Implementasi Algoritma Blowfish Pada Aplikasi CBT Berbasis Mobile Android (Studi Kasus : FKTI Universitas Mularman)

Rosmasari[*1], Fahrul Agus[2], Fajar Khairumman[3]
[1,2,3]Jurusan Teknologi Informasi dan Komunikasi, Universitas Mulawarman, Samarinda
Barong Tongkok Kampus Gn.Kelua Universitas Mulawarman, Telp: 0541753133
e-mail: [*1]**rosmasari.unmul@gmail.com**, [2] fahrulagus@unmul.ac.id, [3]fajarkh9@gmail.com

Abstrak

Pelaksananan ujian khususnya ujian akhir semester pada lembaga pendidikan sering kali dilakukan secara manual sehingga membutuhkan banyak biaya serta tenaga dalam pelaksanaannya serta kemungkinan terjadi tindak kecurangan lebih tinggi. Pelaksanaan ujian akhir semester di Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Mulawarman masih dilakukan secara manual yang mana kurang efisien. Salah satu solusi yang dapat diterapkan untuk menjadikan ujian lebih efisien adalah dengan menerapkan metode komputerisasi atau sering dikenal sebagai Computer Based Test (CBT) pada saat ujian. Akan tetapi resiko keamaan database pada aplikasi CBT nantinya akan menjadi masalah mengingat database tersebut dapat di akses di luar aplikasi CBT. Sehingga perlu ditingkatkannya pengamanan data, oleh karena itu dalam penelitian ini dibangun aplikasi CBT yang mengimplementasikan algoritma keamanan komputer yaitu algoritma Blowfish. Algoritma Blowfish yang merupakan algoritma kunci simetrik cipher blok yang cepat, aman dan mudah dalam implementasinya sangat cocok diterapakan pada database ringan seperti SQLite yang akan di gunakan pada penelitian ini. Hasil dari pembangunan aplikasi ini dapat meningkatkan efisiensi dalam pelaksanaan ujian, serta mengurangi tindak kecurangan saat ujian pada Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Mulawarman.

Kata Kunci : *Computer Based Test, Kriptografi Blowfish, SQLite*

1. PENDAHULUAN

Perkembangan teknologi saat ini keamanan sebuah data, baik data digital maupun data fisik menjadi hal yang sangat perlu diperhatikan mengingat petingnya informasi didalamnya. Khususnya informasi yang tidak boleh bocor ke pihak tertentu. Tidak bisa dipungkiri, hampir sebagian besar kebocoran data sering terjadi pada dokumen atau arsip yang masih berbasis kertas atau sekarang lebih dikenal sebagai arsip konvensional. Saat ini ujian yang dilakukan pada Program Studi Teknik Informatika Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Mulawarman masih melakukan dengan metode Paper-Based-Test (PTB). Ujian dengan menggunakan kertas saat ini masih banyak memiliki kendala seperti, rawan dalam penyimpanan bahan ujian, penggandaan dan proses distribusi soal, rawan tidak kecurangan serta membutuhkan banyak biaya. Untuk menangani masalah-masalah tersebut, maka dirancanglah sistem ujian berbasis komputer atau sering di kenal dengan sebutan Computer Based Test (CBT), yang akan di bangun pada perangkat mobile. Akan tetapi, aplikasi CBT yang nantinya di kembangkan menggunakan database SQLite, yang mana database ini akan tersimpan dalam disk aplikasi sendiri yang bentuknya berupa plaintext, sehinnga siapapun yang memiliki akses ke fisik file database, maka yang bersangkutan akan bisa membukanya dan melihat isi data di dalamnya.

Pemanfaatan teknik algoritma kriptografi adalah salah satu solusi alternatif untuk menyelesaikan masalah di atas. Dengan menerapkan kriptografi, data file fisik tersebut akan terenkripsi sehingga tidak bisa di mengerti oleh pihak yang tidak bertanggung jawab. Oleh karena itu, aplikasi CBT untuk ujian ini mengimplementasikan algoritma kriptografi Blowfish

sebagai keamanan datanya. Blowfish merupakan algoritma kunci simetrik cipher blok yang dirancang pada tahun 1993 oleh Bruce Schneier. Algoritma Blowfish bersifat bebas paten dan akan berada pada domain publik. Selain itu, dari segi keamanan, algoritma blowfish masih belum ditemukan suatu metode khusus untuk diretas. Hal ini membuat peneliti berani mengambil Blowfish sebagai algoritma enkripsi karena keamanan, kecepatan, dan minimnya penggunaan memori.

