Computer Based Test Untuk Seleksi Masuk Politeknik Negeri Bengkalis

Agus Tedyyana[1], Danuri[2]
[1,2] Program Studi Rekayasa Perangakat Lunak Jurusan Teknik Informatika
Politeknik Negeri Bengkalis
Jl. Bathin Alam, Sungai Alam, Kec. Bengkalis, Kabupaten Bengkalis, Riau 28711
e-mail: [1]agustedyyana@polbeng.ac.id, [2]danuri@polbeng.ac.id

Abstrak

Penyeleksian calon mahasiswa baru dapat dilakukan dengan aplikasi Computer Based Test (CBT). Metode yang digunakan meliputi teknik pengumpulan data, analisis sistem, model perancangan, implementasi dan pengujian. Penelitian ini menghasilkan aplikasi CBT dimana soal yang dimunculkan dari bank soal melalui proses pengacakan dengan tidak akan memunculkan soal yang sama dengan menggunakan metoda Fisher-Yates Shuffle. Dalam proses pengamanan informasi soal saat terhubung ke jaringan maka diperlukan teknik untuk penyandian pesan agar soal tersebut sebeum dimunculkan melewati proses enkripsi dan deskripsi data terlebih dahulu maka digunakan algoritma kriptografi RSA. Metode perancangan perangkat lunak menggunakan model waterfall, perancangan database menggunakan entity relationship diagram, perancangan antarmuka menggunakan hypertext markup language (HTML) Cascading Style Sheet (CSS) dan jQuery serta diimplementasikan berbasis web dengan menggunakan bahasa pemrograman PHP dan database MySQL, Arsitektur jaringan yang digunakan aplikasi Computer Based Test adalah model jaringan client-server dengan jaringan Local Area Network (LAN).

Kata kunci: *Computer Based Test, Fisher-Yates Shuffle, Criptography, Local Area Network*

Abstract

Selection of new student candidates can be done with Computer Based Test (CBT) application. The methods used include data collection techniques, system analysis, design model, implementation and testing. This study produces a CBT application where the questions raised from the question bank through randomization process will not bring up the same problem using the Fisher-Yates Shuffle method. In the process of securing information about the problem when connected to the network it is necessary techniques for encoding the message so that the problem before appear through the process of encryption and description of data first then used RSA cryptography algorithm. Software design method using waterfall model, database design using entity relationship diagram, interface design using hypertext markup language (HTML) Cascading Style Sheet (CSS) and jQuery and implemented web-based using PHP programming language and MySQL database, Network architecture used application Computer Based Test is a client-server network model with a Local Area Network (LAN) network.

Keywords: *Computer Based Test, Fisher-Yates Shuffle, Criptography, Local Area Network.*

1. Pendahuluan

Politeknik Negeri Bengkalis merupakan salah satu perguruan tinggi di Propinsi Riau dengan tiga jalur penerimaan mahasiswa baru yaitu Penelusuran Minat dan Bakat-Politeknik Negeri (PMDK-PN), Ujian Masuk Politeknik Negeri (UMPN) dan Ujian Mandiri Politeknik Negeri Bengkalis.

Tes masuk Politeknik Negeri Bengkalis melalui jalur UMPN dan jalur ujian mandiri sampai saat ini dilakukan secara *Paper Based Test* (PBT) yakni melalui tes tertulis dengan membagikan lembar soal dan lembar jawaban kepada peserta tes kemudian peserta mengisi lembar jawaban yang telah disediakan oleh panitia. Model PBT ini memiliki beberapa kelemahan yaitu penggunaan kertas yang cukup banyak, adanya kemungkinan terjadi kebocoran soal, manipulasi data hasil tes dan berbagai kecurangan selama proses tes berlangsung. Untuk meminimalisir hal tersebut diusulkan model CBT dengan menggunakan metode *Fisher-Yates Shuffle* dan algoritma kriptografi RSA pada arsitektur sistem berbasis web server.

CBT didefinisikan sebagai tes atau penilaian yang diberikan oleh komputer baik yang bersifat *stand-alone* maupun yang bersifat *dedicated network*, atau dengan perangkat teknologi lain yang terhubung ke internet atau World Wide Web dan sebagian besar menggunakan *Multiple Choice Question* (MCQS) [1]. Baru-baru ini CBT telah di terapkan di beberapa sekolah di Indonesia untuk Ujian Nasional (UN) tingkat Sekolah Menengah Atas (SMA).

Pada penentuan hasil penilaian secara umum CBT memiliki hasil penilaian yang lebih baik dari pada PBT dan efek yang kedua yaitu uji kinerja dan motivasi peserta tes terhadap CBT dan PBT, motivasi peserta tes untuk mengikuti tes menggunakan PBT maupun CBT hampir sama [2].

Algoritma *Fisher-Yates Shuffle* dapat digunakanuntuk membangkitkan daftar kartu yang muncul secara random dalam fungsi permutasi dan menggunakan bahasa pemrograman VB.Net untuk membuat simulasi permainan kartu. *Fisher-Yates Shuffle* merupakan cara yang optimal dengan waktu eksekusi yang efisien, serta dengan ruang penyimpanan memori yang tidak terlalu besar [3].

Berbeda dengan penelitian sebelumnya, penelitian kriptografi untuk kunci public dengan metode Rivest Shamir Adleman (RSA). Pada penelitiannya menggunakan dua kunci publik dan beberapa relation matematika. Dua kunci publik (*key public*) dikirim secara terpisah sehingga membuat penyerang tidak mendapatkan banyak pengetahuan tentang kunci (*key*) dan tidak mampu mendekripsi pesan yang dikirim. RSA dapat digunakan untuk sistem yang memerlukan keamanan yang tinggi [4].

