Implementasi Kriptografi Algoritma AES Serta Algoritma Kompresi Huffman Dengan Menggunakan Pemograman PHP

Aris[1)],Sanny Sahara[2)],Nurul Aini[3)],Mety Trisna Ajija[4)],Risa Nailil Mauna[5)]
STMIK RAHARJA
Jl.Jendral Sudirman No.40 Modern Cikokol.Kota Tangerang
e-mail: aris@raharja.info,sanny@raharja.info[2],nurul.aini@raharja.info[3],mety@raharja.info[4],
Risa.nailil@raharja.info[5)]

Abstrak

Kemajuan teknologi yang sedang berkembang. Dengan akses yang mudah, fasilitas yang cukup banyak, masyarakat dapat belajar teknologi informatika. Dengan demikian memunculkan sisi positif dan negatif dari hasil pembelajaran ilmu yang dilakukan. Meninjau dari sisi negatif, kasus yang sering terjadi adalah pencurian data penting milik seseorang, perusahaan, ataupun instansi pemerintahan. Oleh karena banyaknya kasus pencurian data yang terjadi, para ahli di bidang informatika melakukan tindakan untuk mencari solusi agar data-data yang bersifat penting dapat dilindungi dengan baik. Dengan metode Kriptografi Algoritma AES adalah merupakan algoritma cryptographic yang dapat digunakan untuk mengamakan data. Algoritma AES merupakan blok chipertext simetrik yang dapat mengenkripsi (encipher) dan dekripsi (decipher) informasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut ciphertext, sebaliknya dekripsi adalah merubah ciphertext data menjadi bentuk semula yang kita kenal sebagai plaintext serta dan menggunakan Algoritma Kompresi Huffman yaitu merupakan algoritma yang paling terkenal untuk mengompres teks .Dengan menggunakan Pemrograman PHP maka dapat di buat sebuah Aplikasi untuk mengamankan data.

***Kata kunci** : Aplikasi, Kriptografi, Keamanan, Algoritma.*

1. Pendahuluan

Perkembangan teknologi informatika yang sangat cepat dan pesat, membawa perubahan besar disegala bidang. Salah satu diantaranya adalah perekonomian. Perkembangan teknologi membangkitkan bidang usaha dengan sangat cepat, setiap kegiatan usaha dapat di topang dengan adanya teknologi yang maju. Perkembangan teknologi menjadikan ketatnya persaingan di dunia usaha.

Dengan memanfaatkan teknologi setiap pelaku usaha dapat dengan mudah berkomunikasi, bertukar data-data penting dalam usaha tidak perlu lagi harus bertatap muka bertemu langsung. Karena dengan memanfaatkan teknologi semua bisa dilakukan dari jarak yang jauh sekalipun. Teknologi memberikan profit yang besar dalam membantu kegiatan usaha mencapai kesuksesan dengan sangat cepat.Tapi selain memberikan keuntungan, teknologi juga memberikan dampak kerugian yang cukup besar. Dengan melakukan pertukaran data-data penting dalam kegiatan usaha, resiko data yang dimiliki untuk dicuri oleh pihak luar masih sangat besar. Karena hal tersebut maka sangat dibutuhkan sebuah cara untuk mengamankan data-data yang dikirimkan melalui sistem komputer.

Untuk mengamankan data-data yang penting dapat dilakukan dengan cara enkripsi (*encryption*) atau sering disebut dengan Kriptografi. Tujuan dari enkripsi/ kriptografi adalah membuat data-data penting sulit untuk dibaca sekalipun data tersebut berhasil dicuri pihak yang tidak bertanggung jawab. Dalam kriptografi terdiri dari dua hal, enkripsi (*encryption*) yaitu proses merubah data asli (*plain text*) menjadi data samaran (*chiper text*) dan dekripsi (*decryption*) yaitu proses pengembalian *chiper text* menjadi *plain text* kembali.

2. Metode Penelitian

Metode Penelitian memberikan penjelasan tentang langkah-langkah, data, lokasi penelitian, metode evaluasi yang digunakan serta penjelasan terstruktur tentang algoritma atau metode dari penelitian yang dibahas.

2.1 Pengumpulan Data

1. Metode Penelitian (*Observasi*)

   Dengan metode *observasi* penulis mendapatkan data dengan cara mendatangi langsung objek yang dijadikan tempat riset.

2. Metode Wawancara (Interview)

   Interview yang berupa tanya jawab penulis lakukan kepada beberapa staff yang terkait langsung dengan instansi, *interview* dilakukan kepada staff bagian keuangan.

