PATJou
patria artha technological journal

Department of Electrical Engineering,
Faculty of Engineering and Informatics
Patria Artha University, South Sulawesi, Indonesia
ISSN: 2549-6131| e-ISSN: 2549-614X

Sistem Informasi Encrypt Dan Decrypt Dengan Algoritma AES Menggunakan Framework Laravel

Tamus Bin Tahir[1], Moch Apriyadi HS[2], Muh. Rais[3], Irwan Syarif[4]

[1,3,4]Fakultas Teknik Dan Informatika, Universitas Patria Artha
[2] Prodi Teknik Elektro, Fakultas Teknik, Universitas Khairun
tamusbintahir@gmail.com,
apriyadisirat@unkhair.ac.id,
muh.raisazisnawawi@gmail.com
firaysnawri88@gmail.com

Abstrak

Perkembangan teknologi informasi yang sangat pesat turut memajukan media komunikasi sebagai media penyampaian informasi dari satu tempat ke tempat lain, sehingga memudahkan orang dalam mengakses media komunikasi, Kemudahan pengaksesan media komunikasi oleh semua orang, membuat informasi menjadi aspek sangat rentan untuk diketahui, diambil dan dimanipulasi oleh pihak - pihak yang tidak bertanggung jawab. Dengan mengamankan data menggunakan kriptografi, diperlukan proses enkripsi dan proses dekripsi. Ada banyak algoritma dalam kriptografi, algoritma AES dipilih karena memiliki kemungkinan kunci yang sangat banyak yaitu 2^{128}. Framemork Laravel dipilih untuk membangun aplikasi ini dikarenakan Laravel memiliki library yang banyak sehingga dapat mempercepat proses pembuatan sebuah aplikasi. Sistem ini dibangun untuk melakukan encrypt dan decrypt teks maupun file. Dari hasil pengujian, sistem dapat melakukan encrypt dengan baik. Dan ketika datanya di decyprt kembali tidak mengalami perubahan informasi.

Kata kunci: Encrypt Dan Decrypt, AES, laravel

PENDAHULUAN

Kemajuan dan perkembangan teknologi informasi dewasa ini telah berpengaruh pada seluruh aspek kehidupan manusia, termasuk bidang komunikasi. Pada saat yang sama keuntungan ini juga digunakan untuk melakukan tindakan ilegal misal peretasan informasi. Mengingat betapa bahayanya dampak yang diberikan, sehingga perlu diterapkan prosedur keamanan pada informasi.

Informasi-informasi rahasia perlu disimpan atau disampaikan melalui suatu cara tertentu agar tidak diketahui oleh pihak lain yang tidak dikehendaki. Sehingga keamanan perlu ditingkatkan dengan membangun aplikasi yang mampu melindungi data. Salah satu teknik pengamanan yang bias dipelajari dan dikembangkan adalah kriptografi

Dengan mengamankan data menggunakan kriptografi, diperlukan proses enkripsi dan proses dekripsi. Terdapat banyak algoritma enkripsi yang dapat digunakan untuk mengenkripsi suatu data. Salah satunya adalah algoritma Advanced Encryption Standard (AES).

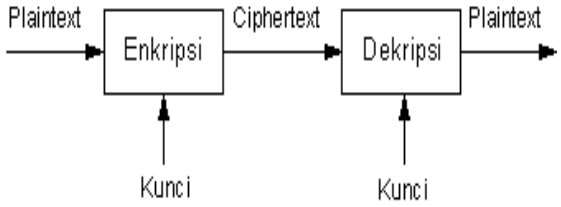
KAJIAN LITERATUR

Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. atau bisa didefinisikan juga Enkripsi merupakan proses untuk mengubah plainteks menjadi chiperteks. Planteks sendiri adalah data atau pesan asli yang ingin dikirim, sedangkan Chiperteks adalah data hasil enkripsi. Enkripsi dapat diartikan sebagai kode atau chiper.

Sebuah chiper mengunakan suatu algoritma yang dapat mengkodekan semua aliran data (stream) bit dari sebuah pesan menjadi cryptogram yang tidak dimengerti (unintelligible). Karena teknik chiper merupakan suatu system yang telah siap untuk di automasi, maka teknik ini digunakan dalam system keamanan computer dan jaringan. Enkripsi dimaksudkan untuk melindungi informasi agar tidak terlihat oleh orang atau pihak yang tidak berhak. Informasi ini dapat berupa nomor kartu kredit, catatan penting dalam komputer, maupun password untuk mengakses sesuatu.

