

BAB I

PENDAHULUAN

I.1. Latar Belakang

Surat adalah sarana komunikasi untuk menyampaikan informasi tertulis oleh suatu pihak kepada pihak lain. Fungsinya mencakup lima hal: sarana pemberitahuan, permintaan, buah pikiran dan gagasan, alat bukti tertulis, alat pengingat, bukti historis, dan pedoman kerja. Surat juga dapat dilengkapi oleh tanda tangan pengirim untuk menjamin keaslian surat yang dibuat oleh seseorang atau suatu lembaga. Perkembangan teknologi yang sangat pesat saat ini terutama *internet* membuat proses pembuatan pada surat mulai di alihkan dari proses yang manual ke proses yang lebih terkomputerisasi, yang mana memiliki beberapa kelebihan dan kekurangan.

Surat yang dibuat nantinya akan memberikan kemudahan dalam pemrosesan dan pertukaran informasi. Namun, konsekuensi logis dari hal itu menyebabkan rentannya surat terhadap penyalahgunaan fungsi atau tujuan dari dibuatnya surat tersebut. Adanya modifikasi secara illegal membuat surat tersebut tidak terjamin keasliannya serta lambatnya proses tanda tangan yang dilakukan secara manual membuat proses pembuatan surat menjadi terhambat. Oleh karena itu, adanya perlindungan pada surat sangat diperlukan dan adanya sistem keamanan menjadi hal yang penting untuk menjadi solusi dalam pemecahan masalah.

Adanya tanda tangan digital yang terdapat pada sebuah surat tentu saja sangat membantu dalam mencegah terjadinya penyalahgunaan pada surat. Proses tanda tangan pada sebuah surat biasanya hanya menggunakan cara manual. Hal tersebut menyebabkan rentannya surat untuk di modifikasi atau disalahgunakan. Untuk itu pada sistem yang akan di bangun, proses pembuatan tanda tangan pada surat dilakukan dengan menyisipkan sebuah *Qrcode* yang berisi data pengirim surat berupa id pengirim, nama dan data diri lainnya yang dimiliki oleh pengirim surat. Pada proses pembentukan tanda tangan digital dengan *Qrcode* adalah dengan mengenkripsi data berupa id pengirim dan beberapa data diri pengirim. Selanjutnya data hasil enkripsi tersebut disimpan ke dalam sebuah *Qrcode*. dan selanjutnya untuk melihat isi dari *Qrcode* tersebut digunakanlah sebuah *scanner Qrcode* yang telah mendukung proses deskripsi didalamnya. Maka saat *Qrcode* di *scan* akan menampilkan data berupa hasil enkripsi yang akan otomatis di dekripsi oleh aplikasi *scanner* dan menampilkan data asli berupa id dan data diri pengirim.

Berdasarkan latar belakang tersebut, maka pada skripsi ini akan diangkat sebuah judul “**Rancang Bangun Sistem Keabsahan Pengirim Algoritma *Affine Cipher* dan *Qrcode* Sebagai Bukti Keaslian Surat**”. Penulis berharap, semoga dengan adanya sistem ini dapat memberikan pemahaman tentang pentingnya keamanan dalam sebuah surat untuk mencegah adanya modifikasi serta penyalahgunaan secara illegal pada sebuah surat.

I.2. Ruang Lingkup Permasalahan

Adapun ruang lingkup permasalahan pada aplikasi ini adalah :

I.2.1. Identifikasi Masalah

Adapun hal-hal yang menjadi identifikasi masalah aplikasi ini adalah :

1. Kurangnya keamanan pada sebuah surat yang dibuat secara manual terkadang menyebabkan surat tersebut mudah dimodifikasi dan disalahgunakan secara illegal.
2. Proses tanda tangan pada surat yang dilakukan secara manual membutuhkan waktu yang cukup lama.
3. Proses pemberian tanda tangan pada surat belum dapat diakses lewat beberapa perangkat berbeda karena masih dilakukan secara manual.

