BAB I

PENDAHULUAN

1.1. Latar Belakang

TOEFL atau singkatan dari *Test Of English as a Foreign Language* merupakan tes standar untuk mengukur kemampuan seseorang dalam hal penguasaan bahasa inggris sebagai bahasa asing bagi *non-native speaker* (bukan penutur asli) dalam bidang akademik. TOEFL biasanya digunakan sebagai salah satu prasyarat untuk studi di luar negeri, terutama negara-negara yang menggunakan bahasa inggris sebagai bahasa pengantar. TOEFL juga biasanya menjadi persyaratan untuk melanjutkan S-2 dan S-3 di dalam negeri. Bahkan saat ini mahasiswa S-1 pada berbagai universitas di Indonesia juga diharuskan untuk memiliki skor TOEFL tertentu sebagai salah satu syarat kelulusannya. Selain itu, TOEFL juga digunakan dalam dunia kerja sebagai salah satu mekanisme perekrutan atau jenjang kenaikan karir.

Universitas Kuningan (UNIKU) merupakan salah satu perguruan tinggi swasta di Indonesia yang mensyaratkan kelulusan ujian TOEFL sebagai hal yang harus dipenuhi untuk mendaftar sidang skripsi. Hal ini dilakukan agar lulusan UNIKU memiliki daya saing dengan perguruan tinggi lain khususnya dalam penguasaan bahasa. UNIKU melalui Pusat Bahasa menyediakan fasilitas ujian kemampuan Bahasa Inggris atau TOEFL bagi mahasiswa dengan skor minimum yang harus diraih yaitu 400.

Mahasiswa yang berhasil lulus ujian akan diberikan sertifikat sebagai bukti kelulusan ujian, dan mahasiswa yang tidak mencapai skor minimum dikatakan tidak lulus dan harus mengulang ujian.

Ujian TOEFL yang cukup sulit menjadi salah satu faktor yang membuat mahasiswa selalu mencari celah untuk mendapatkan sertifikat tanpa harus mengikuti ujiannya. Yang menjadi sorotan penulis disini adalah adanya celah untuk melakukan kecurangan yaitu dengan memalsukan sertifikat. Hal ini dapat terjadi dikarenakan sertifikat TOEFL yang dikeluarkan oleh Pusat Bahasa UNIKU mencantumkan seluruh informasi kepemilikan sertifikat secara langsung. Pemalsuan sertifikat biasanya dilakukan dengan membuat sertifikat baru melalui proses *scan* atau membuat sertifikat dengan desain dan tampilan yang sama dengan aslinya. Selain itu, untuk mengecek keaslian sertifikat TOEFL UNIKU masih dilakukan manual dengan cara menghubungi secara langsung Pusat Bahasa sehingga tidak efektif dan efisien.

Oleh karena itu untuk mengantisipasi adanya pemalsuan sertifikat, diperlukan pengamanan pada sertifikat yaitu dengan menyisipkan nomor induk mahasiswa, nama mahasiswa, skor yang diraih, tanggal ujian dan tanggal berlakunya sertifikat yang disandikan dengan menggunakan teknik kriptografi dan diolah sedemikian rupa ke dalam sebuah objek pengenal yang bisa diidentifikasi dan dicocokan. Kriptografi merupakan teknik penyandian pesan atau informasi yang berkaitan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Dengan

kriptografi, informasi keaslian sertifikat tidak dapat dibaca oleh semua orang sehingga informasi keaslian sertifikat terjamin. Teknik kriptografi yang akan digunakan oleh penulis dalam penelitian ini yaitu penyandian kunci asimetri dengan Algoritma RSA.

Algoritma RSA merupakan algoritma kriptografi yang terdiri dari enkripsi dan dekripsi. Enkripsi adalah proses yang dilakukan untuk mengamankan sebuah pesan atau informasi (*plaintext*) menjadi pesan atau informasi yang tersandikan *(chipertext).* Sedangkan dekripsi adalah proses yang dilakukan untuk menerjemahkan pesan atau informasi yang tersandikan *(chipertext)* menjadi pesan atau informasi asli *(plaintext).* Informasi yang telah disandikan akan disimpan ke dalam bentuk QR-Code.

