut. Hal ini digunakan sebagai media antara manusia dan alat dalam mendukung implementasi penelitian ini. Kebutuhan akan perangkat lunak sebagaisarana non-fisik sangat menunjang hasil kerja.Berikut ini adalah spsesifikasi perangkatlunak yang digunakan pada penelitian ini.

Tabel 4.2 Spesifikasi perangkat lunak

No.	Nama Komponen	Spesifikasi
1	Sistem Operasi	Windows 1064 Bit
2	IDE Pemrograman	Microsoft Visual Basic.NET 2010
3	Tangkap Gambar	Snipping Tool
4	Data Editor	Microsoft Excel

4.2 Implementasi Antarmuka

Implementasi antarmuka program kriptografi memiliki beberapa bagian yang memiliki antarmuka dan fungsi yang berbeda-beda. Antarmuka ini diprogram menggunakan Microsoft Visual Basic.Net 2010.

4.2.1 Halaman Menu Utama

Halaman menu utama adalah tampilan yang pertama sekali muncul pada saat program aplikasi dijalankan. Pada tampilan ini, ada beberapa menu yang akan dieksekusi untuk memberikan pengguna pilihan menu selanjutnya. Halaman ini memiliki empat buah tombol yang memiliki fungsi yang berbeda-beda. Gambar 4.1 adalah hasil tampilan menu utama.

Gambar 4.1 Halaman Menu Utama

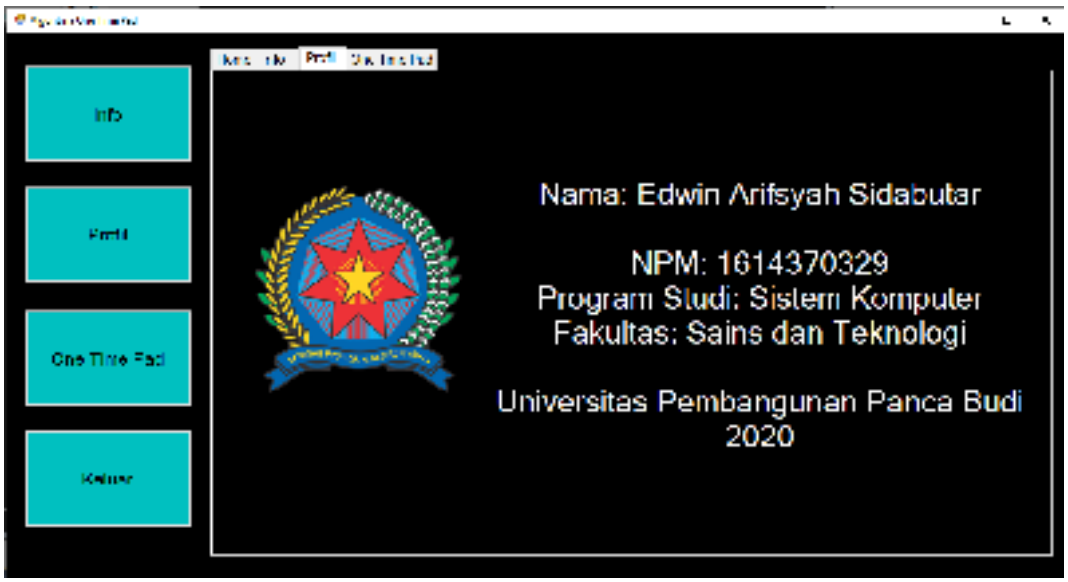
4.2.2 Halaman Info

Halaman info adalah menu yang menampilkan penjelasan singkat tentang penelitian yang penulis lakukan. Halaman ini merupakan abstrak dari penelitian. Gambar 3.2 menunjukkan hasil tampilan dari halaman info.

Gambar 4.2 Halaman Info

4.2.3 Halaman Profil

Halaman about adalah tampilan tentang penulis. Halaman ini menampilkan informasi tentang nama, NPM, fakutas dan program studi. Gambar 4.3 adalah tampilan dari halaman About.