3. Metode Study Pustaka (*Library Search*)

   Metode ini dilakukan guna mendapatkan gambaran secara teoritis yang berkaitan dengan penulisan laporan penelitian sebagai acuan. Penulis mengumpulkan data yang bersumber dari materi yang didapat semasa kuliah, seperti modul pemrograman PHP, berbagai buku panduan dalam mengerjakan laporan penelitian, contoh laporan-laporan terdahulu yang dibuat oleh para mahasiswa yang sudah melakukan penelitian.

2.2 Analisa Data

Analisa data dengan cara mempelajari dan mengevaluasi data serta formulir yang telah diperoleh dari perusahaan.

2.3 Perancangan

Flowchart merupakan sebuah metode penggambaran alur dari logika yang kita terapkan pada sebuah algoritma. Dengan metode flowchart, memudahkan untuk memberikan pejelasan cara kerja program yang dibuat kepada user, sehingga mudah dimengerti.

2.4 Testing

Black – Box testing merupakan pengujian yang berfokus pada spesifikasi fungsional dari perangkat lunak, tester dapat mendefinisikan kumpulan kondisi input dan melakukan pengetesan pada spesifikasi fungsional program.

3. Hasil dan Pembahasan

3.1 Spesifikasi Sistem

Spesifikasi sistem aplikasi enkripsi meliputi input, proses, dan output yang direncanakan.

1. Input

   Input data file yang dapat diproses adalah file dengan format docx, xlsx, dan pdf. Format file memiliki karakter yang mendukung ASCII. Pemilihan tiga jenis data file tersebut disesuaikan dengan kebutuhan user dan juga sistem operasi yang digunakan pada saat ini. Ketiga file yang dipilih dapat dipastikan bisa diproses dengan algoritma AES, sehingga data yang dipilih tidak mengganggu kinerja user.

2. Proses

   Dalam sistem aplikasi enkripsi file masukan tidak lebih dari lima mega bytes (5 MB) hal tersebut dilakukan untuk menjaga kinerja dari kecepatan proses enkripsi sebuah data file. Setelah file masukan dipilih, kemudian user menginput kata kunci yang digunakan untuk melindungi data. Proses akan berlanjut pada proses enkripsi yang kemudian menghasilkan data dalam bentuk chipertext. Langkah-langkah proses yang direncanakan :

   a. Proses enkripsi yang meliputi tahapan sebagai berikut :
      1) Menginputkan data file
      2) Membuat kata kunci
      3) Proses enkripsi dan kompresi
      4) Menyimpan hasil enkripsi
   b. Proses dekripsi yang meliputi tahapan sebagai berikut :
      1) Masukkan kata kunci yang sama dengan proses enkripsi
      2) Proses dekripsi dan dekompresi
      3) Menyimpan hasil dekripsi

3. Output

   Terdapat dua jenis output pada saat menggunakan aplikasi enkripsi yang digunakan, yaitu output pada proses enkripsi dan output pada proses dekripsi. File output pada proses enkripsi tidak akan dapat dibaca, sedangkan file output proses dekripsi hasilnya harus sama dengan data file sebelum digunakan pada aplikasi.

3.2 Parameter Kesuksesan

Sistem aplikasi enkripsi dapat dikatakan berhasil jika sistem memiliki parameter dibawah ini :

1. Memiliki kata kunci
2. Data file sesuai dengan batasan yang dipilih
3. Dapat melakukan proses encode
4. Dapat melakuka proses decode
5. Hasil akhir dari proses tidak berubah dengan data asli

3.3 Flowchart

Flowchart merupakan gambar atau bagan yang memperlihatkan urutan dan hubungan antar proses beserta instruksinya. Gambaran ini dinyatakan dengan simbol. Simbol-simbol dalam flowchart menggambarkan proses tertentu, sedangkan hubungan antar proses digambarkan dengan garis penghubung.

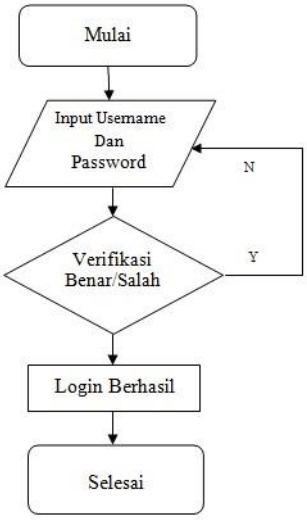
3.4 Rancangan Aplikasi Enkripsi

Aplikasi enkripsi yang akan dibuat, dirancang untuk bisa di akses pada web browser dengan spesifikasi kemampuan komputer minimal berjalan pada sistem 32bit. Dengan penyesuaian, aplikasi dirancang untuk berjalan pada sistem operasi berbasis windows minimum sistem 32bit. Untuk pembuatan aplikasi digunakan bahasa pemrograman berbasis web yaitu PHP dikordinasikan dengan sistem database MySql dan dengan tools bantuan notepad++. Aplikasi enkripsi akan dibuat dengan dua buah fungsi yaitu :