Hasil simulasi yang disajikan menunjukkan bahwa metode RSA umumnya lebih baik dari Logaritma Diskrit (El Gamal) karena RSA menghasilkan cipher dengan jumlah kecil sehingga menghemat memori. Keunggulan lain dari RSA adalah mengurangi lalu lintas (*traffic*) dan menghemat *bandwidth* dalam jaringan [5].

Terkait dengan CBT dalam penelitian yang berjudul "Membangun Webserver Intranet Dengan Linux (Studi Kasus di Laboratorium Komputer SMP Negeri 38 Seluma Bengkulu Selatan)", menjelaskan bahwa Web Server Sekolah secara *offline* sangat membantu cara belajar-mengajar disekolah dan lebih praktis karena guru tidak lagi repot menuliskan materi dipapan tulis. Dengan bantuan infokus para siswa dapat menyimak guru dalam menjelaskan materi Tugas-tugas sekolah dapat langsung dikerjakan melalui fasilitas *E-Learning* dan materi pembelajaran dapat ditambah sesuai kebutuhan [6].

Sistem Computer Based Test (CBT) telah dikembangkan untuk adopsi di Universitas Nigeria. Sistem ujian online memberikan pertanyaan yang ditetapkan oleh dosen kepada mahasiswa dan menghasilkan laporan dari hasil mahasiswa yang mengikuti ujian serta keseluruhan ringkasan hasil ujian berdasarkan permintaan pengguna. Beberapa masalah seperti kesalahan dalam pemeriksaan hasil ujian, kecurangan saat ujian berlangsung, penggunaan kertas yang banyak dan lainnya akan otomatis diminimalisir setelah diadopsi sistem ujian berbasis komputer. Biaya pemeriksaan hasil ujian secara signifikan berkurang karena tidak akan ada kebutuhan untuk mencetak pertanyaan atau jawaban buku lagi. Namun, penelitian selanjutnya harus mengakomodasi pertanyaan berbasis teori dan e-penilaian berbasis video supaya apabila ada kejadian yang tidak diinginkan dapat diselidiki [7].

Metode Fisher-Yates Shuffle (dinamai berdasarkan penemunya, Ronald Fisher dan Frank Yates) digunakan pada proses pengacakan soal dengan mengubah urutan masukan yang

diberikan secara acak. Permutasi yang dihasilkan oleh algoritma ini muncul dengan probabilitas yang sama. Algoritma ini dinyatakan bias karena permutasi yang dihasilkan oleh algoritma ini muncul dengan probabilitas yang sama, hal ini dibuktikan dengan percobaan mengacak suatu set kartu yang dilakukan berulang – ulang kemudian diambil satu per satu, sehingga hasilnya tidak akan sama karena yang diacak adalah urutannya [3].

Kriptografi berasal dari Bahasa Yunani, kripto dan graphia. Kripto artinya menyembunyikan, sedangkan Graphia artinya tulisan. Secara umum, Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Namun, tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi. Selain itu, Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan. RSA adalah sebuah algoritma berdasarkan skema *public-key cryptography*. Diberi nama RSA sebagai inisial para penemunya: Ron Rivest, Adi Shamir, dan Leonard Adleman. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor- faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci pribadi. Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan algoritma yang benar, maka selama itu pula keamanan algoritma RSA tetap terjamin [8].

Web Server adalah sebuah *software* yang memberikan layanan berbasis data dan berfungsi menerima permintaan dari HTTP atau HTTPS pada klien dan biasanya kita kenal dengan nama web browser yang kemudian akan mengirimkan kembali hasilnya dalam bentuk beberapa halaman web dan pada umumnya akan berbentuk dokumen HTML. Dalam bentuk sederhana web server akan mengirim data HTML kepada permintaan web Browser sehingga akan terlihat seperti pada umumnya yaitu sebuah tampilan website. Penggunaan paling umum server web adalah untuk menempatkan situs web, namun pada prakteknya penggunaannya diperluas sebagai tempat peyimpanan data ataupun untuk menjalankan sejumlah aplikasi kelas bisnis [9].

Berdasarkan latar belakang diatas, alternatif yang tepat untuk mengatasi kelemahan-kelemahan yang terjadi ketika menggunakan versi *Paper Based Test* (PBT) yaitu perlu di buat Sistem Ujian Masuk Calon Mahasiswa Baru terutama di Politeknik Negeri Bengkalis dengan versi *Computer Based Test* (CBT) menggunakan Fisher-Yates Shuffle dan Algoritma Kriptografi RSA pada Web Server.

2. Metode Penelitian

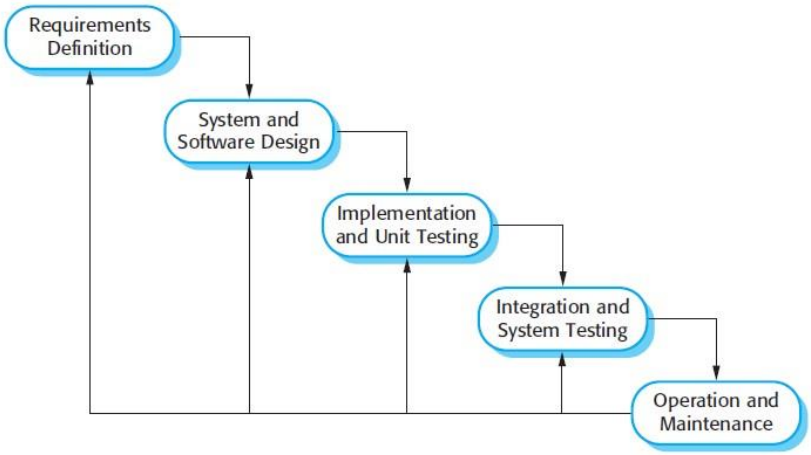
Metode Penelitian yang digunakan pada penelitian ini adalah:

a. Tahapan requirement melakukan pengumpulan data menggunakan metode observasi, studi literatur, dan analisis sistem yang terbagi menjadi dua bagian yaitu analisis sistem yang berjalan dan analisis sistem yang diusulkan.
b. Tahapan perancangan sistem meliputi:
   i. Model pengacakan (*Shuffel*)
      Pada penelitian ini menggunakan model pengacakan (*shuffel*) untuk mengacak soal pada bank soal penyeleksian calon mahasiswa baru.
   ii. Model enkripsi data
      Skema algoritma kunci publik Sandi RSA terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi.
   iii. Model arsitektur jaringan
      Arsitektur jaringan yang digunakan adalah model jaringan client-server dengan jaringan LAN (*Local Area Network*). Dimana terdapat beberapa unit komputer (*client*) dan satu unit komputer yang digunakan sebagai bank data (server). Pada umumnya model client-server berbentuk pesan permintaan untuk melaksanakan berbagai pekerjaan dari client kepada *server*. Setelah *server* selesai melaksanakan pekerjaannya, *server* akan mengirimkan hasilnya kepada *client*.

iv. Perancangan UML
Perancangan UML meliputi *usecase diagram*, *activity diagram*, dan *sequence diagram*.
v. Perancangan *database*
Perancangan database meliputi perancangan *entity relationship diagram* dan perancangan tabel.
vi. Perancangan *interface*
Perancangan *interface* meliputi perancangan *interface input* dan *interface output*.

c. Tahapan implementasi. Implementasi dengan menerapkan *server side scripting* bahasa pemrograman PHP, *database* MySQL dan Jaringan LAN.
d. Pengujian sistem. Pengujian sistem menggunakan metode *blackbox*.

Tahapan penelitian dapat dilihat pada Gambar 1.

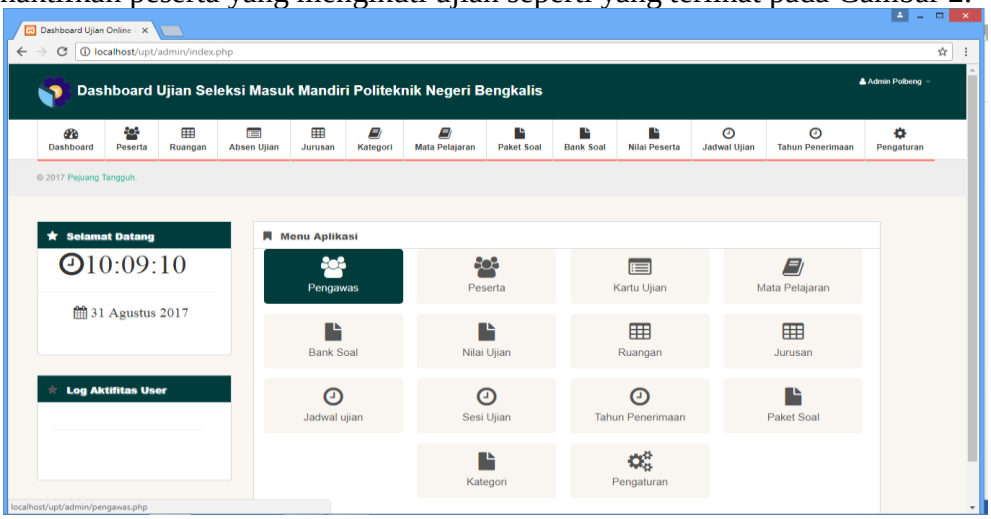


Gambar 1. MetodeWaterfall [10]

3. Hasil dan Pembahasan

3.1 Data Pengawas

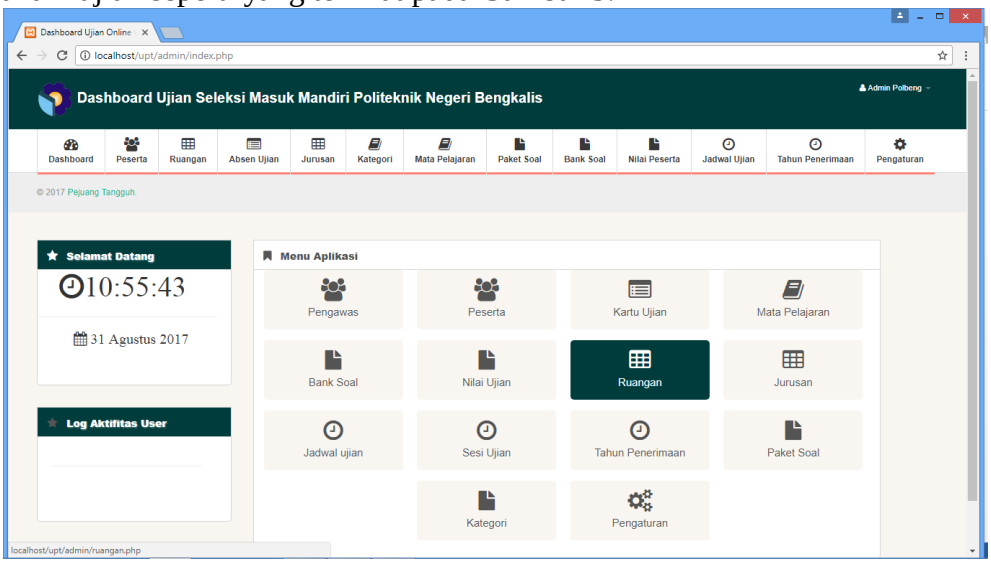
Pengawas disini berperan sebagai pengawas jalannya ujian, peran pengawas disini sangat penting dimana pengawas bertugas untuk mengaktifkan dan menonaktifkan peserta yang mengikuti ujian seperti yang terlihat pada Gambar 2.



