PROSIDING Seminar Nasional SISFOTEK ISSN 2597-3584 (Media Online)
Sistem Informasi dan Teknologi
website : www.seminar.iaii.or.id | email : seminar@iaii.or.id

Pengamanan File Audio Menggunakan Algoritma Kriptografi Blowfish Dan Pengujian UAT

Siswanto[1], Farizal Dias Amsari[2], Basuki Hari Prasetyo[3], Wahyu Pramusinto[4], Gunawan Pria Utama[5], M. Anif[6]
[1,2,3,4,5,6]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
siswanto@budiluhur.ac.id

Abstract

The current problem at PT. Central Asia Insurance is data or information from meeting recordings that have been made without security so that the resulting data is leaked and can be published by unauthorized persons. This study aims to secure the results of the meeting in the form of audio that will be sent to the branch of PT. Central Asia Insurance using blowfish cryptographic algorithm and UAT testing. Therefore, I created an encryption application to secure the audio from the meeting at PT. Central Asia Insurance. The goal is to prevent irresponsible people from being able to know the results of the meeting directly because the Audio file has been encrypted. By making this application, it can guarantee the audio file of the meeting at PT. Central Asia insurance can be accepted by people who are entitled and have keys. The final result of this research is that this application is able to encrypt audio files with a maximum data size of 120 Mb. Based on trials carried out as many as 15 encrypted files, the encrypted file size becomes large with an average value of 12,009,507 bytes and an average encryption process time of 37.0 seconds while the decryption time is 52.2 seconds. So that the files obtained can be protected and can only be accessed by users who have a password lock. In the UAT test, a questionnaire with a Likert scale scale of 5. has been used. As a result, the respondents agree (above 91.23%) that the overall application of the blowfish algorithm to secure data files can be kept confidential.

Keywords: audio file security, blowfish cryptography, UAT testing.

Abstrak

Masalah yang ada pada saat ini di PT. Asuransi Central Asia adalah data atau informasi dari hasil rekaman rapat yang telah dibuat tidak memiliki keamanan sehingga data yang dihasilkan mengalami kebocoran dan dapat terpublikasikan oleh orang yang tidak berkepentingan. Penelitian ini bertujuan untuk mengamankan hasil rapat berupa audio yang akan dikirim ke cabang PT. Asuransi Central Asia dengan menggunakan algoritma kriptografi blowfish dan pengujian UAT. Oleh karena itu saya membuat aplikasi enkripsi untuk mengamankan Audio hasil rapat pada PT. Asuransi Central Asia. Tujuannya adalah mencegah orang yang tidak bertanggung jawab supaya tidak dapat mengetahui hasil rapat secara langsung karena file Audio tersebut telah dienkripsi. Dengan dibuatnya aplikasi ini dapat menjamin file audio hasil rapat pada PT. Asuransi Central Asia dapat diterima oleh orang-orang yang berhak dan memiliki kunci. Hasil akhir penelitian ini bahwa aplikasi ini mampu mengenkripsi file audio dengan ukuran maksimal data 120 Mb. Berdasarkan Uji Coba yang dilakukan sebanyak 15 Buahfile yang dienkripsi maka file yang dienkripsi ukurannya menjadi besar dengannilai rata-rata sebesar 12.009.507 *byte* dan waktu proses enkripsi rata-rata sebesar37.0 *second* sedangkan waktu dekripsi sebesar 52.2 *second*. Sehingga file yang diperoleh dapat terproteksi dan hanya dapat diakses oleh pengguna yang memiliki kunci kata sandi. Pada pengujian UAT, telah digunakan kuesioner dengan *likert scale* skala 5. Hasilnya, para responden setuju (di atas 91,23%) bahwa secara keseluruhan aplikasi penerapan algoritma *blowfish* untuk mengamankan data file dapat terjaga kerahasiannya.

Kata kunci: pengamanan file audio, kriptografi blowfish, pengujian UAT.

1. Pendahuluan

Perkembangan teknologi dalam bidang telekomunikasi menjadikan orang semakin sering melakukan pengiriman data file berupa doc, pdf, xls, *voice*, *image*, video melalui *internet*. karena *internet* merupakan media umum yang rentan akan terjadinya penyusupan dan pencurian informasi terhadap data atau file oleh pihak yang tidak berhak.

Masalah yang ada pada saat ini di PT. Asuransi Central Asia adalah data atau informasi dari hasil rekaman rapat yang telah dibuat tidak memiliki keamanan sehingga data yang dihasilkan mengalami

kebocoran dan dapat terpublikasikan oleh orang yang tidak berkepentingan.

Penelitian ini bertujuan untuk mengamankan hasil rapat berupa audio yang akan dikirim ke cabang PT. Asuransi Central Asia dengan menggunakan algoritma kriptografi blowfish dan pengujian *User Acceptance Test* (UAT).

Algoritma *blowfish* untuk mengamankan data arsip surat yang penting agar data aman dan jauh dari resiko penyalahgunaan. Aplikasi ini dapat mempermudah proses pencarian data, penyimpanan arsip dan mengamankan arsip gambar di BPAD kabupaten malang menggunakan algoritma *blowfish*, sehingga data aman dan jauh dari resiko penyalahgunaan. dari penelitian tersebut dapat disimpulkan yakni adanya kenaikan ukuran file setelah mengalami proses enkripsi sebesar 0.5 % [1].

Pengamanan pesan suara dilakukan dengan menggunakan algoritma kunci simetri *blowfish cipher* blok yang dibuat oleh Bruce Scheiner. Hasil penelitian tersebut adalah kualitas suara setelah mengalami enkripsi dan dekripsi tetap memiliki kualitas yang baik dan ukuran file suara tidak berubah, delay yang dihasilkan saat proses enkripsi dekripsi berlangsung tergantung dari ukuran file yang akan di enkripsi dan dekripsi, sedangkan *delay* yang dihasilkan ketika melakukan proses pengiriman juga tidak memakan waktu yang lama [2].

