PERANCANGAN APLIKASI ENKRIPSI MENGGUNAKAN ALGORITMA VIGENERE CIPHER BERBASIS WEB

Oleh :

ROHANI

16.051.00.048

PROGRAM STUDI MANAJEMEN INFORMATIKA

AMIK LABUHANBATU

2019

PERANCANGAN APLIKASI ENKRIPSI MENGGUNAKAN ALGORITMA VIGENERE CIPHER BERBASIS WEB

DiajukanUntukMemenuhi Salah SatuSyaratMeraih

GelarAhliMadya

Oleh :

ROHANI

16.051.00.048

PROGRAM STUDI MANAJEMEN INFORMATIKA

AMIK LABUHANBATU

2019

KATA PENGANTAR

Puji syukur kita ucapkan kehadirat Allah SWT, yang telah melimpahkan Rahmat, Taufiq dan Hidayah-Nya kepada penulis, sehingga penulis dapat menyelesaikan Tugas Akhir dengan tepat pada waktunya.

Tugas Akhir ini berjudul "**PERANCANGAN APLIKASI ENKRIPSI MENGGUNAKAN ALGORITMA VIGENERE CIPHER BERBASIS WEB".** Adapun tujuan penulisan Tugas Akhir ini adalah untuk melengkapi salah satu syarat untuk memperoleh gelar Ahli Madya (Diploma III) dari Akademik Manajemen Informartika dan Komputer (AMIK) Labuhanbatu. Penulis menyadari bahwa laporan ini masih jauh dari sempurna, baik dari isi maupun penulisannya.

Dalam penyelesaian Tugas Akhir ini, penulis banyak mengalami kesulitan. Namum berkat bantuan dari berbagai pihak kesulitan-kesulitan dapat diatasi. Untuk itulah penulis pada kesempatan ini mngucapkan terima kasih yang sedalam-dalamnya kepada orang tua saya yang telah mendukung sepenuhnya dan mendoakan penulis baik dari segi moral dan material. Dan penulis mengucapkan terima kasih kepada :

1. Bapak Dr.H.Amarullah Nasution, SE, MBA, Selaku Ketua Yayasan Universitas Labuhanbatu.
2. Bapak Ade Parlaungan Nasution, SE, MSi, Selaku Rektor Universitas Labuhanbatu.
3. Ibu Novilda Elizabeth Mustamu, S.Pt, M.Si, Selaku Dekan Fakultas Sains dan Teknologi.

4. IbuMarnis Nasution, S.Kom, M.Kom, Selaku Ka. Program Studi AMIK Labuhanbatu dan Selaku Pembimbing II AMIK Labuhanbatu.
5. Bapak Iwan Purnama, S.Kom, M.Kom, Selaku Pembimbing I AMIK Labuhanbatu.
6. Bapak/Ibu Dosen AMIK Labuhanbatu yang memberikan ilmu pengetahuan komputer baik dalam perkuliahan dan tugas akhir.
7. Seluruh Staff/Pegawai yang telah memberikan masukan, saran dan kerja samanya dalam penyusunan Praktik Kerja Lapangan.
8. Rekan seperjuangan yang telah memberi motivasi dan dukungan yang besar bagi penulis dan banyak terima kasih kepada teman-teman khususnya mahasiswa AMIK Labuhanbatu yang memberikan motivasi dan saling bekerja sama.

Penulis menyadari bahwa Tugas Akhir ini masih jauh dari kesempurnaan, maka dari itu penulis mengharapkan kritik dan saran serta masukan untuk kesempurnaan Tugas Akhir ini, Semoga Tugas Akhir ini bermanfaat bagi kita semua, khususnya bagi para penulis dan para pembaca.

Rantauprapat, 26 Mei 2019

Penulis

ROHANI
Npm : 1605100048

LEMBAR PERSETUJUAN

PERANCANGAN SISTEM INFORMASI PENJUALAN HANDPHONE AND ACCESSORIES PADA TOKO NISA PONSEL BERBASIS WEB

Diajukan Untuk Memenuhi Salah Satu Syarat Meraih

Gelar Ahli Madya

Oleh :

PUTRI AINI

16.051.00.042

Disetujui Oleh :

Dosen Pembimbing I	Dosen Pembimbing II
IWAN PURNAMA,S.KOM.,M.KOM	**DECI IRMAYANI,S.KOM,M.KOM**
NIDN : 0112029202	**NIDN : 0127058602**

Rantauprapat, 26 Mei 2019

Diketahui dan disahkan oleh :

Direktur	Ketua Program Studi
DECI IRMAYANI,S.KOM,M.KOM	**MARNIS_NASUTION,S.KOM.,M.KOM**
NIDN : 0127058602	**NIDN : 0130039001**

SURAT PERNYATAAN
Perihal :PenulisanTugasAkhir

Saya yang membuatpernyataaniniadalahmahasiswa AMIK Labuhanbatudenganidentitasmahasiswasebagaiberikut :

Nama : Rohani

NIM : 16-051-00-048

JenjangPendidikan : Diploma 3

Program Studi : ManajemenInformatikaKomputer

SayatelahmelaksanakanpenelitiandanpenulisanTugasAkhirdenganjudulpenelitiansebagaiberikut :

JudulTugasAkhir :PerancanganAplikasiEnkripsiMenggunakan Vigenere Cipher Berbasis Web

SehubungdenganTugasAkhirinisayamenyatakandengansebenar-benarnyabahwa**LaporanTugasAkhirinimerupakanhasilkaryasayasendiri (tidakmenyuruh orang lain yang mengerjakannya) dantidakmelakukanplagiat.**
Biladikemudianhariternyataterbuktibahwasayamelanggarpernyataanini, makasayabersediadikenakansanksi yang telahditetapkanoleh Program Studi AMIK Labuhanbatuyakni**PencabutanIjazah yang telahsayaterimadanIjazahtersebutdinyatakantidaksah.**

DemikianSuratPernyataaninisayabuatdengansungguh-sungguh, dalamkeadaansadar, dantanpaadatekanandaripihakmanapun.

Rantauprapat, 26 Mei 2019

Saya yang membuatpernyataan,

ROHANI

LEMBAR PERSEMBAHAN

Alhamdulillah saya ucapkan kepada Allah SWT, atas segala rahmat dan juga kesempatan dalam menyelesaikan Tugas Akhir ini dengan segala kekurangannya. Segala syukur saya ucapkan kepada-Mu Ya Rabb karena sudah menghadirkan orang-orang yang sangat berartu disekeliling saya, yang selalu memberikan doa dan semangat sehingga Tugas Akhir ini dapat diselesaikan dengan baik.

Dengan ketulusan hati Tugas Akhir ini saya persembahkan kepada :

Kedua orangtua…

Kedua orangtua saya Bapak WALDI dan Ibu SITI ASIAH NASUTION, apa yang saya dapatkan hari ini belum mampu membayar semua kebaikan, keringat, dan juga air mata bagi saya. Terimakasih atas segala dukungan dari bapak dan ibu saya dalam bentuk materi maupun moril. Tugas Akhir ini saya persembahkan untuk kedua orangtua saya sebagai wujud terimakasih atas pengorbanan dan jerih payah kedua orang tua saya sehingga saya dapat menyelesaikan tugas akhir ini.

Semoga tugas akhir ini adalah awal untuk lebih membahagiaan Bapak dan Ibu saya serta dapat tercapai cita-cita yang diimpikan.

Terimakasih Bapak.. Terimakasih Ibu…

Kembaranku…

Untuk kakakku serta kembaranku ROHANA, tiada waktu yang paling berharga dalam hidup selain menghabiskan waktu dengan dirimu. Walaupun sering bertengkar dan beradu argument, tapi hal itu selalu menjadi warna yang tidak akan bisa tergantikan. Terimakasih untuk bantuan dan semangat darimu, semoga tugas akhir ini menjadikan kesuksesan saya untuk lebih dapat membanggakan dirimu. Untuk kakakku semoga lancar untuk menyusun skripsi dan mencapai apa yang telah dicita-citakan.

Pembimbing dan Dosen…

Kepada Bapak Ronal Watrianthos, S.Kom., M.Kom dan Ibu Marnis Nasution., S.Kom, M.Kom selaku dosen pembimbing saya yang paling baik dan bijaksana, terima kasih karena sudah membimbing saya untuk menyelesaikan tugas akhir ini, tak lupa buat Bapak Direktur Sudi Suryadi, S.Kom, M.Kom dan Bapak Ka. Prodi Ibnu Rasyid Munthe, S.T., M.Komyang sudah membimbing saya dan memberikan motivasi serta semangat sehingga tugas akhir ini terselesaikan.

Terima kasih juga untuk dosen-dosen di AMIK Labuhanbatu yang telah menjadikan orang tua kedua saya yang namanya tak bisa saya sebut satu persatu yang selalu memberikan motivasi, selalu peduli dan perhatian, ucapan terima kasih yang tak terhingga atas ilmu yang bermanfaat telah bapak dan ibu dosen berikan sangatlah berharga untuk saya.

Sahabat dan seluruh teman di kampus tercinta…

Untuk sahabat-sahabat istimewa saya yaitu Yoanda Putri Siregar, Ade Rizki Agustina Siregar, Renny Syahfitri, Difadila Malindo Koto, Ade Sunti Rahmawardhani, dan Fajar Rahmadi, terima kasih telah memberika dukungan, hiburan dan motivasi kepada saya, kalian terhebat.

Tanpa kalian mungkin masa-masa kuliah saya akan menjadi biasa-biasa saja, maaf jika banyak salah selama ini yang membuat kalian sakit hati. Untuk Putri Aini dan Elprida Eleonora Tamba, teman-teman seperjuangan yang sudah menyemangati dan membantu saya selama ini. Terima kasih telah bersama saya selama kuliah dan mungkin terima kasih dan maaf saya belum bisa membalas semua bantuan kalian selama ini. Kalian terbaik.

Diriku

Untuk diriku, terimakasih sudah berjuang semampumu, untuk diriku terimakasih untuk selalu bersemangat mengerjakan sesuatu yang menurut mu benar, untuk diriku terimakasih untuk terus berfikir kalau dirimu berharga, untuk diriku terimakasih untuk

selalu tersenyum bahagia, untuk diriku terimakasih untuk tidak gampang putus asa dan untuk tidak mudah menyerah, untuk diriku terimakasih untuk terus menyukai dirimu sendiri, untuk diriku terimakasih bangkit ketika kau terjatuh, untuk diriku terimakasih untuk segalanya.

UNTUK DIRIKU YANG PALING HEBAT DAN LUAR BIASA❤.

DAFTAR ISI

DAFTAR RIWAYAT HIDUP

Saya yang bertandatangandibawahini :

Nama	: Rohani
Tempattanggallahir	: Rantauprapat, 26 Juni 1997
Jeniskelamin	: Perempuan
Agama	: Islam
Pendidikanterakhir	: Diploma III / ManajemenInformatika
Status	: BelumMenikah
Alamat	: Jl. PerisaiGg. AnggrekMerah
Kewarganegaraan	: Indonesia
No. HP	: 0852-2084-5250

PENDIDIKAN FORMAL

1. SD 116874 BakaranBatu Berijazah
2. SMP N 1 Rantau Selatan Berijazah
3. SMA N 1 Rantau Selatan Berijazah
4. AMIK Labuhanbatu Berijazah

Demikiandaftarriwayathiduinisayaperbuatdengansebenarnya.

Rantauprapat, 26 Mei 2019

Saya yang membuat

ROHANI

DAFTAR LAMPIRAN

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

ABSTRAK

Keamanandanprivasisangatdibutuhkansaatmelakukanpertukaraninformasi pentingpada era teknologiinformasidankomunikasisaatini. Salah satucara yang bisadigunakanuntukmenjadikansuatuinformasipentingtidakdapatdipahamioleh orang yang tidakberhakadalahmengenkripsikaninformasitersebutsehinggainformasisulitdanb ahkantidakdapatdipahamioleh orang lain. Enkripsipadakriptografidigunakanuntukmerubahinformasipentingmenjadisandi-sandi, untukmengenkripsikandibutuhkankalimat yang ingindienkripsikandanmemelurkansebuahkunci.

Salah satucarauntukmengenkripsikaninformasipentingdenganmenggunakanmetodealgor itmavigenere cipher, carauntukmenghasilkanenkripsiyaitudenganmengolahteksaslihurufmenjadiangkay ang menggunakanoperasimatematika. Kunci yang digunakanalgortimavigenere cipher yaituberbentukhuruf, kunci yang berbentukderetanhuruftersebutakanmemungkinkansetiapteksasliuntukdienkripsi. Hasildarienkripsimenggunakanmetodevigenere cipher yaitudapatmenyandikaninformasipentingdengancaramengenkripsikan data tersebutmenjadisandi-sandi yang tidakdapatdibacaoleh orang yang tidakberhakdanaplikasiinijugadapatmengembalikan data yang telahdienkripsikanmenjadi data yang dapatdibacadengancaramendekripsikan data yang telahdienkripsi.