I.2.2. Perumusan Masalah

Berikut perumusan masalah yang akan dicari pemecahannya melalui penulisan skripsi ini, antara lain :

1. Bagaimana cara mengamankan surat agar tidak disalahgunakan secara illegal ?
2. Bagaimana proses tanda tangan pada surat agar tidak dilakukan secara manual lagi ?
3. Bagaimana proses pembuatan surat agar dapat dilakukan dengan mudah dan cepat ?
4. Bagaimana cara memanfaatkan *Qrcode* untuk digunakan sebagai sebuah tanda tangan digital ?
5. Bagaimana agar *Qrcode* yang digunakan sebagai bukti keaslian surat tidak dapat dimodifikasi oleh orang lain ?

I.2.3. Batasan Masalah

Dalam penulisan skripsi ini dibatasi permasalahannya sebagai berikut :

1. Aplikasi ini dirancang menggunakan bahasa pemrograman *php* dengan menggunakan *database mysql*.
2. Sistem yang dibangun digunakan untuk melakukan pembuatan surat dan melakukan penyisipan *Qrcode*.
3. Aplikasi *scanner* dibuat khusus untuk melihat keaslian surat yang dibuat dari sistem yang dibangun
4. Sistem yang dibuat berbasis *website* dan dapat dijalankan pada semua *browser* selain *internet explorer*.
5. Data didalam *Qrcode* telah di enkripsi dan hanya dapat didekripsi khusus saat di *scan* menggunakan *scanner* khusus.

I.3. Tujuan dan Manfaat

Adapun tujuan dan manfaat dari penulisan skripsi ini adalah sebagai berikut :

I.3.1. Tujuan

Tujuan yang ingin dicapai melalui penulisan skripsi ini adalah sebagai berikut :

1. Menghasilkan surat yang memiliki keamanan berupa *Qrcode* yang dapat digunakan juga untuk mengecek keaslian surat.

2. Menghasilkan aplikasi yang dapat membuat surat yang telah memiliki tanda tangan dengan lebih cepat dan dengan keamanan yang lebih baik.
3. Menghasilkan tanda tangan digital berupa *Qrcode* yang memiliki keamanan yang sangat baik untuk menghindari modifikasi secara illegal

I.3.2. Manfaat

Adapun manfaat yang dapat diambil dalam penulisan skripsi ini adalah:

1. Sistem yang dihasilkan memiliki keamanan untuk menjaga surat dari penyalahgunaan atau modifikasi dari pihak lain.
2. Dapat digunakan sebagai *tools* untuk membuat surat yang memiliki tanda tangan digital.
3. Sebagai referensi dalam merancang sebuah sistem dengan memanfaatkan kriptografi *affine cipher* dan *Qrcode*.

I.4. Metodologi Penelitian

Untuk dapat mengimplementasikan sistem di atas, maka secara garis besar digunakan beberapa metode sebagai berikut:

I.4.1. Metode Pengumpulan Data

Sistem yang dirancang tentunya memerlukan pengumpulan data, dalam proses pengumpulan data terdapat beberapa cara, berikut diantaranya :

- a. Studi Literatur, dengan cara mempelajari buku-buku acuan dan literatur yang berhubungan dengan materi dalam penulisan skripsi.

