APLIKASI KRIPTOGRAFI UNTUK MENGAMANKAN FILE AUDIO VIDEO MENGGUNAKAN VISUAL BASIC .NET

Frenky Fernando, Siswanto, Eko Suryana

Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Dehasen Bengkulu
Jl. Meranti Raya No. 32 Kota Bengkulu 38228 Telp. (0736) 22027, 26957 Fax. (0736) 341139

ABSTRACT

In terms of file security is often diminished, because the file with the extension * and * .MP4 .MP3 is like the audio files that we secured was listening to the audio exams and video UAN English as exam for student/student in Ja Al-Haq is not given a security so that everyone can see the file. Application of cryptography to secure audio video files using visual basic Net made to secure the audio video files which are air-extension "* Mp3, Mp4 *" were built using the programming language Visual Basic Net. The encryption process is a process to convert the original video audio files into files that cannot be executed. Decryption process is a process to convert audio and video files into audio files randomly original video. Testing data security system is a test conducted to determine the safety data that has been integrated on a particular file, in this case the video audio file "* Mp3, * mp4".
Keywords: Algorithm AES, Audio Video, Encryption, Decryption.

INTISARI

Dalam hal pengamanan file seringkali dinomorduakan, dikarenakan file dengan *extention* *.MP3 dan *.MP4 yaitu seperti pada file audio yang kita amankan ialah audio listening untuk ujian UAN Bahasa Inggris sedangkan video seperti soal ujian untuk siswa/siswi di Ja Al-haq yang tidak diberikan suatu keamanan sehingga setiap orang dapat melihat file tersebut. Aplikasi kriptografi untuk mengamankan file audio video menggunakan *visual basic .Net* dibuat untuk mengamankan file audio video yang ber-ektensi "*.mp3, *.mp4" yang dibangun menggunakan bahasa pemrograman *Visual Basic .Net*. Proses enkripsi merupakan proses untuk mengubah file audio video asli menjadi file yang tidak dapat dijalankan. Proses dekripsi merupakan proses untuk mengubah file audio video acak menjadi file audio video asli. Pengujian sistem keamanan data merupakan pengujian yang dilakukan untuk mengetahui keamanan data yang telah diintegrasikan pada file tertentu, dalam hal ini adalah file audio video berextensi "*.mp3, *.mp4".
Kata Kunci: Algoritma AES, Audio Video, Enkripsi, Dekripsi.

I. PENDAHULIAN

Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat penting bagi sebuah organisasi, baik yang berupa organisasi komersial, perguruan tinggi, instansi pemerintah, maupun individual. Demikian juga halnya dengan Madrasah Tsanawiyah (MTS) Ja Al-haq. MTS tersebut sudah menggunakan komputer untuk melakukan proses pengolahan file. Dalam hal pengamanan file seringkali dinomorduakan, dikarenakan file dengan *extention* *.MP3 dan *.MP4 yaitu seperti pada file audio yang kita amankan ialah audio listening untuk ujian UAN Bahasa Inggris sedangkan video seperti soal ujian untuk siswa/siswi di Ja Al-haq yang tidak diberikan suatu keamanan sehingga setiap orang dapat melihat file tersebut.

Dari latar belakang diatas, maka penulis mengangkat judul "Aplikasi Kriptografi Untuk Mengamankan File Audio Video Menggunakan Visual Basic .Net" untuk menjaga keamanan file yang berupa file audio video tersebut pada MTS Ja Al-Haq Kota Bengkulu.

Batasan masalah ini membahas mengenai aplikasi kriptografi untuk mengamankan file audio video menggunakan visual basic .net. Data yang akan digunakan merupakan file audio video dengan format extension *.mp3., *mp4.

II. TINJAUAN PUSTAKA

A. *Sistem Komputer*

Komputer berasal dari bahasa latin computare yang mengandung arti menghitung (Irfan, 2013:4).

Dalam sistem komputer terdapat beberapa sistem operasi pendukung yang sangat penting yaitu *Software*, *Hardware*, dan *Brainware*. *Sofware* adalah perangkat lunak atau perintah-perintah komputer yang lebih dikenal dengan istilah program, Dimana *software* ini terdiri dari :