Kata Kunci: Enkripsi, AlgoritmaVigenere Cipher, Php.

ABSTRACT

Security and privacy is needed when exchanging important information in the era of information and communication technology today. One way that can be used to make an important information can not be understood by unauthorized people is encrypt information so that the information is difficult and can not even be understood by others. Encryption cryptography is used to convert key information into ciphers to encrypt the required sentence want encrypted and memelurkan key.

One way to encrypt important information by using the method vigenere cipher algorithm, encryption is a way to produce by processing the original text letters into numbers using mathematical operations. The key used vigenere cipher algorithm that is shaped, in the form of a row of letter keys that will allow each original text to be encrypted. Results of encryption using methods vigenere cipher that can encrypt important information by means of encrypting the data into a code that can not be read by unauthorized people and this application can also restore data that has been encrypted into data that can be read by means of decrypting data has been encrypted.

Keywords: Encryption Algorithm Vigenere Cipher, Php.

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan dan privasi sangat dibutuhkan saat melakukan pertukaran informasi penting pada era teknologi informasi dan komunikasi saat ini.Pada seiring perkembangan teknologi yang semakin pesat maka semakin besar pula penyadapan informasi penting yang bersifat privasi dengan melalui berbagai macam perantara media sosial.Tingkat keamanan dan privasi juga semakin diperlukan untuk menghindari penyadapan informasi yang mungkin bisa kapan pun terjadi, terutama pada era sekarang. Salah satu cara yang bisa digunakan untuk menjadikan suatu informasi yang bersifat privasi dapat tidak diketahui oleh orang yang tidak berhak adalah menyandikan (mengenkripsikan) informasi tersebut sehingga informasi sulit dan bahkan tidak dapat dipahami oleh orang lain.

Kriptografi secara umum adalah ilmu dan seni untuk menjaga kerahasiaan pesan[1]. Kriptografi dapat menyandikan (mengenkripsikan) informasi yang bersifat privasi menjadi informasi yang tidak dapat dipahami oleh orang yang tidak berhak.Enkripsi pada kriptografi digunakan untuk merubah informasi menjadi sandi-sandi dengan menggunakan kunci (*key).*Dekripsi pada kriptografi digunakan untuk membuka sandi-sandi yang telah di enkripsikan sebelumnya dengan menggunakan kunci (*key)* yang sama[2]. Salah satu cara untuk

menyandikan (mengenkripsikan) suatu informasi menjadi sandi-sandi yaitu dengan menggunakan algoritma kriptografi vigenere cipher.

Vigenere cipher adalah salah satu metode kriptografi yang digunakan untuk menyandi (mengenkripsi) informasi[1]. Sandi vigenere merupakan pengembangan dari sandi Caesar. Pada sandi ceasar setiap huruf pada teks diganti dengan huruf teks lain yang mempunyai perbedaan urutan huruf alfabet. Sandi vigenere terdiri dari beberapa sandi ceasar dengan nilai pergeseran huruf alfabet yang berbeda.Metode sandi vigenere menggunakan tabel pemetaan vigenere(bujur sangkar vigenere) untuk menyatakan huruf-huruf alfabet.

Berdasarkan uraian latar belakang diatas bahwa penyandian informasi dapat digunakan untuk pembelajaran dan pengujian enkripsi dan dekripsi kriptografi dengan menggunakan metode algoritma vigenere chiper berbasis web, maka dibuat tugas akhir dengan judul "**PERANCANGAN APLIKASI ENKRIPSI MENGGUNAKAN ALGORITMA VIGENERE CIPHER BERBASIS WEB**"

1.2 Perumusan Masalah

Berdasarkan latar belakang masalah tersebut dapat dibuat suatu rumusan masalah, yaitu:

1. Bagaimana mengimplementasikan vigenere chiper untuk mengamankan informasi penting?
2. Bagaimana cara mengenkripsikan dan mengdekripsikan informasi penting dengan metode algoritma vigenere cipher ?

3. Bagaimana membangun aplikasi enkripsi dan dekripsi menggunakan metode algoritma vigenere cipher berbasis web.

1.3 Batasan Masalah

Batasan masalah yang ada dari aplikasi yang saat ini dibahas dalam pembuatan tugas akhir ini adalah sebagai berikut:

1. Metode yang digunakan untuk mengenkripsikan adalah vigenere chiper.
2. Bahasa pemograman yang digunakan yaitu PHP.
3. Membahas tentang enkripsi dan dekripsi suatu informasi menggunakan metode algoritma vigenere cipher.

1.4 Tujuan Penelitian

Tujuan dari penulisan tugas akhir ini sebagai berikut:

1. Mengetahui cara enkripsi dan dekripsi pada aplikasi vigenere chiper.
2. Untuk membuat aplikasi penyandian atau enkripsi informasi yang bersifat rahasia.
3. Mengetahui hasil dari enkripsi dan dekripsi pada aplikasi enkripsi menggunakan algoritma vigenere cipher berbasis web.

1.5 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam tugas akhir ini terbagi dalam beberapa pokok bahasan, yaitu:

BAB I PENDAHULUAN

Bab ini menguraikan tentang latar belakang masalah, perumusan masalah, batasan masalah, tujuan penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORITIS

Untuk bab ini berisi penulis memberi uraian tentang konsep dasar pembuatan aplikasi enkripsi menggunakan vigenere cipher berbasis web.

BAB III METODOLOGI PENELITIAN

Pada bab ini yang dibahas mengenai metodologi penelitian analisa sistem dan perancangan sistem menggunakan jalur sistem, *UML (Unified modelling language),* dan *Desain Input-output.*

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

Pada bagian bab ini membahas tentang implemetasi dari aplikasi yang dibuat secara keseluruhan dan membuat pengujian terhadap aplikasi yang dibuat untuk mengetahui apakah aplikasi tersebut

bisa menyelesaikan permasalahan yang dihadapi sama seperti yang diinginkan.

BAB V PENUTUP

Pada bab ini berisi tentang kesimpulan dan saran yang didapatkan selama proses perancangan dari aplikasi serta rencana pengembangan aplikasi di masa akan datang.

BAB II

LANDASAN TEORITIS

2.1 Kriptografi

Kriptografi (*cryptography)* berasal dari bahasa Yunani yaitu "*cryptos"* artinya "*secret"* (rahasia), sedangkan "*graphein"* artinya "*writing"* (tulisan). Jadi, kriptografi berarti "*secret writing"* (tulisan rahasia).Ada beberapa defenisi kriptografi yang telah dikemukakan di dalam berbagai literatur. Defenisi yang dipakai di dalam buku-buku yang menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan atau informasi dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Defenisi ini mungkin cocok pada masa lalu di mana kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi dikalangan militer, diplomat, dan mata-mata[3].

Dalam kriptografi sering menemukan berbagai istilah atau terminology. Beberapa istilah kriptograpi yaitu[3] :

1. *Plaintext, chipertext, key,* algoritma

Plaintext adalah pesan yang dapat dibaca.*Ciphertext* adalah pesan sandi atau pesan acak yang tidak dapat dibaca.*Key* yaitu untuk melakukan teknik kriptografi. Algoritmaadalah metode untuk melakukan enkripsi dan deskripsi[2].

2. Enkripsi dan deksirpsi

Enkripsi adalah proses penyandian *plaintext* menjadi *ciphertext.* Sedangkan dekripsi adalah proses mengembalikan *ciphertext* menjadi *plaintext* semula[3].

3. Proses dasar kriptografi

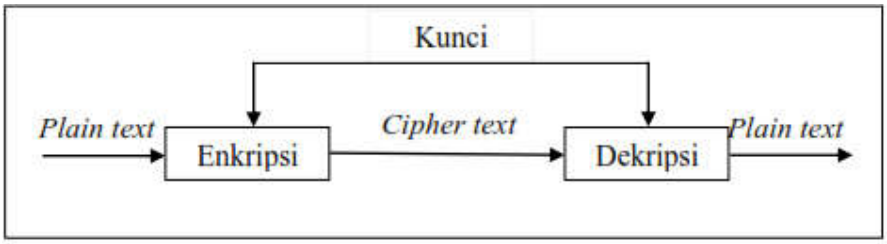
Proses-proses dasar kriptografi dibagi menjadi dua bagian, yaitu enkripsi (*encryption)* dan dekripsi (*decryption).* Ada contoh teknik kriptografi klasik, yaitu:

a. Subtitusi, yaitu teknik ini mengganti satu atau sekumpulan bit pada blok plainteks tanpa mengubah urutannya.
b. Transposisi, yaitu teknik ini memindahkan posisi bit pada blok plainteks berdasarkan aturan tertentu[1].

2.1.1 Algoritmakriptografi

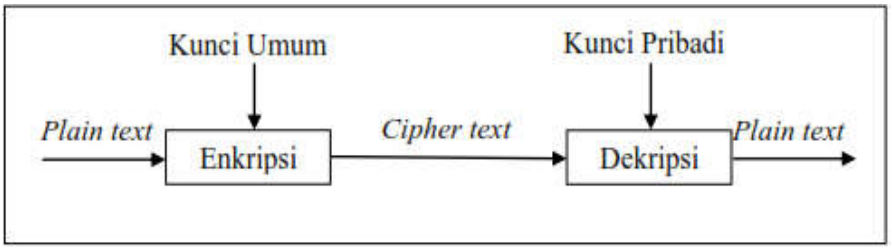
Algoritma dalam kriptografi dibagi menjadi dua, yaitu :

1. Algoritmasimentris atau sering disebut algoritmakriptografi konvensional adalah algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan proses dekripsi. Algoritma kriptografi simentris dibagi menjadi dua kategori yaitu algoritma aliran (*stream cipher)* dan algoritma blok (*block cipher).*



Gambar 2.1.1 Proses Enkripsi dan Dekripsi Algoritma Simetris[1].

2. Algoritma asimentris adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi. Dimana kunci enkripsi dapat disebarkan kepada umum dan dinamakan kunci publik (*public key),* sedangkan kunci dekripsi disimpan untuk digunakan sendiri dan dinamakan kunci pribadi (*private key).* Oleh karena itu, kriptografi ini dikenal dengan nama kriptografi kunci publik (*public key cryptography).* Kriptografi asimentris, dimana setiap pelaku publik informasi akan memiliki sepasang kunci, yaitu kunci publik dan kunci pribadi dimana kunci publik di distribusikan kepada umum sedangkan kunci pribadi disimpan untuk diri sendiri.



Gambar 2.1.1 Proses Enkripsi Dan Dekripsi Algoritma Asimetris[1].

2.1.2 Aspek-aspek keamanan

Kriptografi tidak hanya memberikan kerahasiaan dalam telekomunikasi, namun juga memberikan komponen-komponen berikut ini:

a. *Authentication (*otentikasi), penerima pesan dapat memastikan keaslian pengirimnya.
b. *Integrity* (integritas), penerima harus dapat memeriksa apakah pesan telah dimodifikasi. Seorang penyusup seharusnya tidak dapat memasukkan tambahan ke dalam pesan, mengurangi atau mengubah pesan.
c. *Non-repudiation* (nir penyangkalan), pengirim seharusnya tidak dapat mengelak bahwa dialah pengirim pesan yang sesungguhnya, tanpa kriptografi, seseorang dapat mengelak bahwa dialah pengirim pesan yang sesungguhnya[4].

2.1.3 Vigenere Cipher

Vigenere cipher adalah salah satu algoritma kriptografi klasik yang diperkenalkan pada abad 16 atau kira-kira pada tahun 1986. Algoritma kriptografi ini dipublikasikan oleh seorang diplomat dan juga kriptologis yang berasal dari Prancis, yaitu *Blaise de Vigenere*, namun sebenarnya buku *La Cifra del Sig. Giovan Batista Belaso*, sebuah buku yang ditulis oleh *Giovan Batista Belaso* pada tahun 1553.

Cara kerja dari vigenere cipher ini mirip dengan caesar cipher, yaitu mengenkripsikan plainteks pada pesan dengan cara menggeser huruf pada pesan

tersebut sejauh nilai kunci pada deret *alphabet.* Vigenere cipher adalah salah satu algoritma klasik yang menggunakan metode subsitusi abjad-majemuk. Subsitusi abjad-majemuk mengenkripsikan setiap huruf abjad-tunggal yang semua huruf di suatu pesan dienkripsi menggunakan kunci yang sama[2].

Sandi caesar merupakan sistem persandian klasik berbasis subtitusi yang sederhana. Enkrpsi dan dekripsi pada sistem persandian caesar menggunakan operasi *shift.* Operasi *shift* adalah mensubtituasikan suatu huruf menjadi huruf pada daftar alfabet berada di-*k (key)* = 3 (ganti dengan huruf ke-3 sebelah kanan) maka “A” menjadi “D”, “B” menjadi “E” dan seterusnya. Bagaimana dengan “X”, “Y” dan “Z”. Supaya semuanya memiliki subtitusi, huruf “A” dianggap disebelah kanan huruf “Z” sehingga “X” menjadi “A”, “Y” menjadi “B” dan “Z” menjadi “C”.

