**Naskah Publikasi**

**PROYEK TUGAS AKHIR**

**IMPLEMENTASI ALGORITMA VIGENERE CIPHER UNTUK ENKRIPSI DAN DEKRIPSI TEKS BERBASIS WEBSITE**

Diajukan untuk memenuhi salah satu syarat

Mencapai derajat Sarjana S-1 Program Studi Teknik Informatika

Disusun oleh:

**AHMAD MUSLIHIN**

**5130411021**

**PROGRAM STUDI TEKNIK INFORMATIKA**

**FAKULTAS TEKNOLOGI INFORMASI DAN ELEKTRO**

**UNIVERSITAS TEKNOLOGI YOGYAKARTA**

**2017**

**Naskah Publikasi**

**IMPLEMENTASI ALGORITMA VIGENERE CIPHER UNTUK ENKRIPSI DAN DEKRIPSI TEKS BERBASIS WEBSITE**

Disusun oleh:

**AHMAD MUSLIHIN**

**5130411021**

Telah disetujui oleh pembimbing

Pembimbing

**Iwan Hartadi Tri Untoro, S.T., M.Kom.** Tanggal : …………………...

Implementasi Algoritma Vigenere Cipher Untuk Enkripsi dan Dekripsi Teks Berbasis Website

Ahmad Muslihin

*Program Studi Teknik Informatika,Fakultas Teknologi Informasi dan Elektro  
Universitas Teknologi Yogykarta*

*Jl. Ringroad Utara Jombor Sleman Yogyakarta*

*E-mail :* [ahmadmuslihin.id@gmail.com](mailto:ahmadmuslihin.id@gmail.com)

## ABSTRAK

*Berkembangnya teknologi telah mempengaruhi aspek keamanan teks yang bersifat rahasia, baik untuk keamanan bersama maupun untuk privasi individu. Seseorang yang biasa menyimpan data-data penting ke dalam suatu file dengan karakter yang tidak terkode sangatlah rawan penyadapan apabila tidak berhati-hati. Untuk menjaga keamanan dan kerahasiaan teks maka diperlukan enkripsi guna membuat teks tersebut tidak dapat dibaca atau dimengerti oleh sembarang orang, kemudian teks tersebut didekripsi agar dapat dibaca oleh penerima yang berhak. Tujuan dari penelitian ini adalah untuk membangun sebuah sistem enkripsi dan dekripsi teks menggunakan algoritma Vigenere Cipher dalam menjaga keamanan teks agar pihak yang tidak berwenang kesulitan untuk memecahkan data teks sehingga keamanan dan kerahasiaan tetap terjaga. Sistem ini dirancang menggunakan DAD (Diagram Alir Data), ERD (Entity Relationship Diagram), Diagram Jenjang dan database MySQL. Sedangkan bahasa pemrograman menggunakan HTML (Hypertext Markup Language), PHP (Personal Home Page), Javascript, dan CSS (Cascading Style Sheet). Hasil yang didapat dari pembangunan sistem Enkripsi Dan Dekripsi Teks Menggunakan Algoritma Vigenere Cipher adalah sebuah website untuk mengenkripsi dan mendekripsi file teks yang berekstensi .txt dengan ukuran maksimal 512 KB dan .docx 2 MB dengan menggunakan kunci berlapis dua, sehingga dapat membantu sebuah organisasi maupun individu dalam menjaga keamanan dan kerahasiaan data yang bersifat rahasia.*

Kata kunci : Enkripsi, Dekripsi, Kriptografi, Vigenere Cipher, Website.

### 1. PENDAHULUAN

**1.1 Latar Belakang**

Perkembangan ilmu pengetahuan dan teknologi telah memberikan dampak perubahan yang sangat besar. Salah satu dampak perubahan pada perkembangan ilmu pengetahuan dan teknologi tersebut adalah pada bidang komunikasi informasi, dahulu komunikasi informasi dilakukan secara sederhana dari mulut ke mulut, selain itu penyebaran informasi juga terbatas oleh adanya jarak dan waktu, sehingga komunikasi relatif sulit untuk dilakukan. Seiring dengan perkembangan teknologi, dan tersedianya sarana dan prasarana komunikasi, maka komunikasi telah menjadi suatu hal yang mudah dilakukan melalui internet. Internet merupakan jalur yang tidak terlalu aman karena merupakan media komunikasi umum yang dapat digunakan secara bebas oleh siapapun sehingga rawan penyadapan informasi oleh pihak-pihak yang tidak bertanggung jawab.

Dengan berkembangnya teknologi telah mempengaruhi aspek keamanan teks dimana teks tersebut dapat berupa pesan, laporan, data atau informasi yang bersifat rahasia, baik untuk keamanan bersama maupun untuk privasi individu. Misalnya seseorang yang biasa menyimpan data-data penting ke dalam suatu file dengan karakter yang tidak terkode sangatlah rawan penyadapan apabila tidak berhati-hati. Apabila data tersebut di simpan dalam suatu komputer yang digunakan secara bebas, bagi siapa saja yang ingin menggunakannya karena seperti saat ini aktifitas pencurian data baik itu terhadap komputer yang terhubung pada suatu jaringan maupun tidak, sudah menjadi hal yang sering terdengar dan tidak asing lagi bagi masyarakat luas. Hal-hal yang berkaitan dengan pengamanan data-data penting tersebut haruslah benar-benar diperhatikan agar data yang akan disampaikan atau masih tersimpan dalam komputer kita tetap aman, karena data yang tidak terjamin kerahasiannya akan dapat dengan mudah dimanfaatkan atau diambil oleh orang yang tidak berhak.

Untuk menjaga keamanan dan kerahasiaan teks maka diperlukan beberapa enkripsi guna membuat teks tersebut tidak dapat dibaca atau dimengerti oleh sembarang orang, kemudian teks tersebut dideskripsi agar dapat dibaca untuk penerima yang berhak disertai dengan menggunakan kunci yang benar. Oleh karena itu, perlu dibangun sebuah Sistem Untuk Enkripsi dan Dekripsi Teks Berbasis Website Menggunakan Algoritma *Vigenere Cipher*, sehingga dengan adanya sistem tersebut mampu memberikan keamanan dan kerahasiaan data berupa teks.

**1.2. Rumusan Masalah**

Berdasarkan latar belakang maka rumusan masalah adalah bagaimana mengimplementasikan algoritma *Vigenere Cipher* dalam menjaga keamanan teks agar pihak yang tidak berwenang kesulitan untuk memecahkan data teks sehingga keamanan dan kerahasiaan tetap terjaga.

**1.3. Batasan Masalah**

Adapun batasan masalah terhadap sistem yang akan dibuat adalah sebagai berikut:

1. Aplikasi ini digunakan untuk enkripsi dan dekripsi sebuah teks.
2. Aplikasi ini menggunakan kunci berlapis dua untuk proses enkripsi maupun dekripsi teks.
3. Tipe *file* yang dapat dienkripsi berupa *file* teks yang berekstensi .txt dengan ukuran maksimal 512 KB dan .docx 2 MB.
4. Hasil enkripsi maupun hasil dekripsi dapat disimpan dalam bentuk *file* teks yang berekstensi .txt dan .docx.
5. Enkripsi dan dekripsi teks menggunakan kode ASCII 7 bit.

**1.4. Tujuan Penelitian**

Penelitian ini bertujuan untuk mengimplementasikan algoritma *Vigenere Cipher* dengan proses enkripsi dan dekripsi teksuntuk menjaga keamanan dan kerahasiaan data berupa teks.

**1.5. Manfaat Penelitian**

Adapun manfaat yang diharapkan dapat terwujud dengan adanya penelitian ini yaitu:

1. Diharapkan dengan adanya aplikasi ini dapat meningkatkan keamanan agar data berupa teks tidak dapat dibaca oleh pihak-pihak yang tidak berhak.
2. Diharapkan dengan adanya aplikasi ini dapat menanggulangi penyadapan terhadap data berupa teks.
3. Diharapkan dapat membantu mengatasi masalah keamanan data berupa teks yang tersimpan dalam komputer baik yang terhubung jaringan maupun tidak.