2. METODE PENELITIAN

2.1 Algoritma Blowfish

Algoritma Blowfish atau disebut juga OpenPGP.Cipher.4 adalah metode algoritma kriptografi yang termasuk dalam golongan sematik kriptografi [1]. Blowfish merupakan cipher blok yang bekerja dengan membagi pesan menjadi blok-blok bit dengan ukuran sama panjang (64-bit) dengan panjang kunci bervariasi yang mengenkripsi data dalam 8 byte blok. Pesan yang bukan merupakan kelipatan 8 byte akan dipadding sehingga ukuran untuk tiap blok sama . Algoritma Blowfish terdiri dari dua bagian yaitu key expansion dan enkripsi data. [2].

a. Key Expansion

Key Expansion dimulai dengan inisialisasi P-array dan S-box yang nantinya digunakan untuk pembuatan sub-kunci, yang dilakukan sebelum enkripsi atau dekripsi. P-array memiliki panjang 18 dengan ukuran 32 bit yaitu : P1, P2… P17, P18.

Algoritma blowfish memiliki panjang kunci hingga 448 bit yang diubah menjadi beberapa array sub-kunci. Ada 256 entri untuk masing-masing dari empat S-box 32-bit. Alur proses Key Expansion dapat dijelaskan sebagai berikut :

1. Inisialisasi semua array P dan S secara berurutan menggunakan digit heksadesimal bilangan pi/π misal: P1 = 0x243f6a88, P2 = 0x85a308d3, P3 = 0x13198a2e, dst.
2. Lakukan operasi XOR pada P1 dengan 32 bit pertama dari kunci yang digunakan, XOR P2 dengan 32 bit kedua dari kunci tersebut dan lakukan terus hingga bagian akhir bit kunci (maksimal hingga P14). Ulangi kembali dari bit kunci awal hingga seluruh array P dan S selesai di-XOR-kan dengan bit-bit kunci.
3. Lakukan enkripsi menggunakan algoritma blowfish pada variabel 64 bit yang semua bitnya bernilai 0 menggunakan subkunci pada proses 1 dan 2.
4. Ganti subkunci P1 dan P2 dengan hasil keluaran pada proses 3.
5. Enkripsi hasil keluaran pada proses 3 menggunakan blowfish dengan subkunci yang telah dimodifikasi pada proses 4.
6. Ganti subkunci P3 dan P4 dengan hasil keluaran pada proses 5.
7. Lanjutkan proses diatas untuk mengganti semua nilai array P dan S secara berurutan.

b. Key Expansion

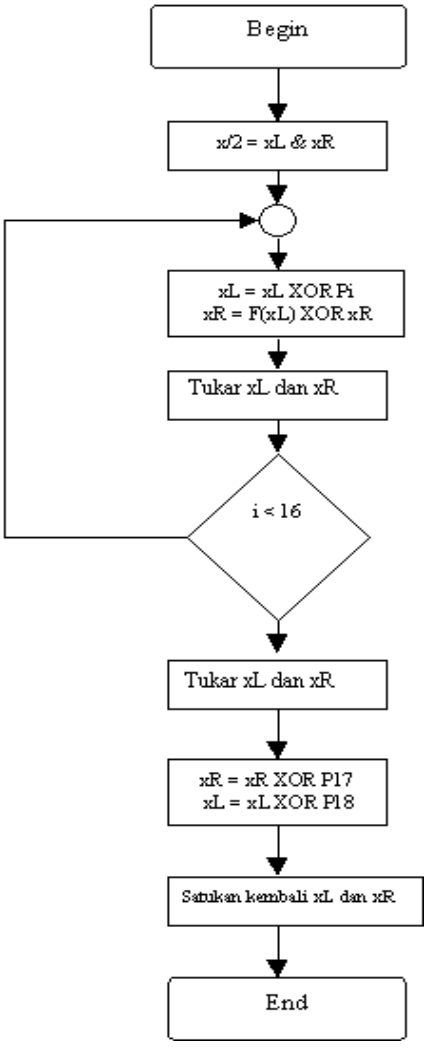
Proses enkripsi dan dekripsi algortima blowfish menggunakan cara yang hampir sama seperti proses key ekpansion, hanya saja urutan penggunaan subkunci pada dekripsi yang terbalik. Masukan dan keluaran dari algoritma blowfish berupa blok-blok data berukuran 64 bit. Berikut ini adalah urutan dalam enkripsi dan dekripsi algoritma blowfish.