Untuk dapat mengolah teks asli yang merupakan deretan simbol huruf diperlukan pemetaan dari huruf menjadi angka dapat diapilikasi operasi matematika. Misalnya huruf “A” sampai “Z” dipetakan ke angka integer dari “0” sampai “25”. Perhatikan nilai yang mungkin bagi teks asli dan teks sandi adalah 0 sampai 25 dan apabila hasil pergeseran (penjumlahan) melebihi 26 angka tersebut dibagi 26 dan nilai yang dipakai adalah sisa bagi. Oleh karena itu sritmatika modular Z_{26} digunakan pada persandian caesar[5].

Sebagai contoh caesar cipher jika terjadi plaintks :

MAKALAH KRIPTOGRAFI

Maka jika dienkripsikan dengan nilai kunci 2 akan didapatkan cipherteks :

OCMCNCJ MTKRVQITCHK

Dari cipherteks yang didapat kita dapat lihat bahwa huruf M dienkripsikan menjadi O, huruf A dienkripsikan menjadi huruf C, dan seterusnya dimana huruf pada pesan digeser sejauh nilai kunci. Algoritma caesar cipher sangat sederhana sehingga sangat berisiko untuk dipecahkan karena hanya dibutuhkan pengetahuan satu huruf dari plainteks untuk mengetahui kunci yang digunakan. Vigenere cipher yang menerapkan metode subtitusi abjad-majemuk tidak memiliki permasalah tersebut karena tergantung dengan kunci yang diberikan. Kunci yang digunakan vigenere cipher berbeda dengan yang digunakan caesar cipher. Jika pada caesar kuncinya hanya satu nilai saja, maka pada vigenere cipher kunci yang digunakan berbentuk deretan huruf. Kunci yang berbentuk deretan kata tersebut akan memungkinkan setiap huruf plainteks untuk di enkripsikan dengan kunci yang berbeda. Jika panjang kunci yang digunakan lebih pendek dari panjang plainteks maka kunci akan diulang sampai panjang kunci sama dengan panjang plainteks. Algoritma ini akan meminimalkan kemungkinan dipecahkannya cipherteks jika satu huruf plainteks diketahui.

Model matematika dari enkripsi pada algoritma vigenere cipher ini adalah seperti berikut:

$C_i = E_k (M_i) = (M_i + K_i) \bmod 26$

Dan model matematika untuk dekripsinya adalah :

$M_i = D_k (C_i) = (C_i - K_i) \bmod 26$

Dengan C memodelkan cipherteks, M memodelkan plainteks, dan K memodelkan kunci.

Contoh dari penerapan algoritma vigenere cipher adalah jika kita memiliki sebuah plainteks yang ingin dienkripsikan :

MAKALAH KRIPTOGRAFI

Dan kita menggunakan kunci :

TUGAS

Maka plainteks akan dienkripsikan dengan cara :

Plainteks : MAKALAH KRIPTOGRAFI

Kunci : TUGASTU GASTUGASTUG

Cipherteks : FUQADTB QRAINUGJTZO

Huruf pada kunci akn dikonversi menjadi sebuah nilai, misalnya A = 0, B = 1, sampai Z = 25. Setelah itu prosesnya sama seperti pada caesar cipher dimana setiap huruf pada plainteks akan digeser sejauh nilai kunci yang posisinya berseuaian. Pergeseran huruf-huruf ini bisa dipetakan dalam bentuk 26x26 yang memetakan antara huruf pada plainteks dengan huruf pada kunci seperti yang di perlihatkan pada gambar dibawah ini :

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Gambar 2.1.3Tabel Pemetaan Vigenere Cipher.

Selain menggunakan algoritma vigenere cipher bujur sangkar vigenere atau tabel pemetaan vigenere cipher untuk melakukan algoritma ini dapat dilakukan dengan menjumlahkan plainteks dengan kunci kemudian di modulo 26[1].

2.2 Kode ASCII

ASCII *(American Standard Code for Information Interchange)* merupakan suatu standard internasional dalam kode huruf dan symbol seperti Hex dan

Unicode tetapi ASCII lebih bersifat universal, contohnya 124 adalah untuk karakter "|". Ia selalu digunakan oleh komputer dan alat komunikasi lain untuk menunjukkan teks. Kode ASCII sebenarnya memiliki komposisi bilangan biner sebanyak 8 bit.Dimulai dari 0000 0000 hingga 1111 1111. Total kombinasi yang dihasilkan sebanyak 256, dimulai dari kode 0 hingga 255 dalam sistem bilangan Desimal.

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

Gambar 2.2 Kode ASCII[6].

2.3 Defenisi Perancangan

Pada saat hendak membuat sebuah sistem yang akan digunakan oleh pengguna (*user*), setiap pengembangan aplikasi diharuskan membuat sebuah rancangan dari sistem yang ingin dibuat. Rancangan ini bertujuan untuk memberi gambaran umum dari sistem yang akan berjalan kepada setiap pengguna. Perancangan adalah sekumpulan aktivitas yang menggambarkan secara rinci

bagaimana sistem akan berjalan. Hal itu bertujuan unutk menghasilkan produk perangkat lunak yang sesuai dengan kebutuhan pengguna (*user*)[7].

2.4 Aplikasi

Pengertian aplikasi menurut para ahli adalah sebagai berikut:

a. Menurut Jogiyanto adalah pengguna dalam suatu komputer, intruksi (*instruction)* atau pernyataan *(statement)* yang disusun sedemikian rupa sehingga komputer dapat memproses *input* menjadi *output.*
b. Menurut Rachmad Hakim S, adalah perangkat lunak yang digunakan untuk tujuan tertentu, seperti mengolah dokumen, mengatur Windows, dan permainan *(game),* dan sebagainya.
c. Menurut Harip Santoso, adalah suatu kelompok *file (from, class, report)* yang bertujuan untuk melakukan aktivitas tertentu yang saling terkait, misalnya aplikasi *payroll,* aplikasi *fixed asset*[8].

2.5 Unified modelling language (UML)

Unified modelling language (UML) adalah salah satu standar bahasa yang banyak digunakan di dunia industri untuk mendefinisikan *requirement,* membuat analisa dan desain, serta menggambarkan arsitektur dalam pemrograman berorientasi objek. *UML* merupakan bahasa visual untuk pemodelan dan komunikasi mengenai sebuah sistem dengan menggunakan diagram dan teks-teks pendukung[9].

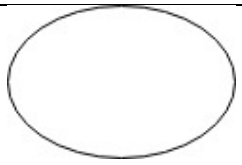
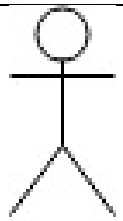
2.5.1 Use Case Diagram

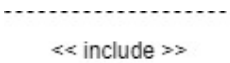
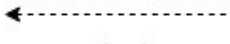
Use case diagram menggambarkan fungsionalitas yang diharapkan dari sebuah sistem. *Use case* merepresentasikan sebuah interaksi antara aktor dengan sistem. Seorang atau sebuah aktor adalah entitas atau mesin yang berinteraksi dengan sistem untuk melakukan pekerjaan-pekerjaan tertentu.*Use case* merupakan sebuah pekerjaan tertentu, misalnya *login* ke sistem, meng-*create* sebuah daftar belanja, dan sebagainya.

Use case diagram dapat digunakan untuk :

1. Menyusun *requirement* sebuah sistem.
2. Mengkomunikasikan rancangan dengan klien, dan
3. Merancang *test case* untuk semua *feature* yang ada pada sistem[10].

Tabel 2.5.1 *Use Case Diagram*[11].

Gambar	Keterangan
	*Use Case* menggambarkan fungsional yang disediakan sistem sebagai unit-unti yang bertukar oesan antar aktir, yang dinyatakan dengan menggunakan kata kerja.
	*Actor* atau aktor adalah *abstraction* dari orang atau sistem yang lain yang mengaktifkan fungsi dari target sistem. Untuk mengidentifikasikan aktir, ditentukan pembagian tenaga kerja dan tugas-tugas yang berkaitan dengan peran pada konteks target sistem. Orang tau sistem bisa muncul dalam beberapa peran. Perlu dicatat bahwa aktor berinteraksi dengan *use case,* tetapi tidak memiliki control terhadap *use case.*
	Asosiasi antara aktor dan *use case,* digambarkan dengan garis tanpa panah yang mengindikasikan siapa atau apa yang meminta interaksi secara langsung dan bukannya mengindikasikan data.

	Asosiasi antara aktor dan *use case* yang menggunakan panah terbuka untuk mengindikasikan bila aktor berinteraksi secara pasif dengan sistem.
	*Include,* merupakan di dalam *use case* lain *(required)* atau pemanggilan *use case* oleh *use case* lain, contohnya adalah pemanggilan sebuah fungsi program.
	*Extend*, merupakan perluasan dari *use case* lain jika kondisi atau syarat terpenuhi.

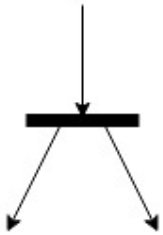
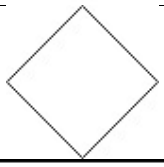
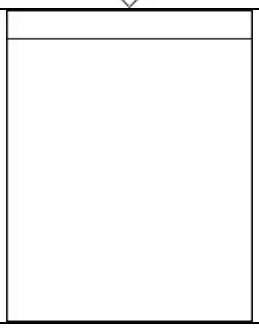
Sumber :A. Hendini, "Pemodelan UML sistem informasi Monitoring Penjualan dan stok barang," Pemodelan Uml Sist. Inf. Monit. Penjualan Dan Stok Barang (Studi Kasus Distro Zhezha Pontianak), vol. IV, no. 2, pp. 107–116, 2016.

2.5.2 Activity Diagram

Activity diagram merupakan sebuah teknik untuk mendeskripsikan logika procedural, proses bisnis dan aliran kerja dalam banyak kasus. *Activity diagram* digunakan untuk menganalisis *behaviour* dengan *use case* yang lebih kompleks dan menunjukkan interaksi-interaksi diantara mereka satu sama lain. *Activity diagram* biasanya digunakan untuk menggambarkan aktivitas bisnis yang lebih kompleks, dimana digambarkan hubungan antara satu *use case* dengan *use case* yang lainnya[12].

Tabel 2.5.2 *Activity Diagram*[11].

Gambar	Keterangan
	*Start Point,* diletakkan pada pojok kiri atas dan merupakan awal aktivitas.
	*End Point,* akhir aktivitas.

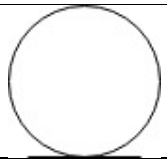
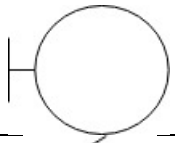
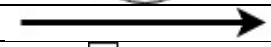
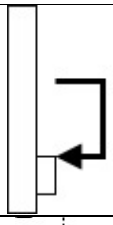
	*Activities,* menggambarkan suatu proses atau kegiatan bisnis.
	*Fork/*percabangan, digunakan untuk menunjukkan kegiatan yang dilakukan secara paralel atau untuk menggabungkan dua kegiatan paralel menjadi satu.
	*Join* (penggabungan) atau *rake,* digunakan untuk menunjukkan adanya dekomposisi.
	*Decision Point,* menggambarkan pilihan untuk pengambilan keputusan, *true* atau *false.*
	*Swimlane,* pembagian *activity diagram* untuk menunjukkan siapa melakukan apa.

Sumber :A. Hendini, "Pemodelan UML sistem informasi Monitoring Penjualan dan stok barang," Pemodelan Uml Sist. Inf. Monit. Penjualan Dan Stok Barang (Studi Kasus Distro Zhezha Pontianak), vol. IV, no. 2, pp. 107–116, 2016.

2.5.3 Sequence Diagram

Sequence Diagram menggambarkan kelakuan objek pada *use case* dengan mendeskripsikan waktu hidup objek dan pesan yang dikirimkan dan diterima oleh objek. Simbol-simbol yang digunakan dalam *Sequence Diagram* yaitu :

Tabel 2.5.3 Tabel *Sequence Diagram*[11].

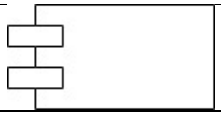
Gambar	Keterangan
	*Entity Class,* merupakan bagian dari sistem yang berisi sekumpulan kelas berupa entitas-entitas yang membentuk gambaran awal sistem dan menjadi landasan untuk menyusun basis data.
	*Boundary Class,* berisi kumpulan kelas yang menjadi *interface* atau interaksi antara satu atau lebih aktor dengan sistem, seperti tampilan *form entry* dan *form* cetak.
	*Control Class,* suatu objek yang berisi logika aplikasi yang tidak memiliki tanggung jawab kepada entitas. Contohnya adalah kalkulasi dan aturan bisnis yang melibatkan berbagai objek.
	*Message,* simbol mengirim pesan antar *class.*
	*Recursive,* menggambarkan pengiriman pesan yang dikirim untuk dirinya sendiri.
	*Activation,* mewakili sebuah eksekusi operasi dari objek, panjang kotak ini berbanding lurus dengan durasi aktivitas sebuah operasi.
	Lifeline, garis titik-titik yang berhubungan dengan objek sepanjang *lifeline* terdapat *activation.*

Sumber :A. Hendini, "Pemodelan UML sistem informasi Monitoring Penjualan dan stok barang," Pemodelan Uml Sist. Inf. Monit. Penjualan Dan Stok Barang (Studi Kasus Distro Zhezha Pontianak), vol. IV, no. 2, pp. 107–116, 2016.