Gambar 2. Menambah, edit dan hapus data pengawas

3.2 Data Ruangan

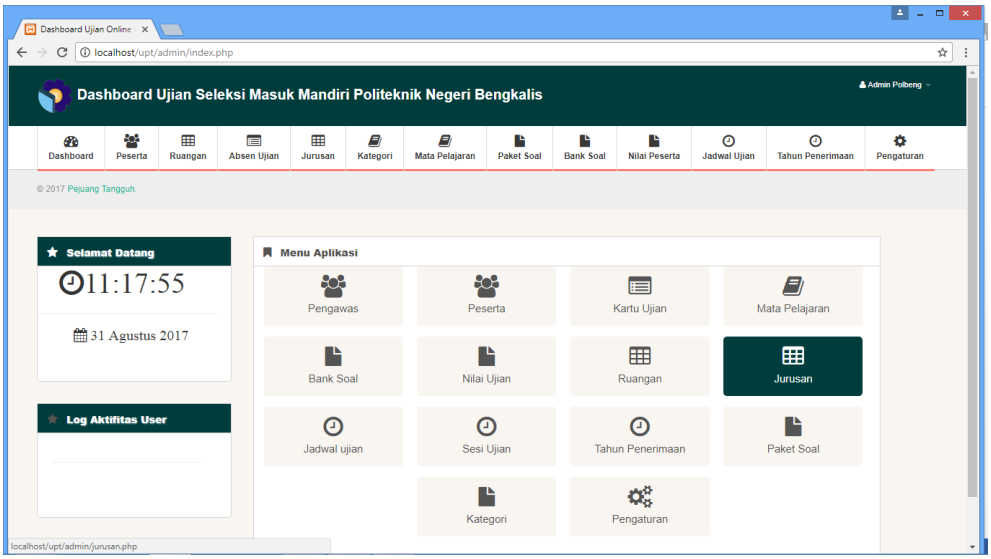
Data ruangan disini sangat dibutuhkan untuk mendata ruangan yang akan digunakan ujian seperti yang terlihat pada Gambar 3.



Gambar 3. Menambah, edit ,hapus data ruangan

3.3 Data Jurusan

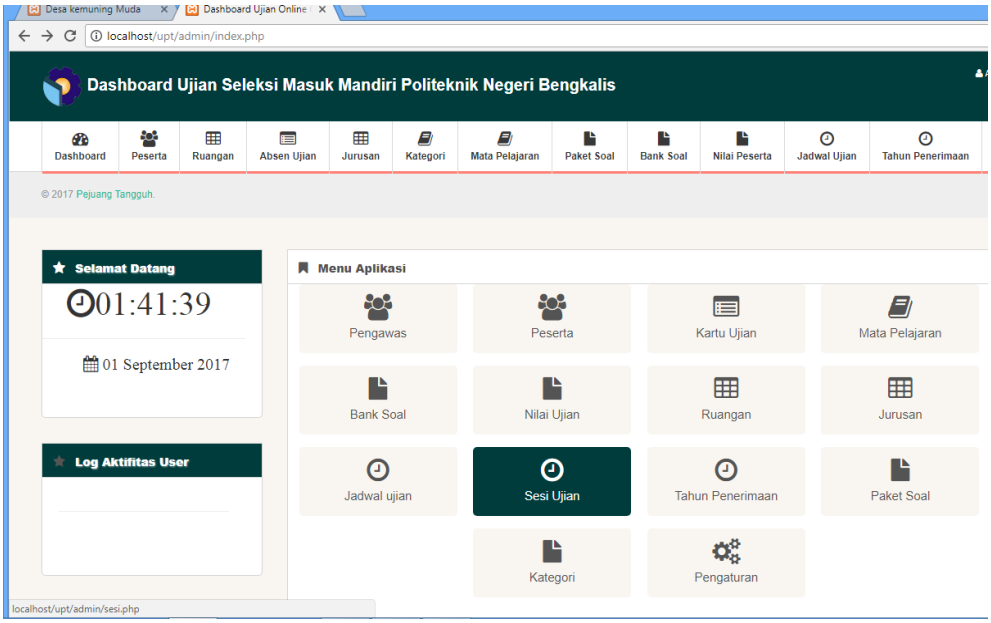
Data Jurusan dibutuhkan untuk mengelola data yang berhubungan dengan jurusan yang akan dipilih peserta yang mengikuti ujian seperti yang terlihat pada Gambar 4.