Gambar 4.3 Halaman Profil

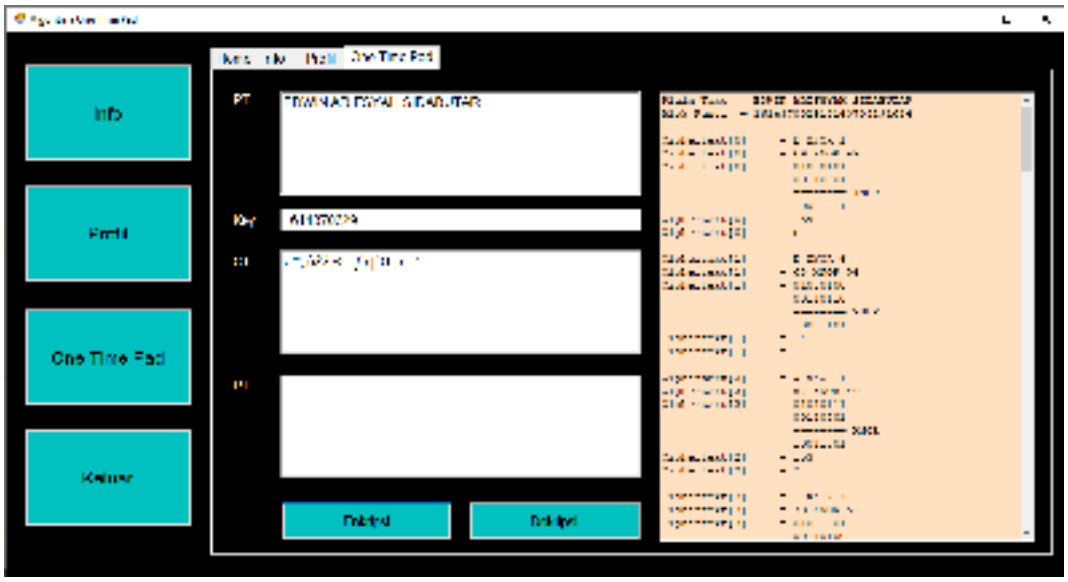
4.2.4 Halaman One Time Pad

Halaman ini merupakan halaman yang akan memproses plaintext sehingga menjadi ciphertext. Halaman ini adalah dimana proses kriptografi dilakukan. Teknik yang digunakan adalah One Time Pad. Halaman ini memiliki duah buah plaintext antara lain sebelum proses enkripsi dan setelah proses dekripsi. Ada juga sebuah textbox yang menampung kunci dan sebuah textbox dimana ciphertext yang dihasilkan akan ditampilkan. Sementara untuk proses eksekusi enkripsi dan dekripsi, halaman ini memiliki beberapa tombol eksekusi yang dibentuk dari objek button. Gambar 4.4 adalah hasil tampilan dari halaman One Time Pad.