2.5.4 Component Digram

Component diagram merupakan diagram yang memiliki tujuan khusus untuk difokuskan pada perangkat lunak dan komponen perangkat keras.Diagram komponen digunakan untuk menggambarkan komponen.Diagram komponen *(component diagram)* digunakan untuk memodelkan aspekfisik dari suatu sistem, komponen diagaram digunakan untuk memvisualkan organisasi dan hubungan antara komponen dalam satu sistem. Diagram ini juga digunakan untuk menjelaskan cara sistem dapat dieksekusi[13].

Tabel 2.5.4 *Component Diagram*[11].

Gambar	Keterangan
	Pada *deployment diagram,* komponen-komponen yang ada diletakkan didalam kode untuk memastikan keberadaan posisi mereka.
	Sebuah *association* digambarkan sebagi sebuah garis yang menghubungkan dua node yang mengindikasikan jalur komunikasi antara *element-elementhardware.*

Sumber :A. Hendini, "Pemodelan UML sistem informasi Monitoring Penjualan dan stok barang," Pemodelan Uml Sist. Inf. Monit. Penjualan Dan Stok Barang (Studi Kasus Distro Zhezha Pontianak), vol. IV, no. 2, pp. 107–116, 2016.

2.6 Internet

Internet adalah sebagai jaringan komputer yang sangat luas dan besar dan mendunia, menghubungkan pemakai komputer dari satu negara ke negara lain diseluruh dunia, dimana di dalamnya terdapat berbagai sumber informasi dan fasilitas-fasilitas layanan internet[14].

2.7 Website

Website adalah lokasi di internet yang menyajikan kumpulan informasi sehubungan dengan profil pemilik situs. Website adalah suatu halaman yang memuat situs-situs *web page* yang berada di internet yang berfungsi sebagai media penyampai informasi, komunikasi, atau transaksi[14]. Mengolah Multimedia Untuk Web) website adalah suatu media publikasi elektronik yang terdiri dari halaman- halaman web (web page) yang terhubung dari satu dengan yang lain dengan menggunakan link yang dilekatkan pada suatu teks atau image[15].

2.8 *Hypertext Markup Language*(HTML)

Hypertext Markup Language (HTML) adalah sebuah bahasa *markup* yang digunakan untuk membuat sebuah halaman web, menampilkan berbagai informasi di dalam sebuah penjelajahan web internet dan formatting *hypertext* sederhana yang ditulis kedalam berkas format ASCII agar dapat menghasilkan tampilan

wujud yang terintegrasi. Dengan kata lain, berkas yang dibuat dalam perangkat lunak pengolah kata dan disimpan kedalam format ASCII normal sehingga menjadi *home page* dengan perintah-perintah HTML. HTML adalah sebuah standar yang digunakan secara luas untuk menampilkan halaman web. HTML saat ini merupakan standar internet yang didefinisikan dan dikendalikan penggunanya oleh *World Wide Web Consortium* (W3C)[16].

2.9 PHP

PHP *Hypertext Preprocessor* atau sering disebut PHP merupakan bahasa pemrograman berbasis *server-side* yang dapat melakukan *parsing script php* menjadi *script web* sehingga dari sisi *client* menghasilkan suatu tampilan yang menarik. Kode PHP seringkali digabungkan dengan kode HTML. Untuk membedakannya dengan HTML, setiap kode PHP ditulis diberi tag pembuka yaitu "<?php" dan pada akhir kode PHP diberi tag penutupan yaitu "?>".

Keunggulan dari bahasa pemrograman PHP yaitu :

a. PHP memiliki native API *(Application Programming Interface)* untuk koneksi ke berbagai *database,* sehingga secara otomatis dalam melakukan koneksi lebih cepat dibandingkan dengan *Open Database Conectivity (ODBC).*
b. Dukungan koneksi yang hampir bisa dilakukan ke semua *database* seperti *MySQL, PostgreSQL, Sybase, Infomix, Interbase, ORACLE, SQL Server,* dan lain-lainnya.

c. PHP dapat dijalankan dibeberapa *web server* seperti *PWS, IIS, Apache, Xitami, Netscape Enterprise, AOL Server,* dan *Orelly website pro, CGI,* dan *ISAPI.*

d. PHP juga dapat berjalan di berbagai *platform* seperti *Unix* dan *Windows*[17].

2.10 XAMPP

XAMPP merupakan sebuah aplikasi perangkat lunak pemrograman dan *database* yang di dalamnya terdapat berbagai macam aplikasi pemrograman seperti :*Apache,* HTTP *server, MySQL, database,* bahasa pemrograman PHP dan *perl.*

Setiap huruf XAMPP memiliki arti sebagai berikut yaitu :

a. huruf X mengandung arti bahwa perangkat lunak pemrogram ini dapat dijalankan di banyak sistem operasi *Windows, Linux, Mac OS* dan *Solaris*.

b. Huruf A merupakan singkatan *Apache,* merupakan sebuah perangkat lunak aplikasi *web server.* Tugas utama *Apache* adalah menghasilkan halaman web yang benar kepada *user* berdasarkan kode PHP yang ditulis oleh pembuat halaman web.

c. Huruf P merupakan singkatan PHP, pada awalnya PHP merupakan singktan dari *Personal Home Page* yang pertama kali dibuat oleh Ramus Lerdoft pada tahun 1995. Pada tahun 1998, perusahaan tersebut merilis

interpreter baru untuk PHP dan meresmikan rilis tersebut sebagai PHP: *Hypertext Preprecessing.*

d. Huruf P yang terakhir merupakan singkatan dari *perl. Perl* merupakan kepanjangan *People Excel at Relational Labor,* untuk mengambarkan bahwa *perl* tidak terlepas dari keterlibatan dan komitmen komunitas pemrograman.

Gambar 2.10 XAMPP Logo[18].

2.11 Notepad ++

Notepad ++ adalah sebuah penyunting teks dan penyunting kode sumber yang berjalan di sistem operasi Windows.Notepad ++ menggunakan komponen *scintilla* untuk menampilkan dan mengedit teks maupun berkas kode sumber beragam bahasa.

Berikut adalah fungsi notepad ++:

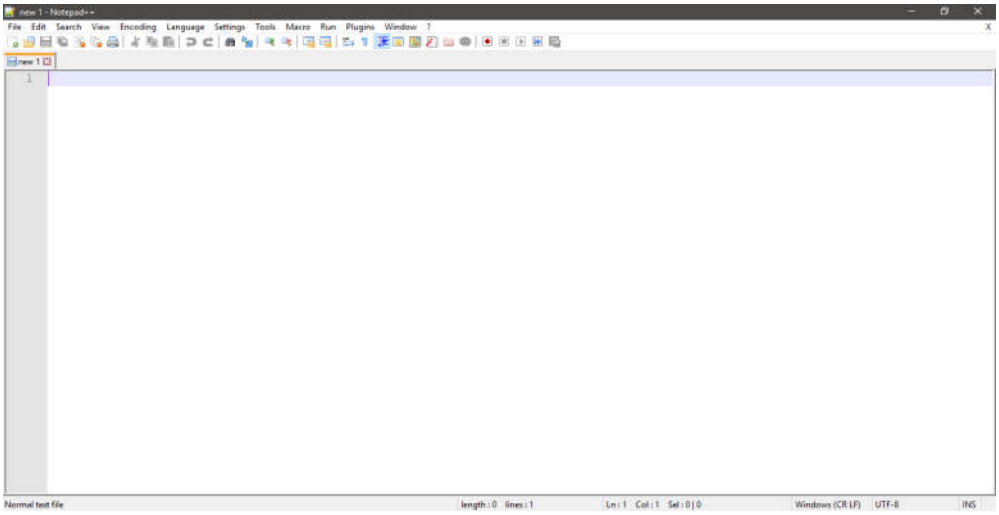
a. Notepad sebagai *digital library* :kita dapat menggunakan notepad *digital library* dan secara otomatis untuk memasukkan tanggal dan informasi waktu.

b. Notepad sebagai HTML *stripper.* Kita dapat mengedit komponen teks saja. Dengan menyalin dari kode HTML yang ada di halaman web dan paste ke notepad yang kemudian dapat disimpan untuk digunakan lagi lain waktu.

c. Notepad sebagai pembuat *script.* Kita dapat membuat *script* yang kompleks.

d. Notepad sebagai jalan pintas Windows Explorer. Ada *file* yang tidak bisa dihapus dengan notepad kita bisa mencoba menghapus *file* tersebut dengan cara*file* > *open* >pada *type file* pilih *all.*

e. Untuk membuat *file* berektensi, membuat atau mengedit *file* berenteksi reg. Reg adalah *file* yang digunakan untuk memasukkan pengaturan Windows melalui *registry* Windows[19].



Gambar 2.11 Notepad ++.

BAB III

METODOLOGI PENELITIAN

3.1 Metode Pengumpulan Data

Metode pengumpulan data salah satu cara yang dilakukan untuk mengumpulkan data yang diperlukan untuk menyusun tugas akhir, dalam penelitian ini data yang digunakan merupakan data sekunder. Penulis memperoleh data dari telaah pustaka dan artikel-artikel yang penulis dapat dari pustaka yang mendukung, informasi dari internet, dan jurnal-jurnal.

3.2 Metode Perancangan Sistem

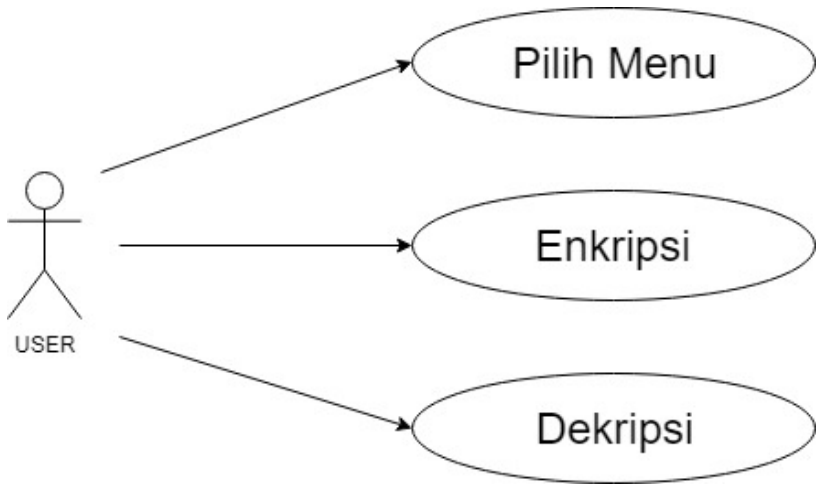
Metode perancangan sistem berisi rancangan yang digunakan dalam membangun sistem, diantaranya membangun rancangan *input,* rancangan proses, rancangan *output,* rancangan sistem dan rancangan *interface*.

Rancangan bertujuan untuk memberikan gambaran umum dari sistem yang akan berjalan kepada setiap pengguna. Perancangan adalah sekumpulan aktivitas yang menggambarkan secara rinci begaimana sistem akan berjalan. Hal itu bertujuan untuk menghasilkan produk perangkat lunak yang sesuai dengan kebutuhan pengguna *(user)*[6].Tahapan perancangan sistem merupakan tahap lanjutan dalam pengembangan sistem, yang dilakukan setelah selesai tahap analisa sistem. Tujuan dari tahapan ini untuk memberikan gambaran kepada *user* tentang bagaimana sistem baru yang diusulkan akan bekerja dan memberikan ilustrasi dan

penjelasan yang lengkap kepada *programmer* dalam mengimplementasikan rancangan sistem ke dalam sebuah program aplikasi atau bahasa pemrograman. *UML (Unified Modelling Language)* adalah tahapan-tahapan pekerjaan yang dilakukan oleh analisis sistem dan *programmer* dalam membangun sebuah sistem. Metode-metode *UML* yang digunakan antara lain *use case diagram, activity diagram, sequence diagram,* dan *component diagram.*

3.2.1 *Use Case Diagram*

Metode penelitian meliputi penentuan model enkripsi dan dekripsi, penyelesaian algoritma enkripsi dan dekripsi, dan analisa hasil dari simulasi enkrispsi dan dekripsi algoritma vigenere cipher. Perancangan *UML* u*se case* diagram dapat diliat pada gambar dibawah ini.