1. Bentuk inisial P-array sebanyak 18 buah (P1,P2,.....P18) masing-masing bernilai 32-bit. Array P terdiri dari delapan belas kunci 32-bit subkunci yang berisi string dari: P1, P2, ... ,P18
2. Bentuk S-box sebanyak 4 buah masing-masing bernilai 32-bit yang memiliki masukan 256. Empat 32-bit S-box masing-masing mempunyai 256 entri :

$S_{1,0}$, $S_{1,1}$,....., $S_{1,255}$
$S_{2,0}$, $S_{2,1}$,....., $S_{2,255}$
$S_{3,0}$,$S_{3,1}$,....., $S_{3,255}$
$S_{4,0}$,$S_{4,1}$,....., $S_{4,255}$

3. Plaintext yang akan di enkripsi diasumsikan sebagai masukan, Plaintext tersebut diambil sebanyak 64-bit, dan apabila kurang dari 64-bit maka kita tambahkan bitnya, agar dalam operasi nanti sesuai dengan datanya.
4. Hasil pengambilan tadi dibagi 2, 32-bit pertama disebut XL, 32-bit yang kedua disebut XR.
5. Selanjutnya lakukan operasi XL = XL xor Pi dan XR = F(XL) xor XR.
6. Hasil dari operasi diatas ditukar XL menjadi XR dan XR menjadi XL.
7. Lakukan sebanyak 16 kali, zperulangan yang ke-16 lakukan lagi proses penukaran XL dan XR.
8. Pada proses ke-17 lakukan operasi untuk XR = XR xor P17 dan XL = XL xor P18.
9. Proses terakhir satukan kembali XL dan XR sehingga menjadi 64-bit kembali.

Untuk poses lebih jelasnya, alur algoritma blowfish dapat digambarkan pada flowchart pada gambar 1.



Gambar 1. Flowchart Algoritma Blowfish

2.2 Computer Based Test (CBT)

CBT (Computer Based Test) merupakan sistem komputer yang bertujuan untuk membantu pengajar dalam pelaksanaan evaluasi, baik itu dari segi penilaian, pelaksanaan tes maupun efektifitas dan efisiensi dalam pelaksanaannya. Sehingga dalam pelaksanaan test nantinya menggunakan sistem tersebut.

Sistem Computer Based Test atau pelaksanaan evaluasi dengan berbantuan komputer merupakan turunan, bagian ataupun pengembangan dari sistem Computer Assisted Instructional

(CAI) atau pembelajaran berbantuan komputer. Namun, hanya dikhususkan pada bidang garapan evaluasi yang meliputi kumpulan kumpulan soal dan proses penskoran otomatis, media audio, video dan interaktif serta autorun. [3].

Manfaat dari implementasi tes berbasis komputer dapat memberikan peserta hasil tes yang lebih akurat karena semuanya dilakukan oleh sistem, mengurangi biaya operasional, meningkatkan konten dari soal. Selain itu, tingkat penipuan peserta dalam mengerjakan tes bisa diminimalkan.

1. Android

Android adalah sebuah sistem operasi pada handphone yang bersifat terbuka dan berbasis pada sistem operasi Linux. Android bisa digunakan oleh setiap orang yang ingin menggunakannya pada perangkat mereka. Android menyediakan platform terbuka bagi para pengembang untuk menciptakan aplikasi mereka sendiri yang akan digunakan untuk bermacam peranti bergerak. [4].

Android Inc yang merupakan pendatang baru yang membuat peranti lunak untuk ponsel awalnya dibeli oelh Google Inc. Kemudian untuk mengembangkan Android, dibentuklah Open Handset Alliance, konsorsium dari 34 perusahaan peranti keras, peranti lunak, dan telekomunikasi, termasuk Google, HTC, Intel, Motorola, Qualcomm, TMobile, dan Nvidia. Pada saat perilisan perdana Android, 5 November 2007, 10 Android bersama Open Handset Alliance menyatakan mendukung pengembangan standar terbuka pada perangkat seluler. Di lain pihak, Google merilis kode–kode Android di bawah lisensi Apache, sebuah lisensi perangkat lunak dan standar terbuka perangkat seluler.