Gambar 4.4 Halaman One Time Pad

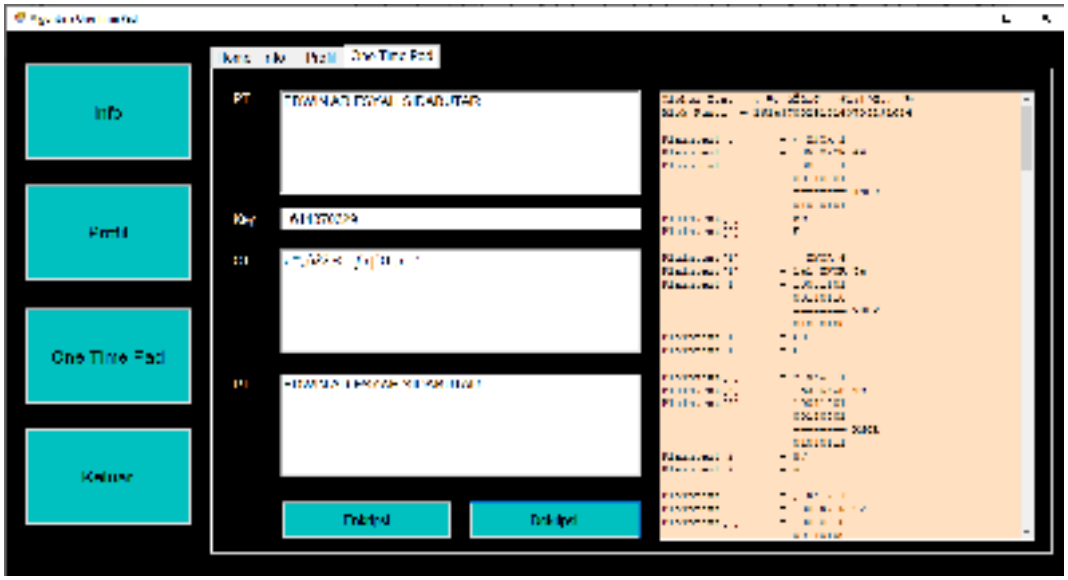
4.2.5 Hasil Perhitungan One Time Pad

Hasil perhitungan One Time Pad akan ditampilkan pada halaman ini. Perhitungan akan menampilkan hasil enkripsi dan dekripsi dari plaintext dan ciphertext yang akan diproses menggunakan teknik One Time Pad. Ada dua buah input yang harus diisi dalam menentukan hasil yaitu plaintext dan kunci. Kedua textbox ini akan diproses sehingga membentuk blok kunci. Blok kunci akan memiliki panjang sama percis dengan panjang dari plaintext. Setiap karakter pada plaintext akan dilakukan operasi exclusive-or terhadap kunci untuk mendapatkan ciphertext. Proses dekripsi akan melakukan hal yang sama yaitu melakukan proses exclusive-or ciphertext terhadap blok kunci yang sudah ditentukan sebelumnya. Hasil yang benar akan menampilkan bahwa plaintext sebelum proses enkripsi harus sama dengan plaintext yang dihasilkan setelah proses dekirpsi. Gambar 4.5 adalah tampilan dari hasil perhitungan proses enkripsi One Time Pad.



Gambar 4.5Hasil enkripsi One Time Pad

Bagian dekripsi akan mengembalikan ciphertext menjadi plaintext seperti sebelumnya.Dekripsi akan mengerjakan urutan yang sama seperti pada proses enkripsi sehingga plaintext dapat ditentukan kembali. Pada textbox, plaintext harus menampilkan deretan karakter yang sama percis pada plaintext pertama sekali agar terbukti perhitungan One Time Pad berjalan dengan benar. Jika ada satu karakter yang tidak memiliki kesamaan dengan plaintext sebelumnya, maka perhitungan ini dinyakatan salah. Gambar 4.6 adalah tampilan dari hasil perhitungan proses dekripsi One Time Pad.



Gambar 4.6Hasil dekripsi One Time Pad

4.3 Uji Coba Perhitungan Manual

Uji coba perhitungan manual dilakukan untuk mendapatkan hasil perhitungan proses enkripsi dan dekripsi dengan teknik One Time Pad.Berikut ini adalah perhitungan lengkap pada proses enkripsi dari teknik One Time Pad.