Deskripsi dalam dunia keamanan komputer merupakan proses untuk mengubah chiperteks menjadi plainteks atau pesan asli. Jadi Deskripsi merupakan kebalikan dari Enkripsi upaya pengolahan data menjadi sesuatu yang dapat diutarakan secara jelas dan tepat dengan tujuan agar dapat dimengerti oleh orang yang tidak langsung mengalaminya sendiri.

Proses enkripsi dan dekripsi diatur oleh satu atau beberapa kunci kriptografi. Proses enkripsi dan deskripsi dapat di gambarkan sebagai berikut:



Gambar 1. Blok diagram enkripsi dan dekripsi

Secara matematis, prosesnya dapat dituliskan sebagaiberikut:

Enkripsi : $E(M) = C$

Deskripsi : $D(C) = M$

dimana: *M* adalah *plaintext* (*message*) dan *C* adalah *ciphertext*.

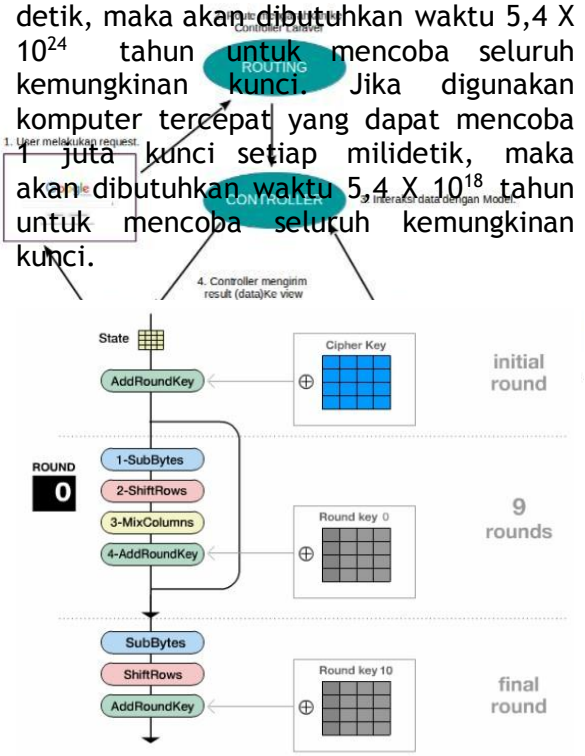
Advanced Encryption Standard (AES) adalah lanjutan dari algoritma enkripsi standar DES (Data Encryption Standard) yang masa berlakunya dianggap telah usai karena faktor keamanan.

AES dibangun dengan maksud untuk mengamankan pemerintahan diberbagi bidang. Algoritma AES di design menggunkan blok chiper minimal dari blok 128 bit input dan mendukung

ukuran 3 kunci (3-key-sizes), yaitu kunci 128 bit, 192 bit, dan 256 bit.

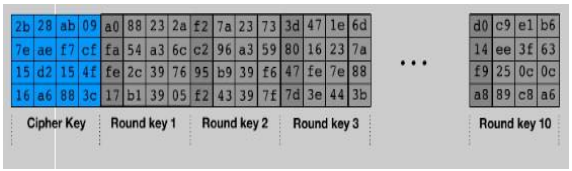
Dalam kriptografi, Advanced Encryption Standard (AES) merupakan standar enkripsi dengan kunci-simetris yang diadopsi oleh pemerintah Amerika Serikat. Standar ini terdiri atas 3 blok cipher, yaitu AES-128, AES-192 dan AES-256, yang diadopsi dari koleksi yang lebih besar yang awalnya diterbitkan sebagai Rijndael. Masing-masing cipher memiliki ukuran 128-bit, dengan ukuran kunci masing-masing 128, 192, dan 256 bit Karena AES mempunyai panjang kunci paling sedikit 128 bit, maka AES tahan terhadap serangan exhaustive key search dengan teknologi saat ini. Dengan panjang kunci 128- bit, maka terdapat sebanyak 2^{128} = 3,4 X 10^{38} kemungkinan kunci.