### 2. LANDASAN TEORI

**2.1 Kajian Hasil Penelitian**

Dalam jurnalnya yang berjudul Bisnis Rental Mobil Melalui Internet (E-Commerce) Menggunakan Algoritma SHA-1 (*Secure Hash Algorithm-1*). Penelitian tersebut membahas keamanan pada sistem *login* baik bagi admin, karyawan dan user dengan menggunakan algoritma SHA-1. Hasil dari sistem ini sangat dibutuhkan untuk keamanan admin dalam mengelola data supir yang keluar, jumlah mobil yang masih ada dan jumlah mobil yang keluar, keamanan untuk karyawan dalam mengelola mobil yang sudah dipesan tetapi belum dibayar dan mobil yang sudah dirental, serta keamanan untuk user dalam penyewaan mobil [1].

Dalam jurnalnya yang berjudul Pengembangan Sistem Keamanan Untuk Toko Online Berbasis Kriptografi AES Menggunakan Bahasa Pemrograman PHP dan MySQL. Penelitian tersebut membahas keamanan pada sesi login baik bagi admin maupun pelanggan. Keamanan pada sistem ini menggunakan algoritma AES (*Advanced Encryption Standard*) dimana login dibatasi hanya dapat dilakukan pada komputer yang t elah diverifikasi, artinya proses login hanya dapat dilakukan pada komputer tertentu. Sistem keamanan ini menjamin admin dalam mengupdate data produk, nomor rekening transaksi dan data lain terkait toko online serta menjamin pelanggan seperti data pemesanan, history transaksi dan data bonus pelanggan [5].

Dalam jurnalnya yang berjudul Aplikasi *Chatting* Rahasia Menggunakan Algoritma *Vigenere Cipher*. Penelitian tersebut membahas tentang keamanan data berupa teks yang disebut sebagai pesan. Aplikasi yang dibuatmenggunakan jaringan LAN (*Local Area Network*) secara *peer to peer* dari *user* 1 ke *user* 2. Agar dapat melakukan pertukaran data, *user* memasukkan alamat IP. Proses enkripsi dan dekripsi pesan menggunakan algoritma *vigenere cipher* dengan menggunakan satu kunci yang telah di sepakati oleh kedua belah pihak, sehingga pesan hanya bisa dibaca oleh orang yang berhak [13].

Perbedaan dari ketiga referensi dengan judul yang diangkat oleh penulis terletak pada algoritma yang digunakan, yaitu dengan penggunaan algoritma *Vigenere Cipher* untuk keamanan data teks agar pihak yang tidak berwenang kesulitan untuk memecahkan data sehingga keamanan dan kerahasiaan tetap terjaga.

**2.2 Dasar Teori**

**2.2.1. Informasi Rahasia**

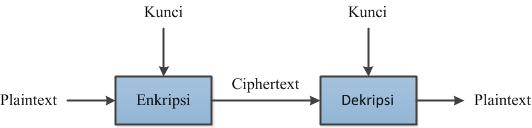
Pengamanan informasi adalah sebuah lingkaran proses yang terjadi secara terus-menerus dengan tujuan mengamankan informasi-informasi penting dan rahasia. Informasi rahasia adalah informasi yang karena nilainya perlu disembunyikan dan dilindungi agar tidak terbuka untuk umum atau jatuh kepada pihak lain. Apabila informasi tersebut diketahui oleh pihak lain, maka akan timbul kerugian pada pihak pemilik informasi. Jenis dan nilai informasi rahasia sangat tergantung pada pemilik, pembuat, atau pengelola informasi tersebut. Untuk informasi yang sama, belum tentu informasi memiliki nilai yang sama. Informasi rahasia bagi satu pihak belum tentu menjadi rahasia bagi pihak yang lain [3]. Informasi rahasia bisa diklarifikasi sesuai kepemilikannya, yaitu:

1. Rahasia Pribadi adalah informasi yang dimiliki oleh masing-masing individu, dimana nilai informasinya sangat lekat dengan kepentingan individu tersebut.
2. Rahasia Perusahaan adalah informasi rahasia yang dimiliki perusahaan dan dilindungi oleh pihak manajemen dan karyawannya dari pihak pesaing.
3. Rahasia Negara adalah informasi yang dimiliki oleh negara dan dilindungi oleh aparat pemerintah dan rakyatnya dari pihak asing. Rahasia negara pada umumnya sangat erat berkaitan dengan kepentingan nasional dan keamanan nasional.

**2.2.2. Definisi Kriptografi**

Kriptografi adalah ilmu yang mempelajari bagaimana supaya pesan atau dokumen kita aman, tidak bisa dibaca oleh pihak yang tidak berhak. Kriptografi juga digunakan untuk identifikasi pengirim pesan dengan tanda tangan digital dan keaslian pesan dengan sidik jari digital (*fingerprint*) [8].

Kriptografi adalah ilmu yang mempelajari bagaimana menyembunyikan pesan, kriptografi juga merupakan ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas [12].



*Gambar 1:**Konsep Enkripsi dan Dekripsi*

Pada Gambar 1 dapat dijelaskan bahwa pesan asli (*plaintext*) dienkripsi melalui kunci. Hasil dari enkripsi adalah berupa *ciphertext* yaitu pesan yang tidak terbaca. Untuk membuka pesan yang tidak terbaca tersebut (*ciphertext*) maka pesan tersebut didekripsi dengan kunci yang sama sehingga menghasilkan pesan teks yang dapat dibaca (*plaintext*).

**2.2.3 Komponen Kriptografi**

Pada dasarnya, kriptografi terdiri dari beberapa komponen [3], yaitu:

1. Enkripsi merupakan hal yang sangat penting dalam kriptografi sebagai pengamanan atas data yang akan dikirimkan agar rahasianya terjaga. Pesan aslinya disebut *plaintext* yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan sebagai *cipher* atau kode.
2. Dekripsi merupakan kebalikan dari enkripsi, pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (*plaintext*), yang disebut dekripsi pesan. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan yang digunakan untuk enkripsi.
3. Kunci adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua bagian yaitu kunci pribadi dan kunci umum.
4. *Ciphertext* merupakan suatu pesan yang sudah melalui proses enkripsi. Pesan yang ada pada *ciphertext* tidak bisa dibaca karena berisi karakter-karakter yang tidak memiliki makna.
5. *Plaintext* atau sering juga disebut *cleartext* merupakan suatu pesan bermakna yang ditulis atau diketik dan *plaintext* itulah yang akan diproses menggunakan algoritma kriptografi agar menjadi *ciphertext*.
6. Pesan bisa berupa data atau informasi yang akan dikirim (melalui kurir, saluran komunikasi data, dan sebagainya) atau disimpan di dalam media perekaman (kertas, storage, dan sebagainya).
7. *Cryptanalysis* bisa diartikan sebagai analisis sandi atau ilmu untuk mendapatkan *plaintext* tanpa harus mengetahui kunci secara wajar. Jika suatu *ciphertext* berhasil menjadi *plaintext* tanpa menggunakan kunci yang sah, maka proses tersebut dinamakan *breaking code* yang dilakukan oleh *cryptanalys*. Analisis sandi juga mampu menemukan kelemahan dari suatu algoritma kriptografi dan akhirnya bisa menemukan kunci atau *plaintext* dari *ciphertext* yang dienkripsi menggunakan algoritma tertentu.

**2.2.4. Tujuan Kriptografi**

Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi [8], yaitu:

1. Autentikasi adalah penerima pesan dapat memastikan keaslian pengirimnya. Penyerang tidak dapat berpura-pura sebagai orang lain.
2. Integritas data adalah penerima pesan harus dapat memeriksa apakah pesan telah dimodifikasi di tengah jalan atau tidak. Seorang penyusup seharusnya tidak dapat memasukkan tambahan ke dalam pesan, mengurangi atau mengubah pesan selama data berada di perjalanan.
3. Non-repudiasi adalah pengirim seharusnya tidak dapat mengelak bahwa dialah pengirim pesan yang sesungguhnya. Tanpa kriptografi, seseorang dapat mengelak bahwa dialah pengirim yang sesungguhnya.
4. Kerahasiaan adalah informasi yang berada pada sistem jaringan seharusnya hanya dapat dimodifikasi oleh pihak yang berwenang. Modifikasi yang tidak diinginkan, dapat berupa penulisan tambahan pesan, pengubahan isi, pengubahan status, penghapusan, pemalsuan, atau menyalin pesan untuk digunakan oleh penyerang.