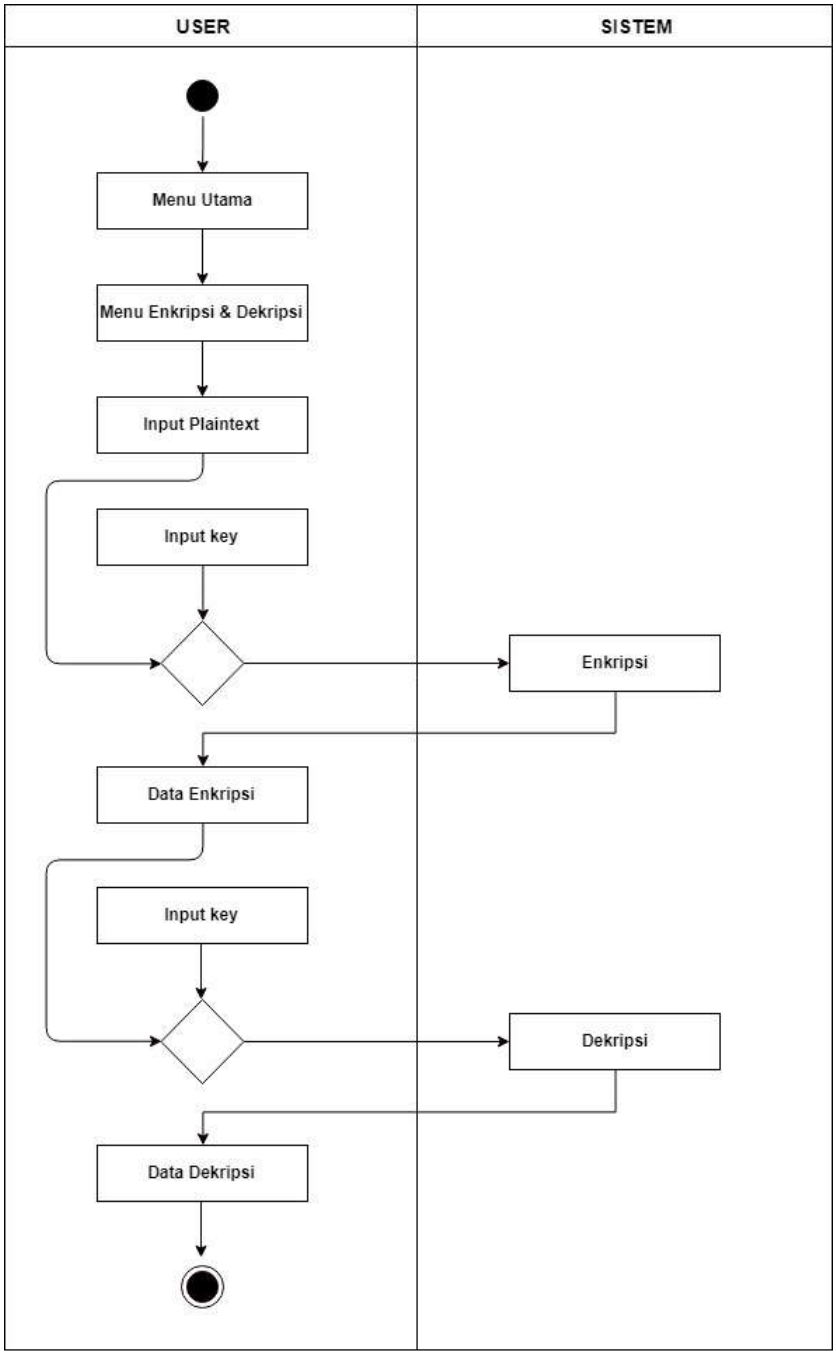


Gambar 3.2.1 *use case diagram.*

Pada gambar 3.2.1 *use case* diagram menjelaskan bahwa *user* dapat melakukan akses ke sisitem untuk memilih menu pada aplikasi enkripsi vigenere cipher, memilih enkripsi dan dekripsi pada aplikasi enkripsi vigenere cipher.

3.2.2 *Activity Diagram*

Gambar perancangan *UML activity diagram*.



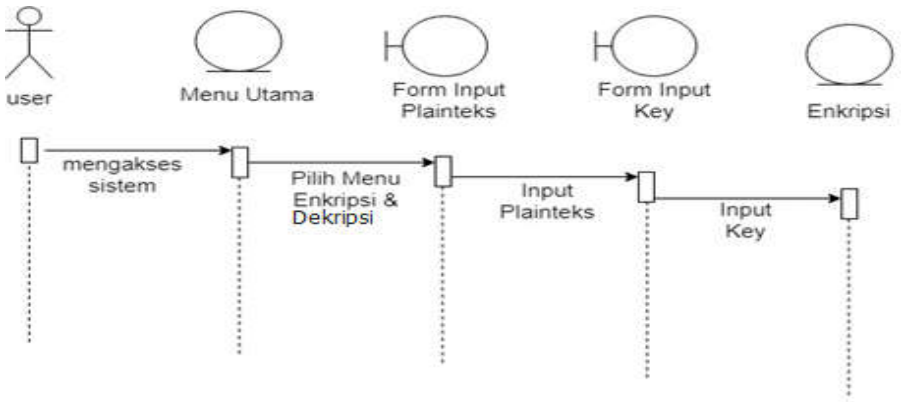
Gambar 3.2.2 *activity diagram.*

Pada gambar 3.2.2 *activity diagram* dapat dijelaskan bahwa :

1. *User* memilih menu utama pada aplikasi enkripsi vigenere cipher.
2. *User* memilih menu enkripsi dan dekripsi.
3. Untuk mengenkripsi, *user* harus mengi-inputkan plainteks dan *key* untuk mendapatkan enkripsi.
4. Sistem akan mengenkripsi plainteks dan *key* yang sudah di *input* oleh *user.*
5. Setelah dienkripsikan *user* akan mendapat data enkripsi.
6. Untuk mendekripsikannya kembali, *user* menginputkan data yang sudah dienkripsikan lalu menginputkan *key* yang sama dengan inputan plainteks sebelumnya.
7. Sistem akan mendekripsikan data enkripsi dan *key* pada sistem.
8. Setelah data enkripsi dan *key* di dekripsikan maka user mendapat data dekripsi.

3.2.3 *Sequence Diagram*

Gambar perancangan *UML sequence diagram* Enkripsi.

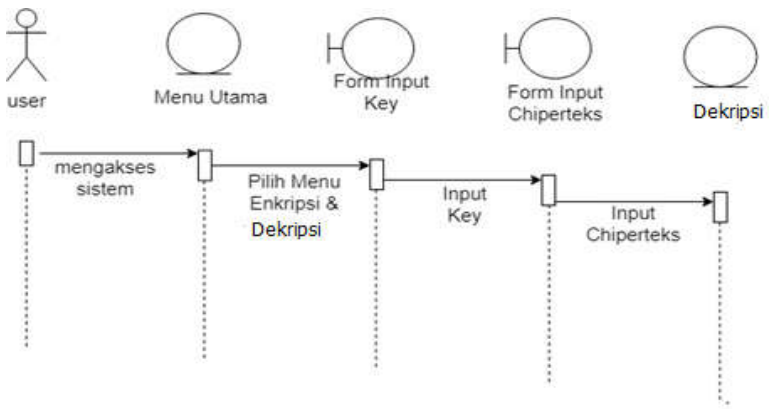


Gambar 3.2.3 *sequence diagram* enkripsi.

Pada gambar 3.2.3 *sequence diagram* enkripsi dapat dijelaskan bahwa :

1. *User* melakukan akses ke sistem.
2. Setalah masuk ke dalam sistem, sistem akan menampilkan menu utama.
3. Setelah tampil menu utama *user* akan memilih menu enkripsi dan dekripsi.
4. Di menu enkripsi dan dekripsi, *user* akan menginputkan plainteks dan *key* untuk mendapatkan kata atapun kalimat yang dienkripsikan.

Gambar perancangan *UML sequence diagram* Dekripsi.



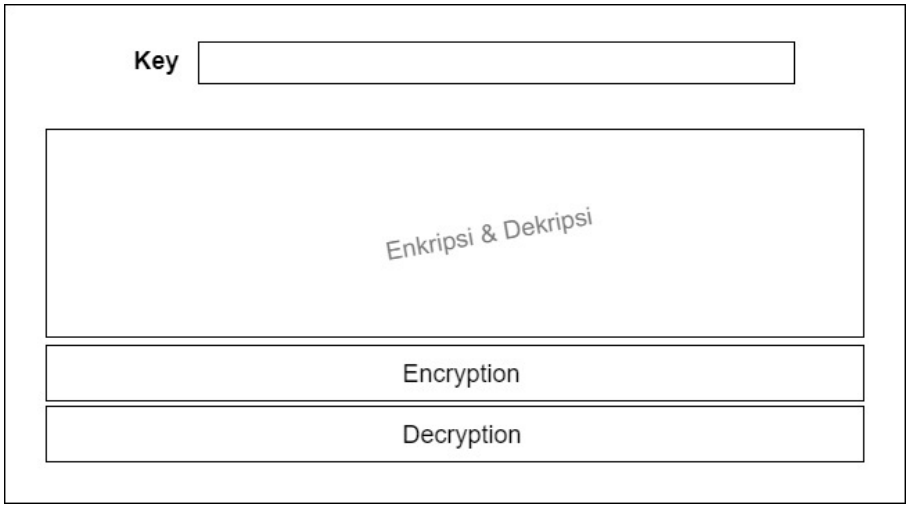
Gambar 3.2.3 *sequence diagram* dekripsi.

Pada gambar 3.2.3 *sequence diagram* dekripsi dapat dijelaskan bahwa :

1. *User* melakukan akses ke sistem.
2. Setalah masuk ke dalam sistem, sistem akan menampilkan menu utama.
3. Setelah tampil menu utama *user* akan memilih menu enkripsi dan dekripsi.
4. Di menu enkripsi dan dekripsi, *user* akan menginputkan *key* dan chiperteksuntuk mendapatkan kata atapun kalimat dekripsi.

3.2.4 Rancangan Masukan (*Input*)

Rancangan masukan *(input)* merupakan rancangan sebuah *form* pengolahan plainteks dan *key* yang masuk pada sistem kemudian diproses oleh sistem sehingga menghasilkan *output.*Pengolahan plainteks dan *key* ini dilakukan oleh sistemvigenere cipher berbasis web. *Form* enkripsi dan dekripsi ini digunakan sebagai inputan plainteks dan *key* untuk menghasilkan enkripsi dan sebagai inputan dari chiperteks dan *key* untuk menghasilkan dekripsi. Rancangan masukan *(input)* enkripsi dan dekripsi dibuat seperti pada gambar dibawah ini :



Gambar 3.2.5 Rancangan Masukan (*Input*).

1. Nama masukan : *Form* enkripsi dan dekripsi
2. Fungsi : Untuk menginputkan Plainteks, key, dan chiperteks
3. Distribusi : *User*
4. Keterangan : Untuk mengenkripsi dan dekripsi

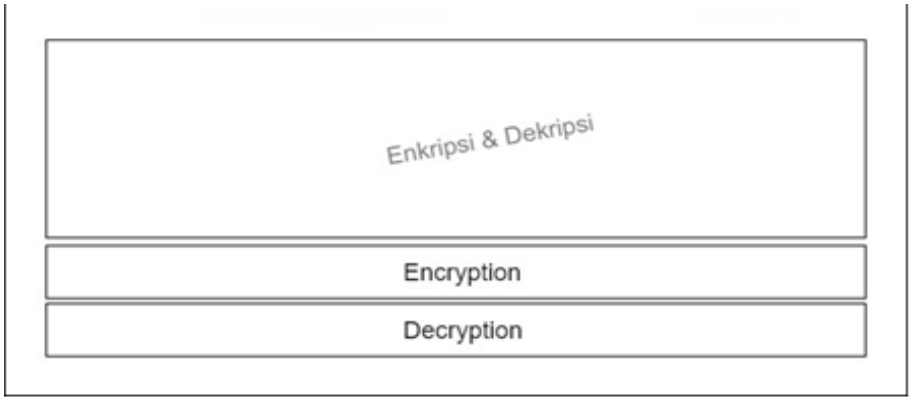
3.2.5 Rancangan proses

Dalam pembuatan sistem alat yang digunakan dalam perancangan dan desain aplikasi enkripsi menggunakan algoritma vigenere cipher yaitu dengan menggunakan *Unified Modelling Language (UML). Unified modelling language (UML)* adalah salah satu standar bahasa yang banyak digunakan di dunia industri untuk mendefinisikan *requirement,* membuat analisa dan desain, serta menggambarkan arsitektur dalam pemrograman berorientasi objek. *UML* merupakan bahasa visual untuk pemodelan dan komunikasi mengenai sebuah sistem dengan menggunakan diagram dan teks-teks pendukung[9].