a. Fungsi Enkripsi
b. Fungsi Dekripsi

3.5 Rancangan Login Pada Aplikasi

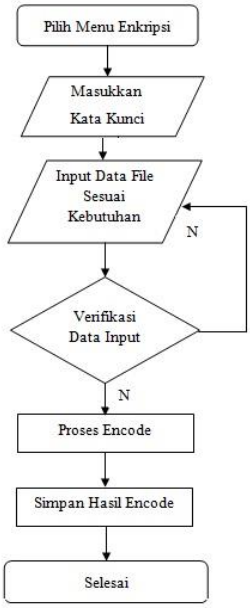
Pada gambar 1. menggambarkan flowchart pada proses menu login aplikasi. Setelah proses login berhasil maka berikutnya aplikasi akan berpindah kepada pilihan menu proses enkripsi atau dekripsi.



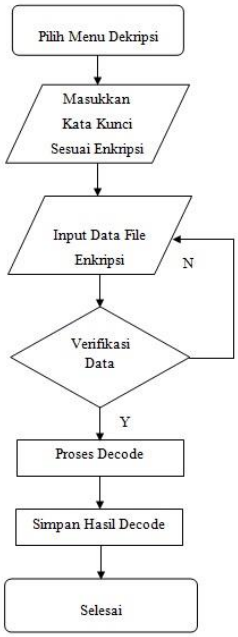
Gambar 1. *Proses Login Aplikasi*

3.6 Rancangan Proses Pada Aplikasi

Pada tahap ini proses dalam aplikasi dibuat sesuai dengan fungsi dari algoritma enkripsi dan dekripsi yang digunakan. Jika langkah-langkah dalam proses enkrip dan dekrip berlawanan dengan fungsi algoritma yang digunakan, maka proses yang di inginkan tidak akan berjalan. Langkah yang harus dilakukan dalam proses enkrip dan dekrip digambarkan dalam flowchart berikut :



Gambar 2. *Proses Enkripsi Data*



Gambar 3. Proses Dekripsi Data

3.7 Interface dan Proses Aplikasi

Sub bab ini meliputi pembahasan tampilan layar user interface, dan proses aplikasi pada setiap interface aplikasi.

1. Layar Utama

   Pada gambar 4. menampilkan menu utama pada layar utama yang terdiri dari pilihan menu home dan login.

Gambar 4. *Tampilan Layar Utama*

2. Menu Login

   Pada gambar 5. menampilkan tampilan menu login aplikasi enkripsi.

Gambar 5. *Tampilan Menu Login*

3. Menu Aplikasi

   Pada gambar 6. menampilkan tampilan menu bar pada aplikasi enkripsi, yang terdiri dari : Home, Encrypt, Decrypt, Help, dan Log Out.

Gambar 6. *Tampilan Menu Utama Aplikasi*

4.Menu Enkripsi

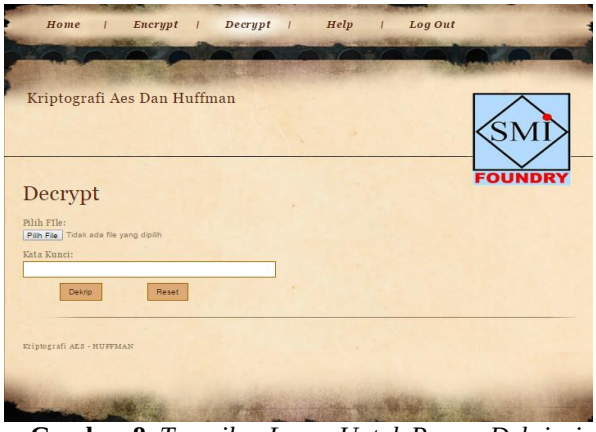
Pada gambar 7. menampilkan tampilan untuk memulai proses enkripsi data.

Gambar 7. *Tampilan Layar Untuk Proses Enkripsi*

Untuk memulai proses enkripsi user terlebih dahulu memilih file yang akan di proses, dengan cara klik tombol pilih file, kemudian pilih file dengan tipe docx, xlsx, atau pdf. Setelah file dipilih, input kata kunci pada kolom yang disediakan dengan digit minimun adalah enam digit yang merupakan gabungan angka dan huruf atau hanya dengan masing-masing jenis, kata kunci tersebut yang akan menjadi master key dalam melakukan proses dekripsi. Setelah proses dilakukan kemudian klik tombol enkrip,maka aplikasi mulai menjalankan proses enkripsi.

5. Menu Deskripsi

Pada gambar 8. menampilkan tampilan untuk mendekripsi data yang sudah di enkripsi pada menu enkripsi.