**2.2.5. Algoritma Kriptografi**

Berdasarkan jenis kunci yang dipakai, algoritma kriptografi dapat dibedakan atas dua jenis [8], yaitu:

1. Algoritma Simetri

Algoritma simetri disebut juga sebagai algoritma konvensional adalah algoritma yang menggunakan kunci enkripsi yang sama dengan kunci dekripsi. Disebut konvensional karena algoritma yang biasa digunakan orang sejak berabad-abad yang lalu adalah algoritma jenis ini. Algoritma simetri sering juga disebut algoritma kunci rahasia, algoritma kunci tunggal, atau algoritma satu kunci, dan mengharuskan pengirim dan penerima menyetujui suatu kunci tertentu sebelum mereka dapat berkomunikasi dengan aman. Keamanan algoritma simetri tergantung pada kunci, membocorkan kunci berarti bahwa orang lain dapat mengenkrip dan mendekrip pesan. Agar kunci tetap aman, kunci harus tetap dirahasiakan. Yang termasuk algoritma kunci simetri adalah OTP, DES, RC2, RC4, RC5, RC6, IDEA, Twofish, Magenta, FEAL, SAFER, LOKI,AES, Blowfish, GOST, dan lain-lain.

1. Algoritma Asimetri

Algoritma asimetri (juga disebut algoritma kunci publik) didesain sedemikian sehingga kunci yang digunakan untuk enkripsi berbeda dari kunci yang digunakan untuk dekripsi. Lebih jauh lagi, kunci dekripsi tidak dapat (sedikitnya dalam waktu yang dapat diterima) dihitung dari kunci enkripsi. Algoritma disebut kunci publik karena kunci enkripsi dapat dibuat publik yang berarti semua orang boleh mengetahuinya. Sembarang orang dapat menggunakan kunci enkripsi tersebut untuk untuk mengenkrip pesan, namun hanya orang tertentu (calon penerima pesan dan sekaligus pemilik kunci dekripsi yang merupakan pasangan kunci publik) yang dapat melakukan dekripsi terhadap pesan tersebut. Dalam sistem ini, kunci enkripsi sering disebut kunci publik, sedangkan kunci dekripsi sering disebut kunci privat. Yang termasuk algoritma asimetri adalah ECC, LUC, RSA, El Gamal dan DH.

**2.2.6. Vigenere Cipher**

*Vigenere cipher* merupakan jenis *cipher* abjad majemuk yang sederhana. *Vigenere cipher* menerapkan metode poli alfabetik dan termasuk ke dalam kategori kunci simetris dimana kunci yang digunakan untuk mengamankan data menggunakan satu kunci. *Vigenere cipher* dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigenere, pada abad 16 (tahun 1586), tetapi algoritma ini baru dikenal luas 200 tahun kemudian [3].

Jika pada *caesar cipher* setiap *ciphertext* selalu menggantikan nilai dari *plaintext* tertentu (tidak peduli apakah jumlah dari *ciphertext* yang ekuivalen dengan *plaintext* tertentu satu atau lebih), pada teknik substitusi *vigenere cipher* setiap *ciphertext* bisa memiliki banyak kemungkinan *plaintext.* Teknik dari substitusi *vigenere* bisa dilakukan dengan dua cara.

a.Angka

Teknik substitusi *vigenere* menukarkan huruf dengan angka. Hal tersebut hampir sama dengan *shift cipher.*

*Tabel 1: Substitusi Angka*

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

Sebagai contoh *plaintext* “PLAINTEXT” dan kunci “CIPHER”.

*Tabel 2:**Contoh Substitusi Angka*

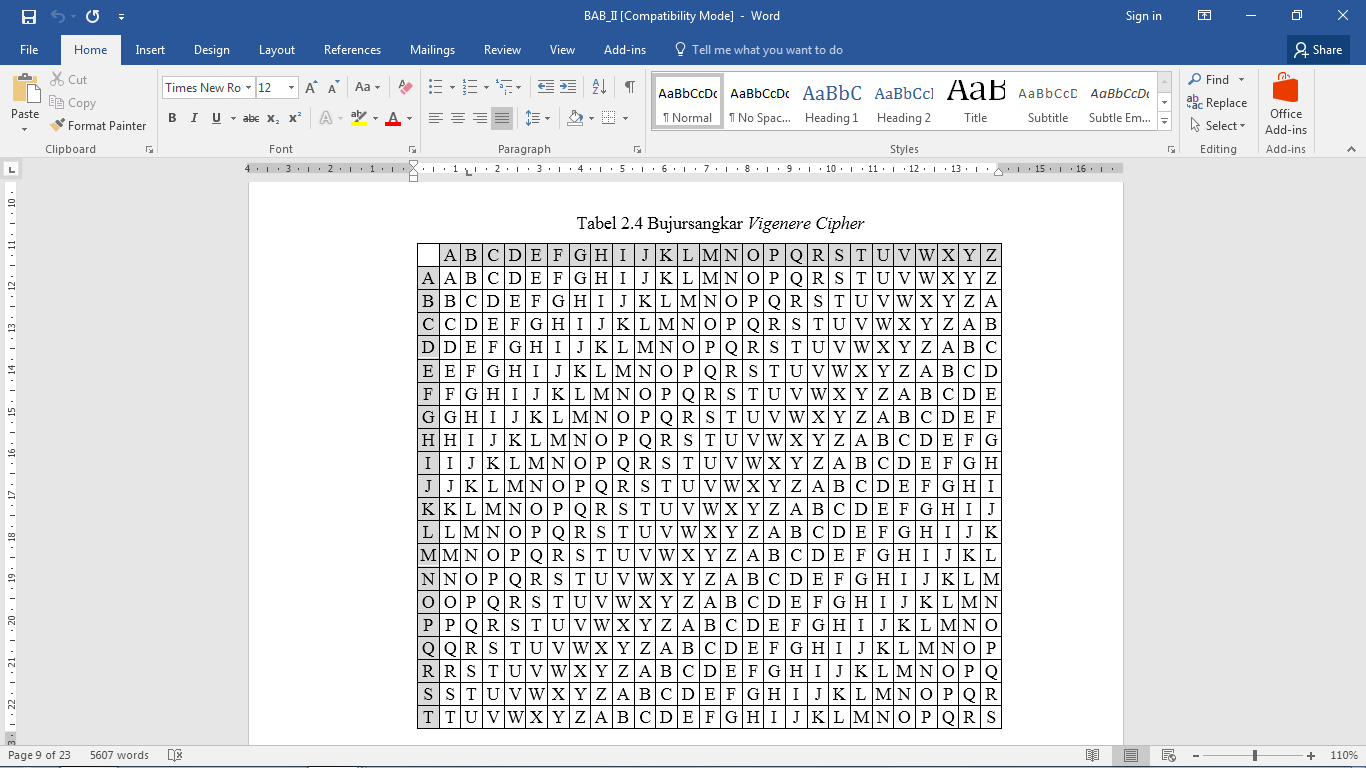
|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Plaintext* | 15 | 11 | 0 | 8 | 13 | 19 | 4 | 23 | 19 |
| Kunci | 2 | 8 | 15 | 7 | 4 | 17 | 2 | 8 | 15 |
| Hasil | 17 | 19 | 15 | 15 | 17 | 10 | 6 | 5 | 8 |
| *Ciphertext* | R | T | P | P | R | K | G | F | I |

Dengan metode pertukaran angka dengan huruf pada tabel 2, diperoleh bahwa teks asli “PLAINTEXT” memiliki kode angka (15, 11, 0, 8, 13, 19, 4, 23, 19), sedangkan kode angka untuk teks kunci “CIPHER” yaitu (2, 8, 15, 7, 4, 17). Setelah dilakukan proses perhitungan, maka dihasilkan kode angka *ciphertext* (17, 19, 15, 15, 17, 7, 4, 17), jika diterjemahkan kembali menjadi huruf sesuai urutan awal maka menjadi huruf “RTPPRKGFI”. Untuk melakukan dekripsi, digunakan kunci yang sama dengan modulo 26.

b. Huruf

Ide dasarnya adalah menggunakan *caesar cipher,* tetapi jumlah pergeseran hurufnya berbeda-beda untuk setiap periode pada beberapa huruf tertentu. Untuk mengenkripsikan pesan menggunakan *vigenere cipher*, digunakan *tabula recta* (disebut juga bujursangkar *Vigenere*) seperti pada tabel 3.