3.2.6 Rancangan Keluaran *(Output)*

Rancangan keluaran *(output)* dalam suatu sistem adalah rancangan hasil keluaran data yang telah diproses dalam sistem. Pengolahan dari plainteks dan *key* akan menghasilkan data yang sudah terenkripsikan oleh sistem. *Form* enkripsi dan dekripsi ini juga digunakan sebagai *output* dari *input* plainteks dan *key* yang telah dienkripsikan dan untuk sebagai hasil dari *output* data enkripsi dan *key* yang sama sebelum dienkripsikan.

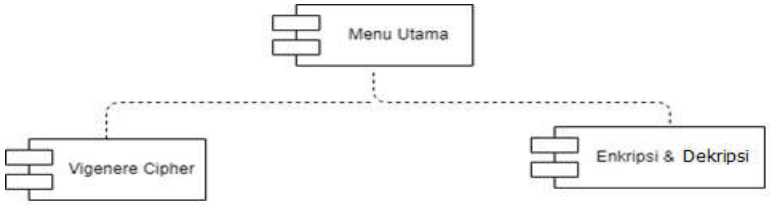
1. Nama keluaran : *Form* enkripsi dan dekripsi
2. Fungsi : Untuk media hasil enkripsi dan dekripsi
3. Distribusi : *User*
4. Keterangan : Untuk *output* dari enkripsi dan dekripsi.



Gambar *3.2.7 Rancangan Keluaran (Output)*

3.2.7 Rancangan *interface*

Gambar rancangan *interface*



Gambar 3.2.7 Rancangan *interface.*

Pada gambar 3.2.7 Rancangan *interface* menjelaskan pada sistem terdapat menu utama, form vigenere cipher bertujuan untuk menjelaskan secara singkat vigenere cipher, dan form enkripsi dan dekripsi bertujuan untuk proses enkripsi dan dekripsi vigenere cipher.

BAB IV

IMPLEMENTASI DAN PENGUJIAN SISTEM

4.1 Implementasi

Tahapan implementasi sistem merupakan tahap penterjemah perancangan berdasarkan hasil analisis ke dalam suatu bahasa pemrograman tertentu serta penerapan perangkat lunak yang dibangun dengan keadaan sebenarnya.Adapun pembahasan implementasi terdiri dari perangkat lunak pembangun, perangkat keras pembangun, dan implementasi antar muka. Penggunaan vigenere cipher berbasis web adalah untuk mempermudah *user* dalam melakukan enkripsi dan dekripsi menggunakan metode kriptografi vigenere cipher.

4.1.1 Perangkat Keras

Perangkat keras pembangun menjelaskan perangkat keras yang digunakan untuk membangun aplikasi enkripsi menggunakan algoritma vigenere cipher berbasis web. Adapun perangkat keras yang digunakan untuk membangun aplikasi ini adalah sebagai berikut :

a. Processor Intel® Celeron® CPU N3060 @ 1.60Ghz (2 CPUs)
b. Kapasitas Memory 2048MB RAM
c. Monitor
d. Keyboard
e. Mouse

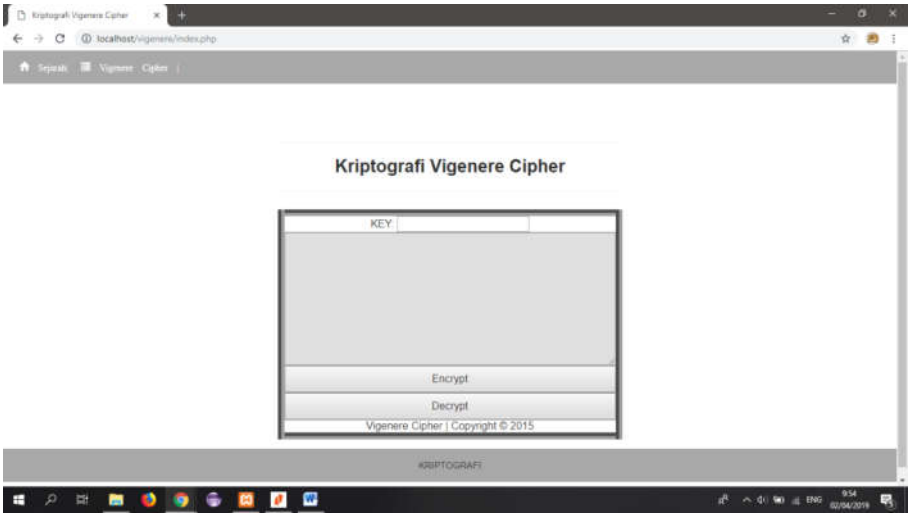
4.1.2 Perangkat Lunak

Secara fungsi perangkat lunak dibagi menjadi tiga yaitu sistem *software, programming language,* dan *application software.*Adapun perangkat lunak yang dibutuhkan pada perancangan aplikasi enkripsi algoritma vigenere cipher yaitu personal *computer* yang terdiri dari :

a. Sistem Operasi *Windows* 10
b. Notepad++
c. XAMPP
d. Web Browser

4.1.3 Tampilan Menu Utama

Tampilan menu utama ini menampilkan menu aplikasi enkripsi algoritma vigenere cipher berbasis web, tampilan dari aplikasi ini dapat dilihat sebagai berikut :



Gambar 4.1.3 Tampilan Menu Utama

Pada gambar 4.1.3 merupakan tampilan dari menu utama dari aplikasi enkripsi algoritma vigenere cipher, tampilan ini juga berfungsi untuk mengenkripsikan plaintek dan *key* serta mendekripsikan kembali ke plainteks. Pada tampilan program terdapat *input key* dan *input* plainteks serta terdapat dua *button* enkripsi dan dekripsi.

4.1.4 Tampilan Sejarah Vigenere Cipher

Gambar 4.1.4 Tampilan Sejarah Vigenere Cipher

Pada gambar 4.1.4 merupakan tampilan dari sejarah singkat tentang vigenere cipher. Pada *form* sejarah vigenere cipher menjelaskan sejarah tentang bagaimana vigenere cihper dibuat dengan menjelaskan tahun dan metode penyandian dari algoritma vigenere cipher sebelumnya.

4.2 Perhitungan Enkripsi dan Dekripsi

Perhitungan dilakukan untuk menguji hasil dari perhitungan enkripsi dan dekripsi pada algoritma vigenere cipher. Pengujian dengan cara model matematika algoritma vigenere cipher sebagai berikut :

Tabel 4.2 Perhitungan Enkripsi dan Dekripsi.

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

Perhitungan enkripsi dengan menggunakan model matematika pada algoritma vigenere cipher dengan jumlah plainteks dan kunci harus sama dan jika kunci memiliki jumlah yang tidak sama dengan plainteks maka kata pada kunci harus diulang untuk menyesuaikan jumlah plainteks, seperti berikut:

Plainteks : MAKALAH KRIPTOGRAFI

Kunci : TUGASTU GATUSGASTUG

Enkripsi :

$$\mathbf{C_i = E_k (M_i) = (M_i + K_i) \bmod 26}$$

$C_i = E_k (M_i) = (12_{(M)} + 19_{(T)}) \bmod 26$

$= 31_{(F)}$

$C_i = E_k (M_i) = (0_{(A)} + 20_{(U)}) \bmod 26$

$= 20_{(U)}$

$C_i = E_k (M_i) = (10_{(K)} + 6_{(G)}) \bmod 26$

$= 16_{(Q)}$

$C_i = E_k (M_i) = (0_{(A)} - 0_{(A)}) \bmod 26$

$= 0_{(A)}$

$C_i = E_k (M_i) = (11_{(L)} - 18_{(S)}) \bmod 26$

$= 29_{(D)}$

$C_i = E_k(M_i) = (0_{(A)} - 19_{(T)}) \bmod 26$

$= 19_{(T)}$

$C_i = E_k(M_i) = (7_{(H)} - 20_{(U)}) \bmod 26$

$= 27_{(B)}$

$C_i = E_k(M_i) = (10_{(K)} - 6_{(G)}) \bmod 26$

$= 16_{(Q)}$

$C_i = E_k(M_i) = (17_{(R)} - 0_{(A)}) \bmod 26$

$= 17_{(R)}$

$C_i = E_k(M_i) = (8_{(I)} - 18_{(S)}) \bmod 26$

$= 26_{(A)}$

$C_i = E_k(M_i) = (15_{(P)} - 19_{(T)}) \bmod 26$

$= 34_{(I)}$

$C_i = E_k(M_i) = (19_{(T)} - 20_{(U)}) \bmod 26$

$= 39_{(N)}$

$C_i = E_k(M_i) = (14_{(O)} - 6_{(G)}) \bmod 26$

$= 20_{(U)}$

$C_i = E_k(M_i) = (6_{(G)} - 0_{(A)}) \bmod 26$

$= 6_{(G)}$

$C_i = E_k(M_i) = (17_{(R)} - 18_{(S)}) \bmod 26$

$= 35_{(J)}$

$C_i = E_k(M_i) = (0_{(A)} - 19_{(U)}) \bmod 26$

$= 19_{(T)}$

$C_i = E_k(M_i) = (5_{(F)} - 20_{(U)}) \bmod 26$

$= 25_{(Z)}$

$C_i = E_k(M_i) = (8_{(I)} - 6_{(G)}) \bmod 26$

$= 14_{(O)}$

Maka cipherteks yang di dapat adalah FUQADTB QRAINUGJTZO

Dekripsi :

Cipherteks :FUQADTB QRAINUGJTZO

Kunci : TUGASTU GATUSGASTUG

$M_i = D_k(C_i) = (C_i - K_i) \bmod 26$

$C_i = E_k(M_i) = (5_{(F)} - 19_{(T)}) \bmod 26$

$= -14_{(M)}$

$C_i = E_k(M_i) = (20_{(U)} - 20_{(U)}) \bmod 26$

$= 0_{(A)}$

$C_i = E_k(M_i) = (16_{(Q)} - 6_{(G)}) \bmod 26$

$= 10_{(K)}$

$C_i = E_k(M_i) = (0_{(A)} - 0_{(A)}) \bmod 26$

$= 0_{(A)}$

$C_i = E_k(M_i) = (3_{(D)} - 18_{(S)}) \bmod 26$

$= -15_{(L)}$

$C_i = E_k(M_i) = (19_{(T)} - 19_{(T)}) \bmod 26$

$= 0_{(A)}$

$C_i = E_k(M_i) = (1_{(B)} - 20_{(U)}) \bmod 26$

$= -19_{(H)}$

$C_i = E_k(M_i) = (16_{(Q)} - 6_{(G)}) \bmod 26$

$= 10_{(K)}$

$C_i = E_k(M_i) = (17_{(R)} - 0_{(A)}) \bmod 26$

$= 17_{(R)}$

$C_i = E_k(M_i) = (0_{(A)} - 18_{(S)}) \bmod 26$

$= -18_{(I)}$

$C_i = E_k(M_i) = (8_{(I)} - 19_{(T)}) \bmod 26$

$= -11_{(P)}$

$C_i = E_k(M_i) = (13_{(N)} - 20_{(U)}) \bmod 26$

$= -7_{(T)}$

$C_i = E_k(M_i) = (20_{(U)} - 6_{(G)}) \bmod 26$

$= 14_{(O)}$

$C_i = E_k(M_i) = (6_{(G)} - 0_{(A)}) \bmod 26$

$= 6_{(G)}$

$C_i = E_k(M_i) = (9_{(J)} - 18_{(S)}) \bmod 26$

$= -9_{(R)}$

$C_i = E_k(M_i) = (19_{(T)} - 19_{(T)}) \bmod 26$

$= 0_{(A)}$

$C_i = E_k(M_i) = (25_{(U)} - 20_{(U)}) \bmod 26$

$= 5_{(F)}$

$C_i = E_k(M_i) = (14_{(O)} - 6_{(G)}) \bmod 26$

$= 0_{(I)}$

Maka cipherteks yang di dapat adalah MAKALAH KRIPTOGRAFI

4.3 Pengujian

Pengujian dilakukan dengan menguji proses *use case* diagram dan kemungkinan kesalahan yang terjadi untuk setiap proses. Pengujian ini dilakukan secara *black box,* yaitu dilakukan dengan memperhatikan masukan sistem dan keluaran dari sistem. Sesuai dengan material pengujian maka akan dilaksanakan pengujian sebagai berikut :

4.3.1 Rancangan Pengujian Enkripsi

Proses ini berfungsi untuk mengenkripsikan plainteks dan *key,* langkah-langkah yang dilakukan *user* dalam proses ini adalah sebagai berikut :

a. *Input key*

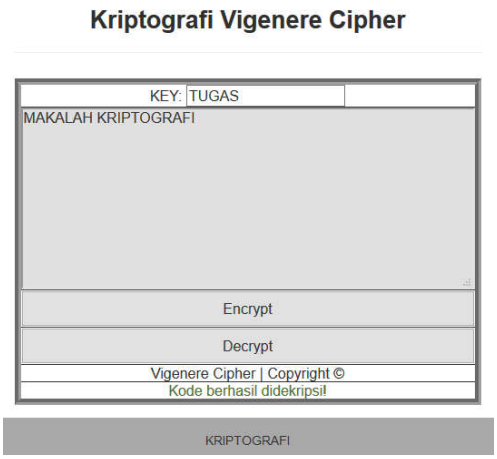
   User diminta untuk menginputkan *key* yang berisikan alfabet sebelum mengenkripsikannya.

b. *Input* plainteks

   User diminta untuk menginputkan plainteks yang berisikan alfabet sebelum mengenkripsikannya.

c. Tombol *buttonencrypt* dan Tombol *buttondecrypt*

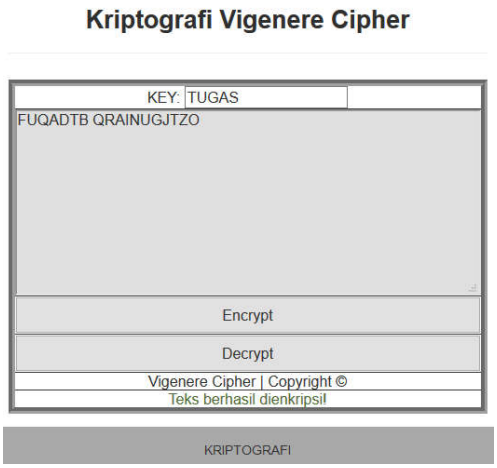
   Pada tombol *button encrypt* dapat mengenkripsikan *key* dan plainteks yang telah di masukkan oleh *user,* pada tombol *button decrypt* dapat mendekripsikan kembali plainteks dan *key* atau mendekripsikan data enkripsi dan *key* yang sama pada saat *user* mengenkripsikan.