2. *Perangkat Mobile*

Perangkat mobile merupakan peralatan ringan yang mudah dibawa kemana-mana atau dalam istilahnya, portabel. Dalam hal ini peralatan ringan yang dimaksud sebenarnya merupakan benda yang sering dibawa oleh setiap orang yakni adalah Handphone, Smartphone atau sejenisnya. Adapun contoh perangkat mobile, telah disebutkan sebelumnya, yakni Handphone (HP), Ponsel dan Smartphone. HP, Ponsel maupun Smartphone sebenarnya sama. Namun yang membedakannya hanyalah teknologi yang digunakan smartphone lebih canggih daripada HP dan ponsel.

Perangkat mobile memiliki sistem operasi sebagai perangkat lunak penghubung antar software pada perangkat tersebut dengan perangkat kerasnya. Jenis system operasi perangkat lunak sangat beragam seperti, Java, Symbian, Android, IOS dan lain-lain.

3. SQLite

SQLite adalah pustaka dalam proses yang mengimplementasikan basis data SQL transaksional yang mandiri, tanpa konfigurasi, tanpa mesin server. Kode sumber untuk SQLite ada di domain publik dan gratis untuk keperluan pribadi dan komersial. [5]. SQLite saat ini digunakan lebih banyak pada aplikasi mobile, termasuk beberapa proyek profil tinggi. SQLite adalah mesin database SQL tertanam dan tidak memiliki proses server terpisah seperti kebanyakan SQL lainnya basis data. SQLite membaca dan menulis langsung ke file disk biasa. Format file basis data adalah lintas platform.

Fitur-fitur ini menjadikan SQLite pilihan populer sebagai format file aplikasi. SQLite adalah pustaka kompak, ukuran pustaka bisa kurang dari 500KiB, tergantung pada platform target dan pengaturan optimisasi kompiler. Jika fitur opsional dihilangkan, ukuran file Perpustakaan SQLite dapat dikurangi di bawah 300KiB.

3. HASIL DAN PEMBAHASAN

3.1 Implementasi Algortima Blowfish

Proses enkripsi dan dekripsi pada aplikasi Computer Based Test dengan menngunakan algoritma blowfish dapat penulis jelaskan melalui contoh perhitungan manual seperti di bawah

ini. Dalam hal ini penulis menggunakan parameter dengan panjang plaintext sama dengan 8 sehingga tidak terjadi padding.
Plaintext = KOTA SMD
Password =1234

1. Key Expansion

Pada proses enkripsi dan dekripsi, kunci akan di pecah menjadi subkunci melalui tahap Key Expansion. Dalam hal ini penulis menggunakan parameter dengan panjang kunci sama dengan 4. Nilai konversi karakter key ke biner dapat di lihat pada tabel 1.

Tabel 1. Konversi kunci ke biner

Karakter	**ASCII (Hexa)**	**Konversi Biner**
1	31	00110001
2	32	00110010
3	33	00110011
4	34	00110100

Biner : 00110001 00110010 00110011 00110100

Inisialisasi P-Array dan S-box, lalu lakukan literasi antara P-Array XOR kunci sehinnga membentuk subkunci :
P0=00010101 00001101 01011001 10111100,
P1 = 10010000 10101111 01010001 01101111,
sampai semua nilai P-array tergantikan.

2. Proses Enkripsi

Pada proses enkripsi, plaintext di pecah mejadi blok-blok berukuran 64 bit lalu memasuki literasi 16 putaran algoritma blowfish. Langkah tersebut adalah sebagai berikut:

1. Bagi 2 blok 64 bit, 32-bit pertama disebut XL, 32-bit yang kedua disebut XR.
2. Selanjutnya lakukan operasi XL = XL xor Pi dan XR = F(XL) xor XR.
3. Hasil dari operasi diatas ditukar XL menjadi XR dan XR menjadi XL.
4. Lakukan sebanyak 16 kali, perulangan yang ke-16 lakukan lagi proses penukaran XL dan XR.
5. Pada proses ke-17 lakukan operasi untuk XR = XR xor P17 dan XL = XL xor P18.
6. Proses terakhir satukan kembali XL dan XR sehingga menjadi 64-bit kembali.