*Tabel 3:**Bujursangkar Vigenere Cipher*



*Tabula recta* digunakan untuk memperoleh *ciphertext* menggunakan kunci yang sudah ditentukan. Jika ukuran kunci lebih pendek daripada *plaintext*, maka penggunaan kunci diulang. Cara menentukan *ciphertext* menggunakan bujursangkar *vigenere* bisa dilihat pada posisi horizontal merupakan *plaintext* dan pada posisi vertikal merupakan kunci. Jika pada *plaintext* huruf K, maka lihat posisi huruf K pada *plaintext* bujursangkar *vigenere.* Jika pada kunci huruf K, maka lihat posisi huruf K pada kunci bujursangkar *vigenere*. Jika sudah menemukan, tarik garis lurus kebawah dari *plaintext* dan garis lurus ke samping dari posisi kunci, sehingga ditemukan huruf U. Dengan begitu, huruf U akan menjadi *ciphertext* dan begitulah seterusnya. Secara matematis proses enkripsi dinyatakan dengan persamaan 1:

(1)

Keterangan:

= *ciphertext* (hasil teks terenkripsi)

= *plaintext* (teks asli)

= kunci

Sebagai contoh kalimat “KEAMANAN DATA MENGGUNAKAN VIGENERE CIPHER” akan dilakukan proses enkripsi dengan menggunakan kunci “Kriptografi”. Perhitungan huruf K dienkripsi dengan kunci K sebagai berikut:

(K + K) mod 26 = (10 + 10) mod 26 = 20 = U

Hal yang sama dilakukan untuk semua huruf, sehingga dihasilkan sebagai berikut:

*Plaintext* : KEAMANAN DATA MENGGUNAKAN VIGENERE CIPHER

Kunci : KRIPTOGRAFI

*Ciphertext* : UVIBTBGE DFBK DMCZUAESPIX MQVXBKIE HQZYMG

Untuk mendekripsi pesan, penerima pesan harus mengetahui kunci yang digunakan. Dekripsi dilakukan dengan cara yang berkebalikan, yaitu menarik garis mendatar dari huruf kunci sampai ke huruf *ciphertext* yang dituju, lalu dari *ciphertext* tarik garis vertikal ke atas sampai ke huruf *plaintext*. Misalnya, pada huruf pertama kunci adalah K dan huruf pertama *ciphertext* adalah U, kemudian tarik garis mendatar dari huruf K sampai ke huruf U, lalu dari huruf U tarik garis vertikal ke atas sampai ke huruf *plaintext* yaitu K. Secara matematis proses dekripsi dinyatakan dengan persamaan 2:

(2)

Keterangan:

= *ciphertext* (hasil teks terenkripsi)

= *plaintext* (teks asli)

= kunci

Perhitungan huruf U didekripsi dengan kunci K sebagai berikut:

(U - K) mod 26 = (20 - 10) mod 26 = 10 = K

Hal yang sama dilakukan untuk semua huruf, sehingga dihasilkan sebagai berikut:

*Ciphertext* : UVIBTBGE DFBK DMCZUAESPIX MQVXBKIE HQZYMG

Kunci : KRIPTOGRAFI

*Plaintext* : KEAMANAN DATA MENGGUNAKAN VIGENERE CIPHER

Salah satu kelebihan *vigenere cipher* adalah kesulitan melakukan *cryptanalysis* dengan metode analisis frekuensi. Pada *vigenere cipher*, sulit untuk melakukan *cryptanalysis* dengan analisis frekuensi karena dua huruf yang sama dalam *ciphertext* belum tentu bisa didekripsi menjadi dua huruf yang sama dalam *plaintext.* Kelemahan utama *vigenere cipher* adalah kuncinya yang pendek dan penggunaannya yang berulang. Jika *cryptanalysis* bisa menentukan panjang kuncinya, maka *ciphertext* bisa diperlakukan seperti rangkaian beberapa *caesar cipher.*

**2.2.7 PHP**

PHP adalah bahasa *server-side scripting* yang menyatu dengan HTML untuk membuat halaman web yang dinamis. Karena PHP merupakan *server-side scripting* maka sintaks dan perintah-perintah PHP akan dieksekusi di server kemudian hasilnya dikirimkan ke browser dalam format HTML. Dengan demikian kode program yang ditulis dalam PHP tidak akan terlihat oleh user sehingga keamanan halaman web lebih terjamin. PHP dirancang untuk membentuk halaman web yang dinamis, yaitu halaman web yang dapat membentuk suatu tampilan berdasarkan permintaan terkini, seperti menampilkan isi basis data ke halaman web [2].

PHP sebagai alternatif lain memberikan solusi dangat murah (karena garatis digunakan) dan dapat berjalan diberbagai jenis platform. PHP adalah skrip bersifat *server-side* yang ditambahkan ke dalam HTML. PHP sendiri merupakan singkatan dari *Personal Home Page Tools*. Skrip ini akan membuat suatu aplikasi dapat diintegrasikan kedalam HTML sehingga suatu halaman web tidak lagi bersifat statis, namun menjadi bersifat dinamis. Sifat *server-side* berarti pengerjaan skrip dilakukan di server, baru kemudian hasilnya di kirimkan ke browser [9].

### 3. METODOLOGI PENELITIAN

Untuk mengurangi terjadinya kesalahan dalam pengambilan data saat melakukan penelitian, maka pengambilan data tersebut dilakukan dengan menggunakan beberapa metodologi penelitian yang umum digunakan.

**3.1. Analisis Sistem**

Yaitu proses mengidentifikasi dan mengevaluasi permasalahan yang terjadi dan kebutuhan yang diharapkan. Langkah-langkah yang harus dilaksanakan dalam analisis sistem:

1. Mengidentifikasi masalah, seseorang yang biasa menyimpan data-data penting ke dalam suatu *file* dengan karakter yang tidak terkode sangatlah rawan penyadapan apabila tidak berhati-hati. Apabila data tersebut di simpan dalam suatu komputer yang digunakan secara bebas, bagi siapa saja yang ingin menggunakannya karena seperti saat ini aktifitas pencurian data baik itu terhadap komputer yang terhubung pada suatu jaringan maupun tidak, sudah menjadi hal yang sering terdengar dan tidak asing lagi bagi masyarakat luas. Hal-hal yang berkaitan dengan pengamanan data-data penting tersebut haruslah benar-benar diperhatikan agar data yang akan disampaikan atau masih tersimpan dalam komputer kita tetap aman, karena data yang tidak terjamin kerahasiannya akan dapat dengan mudah dimanfaatkan atau diambil oleh orang yang tidak berhak.
2. Melakukan perbandingan sistem dengan sistem yang sejenis untuk mendapatkan dekripsi dan kesimpulan untuk melakukan tahap perancangan sistem.
3. Memahami algoritma *vigenere cipher* yang diterapkan pada sistem untuk enkripsi dan dekripsi teks.

**3.2. Perancangan Sistem**

Perancangan sistem merupakan uraian tentang rancangan dari desain sistem. Rancangan sistem dibangun dari desain *file*, desain diagram, desain tabel, relasi tabel dan sebagainya, sehingga membentuk sistem lengkap sesuai dengan fungsi-fungsi yang dikehendaki dan menghasilkan rancangan data dan rancangan *interface* yang sesuai.

**3.3. Implementasi Sistem**

Tahap implementasi sistem merupakan tahap meletakkan sistem supaya siap untuk dioperasikan. Aplikasi akan diimplementasikan berbasis *website* dengan *interface user friendly*. Metode ini mewujudkan hasil rancangan menjadi perangkat lunak. Sistem enkripsi dan dekripsi ini dibangun menggunakan aplikasi Sublime Text 3 sebagai *compailernya* dan basisdata yang digunakan adalah MySQL. Untuk menjalankan aplikasi menggunakan web browser Mozila Firefox, Google Chrome, dan web browser lainnya.