1) *Sistem operasi*: adalah program yang ditulis untuk mengendalikan dan mengkoordinasikan kegiatan sistem.
2) *Program paket* (*package program*): merupakan program yang dikerjakan dalam salah satu bahasa yang disiapkan untuk satu bidang, yang mana terdiri dari program paket atau program aplikasi (*Wordstar, Ms Word, Excel, lotus* dan lain-lain).
3) *Bahasa pemrograman*: Bahasa pemrograman merupakan suatu media yang digunakan untuk komunikasi antara manusia dengan komputer. Dimana bahasa penterjemah komputer terdiri dari bahasa mesin atau bahasa pemrograman tingkat rendah *(low level language*) seperti bahasa mesin atau bahasa *assembler*. Sedangkan untuk *High Level Language* atau bahasa pemrograman tingkat tinggi, bahasa yang digunakan hampir

sama dengan bahasa manusia terutama bahasa inggris, sehingga perintah-perintah yang digunakan lebih mudah dimengerti oleh seseorang *programmer*. Contohnya bahasa pemrograman tingkat tinggi adalah *Bahasa Pascal, Basic, Turbo Basic.*

Perangkat keras *(hardware)* adalah semua peralatan komputer yang dapat dilihat dan diraba secara fisik atau semua komponen fisik yang mendukung sistem komputer (Koememadi, 2005:11). Pada dasarnya perangkat keras terdiri dari 4 (empat) kelompok, yakni:

1) Perangkat Masukan *(input device):* adalah peralatan yang berfungsi untuk membaca dari media pembawa data, yang merupakan bahan masuk bagi sistem pengolah data.
2) Perangkat Keluaran *(output device)*: adalah perangkat yang berfungsi sebagai alat untuk mengeluarkan hasil sistem pengolahan data komputer.
3) CPU (*Control Processing Unit*): merupakan bagian dari sistem komputer yang fungsinya untuk melakukan koordinasi sistem kerja komputer.
4) Unit Penyimpanan Data *(Storage)*: merupakan bagian dari sistem komputer yang berfungsi untuk menyimpan data (data masukan dan program komputer) pada saat tidak diolah.

Brainware adalah manusia yang terlibat dalam mengoperasikan serta mengatur sistem didalam komputer. Diartikan juga sebagai perangkat intelektual yang mengoperasikan dan mengeksplorasi kemampuan dari *Hardware* maupun *Software* (Marzuki, 2010:9).

B. Visual Basic .Net

Platform Microsoft.Net merupakan model untuk development dimana platform dan aplikasi bisa dibuat dan dijalankan tanpa bergantung pada alat (device) yang dipakai. Teknologi ini memungkinkan beberapa aplikasi bekerja sama. Visual Basic.Net merupakann core dari pembuatan aplikasi berbasis .Net. yang merupakan lingkungan pemrograman yang mempermudah tahapan desain, development, debugging, dan deployment dari aplikasi berbasi .Net dan XML web service, serta meningkatkan efisiensi developer dengan menyediakan lingkungan pemrograman yang sudah biasa digunakan (Suharli, 2005:13).

C. Konsep Perancangan Database

Menurut Ladjamudin (2005:62), konsep dan *Implementasi* dari sistem basis data dalam suatu proyek pengembangan sistem informasi sehingga kita tidak harus terpaku pada satu defenisi dari sistem basis data saja. Beberapa defenisi basis data dari beberapa orang ahli data adalah sebagai berikut:

1) *Database* adalah sekumpulan program-program aplikasi umum yang bersifat *"batch"* yang mengeksekusi dan memproses data secara umum (sistem pencarian, peremajaan, dan penghapusan terhadap data).
2) *Database* terdiri dari data yang akan digunakan atau diperuntukkan terhadap banyak *"user",* dimana masing-masing *"user"* (baik menggunakan teknis pemrosesan yang bersifat *batch* atau *on-line*) akan menggunakan data tersebut sesuai dengan tugas dan fungsinya, dan *user* lain dapat juga menggunakan data tersebut dalam waktu yang bersamaan.

Dengan pendekatan DBMS, maka *sharing* data dapat dengan mudah dilakukan siapa saja (program apa saja boleh menggunakan data tersebut, jika memenuhi berbagai prosedur yang ditetapkan pada *interface* yang melindungi database tersebut). Semua tugas termasuk mengkonversi data adalah tanggung jawab program.

D. Sistem Keamanan

Sistem berasal dari bahasa Latin (systēma) dan bahasa Yunani (sustēma) adalah suatu kesatuan yang terdiri komponen atau elemen yang dihubungkan bersama untuk memudahkan aliran informasi, materi atau energi untuk mencapai suatu tujuan. Istilah ini sering dipergunakan untuk menggambarkan suatu set entitas yang berinteraksi, di mana suatu model matematika seringkali bisa dibuat (Anonymous, 2012).

Sistem adalah suatu unit kesatuan yang saling berinteraksi dan bergantung satu dengan lainnya yang diarahkan pada suatu tujuan dan dapat bertahan dalam jangka waktu tertentu (Farhan, 2011).