Pihak lain yang dapat mencuri berkas yang telah diamankan tidak akan mampu membaca isi berkas tersebut karena berkas tersebut sudah diamankan dengan algoritma *blowfish*. Berkas yang telah diamankan hanya dapat terbaca jika pengamanan dari berkas tersebut telah dilepaskan oleh aplikasi dari ponsel yang sama. Oleh karena itu, hanya pengguna ponsel yang dapat membuka pengamanan tersebut sehingga permasalahan privasi akan informasi yang dimiliki oleh pengguna ponsel dengan sistem operasi Android akan terpenuhi [3].

User Acceptance Test (UAT) adalah suatu proses pengujian yang dilakukan oleh pengguna dengan hasil *output* sebuah dokumen hasil uji yang dapat dijadikan bukti bahwa *software* sudah diterima dan sudah memenuhi kebutuhan yang diminta. UAT tidak jauh beda dengan kuesioner pada tahap awal pembuatan aplikasi [4].

User acceptance testing (UAT) merupakan pengujian yang ditujukan di luar sistem yaitu *user*. Tujuan dari *user acceptance testing* adalah untuk mengetahui kelayakan dari perangkat lunak [5].

Pada penelitian sebelumnya, UAT dilakukan dengan metode *survey* yaitu dengan menyebar kuesioner kepada pengguna (petugas TPHD) yang sebelumnya sudah diberikan tutorial penggunaan sistem layanan haji. Model kuesioner menggunakan likert scale dengan skala 5 yaitu *strongly agree; agree; neutral/undecided*; *disagree; strongly disagree*. UAT digunakan untuk menjawab permasalahan perangkat lunak seputar *system metric; usability; satisfaction* dan beberapa setting pada masing – masing fungsi/fitur [6].

Algoritma *blowfish* termasuk ke dalam *cipher* blok yang masih dianggap aman, karena belum ditemukan *attack* yang benar-benar dapat mematahkannya. Di samping analisis kinerja algoritma blowfish, pembahasan ini juga mencoba menguji dan mengimplementasi algoritma *blowfish* pada sebuah aplikasi yang akan melakukan enkripsi dan dekripsi pada teks [7].

Perbandingan algoritma *blowfish* dan *twofish* untuk kriptografi file gambar menunjukkan bahwa rata-rata perbandingan kecepatan dari algoritma *blowfish* dan algoritma *twofish* adalah 4355:4267 milidetik [8].

Aplikasi enkripsi dan dekripsi untuk keamanan komunikasi data pada SMS (*Short Message Service*) berbasis android menggunakan algoritma blowfish. dapat mengatasi permasalahan SMS *snooping* dan SMS *interception* [9].

Analisis perbandingan kinerja algoritma *blowfish* dan algoritma *twofish* pada proses enkripsi dan dekripsi jika ditinjau dari estimasi waktu proses enkripsi dan dekripsi. Algoritma *blowfish* lebih cepat waktu eksekusinya dibandingkan dengan algoritma *twofish*, dan jika ditinjau dari besar ukuran file sebelum dan sesudah proses enkripsi dan dekripsi, algoritma *blowfish* dan algoritma *twofish* memiliki besar ukuran yang sama. [10].

Hasil dari penelitian aplikasi teknik enkripsi dan dekripsi file dengan algoritma *blowfish* pada perangkat mobile berbasis *android* ini menunjukkan bahwa aplikasi yang dibangun mampu melakukan enkripsi dan dekripsi dengan baik [11].

Hasil Program sistem keamanan dengan sistem kriptografi algoritma *blowfish* dan base64 pada Dinas Kependudukan Dan Pencatatan Sipil Kota Tangerang Selatan telah diuji coba, sehingga program dinyatakan sudah sesuai [12].

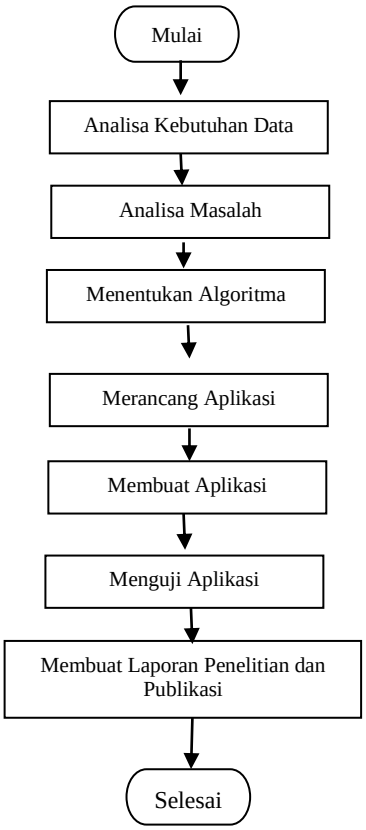
2. Metode Penelitian

Pada penelitian ini telah dilaksanakan dengan kerangka penelitian seperti gambar 1 dan langkah-langkahnya, sebagai berikut:

2.1 Analisis Kebutuhan Data

Analisa kebutuhan digunakan untuk menggambarkan kebutuhan apa saja yang diperlukan did alam proses enkripsi dan dekripsi pada PT. Asuransi Central Asia.

Data yang digunakan untuk dalam penelitian ini adalah data berupa suara hasil rapat pada tahun 2021 yang bersumber dari hasil notulen rapat selama tahun 2021 pada PT. Asuransi Central Asia.



Gambar 1. Kerangka Penelitian Pengamanan File Audio

2.2 Analisa Masalah

Keamanan dan kerahasiaan sebuah data atau informasi dalam komunikasi dan pertukaran informasi menjadi hal yang sangat penting. Itu dikarenakan seringkalinya data atau informasi yang penting kadang tidak sampai ke tangan si penerima atau juga bahkan bisa sampai ke tangan si penerima tetapi data yang diterima tersebut di sadap terlebih dahulu tanpa pengetahuan dari si pengirim maupun oleh si penerima itu sendiri. Begitu juga data yang ada pada PT. Asuransi Central Asia, data informasi berupa audio hasil rapat akan disimpan kedalam arsip hasil rapat. *Audio* tersebut berisi informasi penting baik itu informasi mengenai kemajuan perusahaan atau kemunduran perusahaan. Jika informasi tersebut sampai diketahui oleh pihak yang tidak diinginkan maka sangat membahayakan perusahaan, pihak yang tidak bertanggung jawab dapat saja menggunakan informasi tersebut untuk menyerang perusahaan atau mendapatkan keuntungan pribadi dari hasil mendapatkan informasi tersebut.