Gambar 4.3.1 Rancangan Pengujian Enkripsi

Pada gambar 4.3.1 rancangan pengujian enkripsi menjelaskan bahwa *user* menginputkan *key* dan menginputkan data plainteks. Pada *form* ini *user* menginputkan *key* dengan kata "TUGAS" dan menginputkan data plainteks dengan kalimat "MAKALAH KRIPTOGRAFI".

4.3.2 Hasil Rancangan Pengujian Enkripsi



Gambar 4.3.2 Hasil Rancangan Pengujian Enkripsi

Pada gambar 4.3.2 rancangan hasil pengujian enkripsi adalah tampilan hasil dari data plainteks dan *key* yang berhasil di enkripsikan oleh sistem. Pada *form* ini terlihat hasil dari plainteks dan *key* yang menghasilkan data enkripsi, plainteks yang diinputkan dengan kalimat "MAKALAH KRIPTOGRAFI" dan *key* yang diinputkan dengan kata "TUGAS" menghasilkan data enkripsi "FUQADTB QRAINUGJTZO".

4.3.3 Rancangan Pengujian Dekripsi

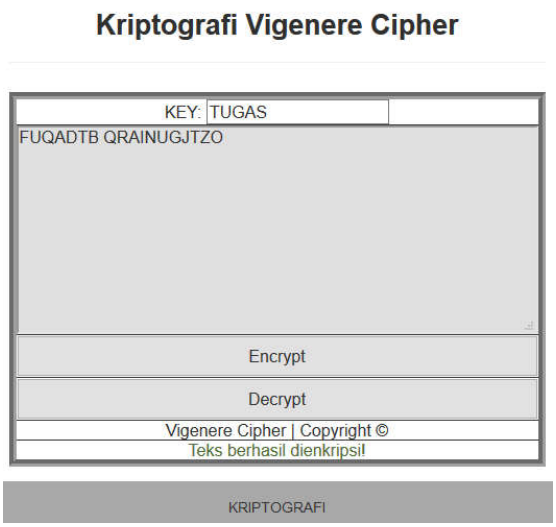
Proses ini berfungsi untuk mendekripsikan data enkripsi dan *key* yang telah diterima oleh *user,* langkah-langkah yang dilakukan *user* untuk mendekripsikan data enkripsi adalah sebagai berikut :

a. *Input* data enkripsi

   User diminta untuk menginputkan data enkripsi yang telah diterimanya.

b. *Input key*

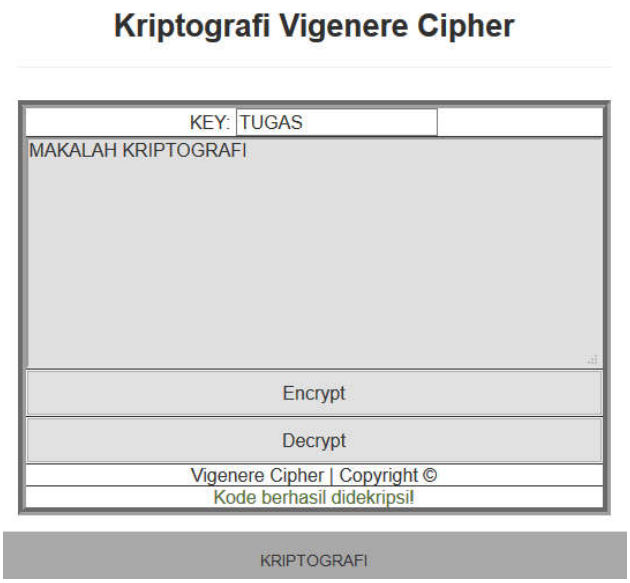
   User diminta untuk menginputkan *key* yang sama saat sebelum dienkripsikannya plainteks.



Gambar 4.3.3 Rancangan Pengujian Dekripsi

Pada gambar 4.3.3 rancangan pengujian dekripsi, pada *form* ini menjelaskan bahwa *user* menginputkan data enkripsi dan *key,* untuk mendekripsikan data enkripsi yang diterima *user* harus menginputkan data enkripsi dan *key* yang sama dikarena ketika *user* menginputkan *key* yang salah maka data dekripsi yang didapatkan tidak akan sesuai ataupun salah sehingga data dekripsi tidak dapat dibaca oleh pendekripsi dan data tidak akan bisa terbaca serta ketika *user* menginputkan data enkripsi yang salah hasil dari dekripsi tidak akan bisa dibaca dan dimengerti.

4.3.4 Hasil Rancangan Pengujian Dekripsi



Gambar 4.3.4 Hasil Rancangan Pengujian Dekripsi

Pada gambar 4.3.4 hasil rancangan pengujian dekripsi adalah tampilan dari hasil pengujian dekripsi yang berhasil di dekripsikan oleh sistem, pada *form* ini menjelaskan bahwa hasil yang diinputkan dengan plainteks "FUQADTB QRAINUGJTZO" dan menginputkan *key* yang sama yaitu "TUGAS" menghasilkan kalimat yang dapat dibaca dan dimengerti oleh *user.* Pada *form* ini menjelaskan bahwa data enkripsi yang didekripsikan kembali ke kalimat yang tidak dapat dibaca dan dimengerti sebelumnya dapat menghasilkan data dekripsi yang dapat dibaca dan dimengerti oleh *user.*

4.3.5 Kasus Dan Hasil Pengujian

Berdasarkan rencana pengujian yang telah dibuat maka dibuatlah pengujian pada sistem dengan tabel pengujian untuk setiap uji yang dilakukan pada bagian yang diisikan oleh data yang benar dan data yang salah.

4.3.5.1 Tabel Pengujian Enkripsi Benar

Tabel 4.3.5.1 Pengujian Enkripsi Benar

Kasus Dan Hasil Uji (Data Benar)	
Data yang diinputkan	Plainteks : MAKALAH KRIPTOGRAFI *Key :* TUGAS
Yang diharapkan	Data dari plainteks dan *key* maka *user* dapat mengenkripsikan plainteks dan *key. User* menginputkan plainteks dan *key* lalu mengklik *button* enkripsi dan berhasil mengenkripsikan.
Pengamatan	Dapat mengisi plainteks dan *key,* tombol enkripsi berfungsi proses enkripsi dapat dilakukan.
Kesimpulan	Data berhasil dienkripsikan.

4.3.5.2 Tabel Pengujian Enkripsi Salah

Tabel 4.3.5.2 Pengujian Enkripsi Salah

Kasus Dan Hasil Uji (Data Salah)	
Data yang diinputkan	Plainteks : MAKALAH KRIPTOGRAFI *Key :* 123
Yang diharapkan	Menampulkan pesan kesalahan “kata sandi hanya boleh berisi karakter alfabet!”
Pengamatan	Pesan kesalahan muncul ”kata sandi hanya boleh berisi karakter alfabet!” sesuai dengan yang diharapkan
Kesimpulan	Data tidak berhasil dienkripsikan.

4.3.5.3 Tabel Pengujian Dekripsi Benar

Tabel 4.3.5.2 Pengujian Dekripsi Benar

Kasus Dan Hasil Uji (Data Benar)	
Data yang diinputkan	Data enkripsi : FUQADTB QRAINUGJTZO *Key :* TUGAS
Yang diharapkan	Data enkripsi dan *key* yang sama di input maka *user* dapat mendekripsikan data enkripsi dan *key. User* menginputkan data enkripsi dan *key* yang samalalu mengklik *button* dekripsi.
Pengamatan	Dapat mengisi data enkripsi dan *key,* tombol dekripsi berfungsi proses dekripsi dapat dilakukan.
Kesimpulan	Data berhasil didekripsikan.

4.3.5.4 Tabel Pengujian Dekripsi Salah

Tabel 4.3.5.2 Pengujian Dekripsi Salah

Kasus Dan Hasil Uji (Data Salah)	
Data yang diinputkan	Data enkripsi : FUQADTB QRAINUGJTZO *Key :* BULAN
Yang diharapkan	Menampilkan data enkripsi yang tidak dapat dimengerti karena *key* yang salah.
Pengamatan	Pesan kesalahan muncul tidak dapat dibaca oleh *users*.
Kesimpulan	Data tidak dapat dibaca.

BAB V

PENUTUP

5.1 Kesimpulan

Dari hasil perancangan dan implementasi aplikasi kriptografi dengan metode algoritma vigenere cipher, maka didapatkan kesimpulan sebagai berikut :

1. Aplikasi kriptografi ini dapat disimpulkan bahwa dengan menggunakan aplikasi algoritma vigenere cipher dapat menyandikan data penting dengan cara mengenkripsikan data tersebut menjadi sandi-sandi yang tidak dapat dibaca oleh orang yang tidak berhak.
2. Aplikasi kriptografi ini juga dapat mengembalikan data yang telah dienkripsikan menjadi data yang dapat dibaca dengan cara mendekripsikan data enkripsi tersebut.

5.2 Saran

Dalam hal ini, penulis memberikan dan memerlukan saran yang kiranya dapat bermanfaat untuk kemajuan aplikasi yang dibuat ini, tentunya masih banyak yang harus dikembangkan agar dapat meningkatkan kualitas dan kegunaannya. Saran untuk pengembangan aplikasi enkripsi menggunakan algoritma vigenere cipher berbasis web ini antara lain :

1. Diharapkan adanya pengembangan lebih lanjut dari pembaharuan *interface* aplikasi enkripsi menggunakan algoritma vigenere cipher berbasis web agar memperbaiki tampilan sehingga dapat lebih menarik lagi digunakan untuk dimasa yang akan datang.
2. Diharapkan untuk kedepannya aplikasi enkripsi menggunakan algoritma vigenere cipher ini dapat dikembangkan dengan kompleks dan dapat ditambah dengan menu-menu baru yang menarik lagi bagi pengguna aplikasi ini.
3. Diharapkan kedepannya website aplikasi algoritma vigenere cipher dapat ditambah dengan metode-metode algoritma lainnya agar lebih menarik bagi pengguna.

DAFTAR PUSTAKA

[1] Muhammad Dedi Irawan, "IMPLEMENTASI KRIPTOGRAFI VIGENERE CIPHER DENGAN PHP," *J. Teknol. Inf.*, vol. 1, no. 1, pp. 12–23, 2017.

[2] Efrandi, Asnawati, and Yupiyanti, "Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Chiper," *J. Media Infotama*, vol. 10, no. 2, pp. 120–128, 2014.

[3] M. K. Harahap and N. Khairina, "Analisis Algoritma One Time Pad Dengan Algoritma Cipher Transposisi Sebagai Pengamanan Pesan Teks," *J. Penelit. Tek. Inform.*, vol. 1, no. 2, pp. 58–62, 2017.

[4] M. K. Ronal Watrianthos, S.Kom, "PERBANDINGAN TEKNIK KRIPTOGRAFI METODE SAPPHIRE II DAN RC4," *J. Inform. AMIK-LB*, vol. 3, no. 2, pp. 24–51, 2015.

[5] R. Sadikin, *Kriptografi Untuk Keamanan Jaringan*. Penerbit Andi, 2017.

[6] R. M. Budiasa, "Makalah IF3058 Analisis Kriptografi dalam penentuan Cipherteks kode ASCII melalui metode Aljabar Boolean," 2010.

[7] A. A. Permana and D. Nurnaningsih, "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes)," *J. Tek. Inform.*, vol. 11, no. 2, pp. 177–186, 2018.