Gambar 4. Menu Data Jurusan

3.4 Sesi Ujian

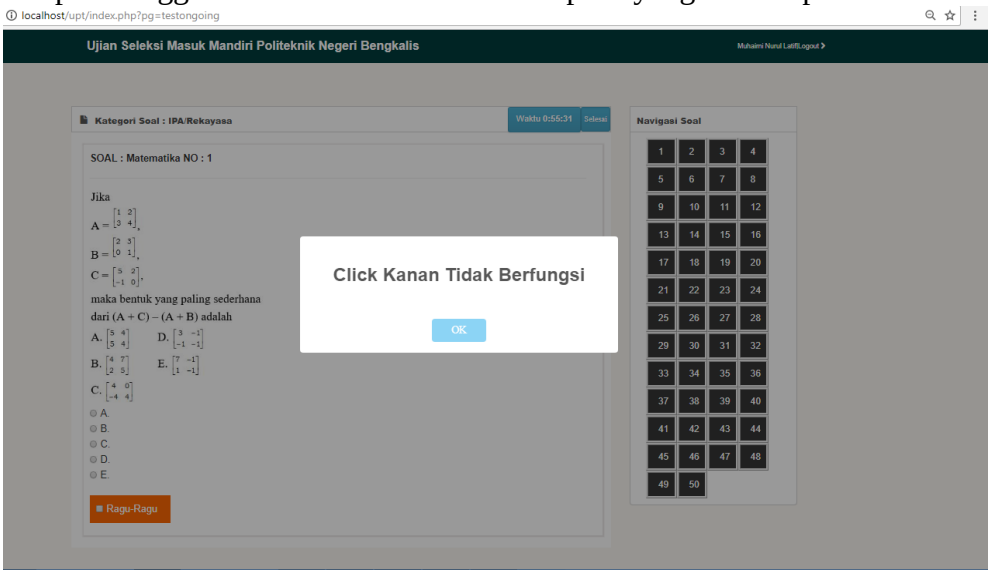
Ini digunakan untuk mengelola sesi ujian yang akan di ujiankan, sesi ini digunakan karena kurangnya fasilitas ruangan yang bisa digunakan untuk ujian Untuk menambah sesi ujian pilih menu sesi ujian seperti yang terlihat pada Gambar 5.



Gambar 5. Menu data sesi ujian

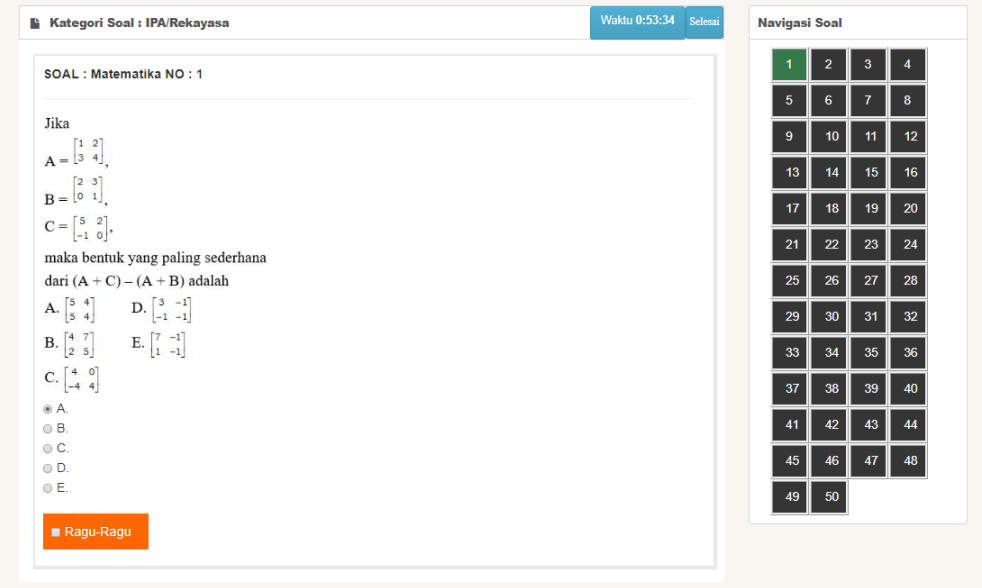
Dalam mengerjakan ujian terdapat beberapa hal yang harus di perhatikan

1. Klik kanan tidak berfungsi, untuk selama proses pengerjaan ujian peserta tidak dapat menggunakan fasilitas klik kanan seperti yang terlihat pada Gambar 6.



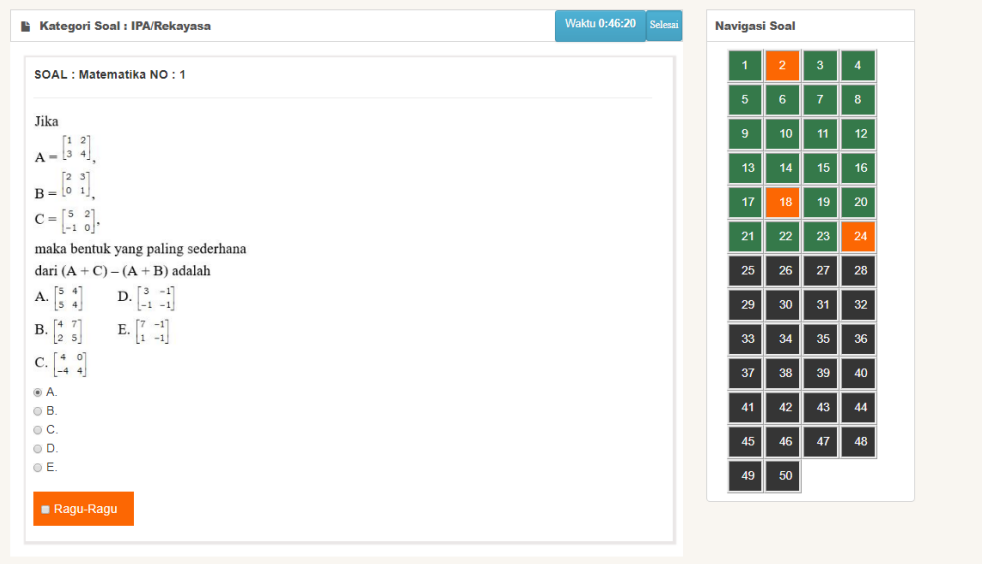
Gambar 6. Fasilitas klik kanan tidak difungsikan

2. Soal yang sudah dijawab akan memberikan efek kepada navigasi soal sehingga navigasi soal akan berwana hijau seperti yang terlihat pada Gambar 7.