2.3 Menentukan Algoritma

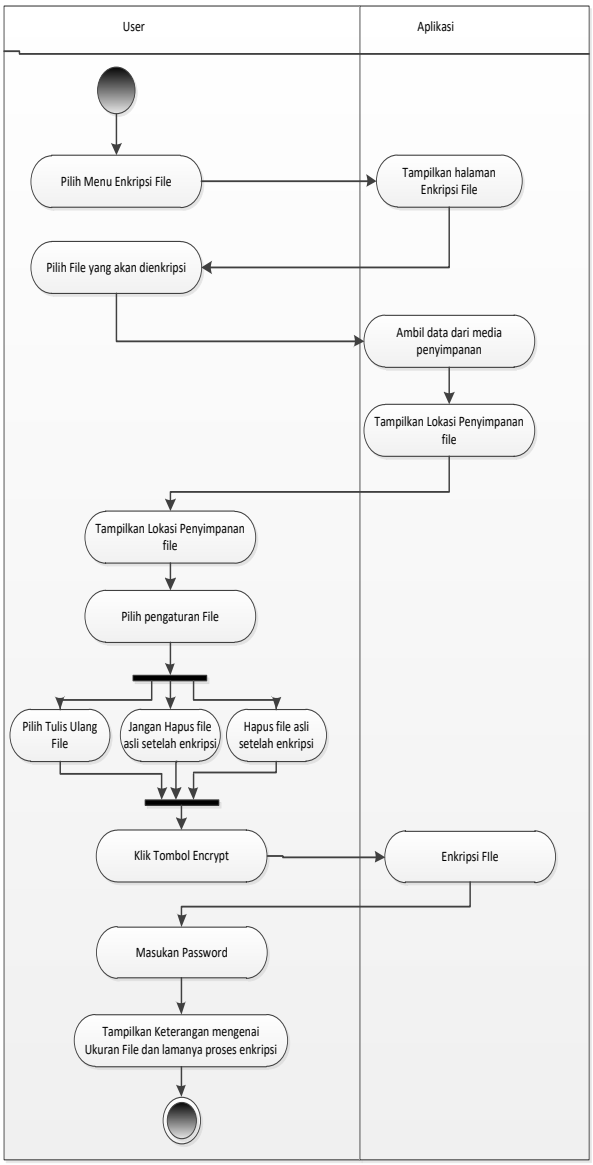
Sebuah metode atau algoritma dapat ditentukan untuk memecahkan permasalahan tersebut, yakni dengan cara menyandikan informasi *audio* tersebut (enkripsi *audio)* ke dalam bentuk suara yang tidak beraturan atau bahkan tidak dapat dibuka sama sekali. Salah satu diantaranya dari algoritma tersebut adalah *Blowfish.* Sehingga keamanan dalam menyimpan data audio hasil rapat dapat dimaksimalkan dengan adanya aplikasi enkripsi menggunakan algoritma *Blowfish*.

2.4 Merancang Aplikasi

Dalam penelitian ini setelah algoritma ditentukan dengan menggunakan algoritma *blowfish*, langkah penelitian berikutnya merancang aplikasi yang meliputi berikut ini:

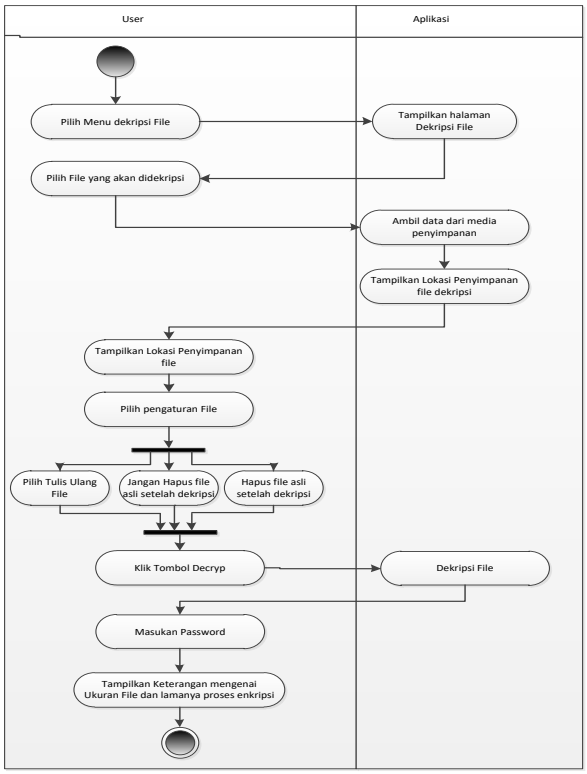
2.4.1 Merancang Proses Enkripsi

Activity diagram proses enkripsi pengamanan *file audio* dengan menggunakan algoritma *blowfish* dapat dilihat pada gambar 2.



Gambar 2. *Activity Diagram* Proses Enkripsi Pengamanan *File Audio*

Activity diagram proses dekripsi pengamanan *file audio* dengan menggunakan algoritma *blowfish* dapat dilihat pada gambar 3.



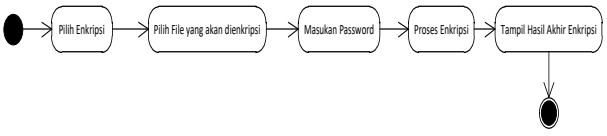
Gambar 4. *Activity Diagram* Proses Dekripsi Pengamanan *File Audio*

Mekanisme proses Algoritma Blowfish:

1) Inisialisasi P-Array (P_0,...P_{17})
2) Inisialisasi S-Array yang berjumlah masing-masing 255 dalam bentuk hexadecimal yang kemudian dikonversi ke biner
3) Ambil *plaintext* / file
4) Kemudian *plaintext* dibagi menjadi 2 bagian XL dan XR
5) Ambil key dan ubah ke ASCII (*hexa*) dan ubah menjadi biner
6) XOR kan key sampai 16 iterasi
7) Setelah melakukan 16 iterasi, maka akan menghasilkan nilai baru XL dan XR masing-masing 32 bit. Tukar kembali XL dan XR. Setelah itu XOR-kan nilai XL dan XR : XR = XR XOR P16 dan XL = XL XOR P_{17}
8) Kemudian XL dan XR digabungkan, sehingga menjadi 64 bit.