[8] A. R. R. Hasan Abdurahman, "Perancangan Aplikasi E-Canteen Berbasis Android Dengan Menggunakan Metode Object Oriented Analysis & Design (OOAD)," *J. Penelit. Komun. dan Opini Publik*, vol. 20, no. 1, pp. 83–92, 2014.

[9] S. Saiful and A. Ambarita, "Pembuatan Aplikasi Web Pencarian Jasa Pembantu Rumah Tangga (Prt) Dikota Ternate," *Indones. J. Inf. Syst.*, vol. 2, no. 2, pp. 77–90, 2016.

[10] A. A. R. P. W. A, M. H. Maulana, C. D. Andini, and F. Nadziroh, "SISTEM PEMINJAMAN RUANGAN ONLINE (SPRO) DENGAN METODE UML (UNFIELD MODELING LANGUAGE)," *urnal Teknol. dan Terap. Bisnis*, vol. 1, no. 1, pp. 1–8, 2018.

[11] A. Hendini, "Pemodelan UML sistem informasi Monitoring Penjualan dan stok barang," *Pemodelan Uml Sist. Inf. Monit. Penjualan Dan Stok Barang (Studi Kasus Distro Zhezha Pontianak)*, vol. IV, no. 2, pp. 107–116, 2016.

[12] A. Anisah and K. Kuswaya, "Analisis Dan Perancangan Sistem Informasi Pengolahan Data Pengeluaran, Penggunaan Bahan Dan Hutang Dalam Pelaksanaan Proyek Pada Pt Banamba Putratama," *Simetris J. Tek. Mesin, Elektro dan Ilmu Komput.*, vol. 8, no. 2, p. 507, 2017.

[13] H. Tohari, *Analisis Serta Perancangan Sistem Informasi Melalui Pendekatan UML*. ANDI Yogyakarta, 2017.

[14] Rulia Puji Hastanti; Bambang Eka Purnama; Indah Uly Wardati, "Sistem Penjualan Berbasis Web (E-Commerce) Pada Tata Distro Kabupaten Pacitan," *J. Bianglala Inform.*, vol. 3, no. 2, pp. 1–10, 2015.

[15] Murdani and I. R. Munthe, "Penerapan web based learning dalam aplikasi pembelajaran sholat," vol. 6, no. 2, pp. 1–4, 2018.

[16] Harison and A. Syarif, "SISTEM INFORMASI GEOGRAFIS SARANA PADA KABUPATEN PASAMAN BARAT," *J. TEKNOIF*, vol. 4, no. 2, pp. 40–50, 2016.

[17] S. T. YM Kusuma Ardhana., *PROJECT PHP & MySQL Membuat Website Buku Digital*. Jasakom, 2014.

[18] ARYANTO, *Soal Latihan dan Jawaban Pengolahan Database Mysql Tingkat Dasar / Pemula*. Deepublish, 2018.

[19] P. P. Widodo and Elisawati, "Penjadwalan Mubaligh Online Pada Persatuan Mubaligh Dumai (Pmd) Kota Dumai," *J. Inform. Manaj. dan Komput.*, vol. 9, no. 2, pp. 25–32, 2017.

D. Listing Program

Index.php

```
<?php
// menginisialvariabel
$pswd = "";
$code = "";
$error = "";
$valid = true;
$color = "#FF0000";
// jikaformulirdikirimkan
if ($_SERVER['REQUEST_METHOD'] == "POST")
{
	// mendeklarasifungsienkripsidandekripsi
	require_once('vigenere.php');
	// mengaturvariabel
	$pswd = $_POST['pswd'];
	$code = $_POST['code'];
	// mengecek password
	if (empty($_POST['pswd']))
	{
		$error = "Silahkan input key!";
		$valid = false;
	}
	// mengecekplainteks
	else if (empty($_POST['code']))
	{
```

```
                $error =
"Silakanmasukkanbeberapateksataukodeuntukmengenkripsiataumendekripsi!";
                $valid = false;
        }
        // memeriksa password alfanumerik
        else if (isset($_POST['pswd']))
        {
                if (!ctype_alpha($_POST['pswd']))
                {
                        $error = "Kata sandihanyabolehberisikarakteralfabet!";
                        $valid = false;
                }
        }
        // inputs valid
        if ($valid)
        {
                // jikatombolmengenkripsikan di klik
                if (isset($_POST['encrypt']))
                {
                        $code = encrypt($pswd, $code);
                        $error = "Teksberhasildienkripsi!";
                        $color = "#526F35";
                }
                // jikatombolmendekripsikan di klik
                if (isset($_POST['decrypt']))
                {
                        $code = decrypt($pswd, $code);
```

```
                        $error = "Kodeberhasildidekripsi!";
                        $color = "#526F35";
                }
        }
}
?>
<html>
        <head>
        <meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta name="description" content="">
<meta name="author" content="">
<linkrel="icon" href="favicon.ico">
                <title>KriptografiVigenere Cipher</title>
                <link href="favicon.ico" rel="shortcut icon" type="image/x-icon"
/>
                <link rel="stylesheet" type="text/css" href="style.css">
                <link href="css/bootstrap.min.css" rel="stylesheet">
                <link href="css/style.css" rel="stylesheet">
                <script type="text/javascript" src="Script.js"></script>
        </head>
        <body>
        <nav class="navbarnavbar-default navbar-fixed-top"
style="background:#A9A9A9;">
<div class="container-fluid">
<div class="collapse navbar-collapse">
<div class="navnavbar-navnavbar-left">
```

```
<ul id="nav">

                <li><a href="sejarah.php"
style="color:#fff;background:#A9A9A9;" ><span class="glyphiconglyphicon-
home">Sejarah| </span></a></li>

<li ><a href="index.php" style="color:#fff;background:#A9A9A9;"><span
class="glyphiconglyphicon-list">Vigenere Cipher | </span></a></li>

</ul>

</div>

                <div class="clear"></div>

</div>

        </div>

</nav>

        <div class="col-md-4" style="margin:0px;">

</div>

                <br><br><br>

                <form action="index.php" method="post">

                        <table cellpadding="5" align="center" cellpadding="5"
border="10">

                                <caption><hr><center><b>KriptografiVigenere
Cipher</b></center><hr></caption>

                                <tr>

                                        <td align="center">KEY: <input type="text"
name="pswd" id="pass" value="<?php echo htmlspecialchars($pswd); ?>"
/></td>

                                </tr>

                                <tr>

                                        <td align="center"><textarea id="box"
name="code"><?php echo htmlspecialchars($code); ?></textarea></td>

                                </tr>

                                <tr>
```

```
                                        <td><input type="submit" name="encrypt"
class="button" value="Encrypt" onclick="validate(1)" /></td>

                                    </tr>

                                    <tr>

                                        <td><input type="submit" name="decrypt"
class="button" value="Decrypt" onclick="validate(2)" /></td>

                                    </tr>

                                    <tr>

                                        <td align="center">Vigenere Cipher  |
Copyright &amp;copy; 2015 <span style="cursor:pointer;color:#0000FF"
onclick="help()"></span></td>

                                    </tr>

                                    <tr>

                                        <td><center><div style="color: <?php echo
htmlspecialchars($color) ?>"><?php echo htmlspecialchars($error)
?></div></center></td>

                                    </tr>

                                </table>

                            </form>

                            <div class="copyright" style="line-height:50px;
background:#A9A9A9;color: ">

<center>KRIPTOGRAFI</center>

</div>

</div>

        </body>

</html>
```

Sejarah.php

```
<!DOCTYPE html>

<html lang="en">
```

```
<head>

<meta charset="utf-8">

<meta http-equiv="X-UA-Compatible" content="IE=edge">

<meta name="viewport" content="width=device-width, initial-scale=1">

<meta name="description" content="">

<meta name="author" content="">

<linkrel="icon" href="favicon.ico">

<title>KriptografiVigenere Cipher</title>

<link href="css/bootstrap.min.css" rel="stylesheet">

<link href="css/style.css" rel="stylesheet">

</head>

<body>

<body>

<nav class="navbarnavbar-default navbar-fixed-top"
style="background:#A9A9A9;">

<div class="container-fluid">

<div class="collapse navbar-collapse">

                    <div class="navnavbar-navnavbar-left">

<ul id="nav">

<li><a href="sejarah.php" style="color:#fff;background:#A9A9A9;" ><span
class="glyphiconglyphicon-home">Sejarah| </span></a>

</span></a></li>

<li ><a href="index.php" style="color:#fff;background:#A9A9A9;"><span
class="glyphiconglyphicon-list">Vigenere Cipher | </span></a></li>

                    </li>

                    </div>
```

```
                    </ul>
</li>
</ul>
</div>
</nav>
</head>
<body>
<center>
<font face=arial size=8 color=black>
<b>.::SejarahVigenere Cipher::.<br>
<font face=calibri size=6 color=black>
<i><center><imgsrc="Vigenere.jpg" height="300" alt=""></center></i>
<hr>
<hr>
<font face=arial size=4 style='text-align:justify;'  color=black>
<p>Sandi
Vigenèreadalahmetodemenyandikanteksalfabetdenganmenggunakanderetansandi
Caesar berdasarkanhuruf-hurufpada kata kunci.

Sandi Vigenèremerupakanbentuksederhanadarisandisubstitusipolialfabetik.

Kelebihansandiinidibandingsandi Caesar
dansandimonoalfabetiklainnyaadalahsandiinitidakbegiturentanterhadapmetodepe
mecahansandi yang disebutanalisisfrekuensi.

Giovan Batista Belasomenjelaskanmetodeinidalambuku La cifra del. Sig. Giovan
Batista Belaso (1553)

dandisempurnakanoleh diplomat PrancisBlaise de Vigenère, pada 1586. Padaabat
ke-19, banyak orang yang mengiraVigenèreadalahpenemusandiini, sehingga,
sandiinidikenalluassebagai "sandiVigenère".</p>

<p></p>
```

Sandi inidikenalluaskarenacarakerjanyamudahdimengertidandijalankan, danbagiparapemulasulitdipecahkan.

Padasaatkejayaannya, sandiinidijuluki le chiffreindéchiffrable (bahasaPrancis: 'sandi yang takterpecahkan').

Metodepemecahansandiinibaruditemukanpadaabad ke-19.

Padatahun 1854, Charles Babbage menemukancarauntukmemecahkansandiVigenère.

MetodeinidinamakantesKasiskikarena Friedrich Kasiski-lah yang pertamamempublikasikannya.

KRIPTOGRAFI

</body>

</html>

Vigenere.php

```
<?php
// berfungsiuntukmengenkripsikanteks yang diberikan
function encrypt($pswd, $text)
{
	// merubahkuncimenjadihurufkecil
	$pswd = strtolower($pswd);
	// menginisialkanvariabel
	$code = "";
	$ki = 0;
```

```
$kl = strlen($pswd);
$length = strlen($text);
// mengulangisetiapbarisdalamteks
for ($i = 0; $i < $length; $i++)
{
    // jikahurufnyaalfa, ENKRIPSI TEKS
    if (ctype_alpha($text[$i]))
    {
        // hurufbesar
        if (ctype_upper($text[$i]))
        {
            $text[$i] = chr(((ord($pswd[$ki]) - ord("a") +
ord($text[$i]) - ord("A")) % 26) + ord("A"));
        }
        // hurufkecil
        else
        {
            $text[$i] = chr(((ord($pswd[$ki]) - ord("a") +
ord($text[$i]) - ord("a")) % 26) + ord("a"));
        }
        // pembaharuanindekskunci
        $ki++;
        if ($ki>= $kl)
        {
            $ki = 0;
        }
```

```
                }
        }
        // mengembalikankodeterenkripsi
        return $text;
}
// berfungsiuntukmendekripsikanteks yang diberikan
function decrypt($pswd, $text)
{
        // merubahkuncimenjadihurufkecil
        $pswd = strtolower($pswd);
        // menginisialkanvariabel
        $code = "";
        $ki = 0;
        $kl = strlen($pswd);
        $length = strlen($text);
        // mengulangisetiapbarisdalamteks
        for ($i = 0; $i < $length; $i++)
        {
                // jikahurufnyaalfa, DEKRIPSI TEKS
                if (ctype_alpha($text[$i]))
                {
                        // hurufbesar
                        if (ctype_upper($text[$i]))
                        {
```

```
                $x = (ord($text[$i]) - ord("A")) - (ord($pswd[$ki]) -
ord("a"));
                if ($x < 0)
                {
                        $x += 26;
                }
                $x = $x + ord("A");
                $text[$i] = chr($x);
        }
        // hurufkecil
        else
        {
                $x = (ord($text[$i]) - ord("a")) - (ord($pswd[$ki]) -
ord("a"));
                if ($x < 0)
                {
                        $x += 26;
                }
                $x = $x + ord("a");
                $text[$i] = chr($x);
        }
        // memperbaharuiindekskunci
        $ki++;
        if ($ki>= $kl)
        {
                $ki = 0;
```

```
                    }
                }
            }
            // mengembalikankodedekripsi
            return $text;
}
?>
```