BAB I
PENDAHULUAN

1.1 Latar Belakang

Kriptografi memiliki sejarah yang sudah sangat lama sekitar 4000 tahun yang lalu yang pertama kali digunakan oleh orang-orang mesir saat terjadi perang. Kriptografi digunakan untuk penyandian pesan yang diberikan kepada pasukan militer saat melakukan perang di lapangan. Di mana dengan kriptografi pesan tersebut tidak dapat dibaca oleh lawan saat di medan perang meskipun pembawa pesan tertangkap dan disandra. Pada zaman romawi Julius Caesar akan mengirimkan pesan rahasia kepada Jendral untuk merahasiakan pesan supaya tidak dapat dibaca Julius Caesar mengacak pesan tersebut dan hanya Jendral saja yang dapat membacanya. Dan sebelum Jendral berada di medan perang Julius sudah memberi kunci cara membaca pesan tersebut. Julius Caesar mengganti alfabet dari a menjadi b, b menjadi c dan seterusnya. Dari pengacakan kata rahasia tersebut kriptografi dipergunakan untuk memberi aktifitas-aktifitas rahasia (Kurniawan, 2004).

Kriptografi merupakan seni dan ilmu yang digunakan untuk menjaga keamanan pesan (Kurniawan, 2004). Kriptografi adalah ilmu mengenai teknik enkripsi di mana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi (Sentot, 2009). Pertukaran informasi ataupun data dapat dikirim berbagai macam bentuknya, dapat pengiriman gambar, teks , suara, dan video. Pada penelitian ini pertukaran informasi ataupun data hanya fokus pada teks, karena teks yang paling sering digunakan dalam melakukan komunikasi. Pengamanan informasi ataupun data yang berupa teks dilakukan dengan menggunakan kriptografi pada saat melakukan pengiriman informasi ataupun data. Kriptografi digunakan untuk mengamankan pesan yang mana kekuatan keamanan terdapat pada kunci yang digunakan. Kunci pada kriptografi digunakan untuk menjembatani saat dilakukannya proses enkripsi-deskripsi atau deskripsi-enkripsi. Pada kunci kriptografi dibedakan menjadi dua

bagian yaitu kunci simetris dan kunci asimetris. Oleh sebab itu dibuatlah sebuah aplikasi yang berfungsi untuk mengamankan pesan teks yang digunakan saat melakukan pertukaran informasi menggunakan metode Bahasa Jawa Walikan. Metode Bahasa Jawa Walikan ini hampir mirip dengan ROT13 yang banyak digunakan dalam kriptografi tradisional di mana karakter akan diganti dengan jaraknya 13 (tigabelas) dari karakter aslinya atau dalam karakter romawi, hurufnya dibagi dua dari 26 (dua puluh enam) huruf yang ada.

Bahasa Jawa Walikan yang digunakan di dalam penelitian ini merupakan Bahasa Jawa Walikan Yogya. Bahasa Walikan Yogya yang bersumber dari karakter dari huruf Jawa yaitu Aksara Jawa yang ditulis dengan aturan mundur dua baris. Dalam karakter bahasa romawi menjadi ha, na, ca, ra, ka, da, ta, sa, wa, la, pa, dha, ja, ya, nya, ma, ga, ba, tha, nga. Karakter huruf Jawa ini ditulis dalam 4 (empat) baris di mana proses pembalikan huruf atau karakter pada Bahasa Jawa Walikan menggunakan mekanisme baris pertama ditukar baris ketiga dan baris kedua ditukar baris keempat begitu juga sebalikanya (Kurniawati, 2012). Proses pertukaran ini tidak bisa dipahami oleh semua orang yang bisa berbahasa Jawa sehingga dalam penelitian ini dibuatlah perangkat lunak untuk membantu proses penterjemahan dari dan ke Bahasa Jawa Walikan.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang masalah yang telah dipaparkan di atas, maka didapatkan perumusan masalah dalam tugas akhir sebagai berikut:

1. Bagaimana cara membuat aplikasi pengamanan pesan dengan kriptografi menggunakan metode Bahasa Jawa Walikan?
2. Bagaimana cara mengamankan pesan pada sebuah aplikasi berupa teks tanpa mengubah menjadi angka, gambar dalam pertukaran pesan?

1.3 Batasan Masalah

Berdasarkan rumusan masalah yang telah dipaparkan di atas didapatkan batasan masalah sebagai berikut:

1. Aplikasi berbasis *web*

2. Menggunakan metode Bahasa Jawa Walikan yogyakarta yaitu metode perubahan kata menggunakan urutan *hanacaraka* yang ditukar setiap barisnya.
3. *Output* untuk hasil deskripsi berupa teks dan Aksara Jawa bukan cara membaca.
4. Aksara Jawa hanya berupa gambar dan tidak menggunakan aksara pasangan.
5. Penulisan Aksara Jawa untuk huruf e menggunakan *sandhangan taling*.
6. Penulisan Aksara Jawa tidak menggunakan *sandhangan paten* untuk aksara mati ra, aksara mati ha, aksara mati nga hanya menggunakan *pangkon* untuk aksara mati.

1.4 Tujuan dan Manfaat Penelitian

Adapun tujuan dari tugas akhir ini adalah :

1. Membangun aplikasi kriptografi pada pesan teks menggunakan metode Bahasa Jawa Walikan berbasis *web*.
2. Mengetahui hasil implementasi metode Bahasa Jawa Walikan untuk kriptografi.

Sesuai dengan permasalahan dan tujuan yang telah dipaparkan di atas, maka manfaat dari tugas akhir ini adalah :

1. Mempermudah dalam memberikan hasil enkripsi dan dekripsi pesan teks pada pengguna disertai Aksara Jawa.
2. Menambah pengetahuan keamanan pesan dengan kriptografi yang menggunakan metode Bahasa Jawa Walikan.

1.5 Metodologi Penelitian

Adapun metodologi dalam penyelesaian masalah pada tugas akhir ini, adalah sebagai berikut :

1. Metode Kepustakaan

Metode kepustakaan digunakan untuk pengumpulan data dengan membaca dan memperlajari melalui buku-buku, artikel, jurnal, internet, dan referensi lain yang berkaitan dengan cara enkripsi-deskripsi pesan, kriptografi dan Bahasa Jawa Walikan.

2. Perancangan Perangkat Lunak Menggunakan *Unified Modeling Language* (UML)

   Penelitian ini membutuhkan perangkat lunak yang dibangun menggunakan bahasa pemrograman *Php*. Di mana pada tahap perancangan menggunakan UML, yang diimplementasikan dalam bentuk diagram usecase, diagram activity, diagram sequence, diagram class. Setelah perancangan dan pembangunan perangkat lunak dalam penelitian ini dilakukan hosting dan pembelian domain agar aplikasi dapat diakses melalui jaringan internet.

3. Pengujian Menggunakan *White Box* dan *Black Box*

   Pengujian yang digunakan untuk menguji aplikasi yaitu dengan menggunakan pengujian *white-box* dan *black-box* yang menguji fungsionalitas dari aplikasi. Pengujian *white-box* digunakan untuk mengecek kode program dan pengujian ini menggunakan *Flowgraph* untuk menggambarkan alur dari proses pada aplikasi *web* ini. Pengujian *black-box* digunakan untuk pengujian fungsionalitas dari aplikasi tanpa mengetahui struktur yang ada di dalam aplikasi.