2.4.2 Merancang *State Chart Diagram*

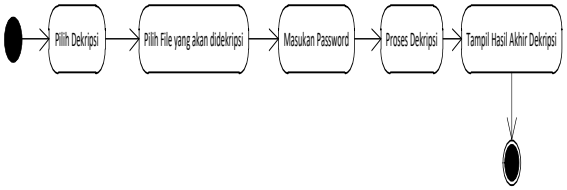
State Chart Diagram proses enkripsi pengamanan *file audio* dengan menggunakan algoritma *blowfish* dapat dilihat pada gambar 5.



Gambar 5. *State Chart Diagram* proses enkripsi pengamanan *file audio*

Pada gambar 5, pertama pilih menu enkripsi, kemudian pilih file *audio* yang akan dienkripsi, setelah file terpilih, maka masukan *password* untuk mengenkripsi *file audio*, kemudian proses enkripsi pengamanan *file audio* dengan menggunakan algoritma *blowfish* dimulai dan setelah proses enkripsi selesai, maka akan tampil hasil akhir enkripsi berupa *file audio* dalam bentuk suara yang tidak beraturan dikuti besar ukuran file dan waktu proses enkripsi.

State Chart Diagram proses dekripsi pengamanan *file audio* dengan menggunakan algoritma *blowfish* dapat dilihat pada gambar 6.

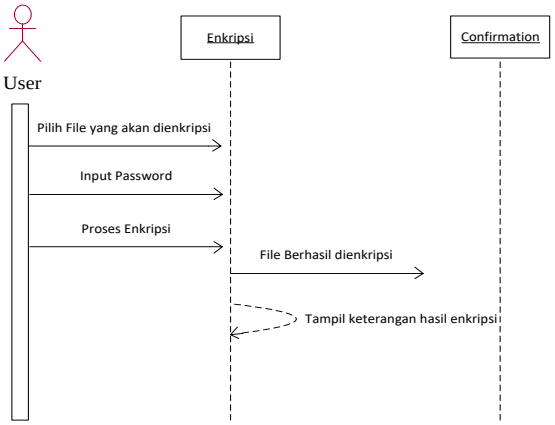


Gambar 6. *State Chart Diagram* proses dekripsi pengamanan *file audio*

Pada gambar 6, pertama pilih menu Dekripsi, kemudian pilih *file audio* yang akan didekripsi, setelah *file audio* terpilih, maka masukan *password* untuk mendekripsi *file audio* dalam bentuk suara yang tidak beraturan, kemudian proses dekripsi pengamanan *file audio* dengan menggunakan algoritma *blowfish* dimulai dan setelah proses dekripsi selesai maka akan tampil hasil akhir dekripsi berupa *file audio* asli dikuti besar ukuran file dan waktu proses dekripsi.

2.4.3 Merancang *Sequence Diagram*

Sequence diagram proses enkripsi pengamanan *file audio* dengan menggunakan algoritma *blowfish* dapat dilihat pada gambar 7.

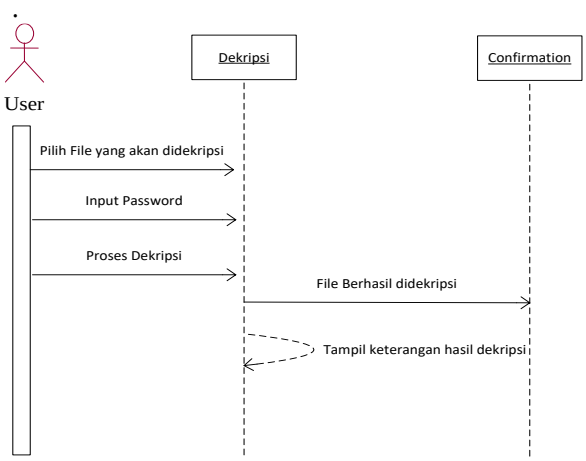


Gambar 7. *Sequence Diagram* Proses Enkripsi Pengamanan *File Audio*

Pada gambar 7, *user* memilih *file* audio yang akan dienkripsi. Kemudian *input password*, setelah *input password* untuk mengenkripsi file audio asli, maka pilih proses enkripsi. Kemudian setelah proses enkripsi pengamanan *file audio* dengan menggunakan algoritma *blowfish* selesai, maka akan tampil keterangan hasil

enkripsi berupa *file audio* dalam bentuk suara yang tidak beraturan dikuti besar ukuran file dan waktu proses enkripsi.

Sequence diagram proses dekripsi pengamanan *file audio* dengan menggunakan algoritma *blowfish* dapat dilihat pada gambar 8.

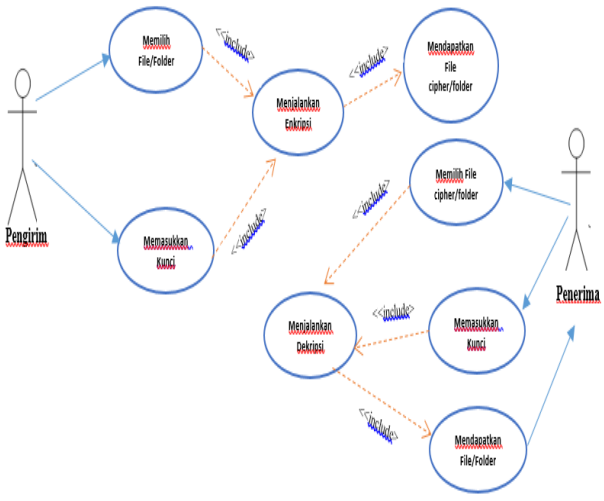


Gambar 8. *Sequence Diagram* Proses Dekripsi Pengamanan *File Audio*

Pada gambar 8, user memilih *file audio* dalam bentuk suara yang tidak beraturan yang akan didekripsi. Kemudian *input password*, setelah password untuk mendekripsi *file audio* dalam bentuk suara yang tidak beraturan dengan menggunakan algoritma *blowfish*, maka pilih proses dekripsi. Kemudian setelah proses dekripsi selesai, maka akan tampil keterangan hasil dekripsi berupa *file audio* asli dikuti besar ukuran file dan waktu proses dekripsi.