**3.4. Pembuatan laporan**

Menyusun laporan dengan permasalahan yang sudah ada secara sistematis, diambil dari permasalahan yang sudah dianalisis. Penyusunan laporan sesuai dengan panduan umum penulisan sehingga laporan tersusun secara sistematis.

**4. HASIL DAN PEMBAHASAN**

**4.1. Analisis Sistem**

Saat ini, sangatlah rawan apabila sebuah organisasi maupun individu yang menyimpan data-data penting kedalam suatu *file* dengan karakter yang tidak terkode. Data penting yang berformat .txt dan .docx seperti teks biasa, kode sumber program (*source code* program), soal ujian, surat, laporan, dan data teks penting lainnya. Untuk data berformat .docx dapat disandikan menggunakan password karena Microsoft Word memiliki fitur enkripsi. Namun, fitur enkripsi pada Microsoft Word tersebut memiliki kelemahan, yaitu adanya aplikasi yang dapat digunakan untuk membobol *file* yang telah terenkripsi. Data penting yang berformat .txt dan .docx tersebut mudah sekali disadap apabila data-data disimpan dalam suatu komputer yang digunakan secara bebas, baik itu komputer yang terhubung pada suatu jaringan maupun tidak. Data penting tersebut biasanya bersifat rahasia dan tidak ingin diketahui oleh pihak yang tidak berhak. Jika keamanan data ini tidak dapat dijaga, pihak-pihak yang tidak berhak dapat memanfaatkan data tersebut sehingga merugikan pihak yang berhak atas data tersebut.

Untuk mengatasi hal tersebut, sistem enkripsi dan dekripsi teks menggunakan algoritma *vigenere cipher* sangat berperan dalam memecahkan permasalahan mengenai penyadapan data teks yang tidak terkode, baik yang disimpan dalam komputer yang terhubung dengan jaringan maupun tidak. Sistem enkripsi dan dekripsi teks mempunyai kemampuan untuk mengenkripsi dan mendekripsi teks yang berekstensi .txt dengan ukuran maksimal 512 KB dan .docx 2 MB. Dengan kemampuan tersebut dapat membantu sebuah organisasi maupun individu dalam meningkatkan keamanan dan kerahasian data yang bersifat rahasia.

**4.2. Analisis Kebutuhan**

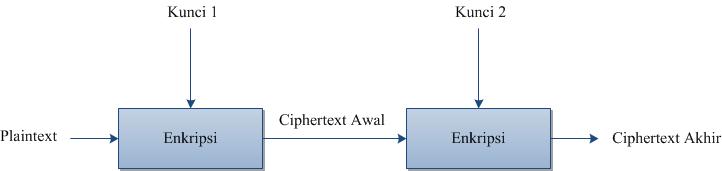
Berdasarkan analisis yang dilakukan, dapat diambil kesimpulan bahwa diperlukan sistem enkripsi dan dekripsi teks menggunakan algoritma *vigenere cipher* yang bertujuan untuk memudahkan sebuah organisasi maupun individu dalam menjaga kerahasiaan data yang bersifat rahasia. Sistem yang dibutuhkan adalah sebagai berikut:

1. Sistem yang dapat melakukan enkripsi dan dekripsi data teks yang berekstensi .txt dengan ukuran maksimal 512 KB dan .docx 2 MB.
2. Sistem yang dapat menyimpan hasil enkripsi maupun dekripsi dalam bentuk *file* .txt dan .docx.
3. Sistem yang dapat melakukan enkripsi maupun dekripsi dengan kunci berlapis dua.

**4.3. Analisis Enkripsi dan Dekripsi**

Analisis enkripsi dan dekripsi merupakan penjelasan mengenai proses enkripsi dan dekripsi yang akan digunakan dalam sistem. Pada penelitian ini, untuk proses enkripsi dan dekripsi teks menggunakan kode ASCII 7 bit yang dapat dilihat pada tabel 2.5. Untuk meningkatkan kekuatan dari hasil *ciphertext vigenere*, maka dibuatkannya kunci lebih dari satu (kunci berlapis). Dalam penelitian ini penulis membuat lapisan kunci sebanyak dua lapisan. Berikut langkah-langkah yang digunakan untuk mengenkripsi teks:

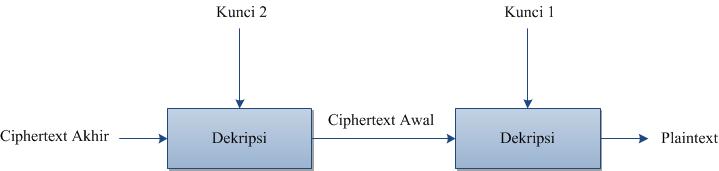
1. Ubah kunci dan *plaintext* kedalam urutan bilangan desimal ASCII.
2. Tambahkan nilai kunci 1 dan nilai *plaintext*, kemudian hasilnya di modulo 128. Dari hasil tersebut didapat nilai *ciphertext* awal. Apabila ukuran *plaintext* lebih panjang daripada kunci 1, maka penggunaan kunci 1 diulang sesuai panjang *plaintext.*
3. Tambahkan nilai kunci 2 dan nilai *ciphertext* awal, kemudian hasilnya di modulo 128. Dari hasil tersebut didapat nilai *ciphertext* akhir. Apabila ukuran *ciphertext* awal lebih panjang daripada kunci 2, maka penggunaan kunci 2 diulang sesuai panjang *ciphertext* awal.
4. Ubah kembali hasil nilai *ciphertext* akhir kedalam karakter ASCII.



*Gambar 2:**Langkah-langkah Enkripsi*

Berikut langkah-langkah yang digunakan untuk mendekripsi teks:

1. Ubah *ciphertext* akhir dan kunci 2 ke dalam urutan bilangan desimal ASCII.
2. Pada masing-masing urutan bilangan yang merupakan *ciphertext* akhir kurangkan dengan nilai kunci 2, kemudian hasilnya di modulo 128. Dari hasil tersebut didapat nilai *ciphertext* awal.
3. Pada masing-masing urutan bilangan yang merupakan *ciphertext* awal kurangkan dengan nilai kunci 1, kemudian hasilnya di modulo 128. Dari hasil tersebut didapat nilai *plaintext.*
4. Ubah kembali hasil nilai *plaintext* kedalam karakter ASCII.



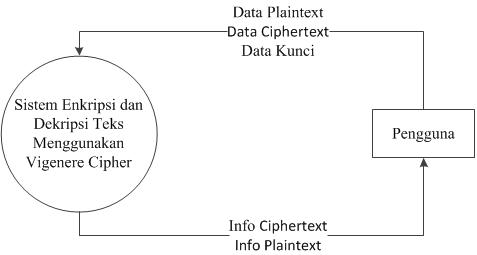
*Gambar 3:**Langkah-langkah Dekripsi*

**4.4 Perancangan Sistem**

Perancangan sistem merupakan bagian yang paling penting dalam perancangan sistem enkripsi dan dekripsi teks menggunakan algoritma *vigenere cipher*. Perancangan sistem dapat diartikan gambaran atau sketsa dari alur proses sistem pengolahan data. Dalam perancangan sistem dapat menggunakan diagram konteks, diagram jenjang dan diagram arus data (DAD) atau *Data Flow Diagram* (DFD).

**4.4.1. Diagram Konteks**

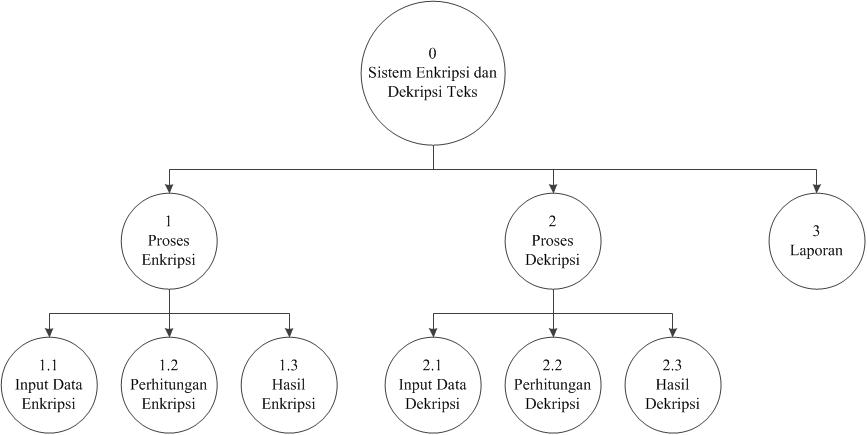
Secara garis besar rancangan diagram konteks digunakan untuk menggambarkan sistem secara umum. Adapun diagram konteks untuk sistem enkripsi dan dekripsi teks menggunakan algoritma *vegenere cipher* dapat dilihat pada gambar 4.