3. Proses Dekripsi

Pada proses dekripsi, prosesnya hampir sama dengan proses enkripsi hanya saja urutan penggunaan subkunci P1 sampai dengan P16 digunakan dalam urutan terbalik sehingga urutannya dari P16 ke P1. Dalam proses dekripsi chiphertext yang awalnya berupa Hexadesimal dirubah kembali kedalam bentuk plaintext atau dalam kondisi sebelum dienkripsi.

3.2 Implementasi Program

Setelah melalui beberapa revisi pada aplikasi yang di buat menggunakan android studio. Maka aplikasi berhasil dibuat yang terdiri atas 5 buah fungsi serta *Interface* utama yaitu :

1. Interface Login

Pengguna yang dapat mengakakses terbagi menjadi dua yakni dosen dan mahasiswa. Untuk dapat login pengguna menginputkan email dan password serta menconteng tetap login jika ingin tetap login di saat aplikasi di buka lagi nantinya.

2. Interface Dashboard

Pada halaman ini terdapat beberapa menu tergantung oleh siapa pengguna yang login. Jika mahasiswa yang masuk maka hanya aka nada menu kelas dan logout, sedangkan jika dosen yang masuk maka aka nada menu soalku.

3. Interface Soalku

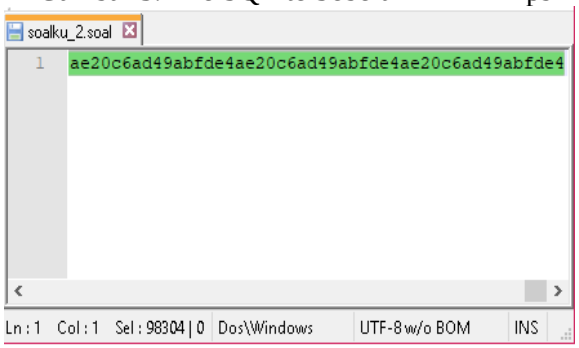
Pada halaman ini berisi tentang list dari soal-soal yang pernah di buat dosen. Selain itu pada halaman ini terdapat tombol tambah soal, hapus dan edit soal.

Gambar 2. Halaman Soalku

Ketika pengguna menekan tombol tambah maka akan muncul halaman buat soal dimana pada halaman tersebut terdapat list dari butir-butir pertanyaan pilihan ganda beserta jawabannya. Terdapat tombol dropdown yang berisi keterangan tambahan seperti nama soal, dan mata kuliah. Setelah soal dan jawaban dirasa cukup user dapat menyimpan soal tersebut dengan menekan tombol save atau juga dengan langsung menekan tombol kembali.

Ketika di simpan maka file soal yang awalnya berupa database sqlite yang tersimpan dalam folder privat android akan di salin ke folder internal perangkat android, lalu di enkripsi dengan algoritma blowfish dengan menggunakan kunci yang sudah di atur dalam aplikasi. File hasil enkripsi akan berekstensi ".soal". bentuk file soal sebelum di eknripsi berupa databse SQLite yang isinya tampak seperti pada gambar di bawah ini.

Gambar 3. File SQLite Sebelum Di Enkripsi

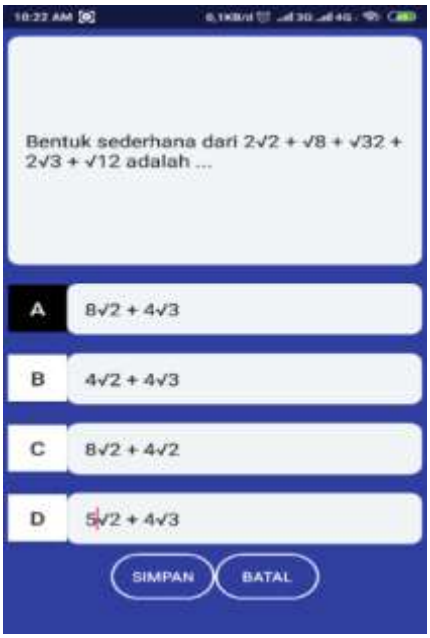


Gambar 4. File SQLite Sstelah Di Enkripsi

Hasil file enkripsi akan mengalami kenaikan ukuran file dikarenakan ciphertext berformat hexadecimal yang mana 1 digit ASCII sama dengan 2 digit Hexadesimal.