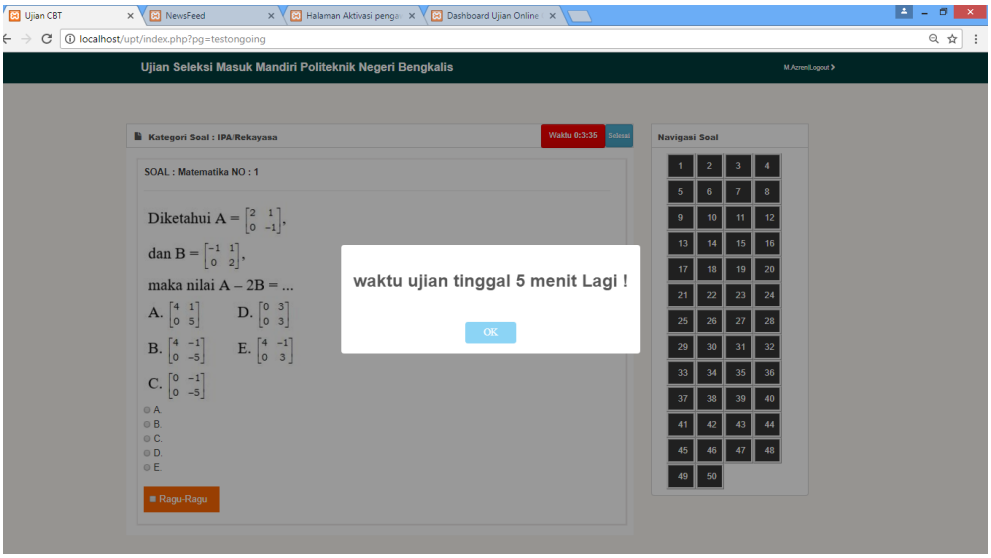
Gambar 7. Efek navigasi soal saat dijawab

3. Jika peserta menjawab dan merasa ragu dalam mengisi soal ujian maka navigasi soal akan berwarna kuning sesuai letak dimana nomor ujian yang dikerjakan seperti yang terlihat pada Gambar 8.



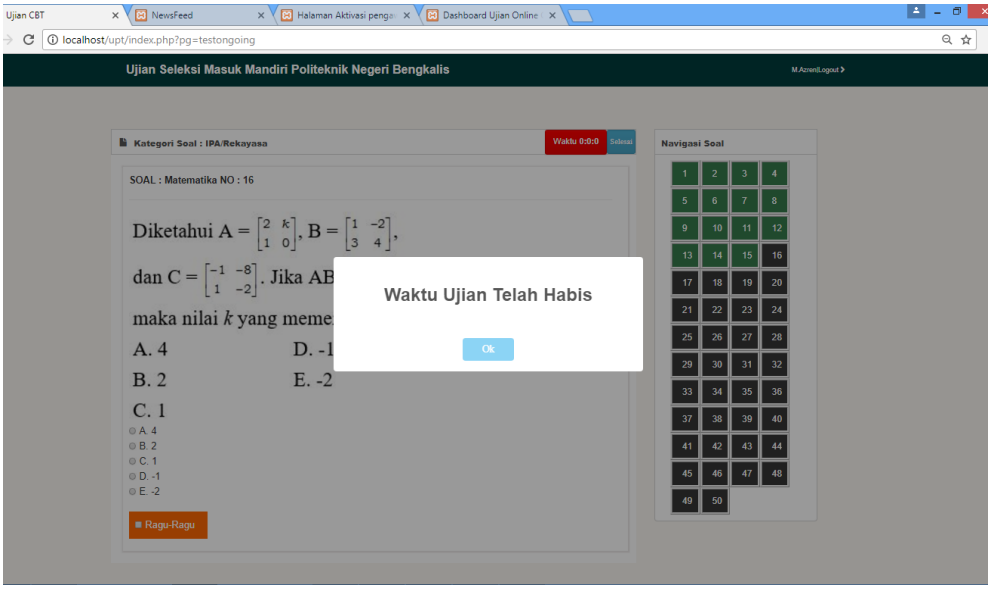
Gambar 8. Efek navigasi soal saat ragu-ragu dalam menjawab soal

4. Jika saat mengisi soal terjadi kendala putus koneksi atau listrik mati, peserta masih tetap dapat menjalankan ujian dan jawaban masih tetap tersimpan.
5. 5 menit sebelum waktu habis, sistem akan memberikan notifikasi kepada peserta bahwa ujian tinggal 5 menit lagi, dan *countdown* akan berwarna merah, hal ini bertujuan agar peserta lebih cepat mengerjakan ujian seperti yang terlihat pada Gambar 9.