Jika digunakan komputer tercepat yang dapat mencoba 1 juta kunci setiap detik, maka akan dibutuhkan waktu 5,4 X 10^{24} tahun untuk mencoba seluruh kemungkinan kunci. Jika digunakan komputer tercepat yang dapat mencoba 1 juta kunci setiap milidetik, maka akan dibutuhkan waktu 5,4 X 10^{18} tahun untuk mencoba seluruh kemungkinan kunci.



Gambar 2. Diagram proses enkripsi Algoritma AES

Algoritma AES mengambil cipher key, K, yang diberikan oleh pengguna, dan memanggil fungsi KeyExpansion() untuk membangkitkan sejumlah round key (banyaknya round key bergantung pada jumlah putaran).



Gambar 3. Round key pada AES

Laravel adalah sebuah framework web berbasis PHP yang open-source dan tidak berbayar, diciptakan oleh Taylor Otwell dan diperuntukkan untuk pengembangan aplikasi web yang menggunakan pola MVC. Struktrur pola MVC pada laravel sedikit berbeda pada struktur pola MVC pada umumnya.

Di Laravel terdapat routing yangmenjembatani antara request dari user dan controller. Jadi controller tidak langsung menerima request tersebut. Berikut adalah ilustrasi dari konsep MVC pada laravel yang ditunjukkan pada Gambar 4.

Gambar 4. Konsep MVC Pada Laravel

Ada 5 konsep arsitektur pada framework laravel yang mempunyai masing-masing fungsi diantaranya:

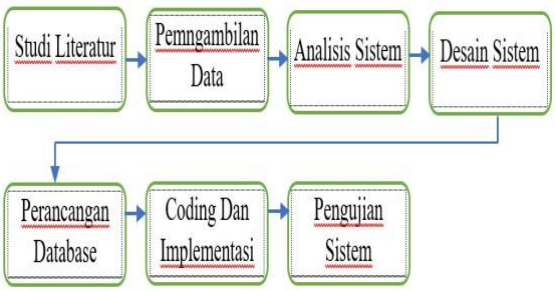
a. Routes, berfungsi sebagai pemberiakses pada setiap request sesuai alur yang telah di tentukan.
b. Controller, adalah bagian yang menjadi penghubung antara model dan view. Controller memiliki perintah-perintah yang berfungsi untuk memproses bagaimana data ditampilkan dari Model ke View atau sebaliknya.
c. Model, merupakan sekumpulan data yang memiliki fungsi-fungsi

untuk mengelola suatu table pada sebuah database. Struktur pemodelan data pada laravel yakni memiliki fungsi yang terdiri dari table, primaryKey dan fillable. Dimana ketiga fungsi tersebut harus di protected.

d. View, merupakan file yang berisi kodehtml (HyperText Markup Language) yang berfungsi untuk menampilkan suatu data ke dalam browser. Format view pada laravel harus menggunakan istilah blade, contohnya seperti: view.blade.php.
e. Migrations, merupakan proses perancangan suatu table, dalam hal ini migrations berfungsi sebagai blueprint database atau dapat diistilahkan sebagai penyedia sistem kontrol untuk skema database.

METODE PENELITIAN

Jenis penelitian ini adalah eksperimental yaitu dengan melakukan perancangan, pembuatan dan pengujian model sistem. Penelitian ini akan melalui 7 tahapan dan akan memeriksa tahapan sebelum dan sesudahnya. Adapun tahapan tersebut adalah sebagai berikut

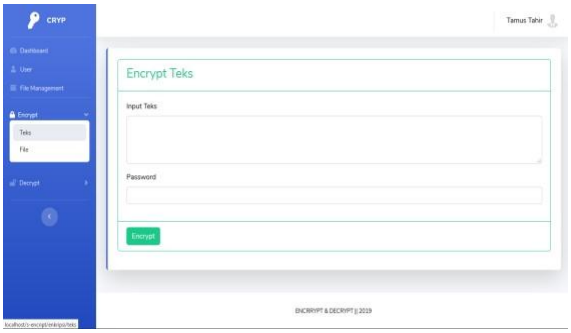


Gambar 5. Tahapan Penelitian

HASIL DAN PEMBAHASAN

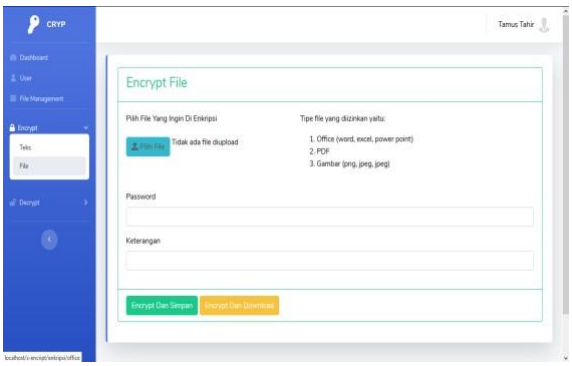
1. Implementasi Sistem

Implementasi sistem informasi encrypt dan decrypt terdiri dari beberapa form yang setiap form memiliki fungsi tersendiri. Form- form tersebut sebagai berikut:



Gambar 6. Form encrypt teks

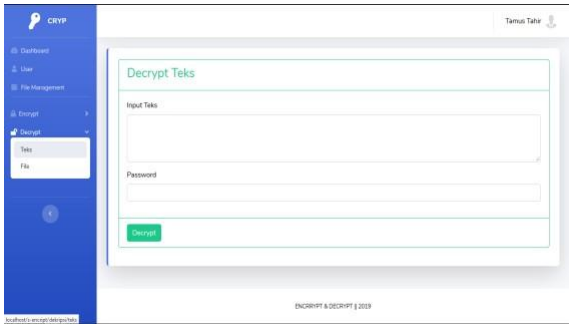
Gambar 6, mrupakan form encrypt teks diaman user dapat menginput teks kemudian input password dan memilih tombol encrypt. Selanjutnya sistem akan melakukan encrypt dan untuk melakukan decrypt user dapat melakukanx pada form decrypt.



Gambar 7. Form encrypt file

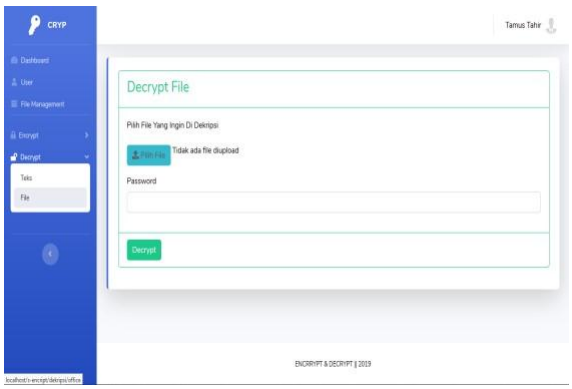
Gambar 7, merupakan form encrypt file. Tipe file yang dapat di encrypt yaitu office

(word, excel, ppt), pdf dan gambar. Untuk melakukan encrypt file user harus mengupload type file yang diizinkan kemudian input password dan input keterangan file. Disini terdapat 2 buah tombol yaitu tombol untuk mengencrypt dan simpan yang akan menyimpan file pada file management. Kemudian tombol kedua yaitu encrypt dan download dimana file tersebut tdk akan tersimpan.



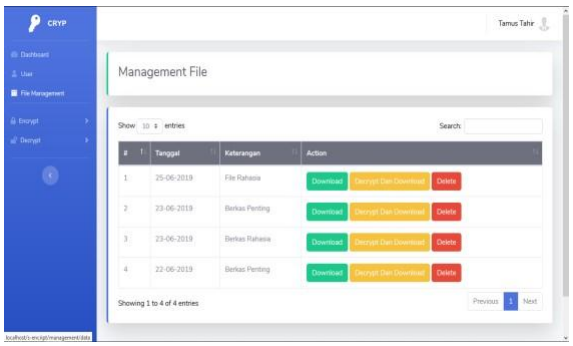
Gambar 8. Form decrypt teks

Gambar 8, merupakan form decrypt teks diaman user dapat melakukan decrypt teks yang telah di encrypt. Untuk melakukanx diperlukan password yang sama ketika melakukan encrypt sebelumnya.



Gambar 9. Form decrypt file

Pada form ini digunakan untuk decrypt file yang telah di encrypt dan juga di butuhkan password yang sama ketika melakukan decrypt. Setelah berhasil di decrypt, file hasil decrypt langsung otomatis terdownload.



Gambar 10. Manajemen File

Manajemen file merupakan tabel yang menampilkan file-file hasil dari encrypt pada sistem ini. Disini user dapat melakukan download file yang telah terencrypt atau langsung melakukan decrypt dengan memasukan password sebelum mendownload file tersebut.

