pendahuluan

## Latar Belakang

Seiring perkembangan teknologi, banyak lembaga pendidikan yang menerapkan sistem ujian *online,* termasuk di dalamnya tingkat universitas. Salah satu Universitas yang sudah menerapkan adalah Universitas Lampung. Penerapan sistem ini merupakan salah satu cara untuk meningkatkan kualitas pendidikan dan pengajaran di Universitas Lampung. Dalam penelitian ini, akan diambil lingkup yang lebih spesifik yaitu Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam (MIPA) Universitas Lampung.

Selain menawarkan banyak kemudahan dalam banyak hal, seperti penilaian, efisiensi ruang dan alat tulis menulis, sistem ujian *online* tersebut juga memiliki sisi negatif. Sistem ini harus terhubung dengan internet yang merupakan jaringan publik. Dengan kata lain, sistem *online* terbuka bagi setiap orang di seluruh dunia untuk menggabungkan diri. Mengingat sistem ujian *online* tersebut masih menggunakan protokol HTTP dalam proses pengiriman data informasi hal ini dapat mengakibatkan sistem rentan terhadap *sniffer* jaringan yang berusaha mencuri informasi autentikasi, seperti *username* dan *password*.

Keamanan menjadi salah satu aspek penting yang harus diperhatikan mengingat banyaknya komputer yang dihubungkan dalam suatu jaringan dan banyaknya *user* yang memakai, suatu data maupun informasi menjadi sangat rentan terhadap serangan-serangan dari pihak yang tidak berwenang. Setiap kali *user* mengidentifikasikan dirinya ke komputer, komputer harus memastikan apakah identifikasi tersebut autentik atau tidak. Cara yang paling umum melakukan proses autentikasi adalah menggunakan *password* (Istihadi Ali, 2004).

Saat memulai ujian, setiap *user* harus melakukan proses *login* dengan memasukkan *password*. Namun yang selama ini diterapkan adalah penggunaan *password* yang sama (*password* statis). Jika *user* menggunakan *password* yang sama untuk masuk ke dalam suatu sistem, hal itu dapat menyebabkan *password* tersebut menjadi rentan terhadap *sniffer* jaringan melakukan *replay attack*. Salah satu bentuk serangan adalah *attacker* mencoba masuk ke dalam suatu koneksi jaringan untuk mendapatkan informasi autentikasi.

Metode autentikasi *one time password* (OTPA) dibuat untuk mengatasi masalah tersebut. Setelah suatu *password* dipakai, maka *password* yang sama tidak dapat dipakai untuk kedua kalinya. *Token* digunakan untuk men-*generate* *password*/PIN, *token* yang digunakan dalam penelitian ini adalah *token* yang berwujud *software* dan diinstal di *handphone,* atau disebut *mobile token*.

Implementasi Metode autentikasi o*ne time password* (OTPA) Berbasis *Mobile Token* Pada Aplikasi Ujian *Online* ini berusaha memperkecil bahkan kalau bisa meniadakan kemungkinan untuk akses ilegal ketika melakukan proses ujian *online*.

## Rumusan Masalah

Dari latar belakang penelitian ini dapat dirumuskan menjadi beberapa masalah sebagai berikut:

1. Bagaimana membuat aplikasi Ujian *Online* dengan tingkat *security* yang lebih baik pada proses autentikasi?.
2. Bagaimana mengimplementasikan metode autentikasi *one time password* (OTPA) pada aplikasi Ujian *Online* jurusan matematika FMIPA Universitas Lampung?.

## Batasan Masalah

Batasan masalah dari penelitian ini adalah sebagai berikut:

1. Aplikasi *Mobile Token* yang dibangun merupakan aplikasi yang tidak terhubung langsung dengan aplikasi Ujian *Online* dan dibangun dengan bahasa *Java2 Micro Edition* (J2ME).
2. *Generate* *secret code* dan sinkronisasi waktu pada aplikasi *Mobile Token* dengan aplikasi Ujian *Online* dilakukan sebelum proses autentikasi dilakukan.
3. *Challenge code* secara otomatis dihasilkan oleh aplikasi Ujian *Online* dan digunakan pada aplikasi *Mobile Token* untuk men-*generate* sebuah PIN atau *one time password*.
4. Algoritma *Message Digest* 5 (MD5) tidak akan dibahas.