****

*Gambar 4****:*** *Diagram Konteks*

**4.4.2 Diagram Jenjang**

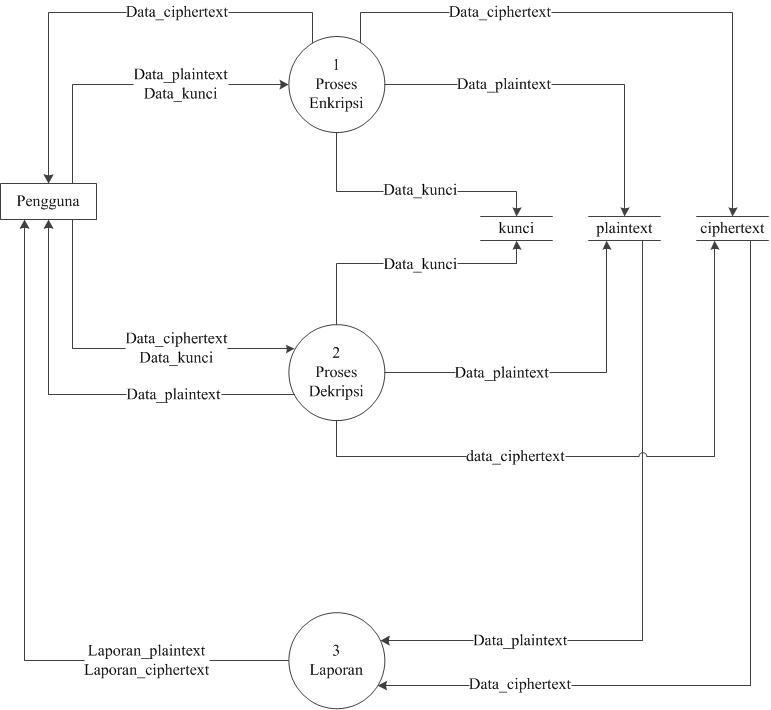
Diagram jenjang digunakan untuk mengatur jalannya sistem baik dari sistem awal sampai akhir, dimana di tunjukkan pada beberapa level, level 0 digunakan untuk nama sistem yaitu sistem enkripsi dan dekripsi teks, level 1 dugunakan untuk sebuah proses enkripsi, proses dekripsi dan proses laporan, kemudian dilanjutkan dengan proses 2 yang masing-masing dibawah level 1. Diagram jenjang ini dapat dilihat pada gambar 5.



*Gambar 5:**Diagram Jenjang*

**4.4.3. Diagram Arus Data Level 1**

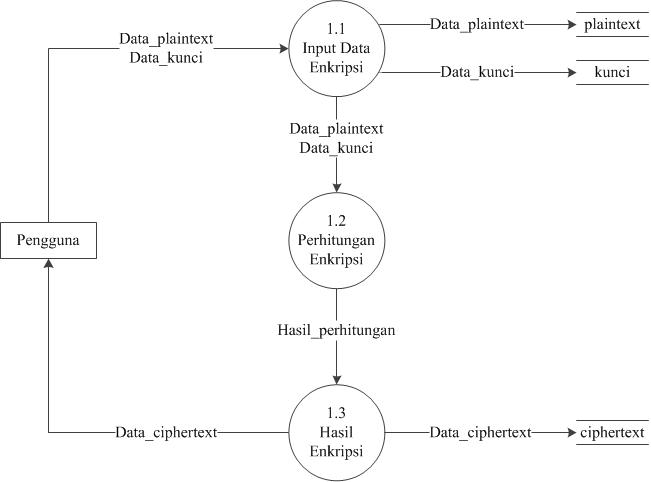
Diagram arus data level 1 menerangkan tentang proses enkripsi, proses dekripsi, serta laporan. Pada proses ini menggambarkan sebuah level yang dikelola oleh masing-masing data sesuai dengan kebutuhan dan selanjutnya diteruskan ke sistem dan disimpan pada database yang disediakan oleh sistem. Diagram arus data level 1 untuk sistem enkripsi dan dekripsi teks dapat dilihat pada gambar 6.



*Gambar 6:**Diagram Arus Data Level 1*

**4.4.4. Diagram Arus Data Level 2 Proses Enkripsi**

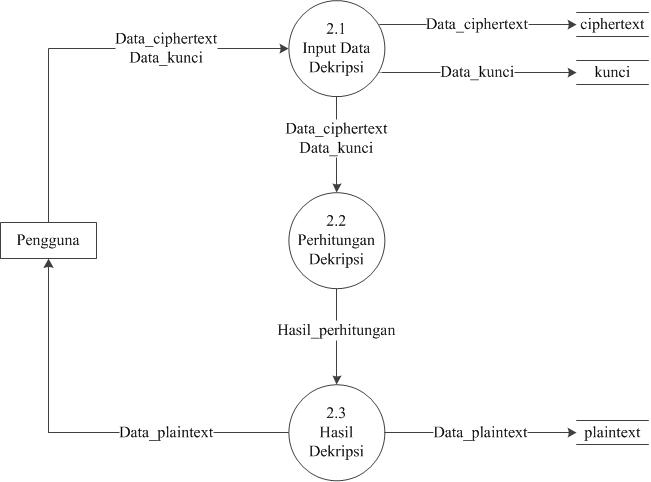
Diagram arus data level 2 proses enkripsi merupakan gambaran dari proses enkripsi yaitu input data enkripsi, perhitungan enkripsi, dan hasil enkripsi. Diagram arus data level 2 proses enkripsi dapat dilihat pada gambar 7.



*Gambar 7:**Diagram Arus Data Level 2 Proses Enkripsi*

**4.4.5. Diagram Arus Data Level 2 Proses Dekripsi**

Diagram arus data level 2 proses dekripsi merupakan gambaran dari proses dekripsi yaitu input data dekripsi, perhitungan dekripsi, dan hasil dekripsi. Diagram arus data level 2 proses dekripsi dapat dilihat pada gambar 8.



*Gambar 8:**Diagram Arus Data Level 2 Proses Dekripsi*

**4.5 Implementasi**

Implementasi sistem merupakan tahap meletakkan sistem yang baru dikembangkan supaya sistem siap dioperasikan sesuai dengan yang diharapkan. Salah satu yang termasuk dalam tahap ini adalah kegiatan menulis kode program yang digunakan. Adapun tujuan dari tahap implementasi ini adalah menyiapkan semua kegiatan penerapan sistem sesuai dengan perancangan sistem pada bab sebelumnya, sehingga alur program akan mengikuti alur penggambaran diagram sistem.