2.4.4 Merancang *Usecase Diagram*

Gambar 9. merupakan *use case diagram* merupakan cerminan dari arsitektur aplikasi yang telah dirancang.



Gambar 9. *Usecase Diagram* Proses Dekripsi Pengamanan *File Audio*

Pada gambar 9 *user* dapat memilih *file/folder file audio* asli dan masukan kunci/*password* yang akan digunakan untuk menjalankan proses enkripsi, termasuk *user* akan mendapatkan *file cipher/folder file audio* dalam bentuk suara yang tidak beraturan. User juga dapat memilih *file/folder file audio* dalam bentuk suara yang tidak beraturan dan masukan kunci/*password* yang akan digunakan untuk menjalankan proses dekripsi, termasuk *user* akan mendapatkan *file/folder file audio* asli.

2.5 Membuat Aplikasi

Pada pembuatan aplikasi ini menggunakan bahasa pemrograman *Visual Basic* 6.0 yang berbasis *Desktop.*

2.6 Menguji Aplikasi

Rancangan pengujian yang akan dilakukan dalam pembangunan Aplikasi Enkripsi data pada PT. Asuransi Central Asia menggunakan metode pengujian *black box*, pengujian *User Acceptence Test* (UAT) dan data yang digunakan adalah data nasabah debitur. Pengujian *black box* ini menitikberatkan pada fungsi sistem, metode ini digunakan untuk mengetahui apakah perangkat lunak berfungsi dengan benar.

2.7 Membuat Laporan Penelitian dan Publikasi

Tahap membuat laporan penelitian dan publikasi penelitian adalah memaparkan hasil penelitian yang dilakukan dari tahap awal hingga membuat laporan akhir penelitian.

3. Hasil dan Pembahasan

Dari beberapa hasil pengujian yang dilakukan terhadap data rekaman audio sebanyak 15 kali, maka didapatkan hasil seperti tabel 1.

Tabel 1. Tabel hasil pengujian Aplikasi

No	Nama File Asli	Ukuran file (*Byte*)	Ukuran file Enkripsi (*Byte*)	Waktu Enkripsi (*Second*)	Ukuran file Dekripsi (*Byte*)	Waktu Dekripsi (*Second*)
1	file 1	5.135.392	5.135.408	36.5	5.135.392	59.6
2	file 2	6.055.111	6.057.128	42.8	6.055.111	66.9
3	file 3	5.033.619	5.033.632	36.1	5.033.619	57.7
4	file 4	4.110.347	4.110.360	34.4	4.110.347	54.0
5	file 5	3.996.244	3.996.256	29.8	3.996.244	45.7
6	file 6	2.815.510	2.815.528	22.8	2.815.510	33.5
7	file 7	3.770.964	3.770.976	36.1	3.770.964	43.4
8	file 8	4.320.999	4.321.016	45.5	4.320.999	49.7
9	file 9	1.671.973	1.671.992	14.4	1.671.973	14.7
10	file 10	2.346.142	2.346.160	24.8	2.346.142	27.9
11	file 11	5.857.417	5.857.432	40.1	5.857.417	62.8
12	file 12	6.757.910	6.757.928	47.5	6.757.910	78.8
13	file 13	6.457.188	6.457.200	45	6.457.188	70.6
14	file 14	3.442.866	3.442.880	24.8	3.442.866	39.2
15	file 15	118.368.685	118.368.704	74.8	118.368.685	79.4
Rata-Rata		12.009.358	12.009.507	37.0	12.009.358	52.2

Berdasarkan Uji Coba yang dilakukan sebanyak 15 Buah file yang dienkripsi maka file yang dienkripsi ukurannya menjadi besar dengan nilai rata-rata sebesar 12.009.507 *byte*. Namun jika file enkripsi akan dikembalikan ke file semua (dekripsi) maka ukuran tidak berubah atau kembali ke ukuran semula serta tidak terjadi kerusakan pada isi file baik pada proses enkripsi maupun dekripsi.Adapun waktu proses enkripsi rata-rata sebesar 37.0 *second* sedangkan waktu dekripsi sebesar 52.2 *second*.

Rangkaian hasil penelitian dari pembuatan aplikasi pengamanan *file audio* menggunakan algoritma kriptografi *blowfish* dan pengujian *black box* dan UAT, sebagai berikut:

3.1 Pengujian *Black Box*

Tabel 2 menjelaskan hasil pengujian *black box* aplikasi pengamanan *file audio* menggunakan algoritma kriptografi *blowfish.*

Tabel 2. Hasil Pengujian *Black Box*

Kelas Uji	Butir Uji	*Tools* Pengujian
Enkripsi	Enkripsi menggunakan algoritma *blowfish*	*Black Boc*
Dekripsu	Dekripsi menggunakan algoritma *blowfish*	*Black Boc*

Hasil pengujian ini akan mengambil contoh kasus dari tahap pengujian aplikasi terhadap kesesuaian dengan kebutuhan aplikasi, seperti yang diperlihatkan tabel 3 dan tabel 4.

Tabel.3. Pengujian Enkripsi

Hasil uji (Data Normal)			
Data Masukan	Yang diharapkan	Pengamatan	Kesimpulan
Pilih file audio asli	Data suara yang berekstension .mp3/.wap yang dapat mauuk	Data suara yang berekstension .mp3/.wap yang dapat masuk ke aplikasi	[X] Diterima [ ] Ditolak
Hasil Uji (Data Salah)			
Data Masukan	Yang diharapkan	Pengamatan	Kesimpulan
Data berjenis selain .mp3/.wap yang diinout ke dalam form enkripsi	Tidak dapat masuk ke input form enkripsi	Tampil pesan error	[X] Diterima [ ] Ditolak

Tabel 4. Pengujian Dekripsi

Hasil uji (Data Normal)			
Data Masukan	Yang diharapkan	Pengamatan	Kesimpulan
Pilih file dekripsi/ *file audio* dalam bentuk suara yang tidak beraturan/.cpw	Data suara yang berekstension .cpw yang dapat masuk	Data suara yang berekstension .mp3/.wap yang dapat masuk ke aplikasi	[X] Diterima [ ] Ditolak
Hasil Uji (Data Salah)			
Data Masukan	Yang diharapkan	Pengamatan	Kesimpulan
Data berjenis selain .cpw yang diinput ke dalam form dekripsi	Tidak dapat masuk ke input form dekripsi	Tampil pesan error	[X] Diterima [ ] Ditolak

