

BAB I

PENDAHULUAN

I.1. Latar Belakang

Diary merupakan curahan hati penulis tentang suatu masalah ataupun kejadian yang dialami pada hari tertentu. *Diary* (Catatan harian) ini merupakan ungkapan yang jujur tentang suatu keadaan. Bersifat pribadi dan tidak boleh orang lain membacanya. Sifat rahasia dari *diary* itu kadang membuatnya disimpan dengan sangat hati-hati dan bahkan di gembok atau disandikan. *Diary* terasa sangat personal, karena mengandung banyak rahasia pribadi yang tidak boleh orang lain tau. Disadari atau tidak, menulis *diary* sebenarnya adalah proses pembelajaran mengungkapkan perasaan dalam bentuk tulisan. Perkembangan teknologi informasi berpengaruh besar pada banyaknya perubahan aktifitas manusia, tak terkecuali dalam menulis *Diary*. Menulis *Diary* yang dulunya ditulis pada buku tulis lalu disimpan pada tempat-tempat tertentu agar isi dari buku tersebut tidak dibaca oleh orang lain, namun seiring dengan berjalannya waktu dan perkembangan teknologi modern, kini menulis *Diary* dapat dilakukan dimanapun dan kapanpun tanpa harus membawa buku *Diary* kita, yaitu dengan *smartphone* atau perangkat lain.

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting pada penulisan *diary* (catatan harian). Dalam hal ini sangat terkait dengan betapa pentingnya pesan, data, atau informasi. Maka ditekankan untuk menjaga kerahasiaan suatu *Diary* itu sendiri menjadi lebih personal atau bersifat privasi.

Hal inilah yang mendorong penulis untuk mendesain aplikasi *Diary* atau buku harian dengan algoritma Kriptografi sehingga kerahasiaan dari isi *Diary* yang ditulis tetap terjaga.

RC4 merupakan salah satu jenis *stream cipher*, yaitu yang memproses unit atau input data, pesan atau informasi pada satu unit tertentu. Pada umumnya sebuah *byte* atau bahkan kadang kadang *bit* (*byte* dalam hal RC4). Dengan cara ini enkripsi atau dekripsi dapat dilaksanakan pada panjang yang variabel. Algoritma ini tidak harus menunggu sejumlah input data, pesan atau informasi tertentu sebelum diproses, atau menambahkan *byte* tambahan untuk mengenkripsinya. (Zain, 2012 : 3).

Berdasarkan paparan permasalahan yang telah dijabarkan dan gagasan solusi pemecahan masalah yang ada, maka pada penelitian ini penulis tertarik mengangkat judul “**Penerapan Algoritma RC4 Dengan Fitur Rich text editor Pada Aplikasi Diary (Catatan Harian) Digital Berbasis Android**”. Penelitian ini bertujuan untuk membuat aplikasi catatan harian berbasis android dengan dilengkapi fitur kriptografi yang dapat mengamankan isi catatan harian sehingga tidak dapat dibaca oleh orang lain yang tidak memiliki hak membaca melalui proses enkripsi dan dekripsi.

I.2. Ruang lingkup Permasalahan

Adapun beberapa tahap yang dilakukan dalam membuat ruang lingkup permasalahan adalah :

I.2.1. Identifikasi Masalah

Berdasarkan penelitian penulis sehubungan dengan materi yang diangkat dalam skripsi ini, penulis menemukan beberapa masalah antara lain :

1. Kebutuhan akan sebuah aplikasi catatan harian (*diary*) yang dapat menjaga keamanan isi catatan harian dengan melauai proses kriptografi, dikarenakan belum adanya jaminan keamanan bahwa sewaktu-waktu pengguna yang tidak diinginkan akan membuka isi dari catatan harian (*diary*) digital tersebut.
2. Penerapan algoritma RC4 dalam menjaga keamanan dari isi catatan harian (*diary*) digital berbasis android.

I.2.2. Rumusan Masalah

Sebagaimana yang telah dikemukakan pada latar belakang masalah di atas, maka rumusan masalahnya adalah sebagai berikut :

1. Bagaimana merancang dan membangun aplikasi catatan harian (*diary*) digital berbasis android yang dilengkapi dengan fitur rich text editor?
2. Bagaimana menerapkan algoritma RC4 pada aplikasi *diary* digital berbasis android yang dapat menjaga keamanan isi dari catatan harian tersebut?

I.2.3. Batasan Masalah

Adapun batasan masalah yang penulis berikan dalam pembuatan skripsi ini adalah sebagai berikut :

1. Algoritma kriptografi yang digunakan dalam proses enkripsi dan dekripsi data adalah algoritma RC4.

2. Software yang digunakan untuk membuat aplikasi adalah Android Studio.
3. Aplikasi ini hanya membahas masalah keamanan tulisan berdasarkan aspek keamanan yang dilengkapi dengan fitur rich text editor.
4. Hasil dari enkripsi data suatu file tidak dapat dikirim keperangkat lain hanya tersimpan di satu perangkat.
5. Aplikasi catatan harian (*diary*) digital yang dibangun dapat digunakan pada perangkat smartphone berbasis sistem operasi android.
6. Program yang dibuat dengan menggunakan bahasa pemrograman Java.
7. Pemodelan sistem dilakukan dengan menggunakan Unified Modelling Language (UML).