Quick Respond Code atau QR-Code merupakan teknik yang mengubah data tertulis menjadi kode-kode 2 dimensi yang tercetak kedalam suatu media yang lebih ringkas. QR-Code mampu menyimpan semua jenis data seperti data numerik, alfanumerik, biner, dan kanji/kana. Dengan menggunakan QR-Code, informasi keaslian sertifikat dibuat menjadi lebih sederhana dan tidak perlu mengetikan pada sertifikat serta memudahkan pihak yang membutuhkan untuk mengecek keasliannya. Saat ini, QR-Code sudah banyak digunakan diberbagai media dan untuk berbagai tujuan diantaranya sebagai pin *Blackberry Messanger*, alamat website perusahaan atau letak geografis suatu lokasi, link download dan lain sebagainya.

Dengan kombinasi QR-Code dan Algoritma RSA ini diharapkan dapat mengantisipasi praktik pemalsuan sertifikat. Berdasarkan uraian diatas,

penulis tertarik untuk melakukan penelitian dengan judul **"Implementasi Algoritma *Rivest Shamir Adleman* (RSA) Berbasis QR-Code pada Aplikasi Pengaman Keaslian Sertifikat TOEFL"**.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang masalah yang telah disampaikan adapun rumusan masalah yang akan dibahas dalam proposal skripsi ini adalah :

1. Bagaimana cara kerja sistem enkripsi dan dekripsi algoritma RSA?
2. Bagaimana mengimplementasikan algoritma RSA ke dalam bentuk QR-Code?

1.3. Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah :

1. Jenis Sertifikat TOEFL yang digunakan pada penelitian ini adalah sertifikat TOEFL Prediction yaitu *Uniku English Proficiency Test* (UEPT).
2. Data yang digunakan sebagai input dalam proses implementasi adalah alfanumerik.
3. Tahapan yang digunakan algoritma RSA ini adalah pembentukan kunci, proses enkripsi pada data yang akan disimpan ke dalam QR-Code, dan melakukan proses dekripsi pada data hasil dari pemindaian QR-Code.

4. Nilai *p* dan *q* telah ditentukan dan tidak di *random* karena nilai *p* dan *q* akan kembali di gunakan ketika proses dekripsi.
5. QR-Code yang digunakan berwarna hitam dengan *background* disesuaikan dengan kertas sertifikat yang dipakai.
6. Pemindaian QR-Code dilakukan pada media kertas / tercetak.
7. Kertas sertifikat yang digunakan minimal BC putih dengan permukaan bersih 160 gram.
8. Alat cetak yang digunakan harus menghasilkan hasil cetak yang jelas, minimal 600 x 600 dpi.
9. Alat pemindai minimal dengan menggunakan kamera1,3 mp.
10. Sertifikat TOEFL dikelola oleh Pusat Bahasa Universitas Kuningan dan pemeriksaan keaslian sertifikat dilakukan oleh pihak yang berkepentingan.
11. Informasi yang dihasilkan dari pemindaian QR-Code yang telah didekripsi adalah Nomor Induk Mahasiswa (NIM**),** nama mahasiswa, skor yang diraih, tanggal ujian dan tanggal berlakunya sertifikat tersebut.
12. Tahapan pengembangan menggunakan metode RUP (*Rational Unified Process*).
13. Bahasa pemrograman yang digunakan adalah PHP dengan database MySQL.
14. Browser yang digunakan harus mendukung HTML5.
15. Pemindaian QR-Code dilakukan dengan QR-Code *Reader* dan algoritma RSA dijalankan di web.

1.4. Tujuan dan Manfaat Penelitian

1.4.1. Tujuan Penelitian

Tujuan dari penelitian ini adalah :

1. Implementasi teknik penyandian teks/numerik.
2. Implementasi teknik enkripsi dan dekripsi algoritma RSA.
3. Mengimplementasikan algoritma RSA pada QR-Code.