4. Interface Buat Soal

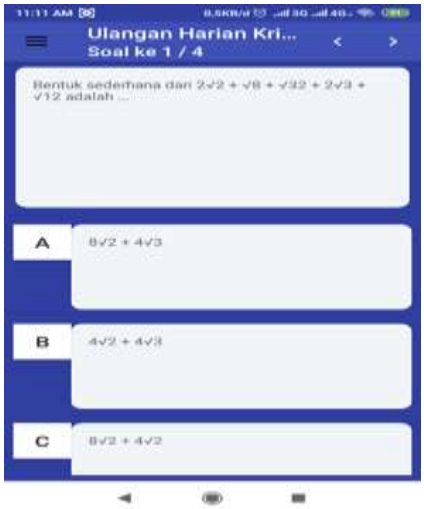
Pada popup buat soal terdapat kolom input pertanyaan juga empat kolom input jawaban. Lalu user memilih jawaban dengan menekan pilihan yang tersedia. Tampilan halaman buat soal biasa di lihat pada gambar di bawah ini.



Gambar 5. Popup Buat Soal

5. Interface Kerjakan Soal

Proses aplikasi menampilkan data soal ketika mahasiswa mengerjakan soal di mulai dari file soal yang telah terenkripsi (yang berekstensi .soal) di download dari server untuk disimpan pada folder privat perangkat android. Kemudian dekripsi file soal dengan menggunakan kunci yang tertanam dalam aplikasi. Hasil dekripsi kemudian disimpan kedalam sebuah file dengan ekstensi ".db" kemudian hapus file soal yang sebelumnya di download. Kemudian tampilkan nomor soal , isi soal, berserta pilihan dan kunci jawabannya pada tampilan aplikasi menggunakan perintah SQL. Tampilan popup kerjakan soal dapat dilihat pada gambar 5.



Gambar 4. Popup Buat Soal

6. Pengujian Terhadap Waktu Proses

Berdasarkan pada beberapa proses pengujian dengan menggunakan beberapa file sqlite dengan ukuran yang berbeda-beda didapatkan waktu proses secara keseluruhan seperti pada tabel berikut.

Tabel 2. Pengujian Terhadap Waktu Proses

No	Ukuran File Database	Waktu (detik)	
		Enkripsi	Dekripsi
1	12 KB	0.330	0.244
2	24 KB	0,482	0,476
3	32 KB	0.628	0.671
4	56 KB	1.765	1.256

Dari hasil pengujian pada uji coba kecepatan proses enkripsi dan dekripsi pada tabel diatas di peroleh rata-rata waktu proses enkripsi sebesar 0,80 detik dan sebesar 0,66 detik untuk proses dekripsi Dari hasil pengujian tersebut proses enkripsi maupun dekripsi dapat ditarik kesimpulan bahwa waktu saat proses enkripsi relatf sama dengan saat proses enkripsi.

7. Pengujian Terhadap Ukuran File

Pengujian terhadap ukuran file dilakukan untuk memastikan apakah nantinya ukuran file setelah di enkripsi tidak terlalu membebani terhadap penyimpanan perangkat.

Tabel 3. Pengujian Terhadap Ukuran File

No	Nama File	Ukuran File (Plaintext)	Ukuran File (Ciphertext)
1	List_soalku.db	12 KB	48 KB
2	Soalku.db	32 KB	84 KB
3	1.db	56 KB	128 KB
4	Gaaa.db	24 KB	66 KB
5	Proposal Penelitian.Pdf	1,21 MB	4,63 MB
6	Laporan Praktek Kerja Lapangan.Pptx	5,52 MB	22,1 MB

Berdasarkan pada beberapa proses pengujian yang di lakukan dengan menggunakan beberapa file dengan ukuran yang berbeda-beda yang dapat di lihat pada table 2, ukuran file mengalami penambahan karena isi dalam file yang telah terenkripsi berisi ciphertext berformat Hexadesimal yang mana 1 karakter ASCII sama dengan 2 karakter Hexadesimal.

4. HASIL DAN PEMBAHASAN

Berdasarkan hasil dan pembahasan yang telah dijabarkan pada bab sebelumya, maka dapat disimpulkan sebagai berikut:

1. Aplikasi Computer Based Test (CBT) yang mengimplementasikan algoritma kriptografi Blowfish sebagai keamanan nya yang di bangun pada platform Android Mobile telah berhasil dirancang dan dibangun dengan memanfaatkan tools Android Studio.
2. File SQLite sebagai database penampung soal, telah berhasil di enkripsi dengan aplikasi ini. Aplikasi ini juga telah berhasil mengembalikan file SQLite yang telah di enkripsi seperti semula sehingga dapat di buka oleh pengguna mahasiswa dengan menggunakan kunci yang sama saat pengguna dosen membuat soal.
3. Aplikasi menggunakan algoritma kriptografi dalam mengamankan file soal sehingga file soal tidak dapat di buka di luar dari aplikasi yang dikembangkan.