Gambar 8. *Tampilan Layar Untuk Proses Dekripsi*

Untuk melakukan proses dekripsi, user terlebih dahulu memilih file yang sudah di enkripsi pada proses enkripsi. Klik tombol pilih file, kemudian cari data yang sudah di enkrip dengan keterangan "Enkrip_(4 digit angka)_namafile". Selanjutnya masukkan kata kunci, kata kunci yang digunakan untuk dekripsi harus sama dengan kata kunci yang digunakan untuk proses enkripsi. Setelah tata cara dekripsi dilaksanakan, klik tombol dekrip pada layar kemudian aplikasi akan melakukan proses dekripsi data. Hasil proses dekripsi akan ditampilkan seperti gambar 9. Berikut:

Gambar 9. *Tampilan Hasil Proses Dekripsi*

Setelah proses selesai, tindakan yang sama dilakukan seperti pada proses enkripsi yaitu klik tombol download dan data dapat di ambil pada folder download sistem komputer yang digunakan.

3.8 Pengujian Aplikasi

Dalam penelitian ini dilakukan pengujian aplikasi antara lain :

a. Membandingkan data file sebelum di proses dan sesudah diproses pada aplikasi.
b. Mencoba membuka data yang sudah dienkripsi, untuk melihat hasil dari proses enkripsi lalu membandingkannya dengan data asli yang belum di enkripsi.
c. Mencoba memproses semua jenis data untuk membuktikan batasan dari aplikasi yang dibuat.

4. Simpulan

Berikut kesimpulan perihal rumusan masalah mengenai Implementasi Kriptografi Algoritma AES Serta Algoritma Kompresi Huffman dengan Pemrograman PHP.

1. Input dan output dari algoritma *AES* terdiri dari urutan data sebesar 128 bit. Urutan data yang sudah terbentuk dalam satu kelompok 128 bit tersebut disebut juga sebagai blok data atau *plaintext* yang nantinya akan dienkripsi menjadi chiphertext. Chiper *key* dari *AES* terdiri dari *key* dengan panjang 128 bit, 192 bit, atau 256 bit. Perbedaan panjang kunci akan mempengaruhi jumlah round yang akan iimplementasikan pada algoritma *AES.* Proses enkripsi pada algoritma AES terdiri dari 4 jenis transformasi *byte*s, yaitu *SubBytes*, *ShiftRows*, *Mixcolumns*, dan *AddRoundKey*. Pada awal proses enkripsi, input yang telah dikopikan ke dalam state akan mengalami transformasi *byte AddRoundKey*.
2. Algoritma AES dapat diterapkan dengan membangun sebuah sistem olah data sederhana berbasis web yang dapat berjalan pada web browser umum digunakan dengan bantuan tools tambahan berupa aplikasi Xampp dan MySql.
3. Algoritma Aes dapat digunakan untuk semua jenis data komputerisasi, pengembangan dan implementasi disesuaikan dengan tingkat kebutuhan masing – masing user client.
4. Sistem yang dibutuhkan untuk menunjang proses enkripsi diantaranya:
   a. Sistem operasi windows
   b. Aplikasi Xampp
   c. Aplikasi MySql
   d. Tools Notepad ++
   e. Web browser goggle chrome, mozila firefox

Daftar Pustaka

[1] Heri Haryanto. Implementasi Kombinasi Algoritma Enkripsi Aes 128 Dan Algoritma Kompresi Shannon-Fano.Jurnal ilmiah Setrum.Untirta.2014;vol(3):1 .
[2] Soni Harza Putra,dkk. Implementasi Algoritma Kriptografi Advanced Endryption Standart (AES) pada Kompresi Data Teks. Repositori Jurnal Mahasiswa PTIIK UB.2013;vol(1):1 .
[3] Heru Cahya Rustamaji,dkk.Aplikasi kompresi data menggunakan Metode Huffman Statik Pada Perangkat Mobile Berbasis Android. TELEMATIKA.2014.vol(11).9-18.
[4] Edmund Ophie.Optimasi Enkripsi Teks Menggunakan AES dengan Algoritma Kompresi Huffman.Informatika.2014;vol(14): 2.
[5] M.Leo Agung,. "*Kupas Tuntas Adobe Dreamweaver CS 5 Dengan Pemrograman PHP Dan MySQL*", Penerbit Andi Dan Madcoms. 2013 .
[6] Zainal Arifin & Smitdev Community. "*Pemanfaatan (implementasi) algoritma kriptografi Advanced Encryption Standard (AES) 128 bit"*,Andi,Yogyakarta.2012
[7] Andre. Belajar cepat Pemograman PHP. Bandung: Andi. 2013