I.3. Tujuan Dan Manfaat

Tujuan dan manfaat yang penulis peroleh dari penelitian skripsi ini adalah sebagai berikut :

I.3.1. Tujuan

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

1. Merancang aplikasi *diary* (catatan harian) digital berbasis *android* dengan penerapan algoritma *RC4* dengan *fitur rich text editor*.
2. Menerapkan algoritma *RC4* dalam proses enkripsi dan dekripsi catatan harian yang terjaga keamanannya.

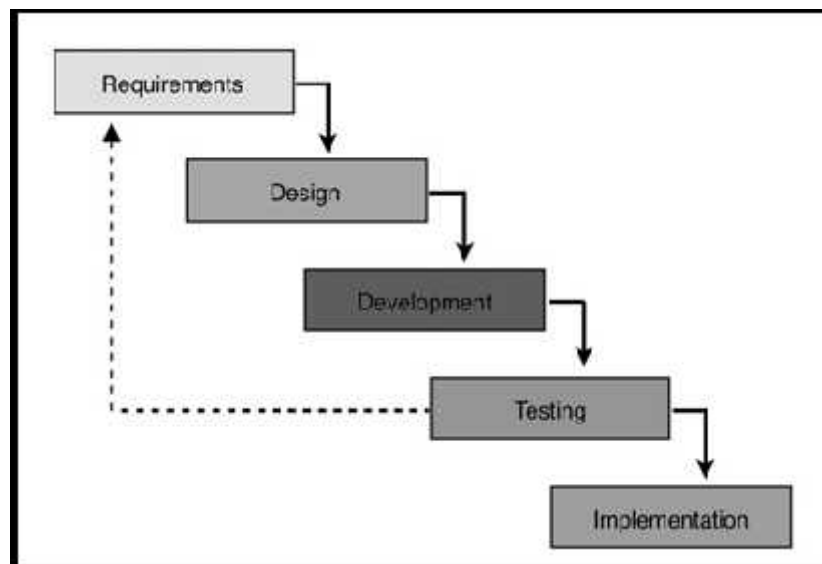
I.3.2. Manfaat

Manfaat yang diharapkan dari penulisan skripsi ini adalah :

1. Memberikan keamanan pada catatan harian (*diary*) yang disimpan pada perangkat *smartphone* android, sehingga tidak perlu khawatir dibaca oleh pengguna yang tidak memiliki hak akses.
2. Menjadi bahan referensi penelitian lanjut yang mengangkat penerapan algoritma RC4 pada aplikasi berbasis sistem operasi android.
3. Menambah wawasan dan pengalaman penulis dalam pembelajaran kriptografi pada perangkat *smartphone* berbasis android.

I.4. Metodologi Penelitian

Metode pengembangan sistem yang digunakan dalam penelitian ini menggunakan model waterfall. Model waterfall merupakan model pengembangan perangkat lunak yang alur kerjanya dilakukan secara sekuensial (terurut). Berikut ini adalah tahapan dari model waterfall :



Gambar III.1 Model Waterfall

1. *Requirement* (Analisa kebutuhan sistem) .

Dalam tahap ini dilakukan proses pencarian bahan-bahan yang berkaitan dengan perancangan aplikasi *diary* digital dengan fitur *strong password* menggunakan algoritma *RC4* pada perangkat *smartphone* android. Pengutipan yang dilakukan dapat berupa teori ataupun beberapa pendapat dari beberapa buku bacaan ataupun buku diktat yang dipergunakan selama kuliah untuk menunjang perancangan program.

2. *Design* (Perancangan Sistem)

Berdasarkan analisa yang telah dilakukan, selanjutnya dilakukan proses perancangan aplikasi *diary* (catatan harian) *digital* berbasis android menggunakan algoritma *RC4* dengan fitur *rich text editor* yang berhubungan dengan perancangan arsitektur sistem, perancangan antarmuka, perancangan modul-modul yang berintegrasi dalam suatu sistem.

3. *Development* (Pembangunan Sistem)

Pada tahap ini akan dilakukan proses pembangunan aplikasi *diary* digital dengan fitur *rich text editor* menggunakan algoritma *RC4* pada perangkat *smartphone* android dengan menggunakan *Android Studio* sesuai dengan hasil perancangan. Implementasi dilakukan dengan menggunakan perangkat yang sudah dieksplorasi sebelumnya.