Berdasarkan definisi sistem tersebut, maka dapat disimpulkan bahwa sistem merupakan suatu kesatuan yang terdiri komponen atau elemen yang saling berinteraksi satu dengan lainnya untuk mencapai suatu tujuan tertentu.

Ada beberapa elemen yang membentuk sebuah sistem, yaitu: tujuan, masukan, proses, keluaran, batas, mekanisme pengendalian dan umpan balik serta lingkungan. Berikut penjelasan mengenai elemen-elemen yang membentuk sebuah sistem (Anonymous, 2012):

1) Tujuan: Setiap sistem memiliki tujuan (Goal), entah hanya satu atau mungkin banyak. Tujuan inilah yang menjadi pemotivasi yang mengarahkan sistem. Tanpa tujuan, sistem menjadi tak terarah dan tak terkendali. Tentu saja, tujuan antara satu sistem dengan sistem yang lain berbeda.

2) Masukan: Masukan (input) sistem adalah segala sesuatu yang masuk ke dalam sistem dan selanjutnya menjadi bahan yang diproses. Masukan dapat berupa

hal-hal yang berwujud (tampak secara fisik) maupun yang tidak tampak. Contoh masukan yang berwujud adalah bahan mentah, sedangkan contoh yang tidak berwujud adalah informasi (misalnya permintaan jasa pelanggan).

3) Proses: Proses merupakan bagian yang melakukan perubahan atau transformasi dari masukan menjadi keluaran yang berguna dan lebih bernilai, misalnya berupa informasi dan produk, tetapi juga bisa berupa hal-hal yang tidak berguna, misalnya saja sisa pembuangan atau limbah. Pada pabrik kimia, proses dapat berupa bahan mentah. Pada rumah sakit, proses dapat berupa aktivitas pembedahan pasien.

4) Keluaran: Keluaran (output) merupakan hasil dari pemrosesan. Pada sistem informasi, keluaran bisa berupa suatu informasi, saran, cetakan laporan, dan sebagainya.

5) Batas: Yang disebut batas (*boundary*) sistem adalah pemisah antara sistem dan daerah di luar sistem (lingkungan). Batas sistem menentukan konfigurasi, ruang lingkup, atau kemampuan sistem. Sebagai contoh, tim sepakbola mempunyai aturan permainan dan keterbatasan kemampuan pemain. Pertumbuhan sebuah toko kelontong dipengaruhi oleh pembelian pelanggan, gerakan pesaing dan keterbatasan dana dari bank. Tentu saja batas sebuah sistem dapat dikurangi atau dimodifikasi sehingga akan mengubah perilaku sistem. Sebagai contoh, dengan menjual saham ke publik, sebuah perusahaan dapat mengurangi keterbasatan dana.

6) Mekanisme Pengendalian dan Umpan Balik: Mekanisme pengendalian (control mechanism) diwujudkan dengan menggunakan umpan balik (feedback), yang mencuplik keluaran. Umpan balik ini digunakan untuk mengendalikan baik masukan maupun proses. Tujuannya adalah untuk mengatur agar sistem berjalan sesuai dengan tujuan.

7) Lingkungan: Lingkungan adalah segala sesuatu yang berada diluar sistem. Lingkungan bisa berpengaruh terhadap operasi sistem dalam arti bisa merugikan atau menguntungkan sistem itu sendiri. Lingkungan yang merugikan tentu saja harus ditahan dan dikendalikan supaya tidak mengganggu kelangsungan operasi sistem, sedangkan yang menguntungkan tetap harus terus dijaga, karena akan memacu terhadap kelangsungan hidup sistem.

Keamanan adalah keadaan bebas dari bahaya. Istilah ini bisa digunakan dengan hubungan kepada kejahatan, segala bentuk kecelakaan, dan lain-lain. Keamanan merupakan topik yang luas termasuk keamananan nasional terhadap serangan teroris, keamanan komputer terhadap hacker, keamanan rumah terhadap maling dan penyelusup lainnya, keamanan finansial terhadap kehancuran ekonomi dan banyak situasi berhubungan lainnya. Kemanan data adalah proses untuk melindungi data dari perusakan atau penyalahgunaan yang dilakukan oleh orang dalam atau di luar sebuah organisasi. (Anonymous, 2012).

Dari definisi tersebut, maka dapat disimpulkan bahwa keamanan merupakan keadaan yang bebas dari bahaya yang dilakukan oleh hacker, cracker, dengan segala bentuk kejahatan.