3.2 Pengujian *User Acceptance Test* (UAT)

Pengujian UAT melibatkan 25 responden pengguna aplikasi penerapan algoritma kriptografi *blowfish* untuk mengamankan data file. Para responden menjawab kuesioner setelah menggunakan aplikasi penerapan algoritma kriptografi *blowfish* untuk mengamankan data *file*. Pada Tabel 5 mempresentasikan daftar pertanyaan survei kuesioner yang terdiri dari 4 bagian: *setting* fungsi; *system metric; user satisfaction;* dan *usability.*

Pertanyaan 1 dan 2 merupakan fokus *setting* fungsi yang meliputi pertanyaan Apakah tampilan aplikasi penerapan algoritma kriptografi *blowfish* menarik dan Apakah Menu-menu aplikasi penerapan algoritma kriptografi *blowfish* ini mudah dipahami bagi pengguna aplikasi penerapan algoritma kriptografi *blowfish* untuk mengamankan data *file* berbasis *web.*

Tabel 5. Daftar Pertanyaan Survei Kuesioner

No	Daftar Pertanyaan
1.	Apakah tampilan aplikasi penerapan algoritma kriptografi *blowfish* menarik?
2.	Apakah Menu-menu aplikasi penerapan algoritma kriptografi *blowfish* ini mudah dipahami?
3.	Apakah aplikasi penerapan algoritma kriptografi *blowfish* ini mudah dioperasikan?
4.	Apakah aplikasi penerapan algoritma kriptografi *blowfish* ini *Responsive*?
5.	Apakah Performa aplikasi penerapan algoritma kriptografi *blowfish* ini baik?
6.	Apakah aplikasi penerapan algoritma kriptografi *blowfish* dapat mengamankan data file?
7.	Apakah Fitur-fitur aplikasi penerapan algoritma kriptografi *blowfish application* ini sudah cukup baik?
8.	Apakah keluaran dari aplikasi penerapan algoritma kriptografi *blowfish* sudah sesuai dengan hasil untuk mengamankan data file.yang melakukannya?

Pertanyaan 3 sampai dengan 5 merupakan fokus *system metric* yang meliputi pertanyaan Apakah aplikasi penerapan algoritma kriptografi *blowfish* ini mudah dioperasikan, Apakah aplikasi penerapan algoritma kriptografi *blowfish* ini *Responsive* dan Apakah Performa aplikasi penerapan algoritma kriptografi *blowfish* ini baik bagi pengguna aplikasi penerapan algoritma kriptografi *blowfish* untuk mengamankan data *file* berbasis *web.*

Pertanyaan 6 merupakan fokus *user satisfaction* yang *meliputi pertanyaan* Apakah aplikasi penerapan algoritma kriptografi *blowfish* dapat mengamankan data file bagi pengguna aplikasi penerapan algoritma kriptografi *blowfish* untuk mengamankan data file berbasis *web.*

Pertanyaan 7 dan 8 merupakan fokus *usability* yang meliputi pertanyaan Apakah Fitur-fitur aplikasi penerapan algoritma kriptografi *blowfish* ini sudah cukup baik dan Apakah keluaran dari aplikasi penerapan algoritma kriptografi *blowfish* sudah sesuai hasil untuk mengamankan data *file*.yang melakukannya bagi pengguna aplikasi penerapan algoritma kriptografi *blowfish* untuk mengamankan data file berbasis *web.*

Aplikasi penerapan algoritma kriptografi *blowfish* untuk mengamankan data file berbasis *web* yang akan diimplementasikan untuk mengetahui tanggapan responden (*user*), maka dilakukan pengujian dengan memberikan pertanyaan kepada 25 responden di mana jawaban dari pertanyaan tersebut terdiri dari tingkatan yang dapat dipilih, seperti Tabel 6.

Tabel 6. Tabel Pilihan Jawaban UAT

Pilihan	Keterangan Jawaban UAT
A	**Sangat**: Mudah/Baik/Sesuai/Jelas/Menarik/Paham/Setuju
B	Mudah/Baik/Sesuai/Jelas/Menarik/Paham/Setuju
C	**Netral**
D	**Cukup**: Sulit/Cukup Baik/Tidak Sesuai/Tidak Jelas/Tidak Menarik/Tidak Paham/Tidak Setuju
E	**Sangat**: Sulit/Jelek/Tidak Sesuai/Tidak Jelas/Tidak Menarik/Tidak Paham/Tidak Setuju

Tabel Bobot Nilai Jawaban UAT dapat dilihat Tabel 7.

Tabel 7. Tabel Bobot Nilai Jawaban UAT

Jawaban UAT	Bobot
A **Sangat**: Mudah/Baik/Sesuai/Jelas/Menarik/Paham	**5**
B **Mudah**/Baik/Sesuai/Jelas/Menarik/Paham	**4**
C **Netral**	**3**
D **Cukup Sulit**/Cukup Baik/Tidak Sesuai/Tidak Jelas/ Tidak Menarik/Tidak Paham/Tidak Setuju	**2**
E **Sangat:** Sulit/Jelek/Tidak Sesuai/Tidak Jelas/Tidak Menarik/Tidak Paham/Tidak Setuju	**1**

Tabel 8 merupakan hasil UAT yang melibatkan pengguna aplikasi penerapan algoritma kriptografi *blowfish* untuk mengamankan data file berbasis *web*. Sebanyak 25 responden melakukan evaluasi dalam pengisian kuesioner. Diperoleh hasil kuesioner dalam bentuk *likert scale* yang akan dianalisis.