**4.5.1. Tampilan Halaman Utama**

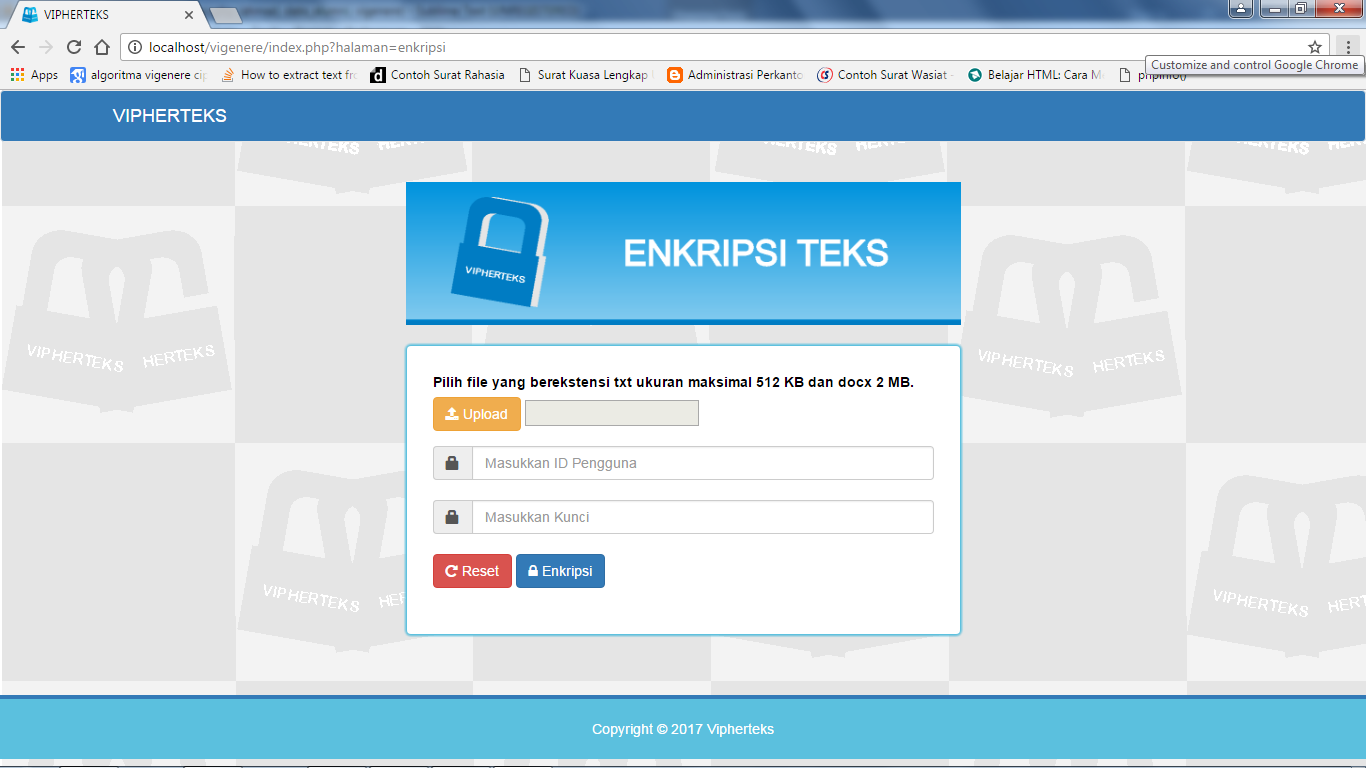
Halaman utama merupakan halaman yang pertama akan tampil apabila pengguna membuka *Website* Sistem Enkripsi dan Dekripsi Teks Menggunakan Algoritma *Vigenere Cipher*. Pada halaman ini pengguna dapat memilih menu enkripsi, dekripsi, dan simulasi. Adapun tampilan halaman utama dapat dilihat pada gambar 9.



*Gambar 9: Tampilan Halaman Utama*

**4.5.2. Tampilan Halaman Enkripsi**

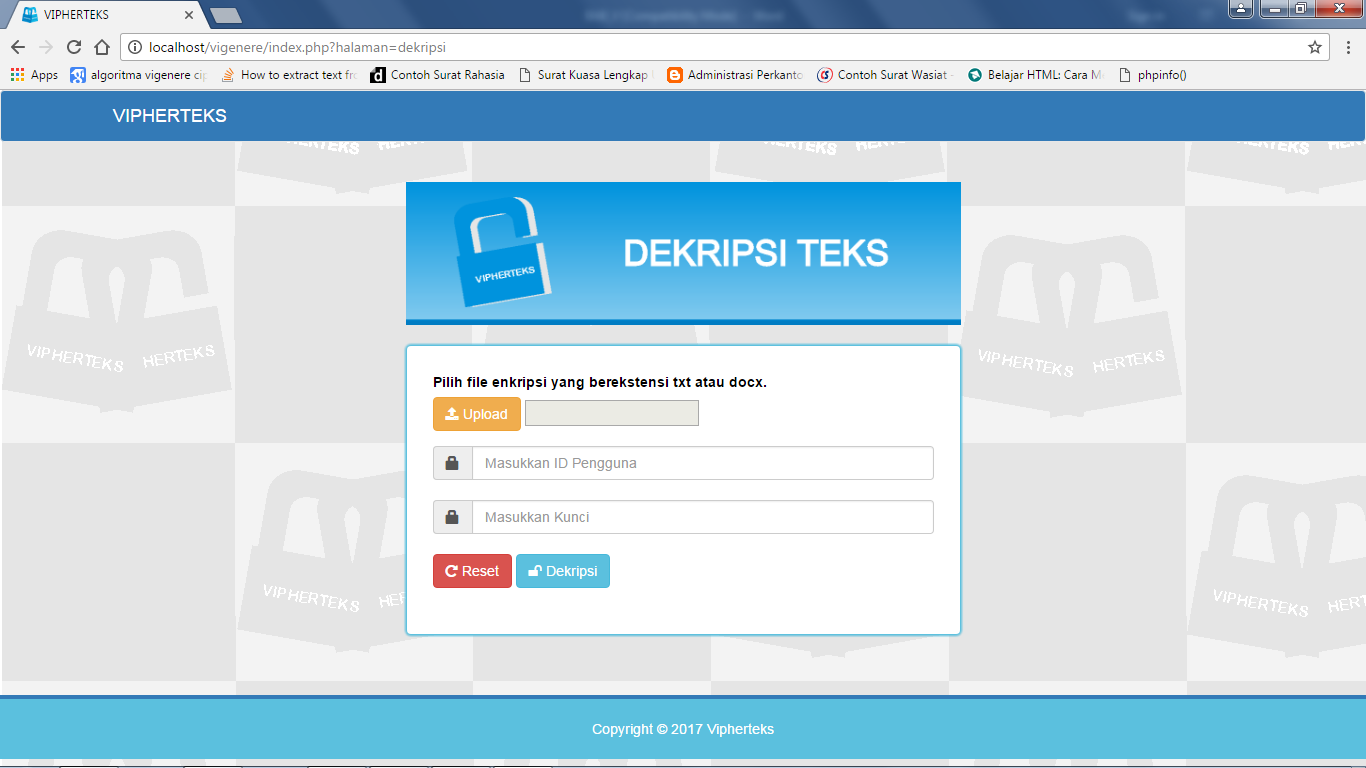
Halaman enkripsi merupakan halaman yang akan muncul setelah pengguna memilih menu enkripsi pada halaman utama. Pada halaman enkripsi ini terdapat tombol reset yang berfungsi untuk mereset inputan dan terdapat tombol enkripsi untuk melakukan proses enkripsi. Untuk melakukan proses enkripsi, pengguna dapat memilih *file* .txt dengan ukuran maksimal 512 KB dan .docx 2 MB, kemudian pengguna memasukkan kunci 1 dan kunci 2 yang bersifat rahasia. Setelah itu, pengguna memilih tombol enkripsi dan hasil enkripsi akan terdownload dalam bentuk *file*. Adapun tampilan halaman enkripsi dapat dilihat pada gambar 10.