Proses Enkripsi

```
Plain Text  = EDWIN ARIFSYAH SIDABUTAR
Blok Kunci  = 16143703291614370329161437032916

Ciphertext[0]      = E XNOR 1
Ciphertext[0]      = 69 XNOR 49
Ciphertext[0]      = 01000101
                     00110001
                     ======== XNOR
                     10001011
Ciphertext[0]      = 139
Ciphertext[0]      = ‹

Ciphertext[1]      = D XNOR 6
Ciphertext[1]      = 68 XNOR 54
Ciphertext[1]      = 01000100
                     00110110
                     ======== XNOR
```

```
                    10001101
Ciphertext[1]     = 141
Ciphertext[1]     = □

Ciphertext[2]     = W XNOR 1
Ciphertext[2]     = 87 XNOR 49
Ciphertext[2]     = 01010111
                    00110001
                    ======== XNOR
                    10011001
Ciphertext[2]     = 153
Ciphertext[2]     = ™

Ciphertext[3]     = I XNOR 4
Ciphertext[3]     = 73 XNOR 52
Ciphertext[3]     = 01001001
                    00110100
                    ======== XNOR
                    10000010
Ciphertext[3]     = 130
Ciphertext[3]     = ,

Ciphertext[4]     = N XNOR 3
Ciphertext[4]     = 78 XNOR 51
Ciphertext[4]     = 01001110
                    00110011
                    ======== XNOR
                    10000010
Ciphertext[4]     = 130
Ciphertext[4]     = ,

Ciphertext[5]     =   XNOR 7
Ciphertext[5]     = 32 XNOR 55
Ciphertext[5]     = 00100000
                    00110111
                    ======== XNOR
                    11101000
Ciphertext[5]     = 232
Ciphertext[5]     = è

Ciphertext[6]     = A XNOR 0
Ciphertext[6]     = 65 XNOR 48
Ciphertext[6]     = 01000001
                    00110000
                    ======== XNOR
                    10001110
Ciphertext[6]     = 142
Ciphertext[6]     = Ž

Ciphertext[7]     = R XNOR 3
Ciphertext[7]     = 82 XNOR 51
Ciphertext[7]     = 01010010
                    00110011
                    ======== XNOR
                    10011110
Ciphertext[7]     = 158
```

```
Ciphertext[7]     = ž

Ciphertext[8]     = I XNOR 2
Ciphertext[8]     = 73 XNOR 50
Ciphertext[8]     = 01001001
                    00110010
                    ======== XNOR
                    10000100
Ciphertext[8]     = 132
Ciphertext[8]     = „

Ciphertext[9]     = F XNOR 9
Ciphertext[9]     = 70 XNOR 57
Ciphertext[9]     = 01000110
                    00111001
                    ======== XNOR
                    10000000
Ciphertext[9]     = 128
Ciphertext[9]     = €

Ciphertext[10]    = S XNOR 1
Ciphertext[10]    = 83 XNOR 49
Ciphertext[10]    = 01010011
                    00110001
                    ======== XNOR
                    10011101
Ciphertext[10]    = 157
Ciphertext[10]    = □

Ciphertext[11]    = Y XNOR 6
Ciphertext[11]    = 89 XNOR 54
Ciphertext[11]    = 01011001
                    00110110
                    ======== XNOR
                    10010000