Beberapa konsep terjadi di beberapa bidang keamanan, antara lain :

1) Risiko, yaitu kemungkinan kejadian yang menyebabkan kehilangan
2) Ancaman, yaitu sebuah metode merealisasikan risiko
3) *Counter measure* yaitu sebuah cara untuk menghentikan ancaman
4) Pertahanan dalam kedalaman, jangan pernah bergantung pada satu pengatasan keamanan saja.
5) Asuransi, yaitu tingkatan jaminan bahwa sebuah sistem keamanan data akan berlaku seperti yang diperkirakan

E. Aplikasi

Menurut Widianti (2000), aplikasi adalah suatu program yang siap untuk digunakan yang dibuat untuk melaksanakan suatu fungsi bagi pengguna jasa aplikasi serta penggunaan aplikasi lain yang dapat digunakan oleh suatu sasaran yang akan dituju.

F. Kriptografi

Ada beberapa definisi kriptografi yang didapat dari berbagai sumber, antara lain:

1) Kriptografi (*Cryptography*) didefinisikan sebagai ilmu sekaligus seni untuk menjaga kerahasiaan pesan (data atau informasi) yang mempunyai pengertian, dengan cara menyamarkannya (mengacak) menjadi bentuk yang tidak dapat dimengerti menggunakan suatu algoritma tertentu (Mulya, 2008).
2) Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga (Candra, 2005).
3) Kriptografi merupakan ilmu yang mempelajari tentang bagaimana cara membuat suatu pesan hanya bisa dibaca oleh pihak yang berwenang untuk membacanya (Setiawan, 2010).
4) Kriptografi adalah ilmu yang khusus mendalami teknik untuk menjaga kerahasiaan data. Algoritma kriptografi ialah mengubah tulisan yang semula bermakna menjadi tidak bermakna isinya dengan menggunakan berbagai algoritma yang dirancang oleh kriptografer. (Soleh, 2010).

Berdasarkan beberapa definisi kriptografi di atas, dapat disimpulkan bahwa Kriptografi merupakan ilmu sekaligus seni untuk menjaga kerahasiaan data atau informasi agar tidak dapat di lihat, dibaca,

dimengerti oleh pihak ketiga yang tidak memiliki wewenang terhadap data atau informasi tersebut.

G. Enkripsi dan Dekripsi

Enkripsi merupakan proses transformasi terhadap teks asli sehingga menghasilkan teks sandi. Sedangkan dekripsi merupakan proses pemulihan kembali teks sandi menjadi teks asli bila kunci rahasia yang dipakai dekripsi sama dengan kunci rahasia yang dipakai untuk enkripsi (Sadikin, 2012).

Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen-elemenantara kedua himpunan tersebut. Misalkan P menyatakan plainteks dan dan Cmenyatakan chiperteks, maka fungsi enkripsi E memetakan P ke C (Munir, 2006) :

$$E(P) = C$$

Dan fungsi dekripsi D memetakan C ke P,

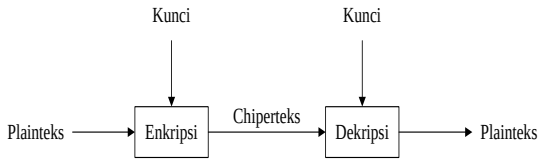
$$D(C) = P$$

Karena proses enkripsi kemudian dekripsi mengembalikan pesan ke pesan asal, makakesamaan berikut harus benar,

$$D(E(P)) = P$$

Keamanan algoritma sering kriptografi diukur dari banyaknya kerja (work) yangdibutuhkan untuk memecahkan chiperteks menjadi plainteksnya tanpa mengetahuikunci yang digunakan. Kerja ini dapat diekivalenkan dengan waktu, memori, uang,dan lain-lain. Semakin banyak kerja yang diperlukan, yang berarti juga semakin lamawaktu yang dibutuhkan, maka semakin kuat algoritma kriptografi tersebut, yangberarti semakin aman digunakan untuk menyandikan pesan.

Adapun skema enripsi dan dekripsi, terlihat pada Gambar 1. (Munir, 2006) :



Gambar 1. Skema Enkripsi dan Dekripsi

H. Enkripsi

Chiper berlangsung dalam rentetan empat fungsi pembangun (primitif) yang telah dijelaskan yaitu: *SubByte(), ShiftRows(), MixColumns(),* dan *AddRoundKey().* Rentetan tersebut dijalankan sebanyak Nr-1 sebagai *loop* utama. Setelah loop utama tersebut berakhir (sembilan *round*), *SubByte(), ShiftRows(),* dan *AddRoundKey().* Dieksekusi secara berturut-turut sebagai *final round.*

I. Dekripsi

Transformasi-transformasi yang merupakan kebalikan dari setiap cipher diterapkan dalam program dekripsi (*inverse cipher*). Fungsi *AddRoundKey()* untuk enkripsi digunakan kembali untuk dekripsi. Adapun yang harus dibuat lagi adalah *InvSubBytes(), InvShiftRows(),* dan *InvMixColumns()*. Beberapa bagian cukup dikopi dari fungsi kebalikannya yang telah digunakan saat enkripsi. *AddRoundKey()* dieksekusi sebagai initial round, diikuti sembilan round rentetan *InvShiftRows(), InvSubBytes(), InvMixColumns(),* dan *AddRoundKey().* Round ke-10 yang mengikutinya tidak menyertakan *InvMixColumns* serupa dengan final round enkripsi.

