BAB I
PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi era digital yang sangat pesat telah berpengaruh besar pada semua aspek kehidupan manusia. Hampir seluruh kegiatan manusia telah memanfaatkan adanya teknologi, contohnya dalam hal berkomunikasi. Media komunikasi umum yang dapat digunakan oleh siapapun saat ini sangat rawan terhadap penyadapan informasi oleh pihak-pihak yang tidak bertanggung jawab dan tidak berhak mengetahui informasi tersebut. Maka dalam era dunia digital saat ini, faktor keamanan dan realibilitas layanan digital menjadi sebuah hal penting (Basheer & Sreedhar, 2015). Berbagai hal telah dilakukan untuk mendapatkan jaminan keamanan informasi yang rahasia. Salah satu cara yang bisa digunakan adalah menggunakan teknik kriptografi. Banyak permasalahan keamanan digital dapat diselesaikan dengan menggunakan kriptografi.

Untuk mengatasi hal tersebut, banyak program studi dalam bidang ilmu komputer khususnya jurusan Teknik Informatika, melengkapi kurikulumnya dengan matakuliah kriptografi. Tetapi banyak para mahasiswa yang sedang menempuh mata kuliah kriptografi mengalami kesulitan untuk memahami kriptografi (Basheer & Sreedhar, 2015). Mahasiswa yang mengalami kesulitan dalam proses belajar matakuliah kriptografi, menjadi salah satu penyebab hasil belajar mahasiswa pada matakuliah kriptografi menjadi rendah (Sry Yunarti, 2018). Hal itu juga menjadi pemicu minat mahasiswa untuk belajar kriptografi menjadi menurun. Faktor penyebabnya yaitu siswa mengalami masalah secara

komprehensip atau secara parsial. Sedangkan dosen yang bertugas sebagai pengelola pembelajaran seringkali belum mampu menyampaikan materi pelajaran kepada mahasiswa secara bermakna, serta penyampaiannya juga terkesan monoton tanpa memperhatikan potensi dan kreativitas mahasiswa sehingga mahasiswa merasa bosan karena hanya dianggap sebagai botol kosong yang siap diisi dengan materi pelajaran.

Hal yang sama juga pernah dialami oleh beberapa dosen ketika menjadi pengampu matakuliah kriptografi. Menurut (Jawa Bendi dkk., 2016) algoritma-algoritma kriptografi yang kompleksitas mengakibatkan mahasiswa menjadi sulit untuk dapat memahami konsep sebuah algoritma kriptografi secara utuh. Akibatnya mahasiswa seringkali tidak dapat mengerjakan latihan yang diberikan dengan baik. Aplikasi media pembelajaran yang dilengkapi dengan materi, simulasi penggambaran enkripsi dan dekripsi, dan latihan soal diyakini dapat membuat minat mahasiswa menjadi tumbuh untuk mempelajari kriptografi.

Berdasarkan uraian permasalahan diatas, maka penulis ingin mengambil judul penilitian "***APLIKASI SIMULASI ENKRIPSI DAN DEKRIPSI SEBAGAI MEDIA PEMBELAJARAN MATA KULIAH KRIPTOGRAFI***" yang diharapkan dapat membantu mahasiswa untuk mengenal dasar-dasar kriptografi serta mempelajari proses dasar enkripsi dan dekripsi dan bisa menjadi media pembelajaran untuk mata kuliah kriptografi.

1.2. Perumusan Masalah

Berdasarkan latar belakang diatas maka perumusan masalah yang akan dibahas pada penelitian ini adalah sebagai berikut :

a. Bagaimana membuat animasi untuk menggambarkan atau menyimulasikan proses dari enkripsi dan dekripsi ?.
b. Bagaimana merancang dan membangun sebuah aplikasi media pembelajaran kriptografi klasik menggunakan software Adobe Flash CS 6 dengan bahasa pemrograman *Actionscript* versi 3.0 ? .

1.3. Batasan Masalah

Agar pembahasan ini lebih terarah dan tidak menyimpang dari pokok permasalahan yang ada maka penulis membatasi penelitian yang akan dilakukan yaitu sebagai berikut :

a. Pembuatan aplikasi menggunakan Adobe Flash CS 6.
b. Karakter yang dapat di enkripsi dan dekripsi yaitu dari A-Z
c. Hanya membahas dua metode kriptografi klasik yaitu *Caesar Cipher* dan *Affine Cipher*.
d. Hanya dapat mengenkripsi dan mendekripsi pesan teks.
e. Hanya membahas simulasi perhitungan dan pembuatan aplikasi simulasi enkripsi dan dekripsi sebagai media pembelajaran matakuliah kriptografi.