Ciphertext[11]    = 144
Ciphertext[11]    = □

Ciphertext[12]    = A XNOR 1
Ciphertext[12]    = 65 XNOR 49
Ciphertext[12]    = 01000001
                    00110001
                    ======== XNOR
                    10001111
Ciphertext[12]    = 143
Ciphertext[12]    = □

Ciphertext[13]    = H XNOR 4
Ciphertext[13]    = 72 XNOR 52
Ciphertext[13]    = 01001000
                    00110100
                    ======== XNOR
                    10000011
Ciphertext[13]    = 131
Ciphertext[13]    = ƒ
```

```
Ciphertext[14]    =   XNOR 3
Ciphertext[14]    = 32 XNOR 51
Ciphertext[14]    = 00100000
                    00110011
                    ======== XNOR
                    11101100
Ciphertext[14]    = 236
Ciphertext[14]    = ì

Ciphertext[15]    = S XNOR 7
Ciphertext[15]    = 83 XNOR 55
Ciphertext[15]    = 01010011
                    00110111
                    ======== XNOR
                    10011011
Ciphertext[15]    = 155
Ciphertext[15]    = ›

Ciphertext[16]    = I XNOR 0
Ciphertext[16]    = 73 XNOR 48
Ciphertext[16]    = 01001001
                    00110000
                    ======== XNOR
                    10000110
Ciphertext[16]    = 134
Ciphertext[16]    = †

Ciphertext[17]    = D XNOR 3
Ciphertext[17]    = 68 XNOR 51
Ciphertext[17]    = 01000100
                    00110011
                    ======== XNOR
                    10001000
Ciphertext[17]    = 136
Ciphertext[17]    = ˆ

Ciphertext[18]    = A XNOR 2
Ciphertext[18]    = 65 XNOR 50
Ciphertext[18]    = 01000001
                    00110010
                    ======== XNOR
                    10001100
Ciphertext[18]    = 140
Ciphertext[18]    = Œ

Ciphertext[19]    = B XNOR 9
Ciphertext[19]    = 66 XNOR 57
Ciphertext[19]    = 01000010
                    00111001
                    ======== XNOR
                    10000100
Ciphertext[19]    = 132
Ciphertext[19]    = „

Ciphertext[20]    = U XNOR 1
Ciphertext[20]    = 85 XNOR 49
```

```
Ciphertext[20]    = 01010101
                    00110001
                    ======== XNOR
                    10011011
Ciphertext[20]    = 155
Ciphertext[20]    = ›

Ciphertext[21]    = T XNOR 6
Ciphertext[21]    = 84 XNOR 54
Ciphertext[21]    = 01010100
                    00110110
                    ======== XNOR
                    10011101
Ciphertext[21]    = 157
Ciphertext[21]    = □

Ciphertext[22]    = A XNOR 1
Ciphertext[22]    = 65 XNOR 49
Ciphertext[22]    = 01000001
                    00110001
                    ======== XNOR
                    10001111
Ciphertext[22]    = 143
Ciphertext[22]    = □

Ciphertext[23]    = R XNOR 4
Ciphertext[23]    = 82 XNOR 52
Ciphertext[23]    = 01010010
                    00110100
                    ======== XNOR
                    10011001
Ciphertext[23]    = 153
Ciphertext[23]    = ™

Cipher Text = ‹□™,,èŽž„€□□□ƒì›†ˆŒ„›□□™
```