2. Pengujian Sistem

Metode pengujian yang digunakan yaitu pengujian black box. Pengujian black box berfokus pada penyerahan fungsional perangkat lunak dengan demikian pengujian black box memungkinkan perekayasa perangkat lunak mendapatkan serangkaian kondisi input yang sepenuhnya menggunakan semua persyaratan fungsional untuk satu program.

Pengujian Black Box berusaha menemukan kesalahan dalam ketegori sebagai berikut :

a. Fungsi-fungsi yang tidak benar atauhilang.
b. Kesalahan Interface.
c. Kesalahan dalam struktur data atau akses database ekternal.
d. Kesalahan lahan kinerja.
e. Inisialisasi dan kesalahan terminasi.

Pengujian Black Box adalah pengujian aspek fundamental sistem tanpa memperhatikan struktur logika internal perangka lunak. Metode ini digunakan untuk mengetahui apakah perangkat lunak berfungsi dengan benar. Pengujian Black Box merupakan metode perancangan data uji yang didasarkan pada spesifikasi perangkat lunak. Data uji dibangkitkan, dieksekusi pada perangkat lunak dan kemudian keluaran dari perangkat lunak dicek apakah telah sesuai dengan yang diharapkan

Tabel 1. Pengujian Black Box

No	Menu	Keterangan
1	Menu Login	berfungsi
2	Menu Dashboard	berfungsi
3	Menu User	berfungsi
4	Menu Encrypt Teks	berfungsi
5	Menu Encrypt File	berfungsi
6	Menu Decrypt Teks	berfungsi
7	Menu Decrypt File	berfungsi
8	Menu File Management	berfungsi

Penelitian ini bertujuan untuk membangun sistem enkripsi dan dekripsi teks maupun file dengan algoritma

Advanced Encryption Standard (AES) yang dibangun dengan menggunakan framework Laravel.

Dengan adanya sistem ini keamanan data dapat lebih terjamin karena sudah terenkripsi. Sehingga jika data tersebut di akses oleh orang-orang yang tidak berkepentingan, informasi pada data tidak dapat diketahui. Karena untuk mengetahuinya harus melakukan decrypt kembali yang tentunya dilengkapi dengan password. Sistem ini juga mempunyai management file, sehingga bisa di manfaatkan untuk menyimpan file-file penting yang tentunya sudah terenkripsi.
Aplikasi ini dibangun dengan menggunakan framework Laravel. Penggunaan laravel sangat membantu peneliti dalam membuat aplikasi karena Laravel mempunyai *library* Object Oriented yang sangat banyak.

KESIMPULAN

Berdasarkan hasil uji coba yang dilakukan, sistem ini berhasil mengimplementasikan proses enkripsi dan dekripsi untuk mengamankan file. Hal ini dibuktikan melalui penujian yang telah dilakukan bahwa teks dan file dapat di enkripsi kemudian dapat di dekripsi kembali. Penggunaan framework laravel sangat membantu programmer dalam membangun sebuah aplikasi. Hal ini tentunya karena karena syntax laravel yang bersih dan fungsional serta library yang banyak dan mudah digunakan sehingga dapat mempercepat pembangunan modul. Hasil pengujian yang dilakukan dengan menggunakan metode Black-Box testing didapati bahwa fungsi yang dibuat pada modul dapat berfungsi dengan baik.

REFERENSI

[1] Gede Handika, I & Ayi Purbasari. 2018.Pemanfaatan Framework Laravel Dalam Pembangunan Aplikasi E-Travel Berbasis Website. Konferensi Nasional Sistem Informasi, STMIK Atma Luhur Pangkalpinang.

[2] Luthfi, Farizan. 2017. Penggunaan Framework Laravel Dalam Rancang Bangun Modul Back-End Artikel Website Bisnisbisnis.ID. JISKa, Vol. 2, No. 1

[3] Hidayat, Akik & Tuty Alawiyah. 2013.Enkripsi dan Dekripsi Teks menggunakan Algoritma Hill Cipher dengan Kunci Matriks Persegi Panjang. Jurnal Matematika Integratif Volume 9 No 1.

[4] Aditya Permana, Angga & Desi Nurnaningsih. 2018. Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (AES). Jurnal Teknik Informatika Vol. 11 No. 2.

[5] Nandar Pabokory, Fresly, dkk. 2015.Implementasi Kriptografi PengamananData Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. Jurnal Informatika Mulawarman Vol. 10 No. 1.