4. *Testing* (Uji Coba Sistem)

Pada tahap ini dilakukan beberapa tes terhadap sistem yang telah diimplementasikan. Testing dilakukan dengan percobaan

mengimplementasikan aplikasi Diary pada perangkat *smartphone* android selanjutnya melakukan percobaan memasukkan beberapa catatan kedalam fitur rich text editor. Setelah itu pengguna melakukan penguncian (penyandian) pada aplikasi Diary dan menyimpan kedalam perangkat. Selain itu dilakukan pengujian algoritma kriptografi RC4 pada aplikasi dengan memberikan informasi kecepatan performa dan hasil dari enkripsi dan deskripsi melalui perangkat mobile menggunakan algoritma kriptografi RC4. Aplikasi Diary akan dikunci oleh sistem menggunakan algoritma RC4. Pengujian ini dilakukan untuk melihat kesiapan sistem di dunia nyata. Adapun pendekatan yang dilakukan penulisan dalam melakukan pengujian sistem yang dibuat adalah *Black Box Testing* dimana pengujian ini bertujuan untuk menunjukkan fungsi perangkat lunak tentang cara beroperasinya, apakah pemasukan data keluaran telah berjalan sebagaimana yang diharapkan dan apakah informasi yang disimpan secara eksternal selalu dijaga kemutakhirannya.

5. Implementation Sistem

Pada tahap ini aplikasi diary digital dengan fitur *rich text editor* menggunakan algoritma *RC4* pada perangkat *smartphone* android sudah melewati tahap pengujian dan siap untuk digunakan oleh pengguna *smartphone* berbasis android. Tidak menutup kemungkinan aplikasi ini mengalami perubahan ketika sudah digunakan oleh pengguna. Perubahan bisa terjadi karena adanya kesalahan yang muncul dan tidak terdeteksi saat pengujian. Tahap pendukung atau pemeliharaan dapat mengulangi proses

pengembangan mulai dari analisis spesifikasi untuk perubahan sistem informasi yang sudah ada, tapi tidak untuk membuat aplikasi yang baru.

I.5. Kontribusi Penelitian

Sebagai bukti penelitian yang akan dibuat, maka penelitian akan dibandingkan terhadap penelitian sejenis yang pernah dilakukan perbandingannya dapat dilihat pada tabel I.1 dibawah ini :

Tabel I.1. Kontribusi Penelitian

No	Materi Perbandingan	Instrumen
<p>Penelitian pertama : Perancangan Dan Implementasi Cryptography Dengan Metode Algoritma RC4 Pada Type File Document Menggunakan Bahasa Pemrograman Visual Basic 6.0</p> <p>Hasil : Algoritma RC4 mampu melakukan proses enkripsi dan dekripsi data, dan sekaligus mampu melakukan pengompresan data sehingga data dienkripsi tersebut terdapat perubahan</p>		
1.	Algoritma yang digunakan	RC4
2.	Penelitian	Implementasi <i>Cryptography Type File Document</i> .
3.	Basis Aplikasi	Desktop
4.	Perangkat Lunak	VB, SQL Server
<p>Penelitian kedua : Aplikasi Kriptografi Dengan Algoritma Message Digest 5 (Md5).</p> <p>Hasil : Hasil pengujian digambarkan dengan tabel hasil pengujian, yang kemudian dijabarkan dengan grafik hasil uji coba terhadap file yaitu Grafik kecepatan aplikasi terhadap besar file, Grafik rerata waktu eksekusi terhadap besar file dan Tabel perbandingan kecepatan maksimum dengan kecepatan rerata terhadap besar file.</p>		
1.	Algoritma yang digunakan	Message Digest 5 (Md5)
2.	Penelitian	Kriptografi

3.	Basis Aplikasi	Tidak Diketahui
4.	Perangkat Lunak	Tidak digunakan
Penelitian yang akan dibuat : <i>Rancang Bangun Aplikasi Kriptografi Email Gmail Menggunakan Algoritma Rc4</i>		
1.	Algoritma/Metode yang digunakan	RC4
2.	Penelitian	Kriptografi.
3.	Basis Aplikasi	Dekstop.
4.	Perangkat Lunak	Algoritma RC4, Java script

I.6. Sistematika Penulisan

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

BAB I : PENDAHULUAN

Pada bab ini menerangkan tentang latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metode penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini menerangkan tentang teori-teori dan metode yang berhubungan dengan topik yang dibahas atau permasalahan yang sedang dihadapi.

BAB III : ANALISA DAN DESAIN SISTEM

Pada bab ini mengemukakan tentang analisa sistem yang sedang berjalan, evaluasi sistem yang berjalan dan desain sistem secara detail.

BAB IV : HASIL DAN UJI COBA

Pada bab ini menerangkan hasil dan pembahasan program yang dirancang serta kelebihan dan kekurangan sistem yang dirancang.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan penulisan dan saran dari penulis sebagai perbaikan di masa yang akan datang untuk sistem.