*Gambar10:**Tampilan Halaman Enkripsi*

**4.5.3. Tampilan Halaman Dekripsi**

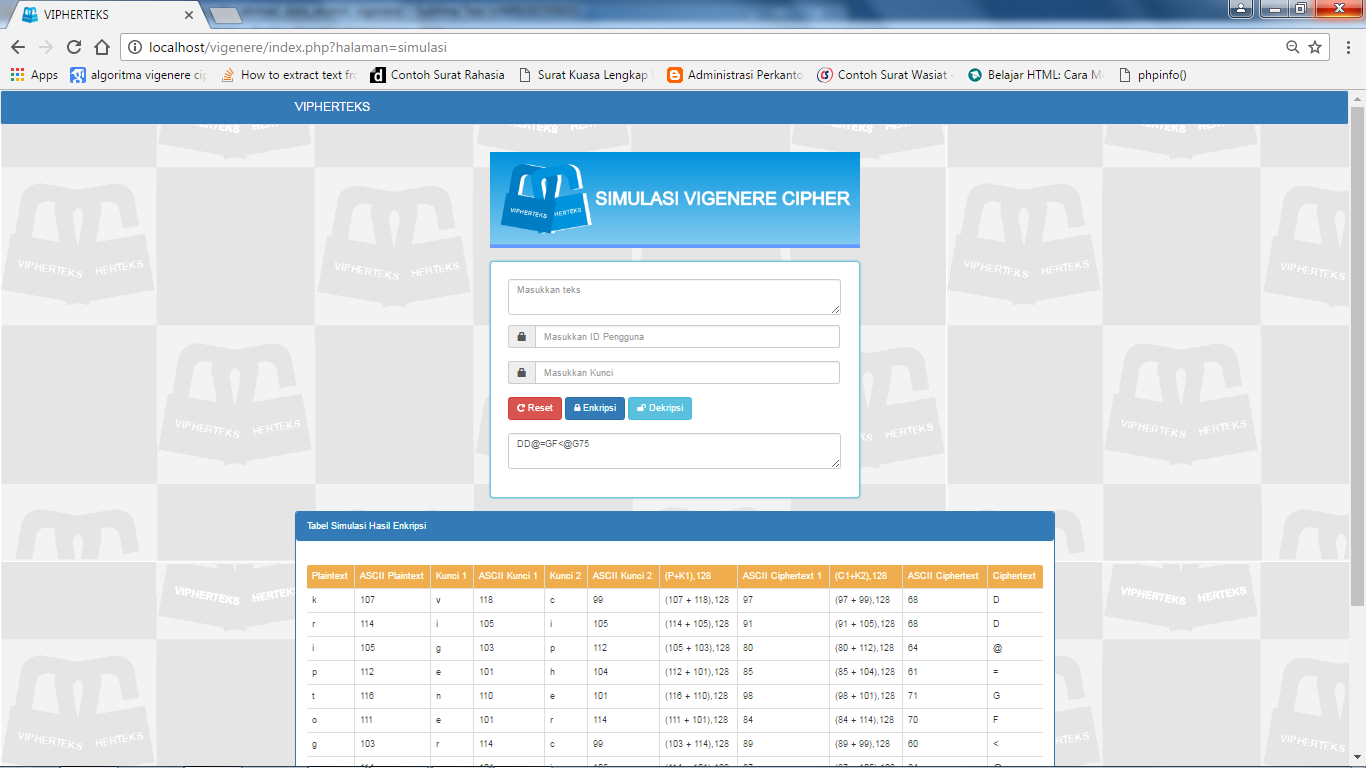
Halaman dekripsi merupakan halaman yang akan muncul setelah pengguna memilih menu dekripsi pada halaman utama. Pada halaman dekripsi ini terdapat tombol reset yang berfungsi untuk mereset inputan dan terdapat tombol dekripsi untuk melakukan proses dekripsi. Untuk melakukan proses dekripsi, pengguna dapat memilih *file* .txt atau .docx yang telah terenkripsi, kemudian pengguna memasukkan kunci 1 dan kunci 2 yang sama saat enkripsi. Setelah itu, pengguna memilih tombol dekripsi dan hasil dekripsi akan terdownload dalam bentuk *file*. Adapun tampilan halaman dekripsi dapat dilihat pada gambar 11.



*Gambar 11:**Tampilan Halaman Dekripsi*

**4.5.4. Tampilan Halaman Simulasi**

Halaman simulasi merupakan halaman yang akan muncul setelah pengguna memilih menu simulasi pada halaman utama. Pada halaman simulasi ini terdapat tombol reset yang berfungsi untuk mereset inputan dan terdapat tombol enkripsi untuk melakukan proses simulai enkripsi serta terdapat tombol dekripsi untuk melakukan proses simulasi dekripsi. Hasil dari proses simulasi enkripsi maupun dekripsi akan ditampilkan pada tabel. Adapun tampilan halaman simulasi dapat dilihat pada gambar 12.



*Gambar 12:**Tampilan Halaman Simulasi*

**5. PENUTUP**

**5.1. Kesimpulan**

Berdasarkan penelitian yang dilakukan penulis tentang Implementasi Algoritma *Vigenere Cipher* untuk Enkripsi dan Dekripsi Teks Berbasis *Website*, penulis mengambil kesimpulan sebagai berikut:

1. Sistem mampu melakukan enkripsi maupun dekripsi *file* yang berekstensi .txt dan .docx.
2. Sistem mampu melakukan enkripsi maupun dekripsi dengan kunci berlapis dua.
3. Sistem mampu melakukan enkripsi *file* .txt dengan ukuran maksimal 512 KB dan .docx 2 MB.
4. Implementasi enkripsi dan dekripsi dengan algoritma *vigenere cipher* pada kode ASCII memberikan kemungkinan yang luas dan lebih banyak karakter yang tercakup, tidak hanya terbatas pada 26 alfabet.
5. Sistem memberikan kemudahan bagi masyarakat individu maupun organisasi dalam meningkatkan keamanan data teks yang bersifat rahasia.
6. Vigenere cipher memiliki rangkaian perulangan kata pada hasil enkripsi. Hal ini dikarenakan kunci yang digunakan untuk penyandian diulang sampai beberapa kata sesuai panjang karakter pesan.

**5.2. Saran**

Dari hasil penelitian yang dilakukan didapatkan saran-saran guna pengembangan lebih lanjut terhadap sistem. Saran-saran tersebut yaitu:

1. Dalam pengembangan sistem ini dapat menambahkan ekstensi *file* teks lainnya (.pdf, .ppt, .doc, .xlsx, .rtf).
2. Dalam pengembangan sistem ini dapat mengenkripsi dan mendekripsi sebuah citra.
3. Penelitian selanjutnya dapat meneliti tentang efektifitas penggunaan memori dan tingkat kecepatan enkripsi.
4. Proses enkripsi dan dekripsi dapat dibuat lebih efisien baik dalam hal penggunaan variabel, tipe data, maupun lainnya, sehingga penggunaan *resource* dapat lebih dimaksimalkan.
5. Penelitian selanjutnya dapat melakukan modifikasi dengan pendekatan Keystream Generator pada pembangkitan kunci, sehingga dapat menambah kekuatan algoritma.

**Daftar pustaka**

[1] Abdullah, D. dan Erliana, C.I. (2013), *Bisnis Rental Mobil Melalui Internet (E-Commerce) Menggunakan Algoritma SHA-1 (Sequre Hash Algorithm-1)*, *Indonesian Jurnal on Computer Science,* 10(4), 152-159.

[2] Arief, M.R. (2011), *Pemrograman Web Dinamis Menggunakan PHP & MySQL,* Yogyakarta: Andi Offset.

[3] Ariyus, D. (2009), *Keamanan Multimedia,* Yogyakarta: Andi Offset.

[4] Ariyus, D. dan Andri, K.R.R. (2008), *Komunikasi Data,* Yogyakarta: Andi Offset.

[5] Candra, B. Wahyudi, J. dan Hermawansyah (2014), *Pengembangan Sistem Keamanan Untuk Toko Online Berbasis Kriptografi AES Menggunakan Bahasa Pemrograman PHP dan MySQL, Media Infotama,* 11(1), 31-34.

[6] Hariyanto, B. (2008), *Dasar Informatika & Ilmu Komputer,* Yogyakarta: Graha Ilmu.

[7] Kristanto, A. (2008), *Perancangan Sistem Informasi dan Aplikasinya,* Yogyakarta: Gava Media.

[8] Kurniawan, Y. (2004), *Kriptografi Keamanan Internet dan Jaringan Komunikasi,* Bandung: Informatika Bandung.

[9] Kustiyahningsih, Y. dan Anamisa, D.R. (2011), *Pemrograman Basis Data Berbasis Web Menggunakan PHP & MySQL*, Yogyakarta: Graha Ilmu.

[10] Nugroho, A. (2011), *Perancangan dan Implementasi Sistem Basis Data,* Yogyakarta: Andi Offset.

[11] Nugroho, B. (2005), *Database Relasional dengan MySQL,* Yogyakarta: Andi Offset.

[12] Sadikin, R. (2012), *Kriptografi Untuk Keamanan Jaringan,* Yogyakarta: Andi Offset.

[13] Yulianingsih, P., Hamdani dan Maharani, S. (2014), *Aplikasi Chatting Rahasia Menggunakan Algoritma Vigenere Cipher, Informatika Mulawarman,* 9(1), 19-22.