1.4. Tujuan

Berdasarkan uraian permasalahan diatas, maka tujuan dari penelitian ini adalah : Membangun aplikasi media pembelajaran yang dilengkapi dengan materi,

soal latihan, dan penggambaran animasi dari simulasi proses enkripsi dan dekripsi kriptografi klasik *Caesar Cipher* dan *Affine Cipher*. Menggunakan software *Adobe Flash CS6* dan *Actionscript 3.0*. Selain itu juga aplikasi ini dapat dijadikan sebagai perangkat ajar untuk matakuliah kriptografi.

1.5. Manfaat Penelitian

Dengan adanya penelitian ini diharapkan bisa memberikan manfaat bagi pengguna, penulis dan pembaca antara lain sebagai berikut :

1.5.1. Bagi Pengguna

a. Dapat menumbuhkan minat belajar mahasiswa.
b. Memberikan solusi agar lebih mudah memahami proses enkripsi dan dekripsi.

1.5.2. Bagi Penulis

a. Penelitian ini dapat menambah pengetahuan dan wawasan penulis mengenai *Adobe Flash CS6* dan bahasa *Actionscript 3.0*, proses enkripsi dan dekripsi, serta untuk memperoleh pengalaman dalam membangun sebuah aplikasi.
b. Hasil penelitian ini dapat meningkatkan pengetahuan penulis tentang enkripsi dan dekripsi dari metode kriptografi klasik.

1.5.3. Bagi Pembaca

a. Penelitian ini dapat memberikan informasi secara tertulis maupun sebagai referensi mengenai dasar proses enkripsi dan dekripsi metode kriptografi klasik.

1.6. Metodologi Penelitian

1.6.1. Waktu dan Tempat

Penelitian ini dilaksanaka pada semester genap tahun akademik 2018/2019 yaitu antara bulan Maret sampai dengan bulan Agustus 2019. Penelitian ini bertempat di Universitas Bina Darma Jl.Jenderal Ahmad Yani No.3, 9/10 Ulu Kecamatan seberang ulu Plaju Palembang.

1.6.2. Metode Pengumpulan Data

Adapun teknik untuk pengumpulan data dan informasi adalah sebagai berikut :

a. Studi Pustaka

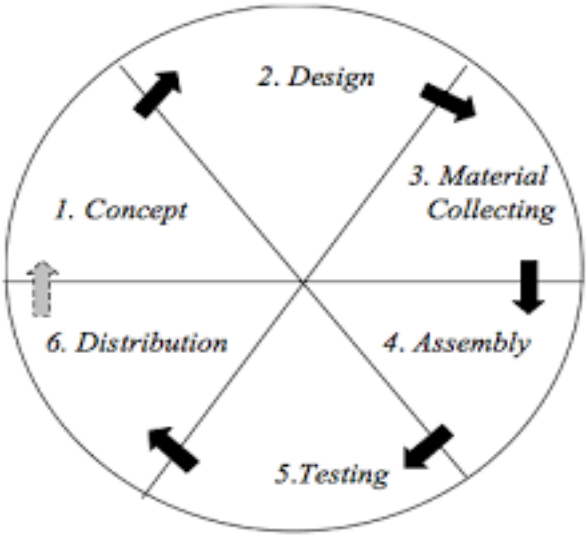
   Untuk mendapatkan data-data yang bersifat teoritis maka penulis melakukan pengumpulan data dengan cara membaca jurnal dan mempelajari buku-buku, makalah ataupun referensi lain yang berhubungan dengan masalah yang dibahas.

b. Pengamatan *(Observasi)*

   Yaitu metode pengumpulan informasi dengan cara mengadakan tinjauan secara langsung pada masalah yang diteliti. Untuk mendapatkan data yang bersifat nyata dan meyakinkan, maka penulis melakukan pengamatan secara langsung untuk mendapatkan informasi dari hasil uji coba aplikasi simulasi enkripsi dan dekripsi yang telah dikembangkan menggunakan metode MDLC. Selain itu penulis juga melakukan pengamatan terhadap aplikasi media pembelajran yang lainnya sebagai referensi dalam pembuatan aplikasi simulasi enkripsi dan dekripsi sebagai media pembelajaran matakuliah kriptografi.

1.6.3. Metode Pengembangan Sistem

Dalam penelitian ini menggunakan metode pengembangan perangkat lunak *Multimedia Development Life Cycle (MDLC)*. *MDLC* memiliki 6 tahapan yaitu : *Concept*, *Design*, *Collecting Content Material*, *Assembly*, *Testing* dan *Distribution* (Luther, 1994). Beberapa tahapan dalam metode pengembangan sistem *MDLC* menurut referensi Luther :



Sumber : (Luther, 1994)

Gambar 1.1 Metode Pengembangan Multimedia

1. *Concept*

   Tahap *concept* (konsep) adalah tahap untuk menentukan tujuan dan siapa pengguna program (identifikasi *audience*). Selain itu menentukan macam aplikasi (presentasi, interaktif, dll) dan tujuan dari aplikasi (hiburan, pelatihan, pembelajaran, dll).