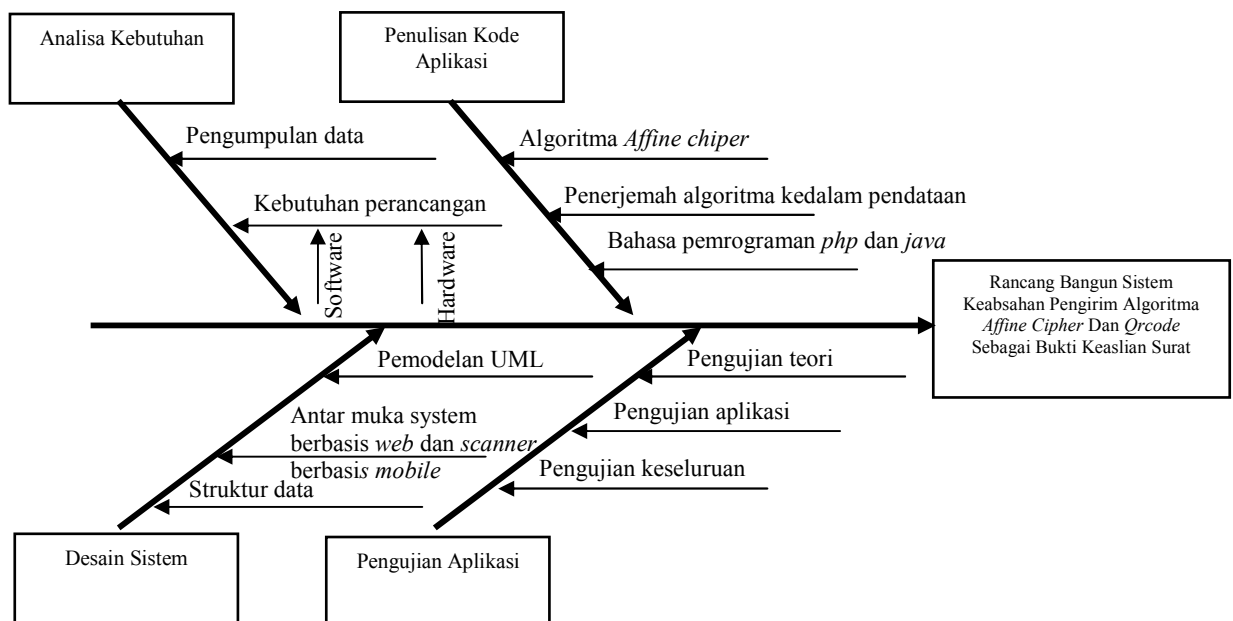
- b. Pengamatan, yaitu pengumpulan data dan informasi yang dilakukan dengan cara menganalisa cara pembuatan surat yang sudah ada.
- c. *Web Browsing*, yaitu penulis mencari data-data yang mendukung penulisan skripsi melalui *internet*.

I.4.2. Metode Perancangan Sistem

Dalam merancang sistem agar mencapai hasil yang diharapkan dilakukan tahap-tahap sebagai berikut :

1. Prosedur Perancangan

Langkah-langkah yang diperlukan untuk mencapai tujuan perancangan dapat dilihat pada *diagram Fishbone* gambar I.1.



Gambar I.1. *Diagram Fishbone* Prosedur Perancangan

1. Analisis Kebutuhan

Setelah melalui tahap prosedur perancangan, maka tahap selanjutnya adalah analisa kebutuhan yaitu hal-hal yang diperlukan untuk perancangan sistem pembuatan surat. Pengumpulan data berupa informasi data diri pengirim dan data lainnya yang bersangkutan dalam pembuatan sistem. Selain itu, juga diperlukan beberapa *software* dan *hardware* antara lain :

1. Perangkat Keras (*Hardware*)

Perangkat keras yang digunakan antara lain :

- a. Laptop : *Core i3 Processor*
- b. *Hard disk* : 500 GB
- c. RAM 4 GB
- d. Smartphone android

2. Perangkat lunak (*Software*)

Software yang digunakan untuk membuat skripsi ini antara lain :

- a. Sistem operasi Windows 10
- b. Sublime Text 3
- c. Xampp
- d. Android studio

2. Penulisan Kode Aplikasi

Pada tahap ini sistem yang akan dirancang menggunakan sebuah algoritma *affine cipher* yang diimplementasikan ke dalam *Qrcode* yang akan digunakan pada surat dan seluruh penulisan kode dalam sistem menggunakan bahasa

pemrograman *html* dan *php*.

3. Desain Sistem

Pada tahap ini dirancang sebuah desain dari perancangan sistem pembuatan surat. Bagaimana desain yang akan digunakan pada antarmuka perangkat berbasis *website*.