1.4.2. Manfaat Penelitian

Adapun manfaat dari penelitian ini sebagai berikut :

1. **Manfaat Bagi Peserta**

   Dengan adanya aplikasi pengaman ini sertifikat TOEFL yang didapat lebih terjamin keasliannya, sehingga dapat digunakan sesuai kebutuhan (seperti melamar pekerjaan).

2. **Manfaat Bagi Pusat Bahasa**

   Aplikasi ini memudahkan pengecekan sertifikat TOEFL yang asli dan palsu. Selain itu, sertifikat TOEFL yang dikeluarkan oleh Pusat Bahasa Universitas Kuningan lebih terjamin keasliannya dan dapat dipertanggung jawabkan. Serta, dengan penggunaan aplikasi ini pengeluaran sertifikat lebih terkelola dengan rapi.

1.5. Metodologi Penelitian

1.5.1. Metode Pengumpulan data

Teknik pengumpulan data yang dilakukan oleh penulis menggunakan cara yaitu :

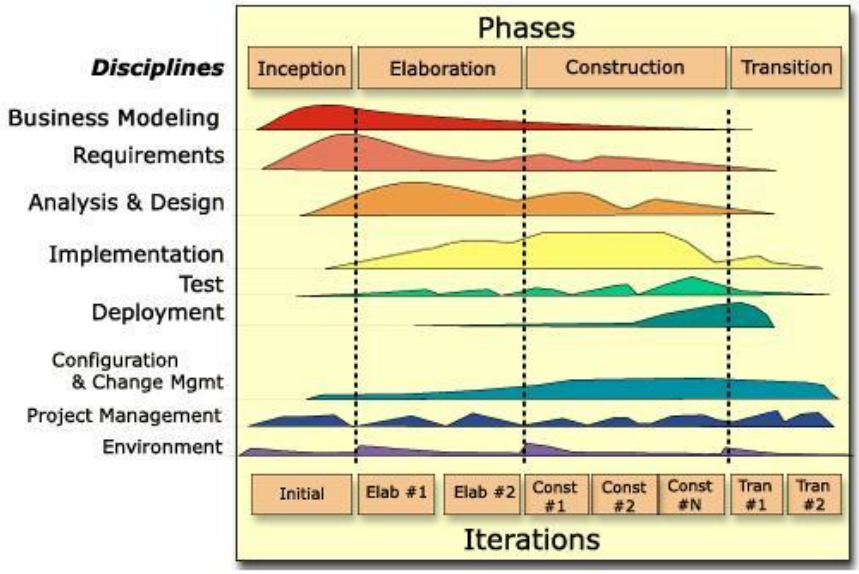
1. Studi Pustaka yaitu teknik pengumpulan data dengan cara pengumpulan informasi yang relevan dan diperoleh dari buku atau jurnal yang ada hubungannya dengan QR-Code dan sistem enkripsi serta dekripsi pada algoritma RSA.
2. Wawancara yaitu teknik pengumpulan data dengan cara melakukan tanya-jawab secara langsung dengan Bapak Marwito Wihadi, M.Pd selaku Kepala Pusat Bahasa Universitas Kuningan, mengenai hal-hal yang berkaitan dengan sistem ujian TOEFL yang sedang berjalan.
3. Observasi yaitu teknik pengumpulan data dengan cara mengamati langsung pada saat sertifikat dibuat oleh Pusat Bahasa Universitas Kuningan.

1.5.2. Metode Pengembangan Perangkat Lunak

Metode pengembangan sistem yang digunakan oleh penulis adalah *Rational Unified Process* (RUP) dengan alasan metode pengembangna ini sangat cocok untuk pemrograman berorientasi objek. *Rational Unified Process* (RUP) merupakan proses pengembangan perangkat lunak yang dilakukan secara iteratif (berulang) dan inkremental (bertahap dengan progres menaik).