Tabel 8. Hasil UAT

Pertanyaan	**Pilihan Jawaban**				
***Setting* Fungsi**	**A**	**B**	**C**	**D**	**E**
Apakah Tampilan aplikasi penerapan algoritma kriptografi *blowfish* menarik?	10	13	1	1	0
Apakah Menu-menu aplikasi penerapan algoritma kriptografi *blowfish* ini mudah dipahami?	14	8	1	2	0
System Metric	**A**	**B**	**C**	**D**	**E**
Apakah aplikasi penerapan algoritma kriptografi *blowfish* ini mudah dioperasikan?	13	9	2	1	0
Apakah aplikasi penerapan algoritma kriptografi *blowfish* ini *Responsive*?	18	6	1	1	0
Apakah Performa aplikasi penerapan algoritma kriptografi *blowfish* ini baik?	19	5	1	0	0
User Satisfaction	**A**	**B**	**C**	**D**	**E**
Apakah aplikasi penerapan algoritma kriptografi *blowfish* dapat mengamankan data file?	20	2	3	0	0
Usability	**A**	**B**	**C**	**D**	**E**
Apakah Fitur-fitur aplikasi penerapan algoritma kriptografi *blowfish* ini sudah cukup baik?	19	4	1	1	0
Apakah keluaran dari aplikasi *penerapan* algoritma kriptografi *blowfish* sudah sesuai hasil mengamankan data file .yang melakukannya?	18	6	1	0	0

Tabel 9 merupakan hasil perkalian masing-masing jawaban UAT dikalikan dengan masing-masing bobot nilai jawaban UAT:

1. Analisa pertanyaan pertama
   Dari tabel 9 dapat dilihat bahwa jumlah nilai dari 25 responden untuk pertanyaan pertama adalah 107. Nilai rata-ratanya adalah 107/25= 4,28. Prosentase nilainya adalah 4,28/5 x 100 %= 85,6%.
2. Analisa pertanyaan kedua
   Dari tabel 9 dapat dilihat bahwa jumlah nilai dari 25 responden untuk pertanyaan kedua adalah 109. Nilai rata-ratanya adalah 109/25 = 4,36. Prosentase nilainya adalah 4,36/5 x 100% = 87,2%.
3. Analisa pertanyaan ketiga
   Dari tabel 5 dapat dilihat bahwa jumlah nilai dari 25 responden untuk pertanyaan ketiga adalah 109. Nilai rata-ratanya adalah 109/25 = 4,36 Prosentase nilainya adalah 4,36/5 x 100% = 87,2%.
4. Analisa pertanyaan keempat
   Dari tabel 5 dapat dilihat bahwa jumlah nilai dari 25 responden untuk pertanyaan keempat adalah 117. Nilai rata-ratanya adalah 117/25 = 4,68. Prosentase nilainya adalah 4,68/5 x 100% = 93,6%.
5. Analisa pertanyaan kelima
   Dari tabel 5 dapat dilihat bahwa jumlah nilai dari 25 responden untuk pertanyaan kelima adalah 118. Nilai rata-ratanya adalah 118/25 = 4,72. Prosentase nilainya adalah 4,72/5 x 100% = 94,4%.
6. Analisa pertanyaan keenam
   Dari tabel 5 dapat dilihat bahwa jumlah nilai dari 25 responden untuk pertanyaan keenam adalah 117 Nilai rata-ratanya adalah 117/25 = 4,68. Prosentase nilainya adalah 4,68/5 x 100% = 93,6%.

Tabel 8. Hasil UAT x Bobot Nilai

Pertanyaan	**Pilihan Jawaban**					**Jumlah**
***Setting* Fungsi**	**A**	**B**	**C**	**D**	**E**	
Apakah Tampilan aplikasi penerapan algoritma kriptografi *blowfish* menarik?	50	52	3	2	0	107
Apakah Menu-menu Sistem pakar berbasis *client-server* ini mudah dipahami?	70	32	3	4	0	109
System Metric	**A**	**B**	**C**	**D**	**E**	
Apakah aplikasi penerapan algoritma kriptografi *blowfish* ini mudah dioperasikan?	65	36	6	2	0	109
Apakah aplikasi penerapan algoritma kriptografi *blowfish* ini Responsive?	90	24	3	0	0	117
Apakah Performa aplikasi penerapan algoritma kriptografi *blowfish* ini baik?	95	20	3	0	0	118
User Satisfaction	**A**	**B**	**C**	**D**	**E**	
Apakah aplikasi penerapan algoritma kriptografi *blowfish* dapat mengamankan data file?	100	8	9	0	0	117
Usability	**A**	**B**	**C**	**D**	**E**	
Apakah Fitur-fitur aplikasi penerapan algoritma kriptografi *blowfish* ini sudah cukup baik?	95	16	3	2	0	116
Apakah keluaran dari aplikasi penerapan algoritma kriptografi *blowfish* sudah sesuai hasil mengamankan data file yang melakukannya?	90	24	3	0	0	117

7. Analisa pertanyaan ketujuh
   Dari tabel 5 dapat dilihat bahwa jumlah nilai dari 25 responden untuk pertanyaan ketujuh adalah 116. Nilai rata-ratanya adalah 116/25 = 4,64. Prosentase nilainya adalah 4,64/5 x 100% = 92,8%.
8. Analisa pertanyaan kedelapan
   Dari tabel 5 dapat dilihat bahwa jumlah nilai dari 25 responden untuk pertanyaan keedelapan adalah 117. Nilai rata-ratanya adalah 117/25 = 4,68. Prosentase nilainya adalah 4,68/5 x 100% = 93,6%.

Dari data di atas dapat disimpulkan bahwa prosentase dari ***setting*** **fungsi sebesar 86,4% setuju** aplikasi penerapan algoritma *blowfish* untuk mengamankan data *file* berbasis web tersebut mempunyai tampilan aplikasi penerapan algoritma *blowfish* menarik dan menu-menu aplikasi penerapan algoritma *blowfish* ini mudah dipahami, dan prosentase dari ***system metric*** **sebesar 91,73% setuju** aplikasi penerapan algoritma *blowfish* ini mudah dioperasikan, aplikasi penerapan algoritma kriptografi *blowfish* ini *responsive* dan performa aplikasi penerapan algoritma *blowfish* ini baik serta prosentase dari ***User Satisfaction*** **sebesar 93,6% setuju** aplikasi penerapan algoritma *blowfish* dapat mengamankan data file dan prosentase dari ***Usability*** **sebesar 93,2% setuju** fitur-fitur aplikasi penerapan algoritma *blowfish* ini sudah cukup baik dan keluaran dari aplikasi penerapan algoritma *blowfish* sudah sesuai hasil mengamankan data file yang melakukannya. Hasil proses pengujian dengan UAT, **para responden setuju (di atas 91,23%)** bahwa secara keseluruhan aplikasi penerapan algoritma *blowfish* untuk mengamankan data *file* dapat terjaga kerahasiannya.