J. Audio Video

Menurut sudjana dan Rivai (2003:129) media audio adalah bahan yang mengandung pesan dalam bentuk auditif (pita suara atau piringan suara), yang dapat merangsang pikiran, perasaan, perhatian dan kemauan siswa sehingga terjadi proses belajar mengajar.

Menurut Aria Pramudito (2013:4) Video adalah teknologi pemrosesan sinyal elektronik mewakilkan gambar bergerak. Jadi audio video adalah teknologi yang mewakili pemerosesan pesan (pita suara atau piringan suara) dalam bentuk auditif dan gerak gambar.

K. Konsep Perancangan Sistem

Perancangan sistem merupakan proses untuk menspesifikasikan rincian solusi yang dipilih dalam menyelesaikan suatu sistem. Dalam perancangan sistem tersebut, dibutuhkan suatu aliran data dari sistem yang disebut juga dengan Diagram Alir Data (DAD).

DAD adalah suatu diagram yang menggunakan notasi-notasi untuk menggambarkan arus dari data sistem, yang penggunaannya sangat membantu untuk memahami sistem secara logika, terstruktur dan jelas (Said, 2010). Ada beberapa simbol yang digunakan dalam DAD yang merupakan karakteristik dari suatu sistem, yaitu dapat dilihat pada Tabel 1. (Juwita, 2005).

Tabel 1. Simbol DAD

No	Nama	Simbol
1.	Entitas	
2.	Proses	
3.	Data Store	
4.	Alur Data	

L. *Flowchart*

Menurut Jogiyanto (2005:802) ”Bagan alir program (program flowchart) merupakan bagan alir yang mirip dengan bagan alir sistem, yaitu untuk menggambarkan prosedur di dalam sistem”.

Ada beberapa simbol yang digunakan dalam *Flowchart* yang digunakan dalam suatu sistem.

III. METODOLOGI PENELITIAN

A. Metode Penelitian

Adapun metode penelitian yang digunakan penulis adalah metode eksperimen. Penulis melakukan eksperimen dengan cara menerapkan algoritma kriptografi untuk mengamankan file audio video.

B. Metode Pengumpulan Data

Metode pengumpulan data digunakan untuk memperoleh data yang dapat mendukung permasalahan yang akan dibahas. Sehubungan dengan hal ini maka digunakan metode pengumpulan data yang meliputi :

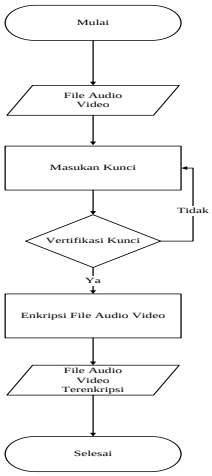
1) *Observasi*: dalam pengumpulan data ini, data diperoleh dengan mengikuti pelaksanaan sistem keamanan data yang terjadi pada Madrasah Tsanawiyah Ja-Alhaq.
2) *Studi Pustaka*: adalah suatu metode pengumpulan data yang diambil dari perpustakaan atau instansi yang berupa karya ilmiah, jurnal, buku-buku serta dari *internet* yang berhubungan dengan penulisan ini. Tujuan dari studi pustaka ini adalah untuk mendalami dan memperoleh keterangan yang lengkap terhadap obyek yang diteliti.

C. Metode Perancangan Sistem

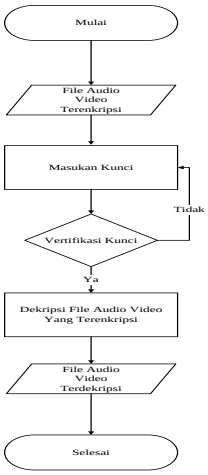
Algoritma kriptografi memiliki kunci yang sama untuk proses enkripsi dan dekripsi dengan catatan bahwa kunci tersebut sudah disepakati oleh kedua belah pihak antara pengirim dan penerima. Salah satu algoritma kriptografi adalah algoritma *Advanced Encryption Standard* (AES). Adapun proses enkripsi dan dekripsi yang terjadi pada algoritma kriptografi yaitu dengan sistem *flowchart* terlihat pada Gambar 2 dan 3.