Proses Dekripsi

```
Cipher Text = ‹□™,,èŽž„€□□□ƒì›†ˆŒ„›□□™
Blok Kunci  = 16143703291614370329161

Plaintext[0]      = ‹ XNOR 1
Plaintext[0]      = 139 XNOR 49
Plaintext[0]      = 10001011
                    00110001
                    ======== XNOR
                    01000101
Plaintext[0]      = 69
Plaintext[0]      = E

Plaintext[1]      = □ XNOR 6
Plaintext[1]      = 141 XNOR 54
Plaintext[1]      = 10001101
```

```
                    00110110
                    ======== XNOR
                    01000100
Plaintext[1]      = 68
Plaintext[1]      = D

Plaintext[2]      = ™ XNOR 1
Plaintext[2]      = 153 XNOR 49
Plaintext[2]      = 10011001
                    00110001
                    ======== XNOR
                    01010111
Plaintext[2]      = 87
Plaintext[2]      = W

Plaintext[3]      = , XNOR 4
Plaintext[3]      = 130 XNOR 52
Plaintext[3]      = 10000010
                    00110100
                    ======== XNOR
                    01001001
Plaintext[3]      = 73
Plaintext[3]      = I

Plaintext[4]      = , XNOR 3
Plaintext[4]      = 130 XNOR 51
Plaintext[4]      = 10000010
                    00110011
                    ======== XNOR
                    01001110
Plaintext[4]      = 78
Plaintext[4]      = N

Plaintext[5]      = è XNOR 7
Plaintext[5]      = 232 XNOR 55
Plaintext[5]      = 11101000
                    00110111
                    ======== XNOR
                    00100000
Plaintext[5]      = 32
Plaintext[5]      =

Plaintext[6]      = Ž XNOR 0
Plaintext[6]      = 142 XNOR 48
Plaintext[6]      = 10001110
                    00110000
                    ======== XNOR
                    01000001
Plaintext[6]      = 65
Plaintext[6]      = A

Plaintext[7]      = ž XNOR 3
Plaintext[7]      = 158 XNOR 51
Plaintext[7]      = 10011110
                    00110011
                    ======== XNOR
```

```
                    01010010
Plaintext[7]      = 82
Plaintext[7]      = R

Plaintext[8]      = „ XNOR 2
Plaintext[8]      = 132 XNOR 50
Plaintext[8]      = 10000100
                    00110010
                    ======== XNOR
                    01001001
Plaintext[8]      = 73
Plaintext[8]      = I

Plaintext[9]      = € XNOR 9
Plaintext[9]      = 128 XNOR 57
Plaintext[9]      = 10000000
                    00111001
                    ======== XNOR
                    01000110
Plaintext[9]      = 70
Plaintext[9]      = F

Plaintext[10]     =  XNOR 1
Plaintext[10]     = 157 XNOR 49
Plaintext[10]     = 10011101
                    00110001
                    ======== XNOR
                    01010011
Plaintext[10]     = 83
Plaintext[10]     = S

Plaintext[11]     =  XNOR 6
Plaintext[11]     = 144 XNOR 54
Plaintext[11]     = 10010000
                    00110110
                    ======== XNOR
                    01011001
Plaintext[11]     = 89
Plaintext[11]     = Y

Plaintext[12]     =  XNOR 1
Plaintext[12]     = 143 XNOR 49
Plaintext[12]     = 10001111
                    00110001
                    ======== XNOR
                    01000001
Plaintext[12]     = 65
Plaintext[12]     = A

Plaintext[13]     = ƒ XNOR 4
Plaintext[13]     = 131 XNOR 52
Plaintext[13]     = 10000011
                    00110100
                    ======== XNOR
                    01001000
Plaintext[13]     = 72
```

```
Plaintext[13]     = H

Plaintext[14]     = ì XNOR 3
Plaintext[14]     = 236 XNOR 51
Plaintext[14]     = 11101100
                    00110011
                    ======== XNOR
                    00100000
Plaintext[14]     = 32
Plaintext[14]     =

Plaintext[15]     = › XNOR 7
Plaintext[15]     = 155 XNOR 55
Plaintext[15]     = 10011011
                    00110111
                    ======== XNOR
                    01010011
Plaintext[15]     = 83
Plaintext[15]     = S

Plaintext[16]     = † XNOR 0
Plaintext[16]     = 134 XNOR 48
Plaintext[16]     = 10000110
                    00110000
                    ======== XNOR
                    01001001
Plaintext[16]     = 73
Plaintext[16]     = I

Plaintext[17]     = ˆ XNOR 3
Plaintext[17]     = 136 XNOR 51
Plaintext[17]     = 10001000
                    00110011
                    ======== XNOR
                    01000100
Plaintext[17]     = 68
Plaintext[17]     = D

Plaintext[18]     = Œ XNOR 2
Plaintext[18]     = 140 XNOR 50
Plaintext[18]     = 10001100
                    00110010
                    ======== XNOR
                    01000001
Plaintext[18]     = 65
Plaintext[18]     = A

Plaintext[19]     = „ XNOR 9
Plaintext[19]     = 132 XNOR 57
Plaintext[19]     = 10000100
                    00111001
                    ======== XNOR
                    01000010
Plaintext[19]     = 66
Plaintext[19]     = B
```

```
Plaintext[20]     = › XNOR 1
Plaintext[20]     = 155 XNOR 49
Plaintext[20]     = 10011011
                    00110001
                    ======== XNOR
                    01010101
Plaintext[20]     = 85
Plaintext[20]     = U

Plaintext[21]     = □ XNOR 6
Plaintext[21]     = 157 XNOR 54
Plaintext[21]     = 10011101
                    00110110
                    ======== XNOR
                    01010100
Plaintext[21]     = 84
Plaintext[21]     = T

Plaintext[22]     = □ XNOR 1
Plaintext[22]     = 143 XNOR 49
Plaintext[22]     = 10001111
                    00110001
                    ======== XNOR
                    01000001
Plaintext[22]     = 65
Plaintext[22]     = A

Plaintext[23]     = ™ XNOR 4
Plaintext[23]     = 153 XNOR 52
Plaintext[23]     = 10011001
                    00110100
                    ======== XNOR
                    01010010
Plaintext[23]     = 82
Plaintext[23]     = R

Plain Text  = EDWIN ARIFSYAH SIDABUTAR
```