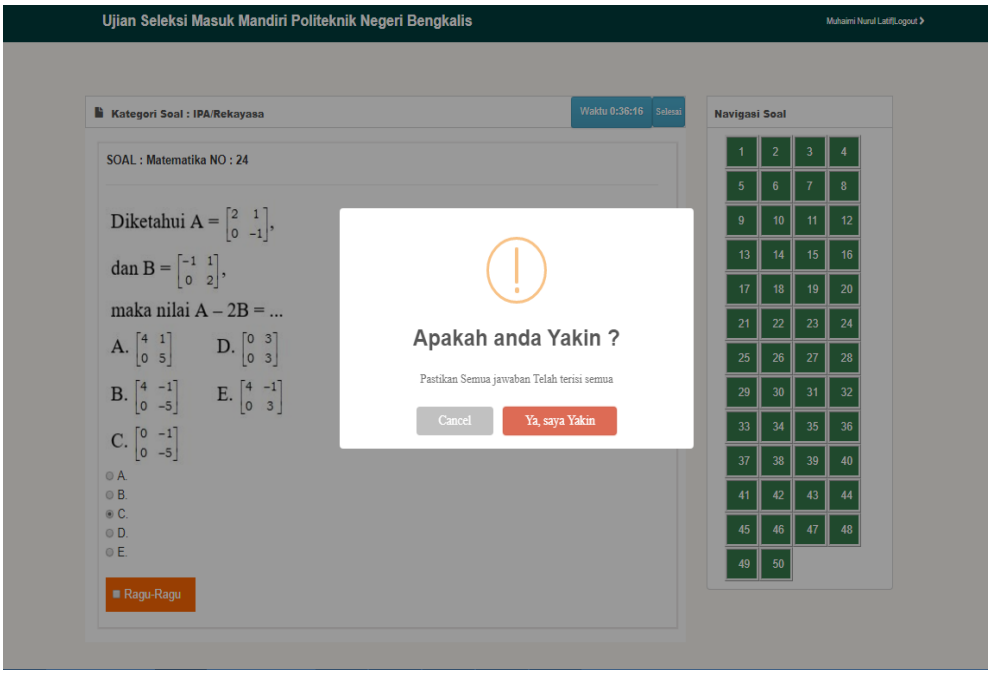
Gambar 9. Peringatan sisa waktu 5 menit terakhir

Apabila batas waktu ujian selesai dan peserta masih mengerjakan ujian maka secara otomatis sistem akan mensubmit ujian peserta seperti yang terlihat pada Gambar 10.



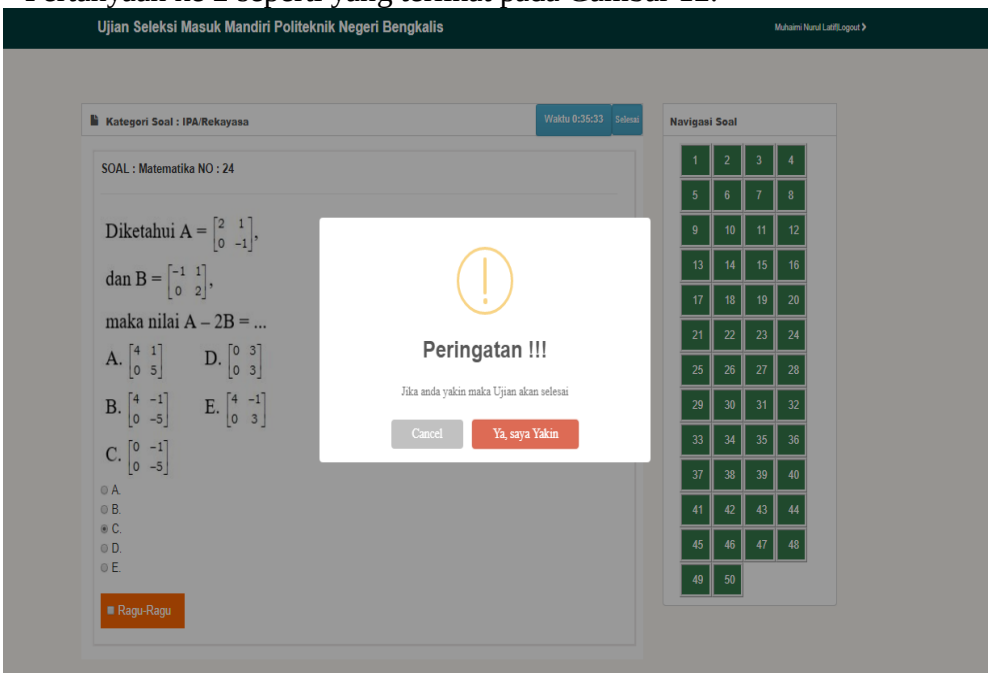
Gambar 10. Peringatan waktu ujian selesai

6. Jika anda sudah selesai mengerjakan ujian, peserta akan ditanyakan beberapa pertanyaan hal ini untuk memastikan bahwa peserta benar-benar sudah mengerjakan ujian, untuk jumlah pertanyaan terdapat 2 pertanyaan. Pertanyaan 1 seperti yang terlihat pada Gambar 11.



