

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Ujian adalah kegiatan yang dilakukan untuk mengukur pencapaian kompetensi peserta didik sebagai pengakuan prestasi belajar dan/atau penyelesaian dari suatu satuan pendidikan[1].

Dalam permasalahan kali ini, akan membahas tentang aplikasi pelatihan yang disebut ICT (*Information and Communication Technology*). Aplikasi ICT ini sudah dikembangkan pada tahun 2017. Aplikasi ini mempunyai fitur seperti pendaftaran pengguna, pemilihan kelas, serta sertifikat kelulusan ICT. Akan tetapi untuk ujian online atau ujian berbasis komputer masih menggunakan Aplikasi CBT (*Computer Based Text*) sehingga aplikasi ini belum sepenuhnya lengkap.

Namun selain belum mempunyai fitur ujian berbasis komputer, aplikasi ICT ini mempunyai permasalahan dalam *backup* data. Karena persyaratan untuk melakukan ujian CBT yaitu memerlukan data peserta, maka data formulir dari ICT perlu melakukan *backup* agar ujian dapat dilaksanakan. *Backup* data dilaksanakan setiap periode dengan jumlah lebih dari 1000 peserta, akan tetapi lebih dari 1000 peserta juga mengalami beberapa kesulitan yaitu beberapa peserta yang tidak disebutkan dalam ujian CBT karena performa dari *backup* data.

Dalam penelitian ini akan membahas tentang perancangan perangkat lunak ujian online berbasis web menggunakan *Fisher-Yates Shuffle* dan *MD5*. Dimana ujian online akan melakukan permutasi bilangan acak dari satu set terbatas menggunakan Algoritma *Fisher-Yates Shuffle* dan soal ujian akan melakukan enkripsi satu arah dengan menggunakan Algoritma *MD5* sehingga pengguna tidak

akan bisa melihat soal ujian secara publik dan akan dipulihkan kembali dengan melaksanakan ujian sesuai jadwal yang ditentukan.

Dengan diterapkannya soal ujian acak ini, mahasiswa dapat mengisi soal-soal ujian dengan nomor soal yang berbeda. Dalam segi keamanan, secara eksternal soal ujian akan ditampilkan dan diurutkan seperti biasa dan soal ujian akan terenkripsi sebelum memulai ujian namun secara internal soal ujian akan diproses menggunakan algoritma. Hal ini dilakukan agar mahasiswa dapat mengerjakan soal ujian dengan nomor soal yang berbeda serta tidak bisa melakukan pembocoran soal ke publik.

Untuk penelitian tugas akhir ini, maka penulis akan memberikan tema yang berjudul **“Perancangan Sistem Ujian Berbasis Komputer Menggunakan Fisher–Yates Shuffle Dan Message Digest 5 (MD5)”**



1.2. Perumusan Masalah

Sesuai dari latar belakang masalah yang telah diuraikan di atas, maka dapat dirumuskan masalah sebagai berikut :

- a. Bagaimana algoritma *Fisher-Yates Shuffle* dapat mengacak soal ujian berbasis komputer ?
- b. Bagaimana algoritma *MD5* bekerja supaya soal ujian tidak dapat terbaca oleh publik ?
- c. Bagaimana penerapan implementasi algoritma *Fisher-Yates Shuffle* dan *MD5* pada sistem ujian berbasis komputer ?

1.3. Batasan Masalah

Untuk penelitian sistem ujian online berbasis komputer ini, akan ditetapkan beberapa batasan masalah diantaranya :

- a. Aplikasi ujian ini berbasis komputer.
- b. Satu komputer hanya bisa digunakan oleh satu pengguna.
- c. Aplikasi ini dilakukan untuk mahasiswa tetap UIN Sunan Gunung Djati Bandung.

1.4. Tujuan Penelitian

Untuk penelitian sistem ujian berbasis komputer ini, akan ditetapkan tujuan dari penelitian ini yaitu :

- a. Mengetahui penerapan dari algoritma *Fisher-Yates Shuffle* dalam mengacak beberapa angka ketika ujian akan dimulai.
- b. Mengetahui penerapan dari algoritma *Message Digest 5 (MD5)* dalam segi keamanan.

- c. Membangun sistem ujian berbasis komputer dengan algoritma *Fisher-Yates Shuffle* dari segi tampilan kemudian algoritma *Message Digest 5 (MD5)* dalam segi keamanan.