Iteratif bisa dilakukan dalam setiap tahap atau iteratif tahap pada proses pengembangan perangkat lunak untuk menghasilkan perbaikan fungsi yang inkremental (bertambah naik) dimana setiap iterasi akan memperbaiki iterasi berikutnya. **(AS Rosa dan M. Shalahuddin, 2013.124).**

Gambar dibawah menunjukkan secara keseluruhan arsitektur yang dimiliki RUP. Melalui gambar dibawah dapat dilihat bahwa RUP memiliki, yaitu:



Gambar 1.1 Arsitektur *Rational Unified Process* **(Suryana, 2007)**

1. **Dimensi pertama** digambarkan secara horizontal. Dimensi ini mewakili aspek-aspek dinamis dari pengembangan perangkat lunak. Aspek ini dijabarkan dalam tahapan pengembangan atau fase. Setiap fase akan memiliki suatu *major milestone* yang menandakan akhir dari awal dari phase selanjutnya. Setiap phase dapat berdiri dari satu beberapa iterasi. Dimensi ini terdiri atas

Inception, *Elaboration*, *Construction*, dan *Transition*.

2. **Dimensi kedua** digambarkan secara vertikal. Dimensi ini mewakili aspek-aspek statis dari proses pengembangan perangkat lunak yang dikelompokkan ke dalam beberapa disiplin. Proses pengembangan perangkat lunak yang dijelaskan kedalam beberapa disiplin terdiri dari empat elemen penting, yakni *who is doing*, *what*, *how* dan *when*. Dimensi ini terdiri atas *Business Modeling, Requirement, Analysis and Design, Implementation, Test, Deployment, Configuration* dan *Change Manegement, Project Management, Environtment.* **(Suryana, 2007)**.

Ada 4 fase yang akan digunakan dalam metode RUP yaitu:

1. *Inception* (permulaan)

   Pada tahap ini pengembang mendefinisikan batasan kegiatan, melakukan analisis kebutuhan user, dan melakukan perancangan awal perangkat lunak (perancangan arsitektural dan *use case*). Pada akhir fase ini, prototipe perangkat lunak masih belum diterapkan pada program.

2. *Elaboration* (perluasan/rencana)

   Pada tahap ini dilakukan perancangan perangkat lunak mulai dari menspesifikasikan fitur perangkat lunak, mencari resiko terburuk dalam perancangan aplikasi dan mencari solusi terbaik untuk mengurangi resiko program yang tidak diharapkan, pada tahap ini juga program sudah mulai di buat.

3. *Construction* (konstruksi)

Pengimplementasian rancangan perangkat lunak yang telah dibuat dilakukan pada tahap ini. Pada akhir tahap ini, perangkat lunak versi awal harus sudah jadi dan aplikasi sudah berjalan sesuai dengan rancangan .

4. *Transition* (transisi)

Tahap penyelesaian mencari *bug* pada program dan memperbaikinya Program harus sudah benar-benar berjalan sesuai rancanngan . Instalasi , *deployment* perangkat lunak dilakukan pada tahap ini.

1.6. Sistematika Penulisan

Sistematika penulisan yang digunakan untuk mengembangkan skripsi ini adalah sebagai berikut :

BAB I : PENDAHULUAN

Bab ini menjelaskan secara singkat mengenai latar belakang masalah, identifikasi masalah, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, metode penelitian dan sistematika penulisan.

BAB II : LANDASAN TEORI

Bab ini menjelaskan tentang teori-teori yang mendukung dalam menyelesaikan permasalahan yang akan dibahas serta menjadi landasan dalam memecahkan masalah yang sedang dihadapi.

BAB III : ANALISIS DAN PERANCANGAN

Bab ini berisi analisis masalah, analisis sistem, analisis kebutuhan user (pengguna), analisis algoritma *Rivest Shamir Adleman* (RSA) dalam sistem enkripsi dan dekripsi, desain sistem dan perancangan antar muka (*interface design*) perangkat lunak.

BAB IV : HASIL DAN PEMBAHASAN

Bab ini membahas implementasi dari tahapan analisis dan perancangan sistem ke dalam perangkat lunak (dalam bahasa pemrograman) dan membahas mengenai hasil dari pengujian sistem.

BAB V : PENUTUP

Bab ini berisi kesimpulan dan saran. Kesimpulan berisi ringkasan hasil implementasi dan pengujian. Sedangkan saran berisi usulan-usulan lanjut dari permasalahan yang ditinjau.