## Tujuan Penelitian

Tujuan yang diharapkan dapat tercapai melalui penelitian ini adalah sebagai berikut:

1. Tercipta-nya aplikasi Ujian *Online* Jurusan Matematika FMIPA Universitas Lampung dengan tingkat keamanan yang lebih baik pada proses autentikasi.
2. Menerapkan metode autentikasi *one time password* (OTPA) yang akan diimplementasikan pada proses autentikasi aplikasi Ujian *Online* Jurusan Matematika FMIPA Universitas Lampung.

## Manfaat Penelitian

Pelaksanaan penelitian ini diharapkan bermanfaat untuk:

1. Meningkatkan keamanan aplikasi Ujian *Online* Jurusan Matematika FMIPA Universitas Lampung pada proses autentikasi.
2. Dapat menerapkan metode autentikasi o*ne time password* (OTPA) dalam bidang keamanan sistem informasi.
3. Pengembangan aplikasi yang serupa dalam penelitian-penelitian lainnya.

## Metodologi Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Studi Pustaka

Studi kepustakaan dilakukan dengan cara mengumpulkan data atau informasi yang diperlukan melalui buku-buku komputer, jurnal ilmiah, dan halaman website yang menjelaskan tentang metode autentikasi o*ne time password* (OTPA), pemrograman perangkat telekomunikasi *mobile* (J2ME) dan bahasa pemrograman PHP-MYSQL.

1. Model Pengembangan Aplikasi

Model pengembangan aplikasi yang digunakan adalah model *Waterfall*, adapun tahap-tahap pengembangan model *Waterfall* adalah:

1. Analisis dan definisi persyaratan

Pelayanan, batasan, dan tujuan sistem ditentukan melalui konsultasi dengan *user*. Bisa melalui wawancara secara langsung atau menggunakan kuesioner untuk mengetahui keinginan dari *user* mengenai perangkat lunak yang akan dibuat.

1. Perancangan sistem dan perangkat lunak

Kegiatan ini menentukan arsitektur sistem secara keseluruhan. Proses desain mengubah kebutuhan-kebutuhan menjadi bentuk karakteristik yang dimengerti perangkat lunak sebelum dimulai penulisan program.

1. Implementasi dan pengujian unit

Perancangan perangkat lunak direalisasikan sebagai serangkaian program.

1. Integrasi dan pengujian sistem

Unit program diintegrasikan atau diuji sebagai sistem yang lengkap untuk menjamin bahwa persyaratan sistem telah terpenuhi. Setelah kode program selesai dibuat, dan program dapat berjalan, testing dapat dimulai. Testing difokuskan pada logika internal dari perangkat lunak, fungsi eksternal, dan mencari segala kemungkinan kesalahan.

1. Operasi dan pemeliharaan

Merupakan fase siklus yang paling lama. Sistem di install dan dipakai. Perbaikan mencakup koreksi dari berbagai error, perbaikan dan implementasi unit sistem dan pelayanan sistem.

## Sistematika Penulisan

Sistematika penulisan skripsi ini disusun dari beberapa BAB yang berurutan sebagai berikut:

**BAB I PENDAHULUAN**

Menjelaskan tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

**BAB II TINJAUAN PUSTAKA**

Menjelaskan tentang dasar teori yang digunakan sebagai sumber untuk memahami permasalahan yang ada pada penelitian.

**BAB III METODOLOGI PENELITIAN**

Menjelaskan tentang obyek dan tahapan yang dilakukan pada penelitian.

**BAB IV HASIL DAN PEMBAHASAN**

Menjelaskan tentang analisis kebutuhan, desain proses, implementasi dan pengujian metode *one time password* (OTP).

**BAB V KESIMPULAN DAN SARAN**

Bab ini berisi kesimpulan yang merupakan hasil dari implementasi program dan saran untuk pengembangan program untuk penelitian di masa yang akan datang.