BAB V

PENUTUP

5.1 Kesimpulan

Ada beberapa kesimpulan yang dapat dipaparkan setelah menjalani serangkaian test dan uji coba pada teknik One Time Pad. Beberapa kesimpulan yang diperoleh adalah antara lain:

1. Teknik One Time Pad bekerja dengan menggunakan proses XNOR pada deretan bit pada plaintext dan ciphertext dalam melakukan proses enkripsi dan dekripsi.
2. Panjang kunci yang dapat digunakan adalah sepanjang plaintext yang ada
3. Proses dekripsi teknik One Time Pad bekerja dengan baik sehingga dapat menghasilkan kembali plaintext seperti sebelum dilakukan enkripsi.

5.2 Saran

Saran harus tetap diajukan dengan tujuan mengembangkan penelitian dan program aplikasi yang telah penulis lakukan. Ada beberapa saran yang dapat penulis paparkan untuk meningkatkan kualitas penelitian ini. Beberapa saran tersebut adalah antara lain:

1. Proses enkripsi dan dekripsi dapat memberikan pilihan XOR atau XNOR.
2. Teknik One Time Pad lebih baik jika menggunakan skema Three-pass Protocol untuk menghindari pertukan Kunci.
3. Program aplikasi hendaknya digunakan secara online dan mobile.

DAFTAR PUSTAKA

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

Barone, L., Williams, J., & Micklos, D. (2017). Unmet needs for analyzing biological big data: A survey of 704 NSF principal investigators. *PLOS Computational Biology*, *13*(10), e1005755. https://doi.org/10.1371/journal.pcbi.1005755

Cokro, A. (2016). *Belajar Kriptografi dan Steganografi*. Kumpulan Tutorial.

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

Kurniawan, T. A. (2018). Pemodelan Use Case (UML): Evaluasi Terhadap beberapa Kesalahan dalam Praktik. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *5*(1), 77. https://doi.org/10.25126/jtiik.201851610

Ladjamudin, A.-B. bin. (2017). *Analisis dan Desain Sistem Informasi*. Graha Ilmu.

Lee, C. (2014). *Buku Pintar Pemrograman Visual Basic 2010*. Elex Media Komputindo.

Nakatsu, R. T. (2019). *Reasoning with Diagrams : Decision-Making and Problem-Solving with Diagrams*. John Wiley & Sons.

Rahmel, D. (2018). *Visual Basic.NET*. McGraw-Hill.

Rao, R. V., & Selvamani, K. (2015). Data Security Challenges and Its Solutions in Cloud Computing. *Procedia Computer Science*, *48*, 204–209. https://doi.org/10.1016/j.procs.2015.04.171

S., G., L. Ribeiro, A. R., & David, E. (2012). Asymmetric Encryption in Wireless Sensor Networks. In *Wireless Sensor Networks - Technology and Protocols*. InTech. https://doi.org/10.5772/48464

Siahaan, A. P. U. (2016). Rail Fence Cryptography in Securing Information. *International Journal of Scientific & Engineering Research*, *7*(7), 535–538.

Sukmawati, R., & Priyadi, Y. (2019). Perancangan Proses Bisnis Menggunakan UML Berdasarkan Fit/Gap Analysis Pada Modul Inventory Odoo. *INTENSIF: Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem*

Informasi, *3*(2), 104. https://doi.org/10.29407/intensif.v3i2.12697

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

Technopedia. (2019). *Unified Modeling Language (UML)*. Technopedia. https://www.techopedia.com/definition/3243/unified-modeling-language-uml

Uml-diagrams.org. (2019). *Use case diagrams are UML diagrams describing units of useful functionality (use cases) performed by a system in collaboration with external users (actors).* https://www.uml- diagrams.org/use-case-diagrams.html

UTM. (2019). *Concept: Use-Case Model*. Univesidad Technologica de La Mixteca. http://www.utm.mx/~caff/doc/OpenUPWeb/openup/guidances/concepts/use_case_model_CD178AF9.html

Wasserkrug, S., Dalvi, N., Munson, E. V., Gogolla, M., Sirangelo, C., Fischer-Hübner, S., Ives, Z., Velegrakis, Y., Bevan, N., Jensen, C. S., & Snodgrass, R. T. (2019). Unified Modeling Language. In *Encyclopedia of Database Systems* (pp. 3232–3239). Springer US. https://doi.org/10.1007/978-0-387-39940-9_440