Berdasarkan proses *flowchart* enkripsi file audio video (Gambar 2), maka dapat penulis simpulkan dalam proses enkripsi tersebut maka disaat memulai proses enkripsi yang pertama yang harus dilakukan yaitu dengan menginputkan file audio video yang akan dienkripsi kemudian pengguna memasukan kunci untuk proses enkripsi.

Apabila kunci yang dimasukan salah maka akan diminta memasukan kunci enkripsi kembali, dan apabila kunci yang dimasukan benar maka proses enkripsi berlanjut dan file audio video akan terenkripsi selanjutnya pengguna akan mendapatkan hasil yaitu file audio video terenkripsi.



Gambar 2. *Flowchart* Enkripsi File Audio Video



Gambar 3. *Flowchart* Dekripsi File Audio Video

Berdasarkan proses flowchart dekripsi file audio video yang terenkripsi (Gambar 3), maka dapat penulis dapat jelaskan proses dekripsi tersebut disaat memulai proses dekripsi yang pertama yang harus dilakukan yaitu dengan menginputkan file audio video yang terenkripsi kemudian pengguna memasukan kunci yang sama disaat kita melakukan enkripsi tadi.

Apabila kunci yang dimasukan tidak sama disaat enkripsi maka akan diminta memasukan kunci dekripsi kembali, dan apabila kunci yang dimasukan benar maka proses dekripsi berlanjut dan file audio video akan terenkripsi tadi akan berubah menjadi file audio video yang terdekripsi selanjutnya pengguna akan mendapatkan hasil yaitu file audio video terdekripsi.

D. Prosedur Sistem Keamanan Data Menggunakan Algoritma Kriptografi

Sistem keamanan data digunakan sebagai media untuk mengamankan data-data penting, yang

prosesnya akan dilakukan proses enkripsi dan dekripsi pada data tersebut.Prosedur yang dilakukan pada sistem keamanan data yaitu dengan mempersiapkan :

1) Kunci yang telah disepakati antara pengirim dan penerima
2) File audio video yang akan di enkripsi
3) File ausdio video yang akan didekripsi

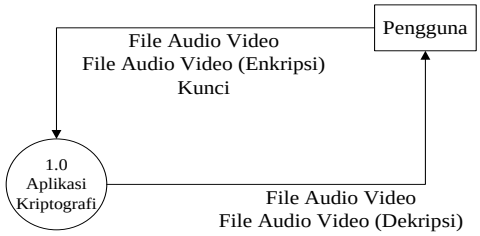
Setelah mempersiapkan hal-hal yang diperlukan, maka peneliti akan menggunakan file asli dan kunci untuk melakukan proses enkripsi, begitu juga sebaliknya dalam proses dekripsi.

E. Diagram Alir Data

Diagram alir data digunakan untuk menggambarkan proses dari suatu sistem yang akan dibuat.

1. Diagram Konteks

Diagram konteks merupakan gambaran secara umum dari proses suatu sistem, seperti ditunjukkan pada Gambar 4.

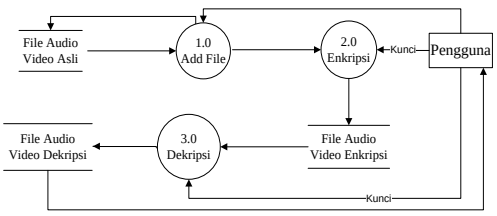


Gambar 4. Diagram Konteks

Gambar 4 menjelaskan proses dari sistem keamanan data yang dilakukan oleh pengguna. Pengguna dapat mengenkripsi file, dengan cara menginputkan file audio video (file extension *.mp3 atau *.mp4) dan kunci, hasil dari proses enkripsi akan menghasilkan file audio video palsu. Pengguna juga dapat melakukan dekripsi file atau mengembalikan file audio video palsu tadi ke file audio video asli, dengan cara menginputkan file audio video palsu (file hasil enkripsi extension *.mp3 atau *.mp4) dan kunci, hasil dari proses dekripsi akan menghasilkan file audio video asli.

2. DAD Level 0 (*Overview*)

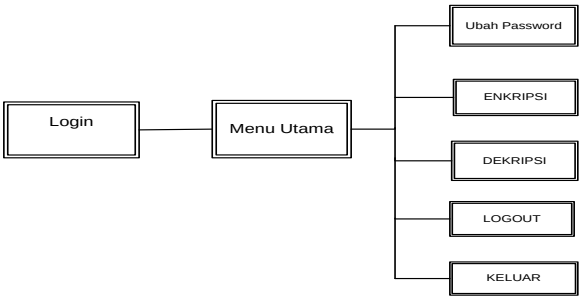
DAD Level 0 (*Overview*) merupakan pemecahan dari proses yang terdapat pada diagram dibawah ini, seperti terlihat pada Gambar 5.