4. Pada pengujian terhadap waktu proses enkripsi dan dekripsi dapat di simpulkan bahwa proses enkripsi dan proses dekripsi memiliki waktu proses yang relatif sama, dan juga lama dari proses enkripsi dan dekripsi berbanding lurus dengan ukuran file.
5. Pada pengujian terhadap ukuran file, dapat disimpulkan bahwa ukuran file setelah di enkripsi akan mengalami kenaikan, namun akan kembali ke ukuran awalnya saat sebelum di enkripsi.
6. Tipe soal yang dapat di buat dalam aplikasi adalah pilihan ganda dengan kemampuan dapat membuat soal dengan karakter-karakter unik seperti pada soal matematika serta memiliki kapasitas pembuatan soal

5. SARAN

Berdasarkan hasil evaluasi pada aplikasi Computer Based Test (CBT) dengan mengimplementasikan algoritma kriptografi Blowfish, terdapat beberapa saran untuk pengembangan aplikasi selanjutnya sebagai berikut :

1. Aplikasi ini memerlukan GUI (Graphic User Interface) yang lebih baik lagi , sehingga memudahkan user dalam menggunakan aplikasi.
2. Sistem kelas pada aplikasi masih menggunakan server gratis sehingga memiliki keterbatasan seperti kecepatan server serta seringnya terjadi error pada server.
3. Pada pengembangan selanjutnya peneliti berharap ditambahkannya beberapa fitur tambahan seperti adanya timer saat mengerjakan soal guna mengetahui lama mahasiswa dalam mengerjakan soal, lalu adanya fitur pengacakan soal sehingga soal pada tiap mahasiswa akan berbeda, dan juga perlu adanya sistem pencatatan aktifitas saat mengerjakan soal guna mengetauhi bagaimana pola mahasiswa dalam mengerjakan soal.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Tuhan yang Maha Esa yang telah memberikan rahmat dan nikmatnya sehingga penulis diberikan kemudahan didalam penelitian ini. Terima kasih kepada kedua orang tua yang senantiasa mendukung dalam bentuk finansial maupun dalam bentuk doa. Terimakasih pula kepada kampus FKTI sebagai tempat dilakukannya penelitian dan terima kasih kepada teman-teman mahasiswa FKTI yang selalu memberikan dukungan, masukan dan sarannya dalam penelitian ini.

DAFTAR PUSTAKA

[1] Rosmasari, R. A. D. RA, N. Dengen, and M. Taruk, “Implementasi Metode Kriptografi International Data Encryption Algorithm (IDEA) Untuk Pengamanan Data Berita Publik Khatulistiwa Televisi Bontang,” *J. Rekayasa Teknol. Inf.*, vol. 2, no. 2, pp. 172–181, 2018.

[2] B. Schneier, Applied Cryptography, Second Edition, New York: John Wiley & Son, 1996.

[3] B. Schneier, "Description of a New Variable -Length Key, 64 Bit Block Chipper," 1993. [Online]. Available: http://schneizer.com. [Accessed january 2019].

[4] Romiszowski, The Selection and Use of Intructional Media, New York: Kogan, 1988, p. 306.

[5] N. Safaat H, (Edisi Revisi). Pemograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android, Bandung: Informaika, 2012.

[6] SQLite, "About : SQLite," [Online]. Available: https://www.sqlite.org/about.html. [Accessed 2019].

[7] W. J. and W. L. , "The comparison of Embedded Database Berkeley DB and SQLite," *The application of SCM and Embedded System*, pp. 5-7, 2005.

[8] Haviluddin, "Memahami Penggunaan UML (Unified Model," *Jurnal Informatika*

Mulawarman, vol. 6, February 2011.
[9] A. Nugroho, Rekayasa Perangkat Lunak Menggunakan UML & Java, Yogyakarta, 2010.
[10] R. A. Sukamto and M. S. , "Rekayasa Perangkat Lunak," *Informatika*, 2013.