4. Kesimpulan

Kesimpulan yang dapat diambil dari penelitian ini adalah spesifikasi hasil pengujian *blackbox*, keempat fungsi dapat berfungsi sesuai dengan spesifikasi yang dinginkan. Hasil uji coba yang dilakukan sebanyak 15 Buah file yang dienkripsi maka file yang dienkripsi ukurannya menjadi besar dengan nilai rata-rata sebesar 12.009.507 *byte* dan waktu proses enkripsi rata-rata sebesar 37.0 *second* sedangkan waktu dekripsi sebesar 52.2 *second*. Hasil proses pengujian dengan UAT, para responden setuju (di atas 91,23%) bahwa secara keseluruhan aplikasi penerapan algoritma *blowfish* untuk mengamankan data file cabang perusahaan dapat terjaga kerahasiaannya.

Saran untuk pengembangan aplikasi ini ke depannya agar dibuat berbasis *mobile* android dan ditambah metode kompesi data *file*, agar data *file cipher* ukurannya tidak menjadi lebih besar.

Daftar Pustaka

[1] Chandra S. P., Banni S. A., 2016, Sistem Informasi Manajemen Pengarsipan Dengan Menggunakan Algoritma Blowfish , Jurnal Informatika Polinema, ISSN: 2407-070X, Volume 2, Edisi 2, Februari 2016, pp.50-54. DOI: https://doi.org/10.33795/jip.v2i2.55 .

[2] Novrido C., Fitrianty dan Bambang Y. 2016, Aplikasi Enkripsi Pengiriman file Suara Menggunakan Algoritma Blowfish, Seminar Nasional Informatika 2011 (semnasIF 2011), ISSN: 1979-2328, UPN "Veteran" Yogyakarta, 2 Juli 2011, pp. E-201 – E-207, Tersedia di: http://jurnal.upnyk.ac.id/index.php/semnasif/article/view/1298/1172, [Accessed tanggal 12 Juli 2021]**.**

[3] Aldo Adrian et al. 2017, Pengembangan Aplikasi Pengaman Berkas Menggunakan Algoritma Blowfish, Jurnal Sisfo Vol. 07 No. 01, pp. 15–26, doi: https://doi.org/10.24089/j.sisfo.2017.09.002

[4] Endang C. P., 2017. Pengujian UAT (User Acceptance Test). Tersedia di: https://endangcahyapermana.wordpress.com/2017/03/14/pengujian-uat-user-acceptance-test/, [Accessed 12 Maret 2021].

[5] C. S. Theng, 2017. "Leisure Technology for the Elderly : A Survey , User Acceptance Testing and Conceptual Design," Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 12, pp. 100–115, 2017.

[6] Danang W. U., Defri K. dan Yani P. A.. 2018. Teknik Pengujian Perangkat Lunak Dalam Evaluasi Sistem Layanan Mandiri Pemantauan Haji Pada Kementerian Agama Provinsi Jawa Tengah. Jurnal SIMETRIS, Vol. 9 No. 2 November 2018, P-ISSN: 2252-4983, E-ISSN: 2549-3108, pp.731–746.

[7] Hendri M., Basorudin, 2017, Analisis Algoritma Blowfish Pada Proses Enkripsi Dan Dekripsi File, Riau Journal of Computer Science Vol. 3 No. 2, eISSN 2477-6890, pISSN 2460-0679, pp. 156-168, doi: https://doi.org/10.30606/rjocs.v3i2.1348.

[8] Muhathir, 2018, Perbandingan Algoritma Blowfish Dan Twofish Untuk Kriptografi File Gambar, JITE, 2 (1) Juli 2018, ISSN 2549-6255 (Print), ISSN 2549-6247 (Online), pp. 23-32, Tersedia di: https://ojs.uma.ac.id/index.php/jite/article/view/1673/1601, [Accessed 13 Maret 2021].

[9] Ibrahim M. S., Anggi P. S. dan Wawan G., 2019, Aplikasi Enkripsi dan Dekripsi untuk Keamanan Komunikasi Data pada SMS (Short Message Service) Berbasis Android Menggunakan Algoritma Blowfish, Jurnal FORMAT, Volume 8, Nomor 1, Tahun 2019, ISSN : 2089–5615 , pp. 34-41, Tersedia di: https://publikasi.mercubuana.ac.id/index.php/format/article/view/5716/2761, [Accessed 15 Maret 2021].

[10] Dimas A. T. dan Herlina L. S., 2016, Analisis Perbandingan Kinerja Algoritma Blowfish Dan Algoritma Twofish Pada Proses Enkripsi Dan Dekripsi, ,Jurnal Pseudocode, Volume 2 Nomor 1, Februari 2015, ISSN 2355 – 5920, pp. 37-44, Tersedia di: https://ejournal.unib.ac.id/index.php/pseudocode/article/view/424/368, [Accessed 15 Maret 2021], DOI: https://doi.org/10.33369/pseudocode.2.1.37-44,

[11] Siswo W., Zaldi I, Rian F, Enkripsi Dan Dekripsi File Dengan Algoritma Blowfish Pada Perangkat Mobile Berbasis Android, Jurnal Nasional Teknik Elektro, Vol: 5, No. 1, Maret 2016, ISSN: 2302 – 2949, pp. 36-44, Tersedia di: http://jnte.ft.unand.ac.id/index.php/jnte/article/view/199/209, [Accessed 25 Maret 2021], DOI : 10.20449/jnte.v5i1.199.2016..

[12] Mujito, Anugrah, 2016. Aplikasi Kriptografi File Menggunakan Metode Blowfish dan Metode Base64 pada Dinas Kependudukan dan Pencatatan Sipil Kota Tangerang Selatan, Jurnal SISFOKOM, Volume 05, Nomor 01, September 2016, pp. 54-60, Tersedia di: http://jurnal.atmaluhur.ac.id/index.php/sisfokom/article/view/39/511., [Accessed 25 Maret 2021], DOI: https://doi.org/10.32736/sisfokom.v5i2.39.