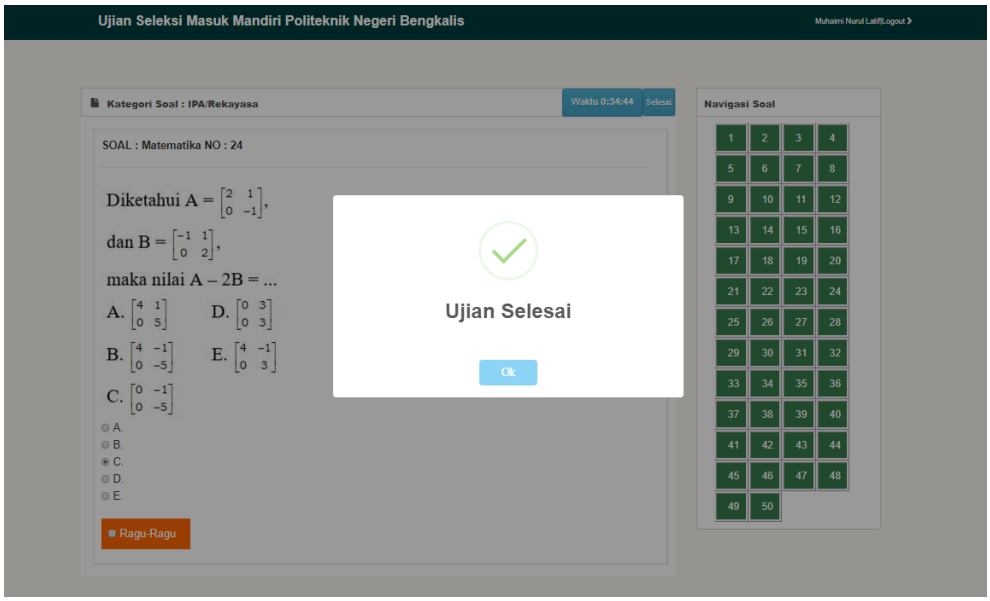
Gambar 11. Pertanyaan 1 untuk menyelesaikan ujian

Pertanyaan ke 2 seperti yang terlihat pada Gambar 12.



Gambar 12. Pertanyaan 2 untuk menyelesaikan ujian

Setelah itu ujian akan di nyatakan selesai seperti yang terlihat pada Gambar 13.



Gambar 13. Konfirmasi telah menyelesaikan ujian

Setelah selesai, sistem akan memberitahu score yang sudah didapat peserta hal ini bertujuan agar kegiatan ujian bersifat transparan terhadap nilai

5. Kesimpulan

Hasil Penelitian berupa aplikasi *Computer Based Test* untuk seleksi masuk Politeknik Negeri Bengkalis yang digunakan pada seleksi penerimaan melalui ujian masuk jalur mandiri Politeknik Negeri Bengkalis, arsitektur jaringan yang digunakan aplikasi *Computer Based Test* adalah model jaringan *client-server* dengan jaringan *Local Area Network* dengan sistem soal menggunakan *Multiple Choice Question* (MCQS). Pada aplikasi CBT soal yang dimunculkan dalam bank soal dilakukan proses pengacakan soal dengan menggunakan metoda Fisher-Yates Shuffle, sesuai dengan fungsinya untuk mengubah urutan masukan yang diberikan secara acak dan tidak akan memunculkan soal yang sama. Dalam proses pengamanan informasi soal saat terhubung ke jaringan digunakan teknik penyandian pesan agar soal tersebut sebeum dimunculkan melewati proses enkripsi dan deskripsi data terlebih dahulu maka digunakan algoritma kriptografi RSA.

Daftar Pustaka

[1] Bolboaca, S.D., and Jantschi, L., 2007, Computer-based testing on physical chemistry topic: A case study, *International Journal of Education and Development using Information and Communication Technology* (IJEDICT), Vol.3, Issue 1, page 94-104.

[2] Chua,Y.P., and Don,Z.M., 2013, Effects of computer-based educational achievement test on test performance and test takers' motivation, *Computers in Human Behavior*, page 1889– 1895.

[3] Ibijola, A., and Olu, A., 2012, A Simulated Enhancement of Fisher-Yates Algorithm for Shuffling in Virtual Card Games using Domain-Specific Data Structures**,** *International Journal of Computer Applications*, September 2012, Vol.54, No.11 0975 – 8887, page 24 – 28.

[4] Ayele, A.A, and Sreenivasarao,V., 2013, A Modified RSA Encryption Technique Based on Multiple public keys, *International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)*, Vol. 1, Issue 4, June 2013, ISSN (Online):2320 – 9801, page 859 – 864.

[5] John, A.O., Philip, S., and Shola, P.B, 2015, Comparative Analysis Of Discrete Logarithm And RSA Algorithm In Data Cryptography, *International Journal of Computer Science & Information Security* (IJCSIS), February 2015, Vol. 13, No. 2, ISSN 1947-5500, page 24 – 31.
[6] Khairil, Riyanto, N.P, dan Rosmeri, 2013, Membangun Webserver Intranet Dengan Linux (Studi Kasus di Laboratorium Komputer SMP Negeri 38 Seluma Bengkulu Selatan), *Jurnal Media Infotama*, Februari 2013, Vol.9, No.1, ISSN : 1858 – 2680
[7] Temitayo M,F., Adebisi A,A., and Alice O,O., 2013, Computer-Based Test (Cbt) System For University Academic Enterprise Examination, *International Journal Of Scientific & Technology Research (IJSTR)*, Vol.2, Issue 8, ISSN 2277-8616, page 336 - 342
[8] Arifin, 2009, Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman, *Jurnal Informatika Mulawarman*, Vol. 4, No 3
[9] Maitimu,T.R., 2008, Perancangan dan Implementasi Web Server Clustring dan Skema Load Balance Menggunakan Linux Virtual Server Via NAT, *Jurnal Teknologi Informasi – Aiti*, Februari 2008, Vol.5, No.1, hal. 14-27
[10] Somerville, I., 2011, *Software engineering, 9th edition*, Pearson Education, Addison-Wesly, Boston, Massachusetts.