2. *Design*

   Dalam tahap ini dilakukan pembuatan dan perancangan desain aplikasi arsitektur program, desain visual tampilan interface *storyboard*, dan

struktur navigasi. Di samping itu, pada tahap ini juga dibuat perancangan algoritma untuk aplikasi evaluasi pembelajaran.

3. *Obtaining content material*

   Pada tahap ini dilakukan pengumpulan bahan seperti image, animasi, audio dan video. Bahan yang diperlukan dapat diperoleh dari perpustakaan, atau pembuatan khusus untuk aplikasi.

4. *Assembly*

   Tahap *assembly* (pembuatan) adalah tahap dimana semua objek atau bahan multimedia dibuat. Pembuatan aplikasi didasarkan pada tahap design.

5. *Testing*

   Tahap *testing* (uji coba) dilakukan setelah selesai tahap pembuatan. Pertama - tama dilakukan uji coba secara modular untuk memastikan apakah hasilnya seperti yang diinginkan. Dari hasil uji coba dilakukan perbaikan sesuai dengan saran dan masukan. Dari hasil perbaikan dilakukan uji coba lagi agar meningkatkan kinerja aplikasi sehingga memenuhi kebutuhan.

6. *Distribution*

   Setelah tahap uji coba yang mungkin perlu dilakukan beberapa kali, dalam tahap ini dilakukan pembuatan master file, pedoman penggunaan aplikasi, serta dokumentasi sistem.

Pada penelitian penulis membatasi pengembangan aplikasi simulasi enkripsi dan dekripsi. Pengembangan aplikasi simulasi enkripsi dan dekripsi hanya di lakukan sampai pada tahap *testing* saja.

1.6.4. Metode Pengujian

Pada penelitian ini, metode pengujian yang akan digunakan untuk mengembangkan aplikasi ini adalah *Blackbox Testing*. *Blackbox Testing* atau bisa disebut tes fungsional ini adalah pengujian yang dilakukan hanya dengan mengamati hasil eksekusi melalui data uji dan memeriksa fungsional dari aplikasi yang sedang dikembangkan (Yuwanda, 2016). Pengujian aplikasi ini dilakaukan oleh pengembang dan user yang terlibat untuk memberi data yang akan diinputkan. Selain itu user mencoba berbagai fitur pada aplikasi.

1.7. Sistematika Penulisan

Sistematika penulisan skripsi ini dimaksudkan agar dapat menjadi pedoman atau garis besar penulisan laporan penelitian ini, dan dapat menggambarkan secara jelas isi dari laporan penelitian sehingga terlihat hubungan antara bab awal hingga bab terakhir. Sistem penulisan laporan penelitian ini terdiri atas :

BAB I PENDAHULUAN

Pada bab ini dibahas tentang latar belakang penelitian, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, waktu penelitian, metode pengumpulan data, metode pengembangan sistem, metode pengujian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab II ini berisi landasan teori yaitu teori-teori umum dan khusus yang mendukung penulisan skripsi ini. Hal-hal yang tercakup didalamnya adalah pembahasan kriptografi klasik, *Caesar Cipher* dan *Affine Cipher* serta berisi penelitian terdahulu dan kerangka berpikir.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Pada bab ini membahas tentang analisis kebutuhan sistem, dan perancangan aplikasi yang menerapkan tahapan-tahapan dari metode pengembangan sistem *Multimedia development Life Cycle* (MDLC) yaitu meliputi perancangan *use case diagram*, *activity diagram*, dan desain yang meliputi arsitektur perangkat lunak, struktur navigasi, *storyboard* ,serta *flowchart*.

BAB IV HASIL DAN PEMBAHASAN

Bab IV ini berisi screenshoot tampilan hasil aplikasi yang telah dibuat sesuai dengan perancangan pada bab III sebelumnya, implementasi kode program, serta pembahasan contoh perhitungan algoritma *caesar cipher* dan *affine cipher*. Pada bab IV ini juga membahas tentang hasil uji coba perangkat lunak yang di lakukan dengan menggunakan metode *black box* testing.

BAB V KESIMPULAN DAN SARAN

Bab V berisi kesimpulan-kesimpulan yang didapat dari hasil penelitian dan saran-saran untuk perbaikan atau pengembangan selanjutnya dari hasil penelitian ini.