1.5. Kerangka Pemikiran

Kerangka pemikiran berisikan tentang *problem*, *opportunity*, *approach*, *software development*, *software implementation*, dan *result*. Untuk kerangka pemikiran pada sistem ujian online berbasis komputer dapat digambarkan dengan tabel seperti berikut :

Tabel 1.1 Kerangka Pemikiran

<i>Problem</i>	Aplikasi ICT belum memiliki fitur ujian berbasis komputer.
<i>Opportunity</i>	Merancang sistem ujian berbasis komputer
<i>Approach</i>	Sistem ujian berbasis komputer dengan algoritma <i>Fisher-Yates Shuffle</i> dan <i>Message Digest 5 (MD5)</i>
<i>Software Development</i>	<ul style="list-style-type: none"> • Metode Pengembangan <i>Prototype</i> • <i>Framework Codeigniter</i>
<i>Software Implementation</i>	<ul style="list-style-type: none"> • Algoritma <i>Fisher-Yates Shuffle</i> dan <i>Message Digest 5 (MD5)</i> • Web Based <i>PHP</i> • DBMS <i>MySQL</i>
<i>Result</i>	Sistem Ujian Berbasis Komputer Menggunakan Algoritma <i>Fisher-Yates Shuffle</i> dan <i>Message Digest 5 (MD5)</i>

1.6. Metodologi

1.6.1. Metodologi Penelitian

Metodologi yang dipakai untuk penelitian sistem ujian berbasis komputer ini meliputi : [2]

a. Pengumpulan Data

Metode ini merupakan penelitian pengumpulan informasi berupa data-data sebagai berikut :

1. Observasi

Observasi merupakan pengumpulan data dengan mengamati penelitian dan percobaan langsung terhadap objek penelitian.

2. Studi Literatur

Studi Literatur merupakan pengumpulan data dengan mengumpulkan sumber dari jurnal, buku, dan sumber lain yang berhubungan dengan tugas akhir.

b. Analisis dan Perancangan

Analisis merupakan data yang sudah dikumpulkan untuk kebutuhan perangkat lunak yang akan dirancang, kemudian penulisan perancangan program kemudian yang terakhir adalah pengujian. Perancangan dilakukan setelah tahapan analisis dimana awal dari perancangan akan dilakukan perubahan pada fitur perangkat lunak menjadi fitur yang jelas sehingga mudah dipahami.

c. Penulisan Program

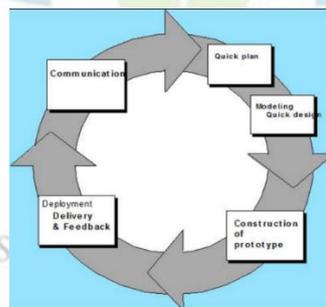
Penulisan program merupakan perancangan program aplikasi dimana pada penulisan ini akan digunakan bahasa pemrograman PHP dengan framework Codeigniter.

d. Pengujian

Pengujian merupakan ujicoba program aplikasi dimana program yang telah dirancang akan ditinjau supaya program yang sudah jadi bisa diperbaiki kembali.

1.6.2. Metodologi Pengembangan

Penelitian ini akan menggunakan pengembangan perangkat lunak dengan model *prototype*. Model pengembangan *prototype* berguna untuk mengetahui ketidakpahaman *customer* mengenai alur dari program dan memperjelas kebutuhan yang diinginkan *customer* kepada pengembang perangkat lunak [2].



Gambar 1.1 Ilustrasi Model Prototype

1.7. Sistematika Penulisan

Ada 5 (lima) bab dalam sistematika penulisan perangkat lunak yang telah disusun dengan tujuan tertentu. Berikut sistematika penulisan tentang masing-masing bab :

BAB I PENDAHULUAN

Pendahuluan menjelaskan latar belakang permasalahan tentang judul tugas akhir. Permasalahan ini diharuskan mengandung alasan yang kuat agar dapat dimengerti.

BAB II STUDI PUSTAKA

Studi pustaka menjelaskan beberapa karya jurnal dan teori yang berhubungan dengan judul tugas akhir serta menyelesaikan latar belakang masalah.

BAB III ANALISIS DAN PERANCANGAN APLIKASI

Analisis dan perancangan aplikasi menjelaskan perencanaan pengembangan aplikasi yang akan dibangun serta menggambarkan alur perencanaan untuk pengembangan aplikasi.

BAB IV IMPLEMENTASI DAN PENGUJIAN APLIKASI

Implementasi dan pengujian aplikasi menjelaskan proses pengkodean aplikasi, mengetahui kebutuhan perangkat keras, perangkat lunak yang dibutuhkan untuk melakukan pengkodean aplikasi. Pengujian menjelaskan hasil dari pengkodean aplikasi serta kebutuhan perangkat keras dan perangkat lunak.

BAB V PENUTUP

Penutup menjelaskan beberapa kesimpulan dan saran.