Gambar 5. DAD Level 0 (*Overview*)

F. Rancangan Struktur Menu

Rancangan struktur menu menggambarkan sistematika atau susunan menu serta sub menu yang terdapat pada aplikasi sistem keamanan data. Adapun rancangan struktur menu dapat di lihat pada Gambar 6.



Gambar 6. Rancangan Struktur Menu

Dari Gambar 8, dapat diketahui bahwa rancangan struktur menu pada aplikasi *kriptografi* ini yaitu sebelum kita menggunakan aplikasi kriptografi ini maka yang pertama yang kita lakukan ialah login sebagai admin agar bisa menggunakan aplikasi kriptografi ini, setelah itu kita akan disajikan dengan tampilan menu utama. Dari menu tersebut terdapat beberapa proses yang bisa kita gunakan.

G. Rancangan Antarmuka

Rancangan antarmuka merupakan halaman-halaman menu yang terdapat pada sistem keamanan data. Adapun rancangan antarmuka sistem keamanan data, antara lain :

Menu Login: Menu login muncul ketika pertama kali aplikasi sistem keamanan ini dijalankan. Pengguna harus menginputkan username dan password yang valid untuk masuk ke menu utama. Adapun halaman menu *login*, terlihat pada gambar di bawah ini :

Menu Utama: Menu utama muncul ketika proses validasi di menu login berhasil, menu utama memiliki beberapa menu yang dapat di akses oleh pengguna, yakni ubah *password*, enkripsi, dekripsi, logout, keluar.

Menu Ubah Password: Menu ubah password digunakan untuk mengubah password pengguna aplikasi sistem keamanan data, sehingga hanya pengguna yang tau password yang digunakan sebelum masuk ke menu utama.

Menu Proses Enkripsi: Menu enkripsi digunakan untuk mengamankan file audio video dengan aplikasi kriptografi, sehingga file audio video tersebut tidak bisa dibuka.

Menu Proses Dekripsi: Menu dekripsi digunakan untuk membuka keamanan file audio video tersebut sehingga yang awalnya tidak bisa dibuka, menjadi bisa terbuka dengan catatan menggunakan variasi kunci yang sama pada aplikasi kriftografi.

H. Metode Pengujian Sistem

Pengujian sistem merupakan proses eksekusi sistem dengan tujuan mencari kesalahan atau kelemahan dari program tersebut. Proses tersebut dilakukan dengan mengevaluasi kemampuan program. Metode pengujian yang dipakai dalam sistem ini adalah metode *black box*.

Metode pengujian *black box* merupakan metode pengujian dengan pendekatan yang mengasumsikan sebuah sistem perangkat lunak atau program sebagai suatu kotak hitam (Rifai, 2003:50). Pengujian dilakukan dengan memberi masukan pada form yang tersedia dengan beberapa data yang dikategorikan dalam kategori data yang sah (sesuai dengan peruntukannya), dan data yang tidak sah (data yang berfungsi untuk mengeksploitasi sistem). Setelah itu tanggapan yang diberikan oleh sistem akan dicatat.

IV. PEMBAHASAN

A. Aplikasi Kriptografi untuk Mengamankan FileAudio Video Menggunakan Visual Basic.Net

Aplikasi kriptografi untuk mengamankan file audio video menggunakan *visual basic .Net* dibuat untuk mengamankan file audio video yang ber-ektensi "*.mp3, *.mp4" yang dibangun menggunakan bahasa pemrograman *Visual Basic .Net*. Sistem keamanan data memiliki beberapa menu yang dapat diakses oleh pengguna untuk mengamankan *file* audio *video*, yakni Menu utama, ubah Password, enkripsi, dekripsi. Namun sebelum menggunakan aplikasi ini, pengguna harus login terlebih dahulu menggunakan username dan password yang valid untuk masuk ke menu utama. Adapun interface menu yang terkait dalam sistem keamanan data, antara lain :

1) Menu Login
2) Menu Utama
3) Menu Ubah Password
4) Menu Enkripsi
5) Menu Dekripsi

B. Proses Enkripsi

Proses enkripsi merupakan proses untuk mengubah file audio video asli menjadi file yang tidak dapat dijalankan. Adapun proses enkripsi yang dilakukan dalam sistem keamanan data, yakni sebagai berikut :

1) Pilih file audio video yang akan diamankan
2) Masukkan variasi kunci untuk mengamankan file audio video tersebut.
3) Kemudian proses enkripsi file audio video dapat dijalankan.