4. Pengujian Aplikasi

Pengujian aplikasi dilakukan untuk memeriksa ulang apakah aplikasi telah dibuat sesuai dengan apa yang direncanakan dalam perancangan yang akan digunakan dalam pembuatan aplikasi ini. Apakah desain yang dirancang dapat diimplementasikan kedalam bahasa pemrograman.

Pada tahap ini juga dilakukan pengujian perancangan sistem pembuatan surat secara menyeluruh, meliputi pengujian fungsional dan pengujian ketahanan aplikasi. Pengujian fungsional dilakukan untuk mengetahui bahwa perancangan sistem pembuatan surat telah berjalan sesuai dengan perancangan. Pengujian ketahanan merupakan kemampuan aplikasi untuk berjalan dengan baik pada spesifikasi minimum komputer sesuai dengan yang telah dicantumkan.

Pada tahap ini pun akan diambil kesimpulan dari perancangan sistem pembuatan surat yang telah dihasilkan, seperti apa saja kelebihan dan kekurangan dari perancangan aplikasi. Sehingga didapatkan kesimpulan untuk menambahkan fungsi-fungsi tertentu sesuai dengan kebutuhan kedalam aplikasi.

I.5. Keaslian Penelitian

Terdapat beberapa penelitian sebelumnya yang berhubungan dengan penelitian yang akan penulis lakukan. Penelitian yang dilakukan oleh Abdul Gani Putra Suratma dan Abdul Azis yang berjudul “**Tanda Tangan Digital Menggunakan *Qrcode* dengan Metode *Advance Encryption Standard***”, penelitian tersebut telah menghasilkan sebuah aplikasi pembuatan tanda tangan digital menggunakan *Qrcode* yang mengutamakan keamanan data. Sistem ini memiliki kelebihan yaitu menggunakan algoritma kriptografi yang akan memberikan tingkat keamanan yang jauh lebih baik.

Penelitian yang dilakukan oleh Rezanisa Agramanisti Azdy yang berjudul “**Tanda Tangan Digital Menggunakan Algoritme Keccak dan RSA**”, penelitian tersebut telah menghasilkan sebuah aplikasi pembuatan tanda tangan digital namun tanpa menggunakan *Qrcode*. Kelebihan dari sistem ini adalah penggunaan dua algoritma yang menambah tingkat keamanan data dalam tanda tangan digital.

Perbedaan dari penelitian sebelumnya, penulis membuat sebuah sistem pembuatan surat dengan menggunakan *Qrcode* yang telah di enkripsi dengan algoritma *Affine Cipher* yang memberikan keamanan surat yang lebih baik. Selain itu, aplikasi ini dibangun berbasis *website* agar aplikasi ini dapat digunakan di berbagai perangkat yang berbeda yang telah mendukung penggunaan *browser*.

I.6. Sistematika Penulisan

Adapun sistematika penulisan yang diajukan dalam penulisan skripsi ini adalah sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini menerangkan tentang latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metodologi penelitian dan sistematika penulisan yang berkaitan pada sistem pembuatan surat dengan algoritma *Affine Cipher* dan *Qrcode*

BAB II : TINJAUAN PUSTAKA

Pada bab ini menerangkan tentang teori-teori dan metode yang berhubungan dengan judul yang diangkat penulis diantaranya tentang algoritma *Affine Cipher*, *Qrcode*, dan proses pembuatan surat.

BAB III : ANALISA DAN DESAIN SISTEM

Pada bab ini mengemukakan tentang analisa sistem yang akan dibuat, melakukan pembuatan desain sistem yang akan diterapkan pada aplikasi

BAB IV : HASIL DAN UJI COBA

Pada bab ini menerangkan hasil dan proses pengujian dari aplikasi tanda tangan digital pada surat dengan menggunakan *Qrcode*, pengujian pada proses enkripsi dan deskripsi data serta pengujian

aplikasi yang di jalankan pada *browser* dengan spesifikasi yang telah ditetapkan.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan dan saran dari penulis sebagai perbaikan di masa yang akan datang untuk sistem pembuatan surat dengan algoritma *Affine Cipher* dan *Qrcode*.