Zhang, D., Tsotras, V. J., Levialdi, S., Grinstein, G., Berry, D. A., Gouet-Brunet, V., Kosch, H., Döller, M., Döller, M., Kosch, H., Maier, P., Bhattacharya, A., Ljosa, V., Nack, F., Bartolini, I., Gouet-Brunet, V., Mei, T., Rui, Y., Crucianu, M., … Pitoura, E. (2009). Indexed Sequential Access Method. In *Encyclopedia of Database Systems* (pp. 1435–1438). Springer US. https://doi.org/10.1007/978-0-387-39940-9_738

Badawi, A. (2018). Evaluasi Pengaruh Modifikasi Three Pass Protocol Terhadap Transmisi Kunci Enkripsi.

Batubara, Supina. "Analisis perbandingan metode fuzzy mamdani dan fuzzy sugeno untuk penentuan kualitas cor beton instan." IT Journal Research and Development 2.1 (2017): 1-11.

Bahri, S. (2018). Metodologi Penelitian Bisnis Lengkap Dengan Teknik Pengolahan Data SPSS. Penerbit Andi (Anggota Ikapi). Percetakan Andi Ofsset. Yogyakarta.

Erika, Winda, Heni Rachmawati, and Ibnu Surya. "Enkripsi Teks Surat Elektronik (E-Mail) Berbasis Algoritma Rivest Shamir Adleman (RSA)." Jurnal Aksara Komputer Terapan 1.2 (2012).

Fitriani, W., Rahim, R., Oktaviana, B., & Siahaan, A. P. U. (2017). Vernam Encypted Text in End of File Hiding Steganography Technique. Int. J. Recent Trends Eng. Res, 3(7), 214-219.

Hardinata, R. S. (2019). Audit Tata Kelola Teknologi Informasi menggunakan Cobit 5 (Studi Kasus: Universitas Pembangunan Panca Budi Medan). Jurnal Teknik dan Informatika, 6(1), 42-45.

Hariyanto, E., Lubis, S. A., & Sitorus, Z. (2017). Perancangan prototipe helm pengukur kualitas udara. KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer), 1(1).

Hariyanto, E., & Rahim, R. (2016). Arnold's cat map algorithm in digital image encryption. International Journal of Science and Research (IJSR), 5(10), 1363-1365.

Harumy, T. H. F., & Sulistianingsih, I. (2016). Sistem penunjang keputusan penentuan jabatan manager menggunakan metode mfep pada cv. Sapo durin. In Seminar Nasional Teknologi Informasi dan Multimedia (pp. 6-7).

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.

Marlina, L., Muslim, M., Siahaan, A. U., & Utama, P. (2016). Data Mining Classification Comparison (Naïve Bayes and C4. 5 Algorithms). Int. J. Eng. Trends Technol, 38(7), 380-383.

Muttaqin, Muhammad. "ANALISA PEMANFAATAN SISTEM INFORMASI E-OFFICE PADA UNIVERSITAS PEMBANGUNAN PANCA BUDI MEDAN DENGAN MENGGUNAKAN METODE UTAUT." Jurnal Teknik dan Informatika 5.1 (2018): 40-43.

Ramadhan, Z., Zarlis, M., Efendi, S., & Siahaan, A. P. U. (2018). Perbandingan Algoritma Prim dengan Algoritma Floyd-Warshall dalam Menentukan Rute Terpendek (Shortest Path Problem). JURIKOM (Jurnal Riset Komputer), 5(2), 135-139.

Rahim, R., Aryza, S., Wibowo, P., Harahap, A. K. Z., Suleman, A. R., Sihombing, E. E., ... & Agustina, I. (2018). Prototype file transfer protocol application for LAN and Wi-Fi communication. Int. J. Eng. Technol., 7(2.13), 345-347.

Wahyuni, Sri. "Implementasi Rapidminer Dalam Menganalisa Data Mahasiswa Drop Out." Jurnal Abdi Ilmu 10.2 (2018): 1899-1902.