C. Proses Dekripsi

Proses dekripsi merupakan proses untuk mengubah file audio video acak menjadi file audio video asli. Adapun proses dekripsi yang dilakukan dalam sistem keamanan data, yakni sebagai berikut :

1) Pilih file audio video yang telah terenkripsi.
2) Masukkan variasi kunci yang sama ketika proses enkripsi dilakukan.
3) Kemudian proses dekripsi file audio video dapat dijalankan.

D. Pengujian Sistem Keamanan Data

Pengujian sistem keamanan data merupakan pengujian yang dilakukan untuk mengetahui keamanan data yang telah diintegrasikan pada file tertentu, dalam hal ini adalah file audio video berextensi "*.mp3, *.mp4". Pengujian dilakukan menggunakan metode black box, yang artinya pengujian pada input data di sistem keamanan, yakni yang berkaitan dengan menu login, menu enkripsi, dan menu dekripsi.

Pengujian Login: Pengujian pada menu login menggunakan data yang sah maupun tidak sah. Apabila diinputkan data yang sah untuk username dan password, maka akan muncul halaman menu utama, namun apabila data yang diinputkan tidak sah, maka akan muncul pesan bahwa username dan password yang digunakan salah.

Pengujian Enkripsi: Pengujian pada proses enkripsi menggunakan file yang akan diacak. Apabila pengguna belum sama memasukan kunci antara password dan konfirmasi password, maka akan muncul pesan bahwa "pengguna diminta untuk memeriksa passwordnya kembali".

Pengujian Dekripsi: Pengujian pada proses dekripsi menggunakan file yang sudah diacak untuk dikembalikan ke file asli. Apabila pengguna memasukkan variasi kunci yang salah, maka akan menampilkan pesan yang menyatakan error dan pengguna diminta untuk memasukan variasi kunci hingga valid.

V. PENUTUP

A. Kesimpulan

Berdasarkan hasil dari pembahasan di atas, maka dapat disimpulkan bahwa :

1. Sistem keamanan data menggunakan aplikasi kriptografi dibuat untuk mengamankan file audio video ber-ektensi "*.mp3, *.mp4" yang dibangun menggunakan bahasa pemrograman Visual Basic .Net.
2. Pengujian pada menu login menggunakan data yang sah maupun tidak sah. Apabila diinputkan

data yang sah untuk username dan password, maka akan muncul halaman menu utama, namun apabila data yang di inputkan tidak sah, maka akan muncul pesan bahwa username dan password yang digunakan salah

3. Pengujian pada proses enkripsi menggunakan file yang akan diacak. Apabila pengguna memasukkan variasi kunci yang tidak sama dengan konfirmasi password, maka akan muncul pesan bahwa "periksa kembali password yang anda masukan"
4. Pengujian pada proses dekripsi menggunakan file yang sudah diacak untuk dikembalikan ke data asli. Apabila pengguna memasukkan variasi kunci yang salah, maka pengguna akan diminta memasukan variasi kunci kembali.

B. Saran

Berdasarkan penelitian yang penulis lakukan di Madrasah Tsanawiyah Ja-alHaq, maka penulis menyarankan agar dapat menerapakan sistem keamanan file-file audio video yang ber-extensi "*.mp3, *.mp4" menggunakan aplikasi kriptografi agar file tersebut tidak disalah gunakan.

DAFTAR PUSTAKA

Irfan, 2013, *Pengantar Sistem Komputer dan Sistem Operasi*. Sekolah Tinggi Manajemen Informatika dan Komputer.

Candra, R. 2005. *Bahan Ajar Jaringan Komputer Lanjut*. Universitas Gunadarma.

Munir, Rinaldi 2005. *Kriptografi*. Sekolah Teknik Elektro dan Informatika ITB.

Mulya, M. 2008. *Bahan Ajar Kriptografi S-1*. Fakultas Ilmu Komputer Universitas Sriwijaya.

Sadikin, Rifki. 2012. *Kriptografi Untuk Keamanan Jaringan.* CV Andi Offset. Yogyakarta. 392 hal

Soleh, M.Y. 2010. *Studi Perbandingan Algoritma Kunci-Simetris Serpent dan Twofish*. Program Studi Teknik Informatika Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung.

Suharli, Suryanto. 2005. *Membangun Aplikasi Berbasis Windows dengan Visual Basic.Net*.PT.Elex Media Komputindo.

Tim Penyusun Kamus Pusat Pembinaan dan Pengembangan Bahasa, 2009, *Kamus Besar Bahasa Indonesi*a, Balai Pustaka, Jakarta.