Analisa Dan Perancangan Sistem Informasi Pengaman Dokumen Dengan Metode Algoritma *XOR* dan *AES* Berbasis Web (Studi Kasus : Bimbingan Belajar Matriks Pamulang)

Mochammad Bagoes Satria J[1], Hendri Ardiansyah[2], and Miftahudin[3]

[1]Jurusan Teknik Informatika, Fakultas Teknik, Universitas Pamulang, Jalan Surya Kencana No.1, Pamulang – Tangerang Selatan, 15417, Indonesia
e-mail: [1]bagoes.satria16@gmail.com

[2, 3]Jurusan Teknik Informatika, Fakultas Teknik, Universitas Pamulang, Jalan Surya Kencana No.1, Pamulang – Tangerang Selatan, 15417, Indonesia
e-mail: [2]hendri.pirlo@gmail.com, [3]miftah1427@gmail.com

Abstract

Critography is very closely related to aspects of information security and confidentiality. A common problem in a profit or non-profit institution is data security. Some data that should be confidential and not intended for the public must be kept confidential from those who are not responsible. Bimbingan Belajar Matriks is one of the profit institutions that has a lot of confidential data that is not intended for the public such as financial data, student data, book data, etc. Frequent data leakage both when the data is stored in the branch computer or when doing daily and monthly reports that are carried out between branches and branches and the head office that have a loss impact. AES Algorithm and XOR Algorithm were chosen as the method used in this cryptography because both methods are easy to implement and powerful in doing encryption. The results of this study are expected to produce a web-based document security information system that can solve problems that occur in maintaining the confidentiality of data, both before being sent and after arriving to the destination so that the confidentiality and information security aspects of it are maintained.

Keywords: Cryptography, Data Security, XOR, AES.

Abstrak

Kritografi sangat erat kaitannya dengan aspek keamanan dan kerahasiaan informasi. Masalah yang biasa terjadi dalam sebuah lembaga profit ataupun non-profit adalah keamanan data. Beberapa data yang harusnya bersifat rahasia dan tidak diperuntukan untuk umum harus dijaga kerahasiaannya dari orang yang tidak bertanggung jawab. Bimbingan belajar Matriks adalah salah satu lembaga profit yang mempunyai banyak data rahasia yang tidak diperuntukan untuk umum seperti, data keuangan, data siswa, data buku dll. Sering terjadinya kebocoran data baik ketika data disimpan didalam komputer cabang maupun ketika melakukan laporan harian dan bulanan yang dilakukan antar cabang maupun cabang dan kantor pusat yang berdampak kerugian. Algoritma *AES* dan Algoritma *XOR* dipilih sebagai metode yang digunakan dalam kriptografi ini karena kedua metode tersebut mudah diimplementasikan dan kuat dalam melakukan enkripsi. Hasil dari penelitian ini diharapkan dapat menghasilkan sebuah sistem informasi berbasis web pengamanan dokumen yang dapat menyelesaikan masalah yang terjadi dalam menjaga kerahasiaan data, baik sebelum dikirim maupun setelah sampai ke tujuan agar aspek kerahasiaan dan keamanan informasi didalammya terjaga.

Kata Kunci : Kriptografi, Keamanan Data, XOR, AES.

1. PENDAHULUAN

Seiring dengan perkembangannya teknologi dan komunikasi yang begitu pesat, akan memudahkan kita untuk melakukan pertukaran data dengan orang lain secara cepat. Baik yang terhubung dengan jaringan internet maupun yang tidak. Namun terkadang keamanan pertukaran data tersebut kurang disadari oleh pemilik data karena kurangnya penjagaan aspek keamanan dalam hal pertukaran data tersebut memiliki

resiko yang sangat tinggi dalam perkembangan teknologi yaitu adanya pencurian data. Pencurian data merupakan salah satu masalah besar yang paling ditakuti oleh pengguna jaringan komunikasi. Karena apabila data atau informasi yang sensitif atau berharga tersebut yang ada didalam sebuah dokumen atau file jatuh ke tangan orang yang bukan semestinya mengetahui isi file tersebut atau ke tangan orang yang tidak bertanggung jawab maka dapat berakibat fatal. Dengan terjadinya pencurian data ini maka penjagaan aspek keamanan dalam pertukaran informasi serta penyimpanan data dianggap sesuatu hal yang penting. Salah satu usaha dalam mengamankan data atau informasi yang terdapat dalam dokumen atau file tersebut dapat menggunakan kriptografi.[1]

Bimbingan belajar adalah bimbingan yang ditunjukkan kepada siswa untuk mendapat pendidikan yang sesuai dengan kebutuhan, bakat, minat, kemampuannya dan membantu siswa untuk menentukan cara-cara yang efektif dan efisien dalam mengatasi masalah belajar yang dialami oleh siswa [2]

Setiap tahunnya Bimbingan Belajar Matriks mengelola 300 sampai 600 siswa mulai dari tingkat sekolah dasar, sekolah menengah pertama dan sekolah menengah atas yang membutuhkan tambahan intensif untuk memperoleh tambahan belajar. Dari jumlah siswa yang banyak tersebut tentu banyak data dan informasi penting yang harus dikelola oleh Bimbingan Belajar Matriks seperti data siswa, data pembayaran siswa, data soal atau buku, dan data pelaporan pemasukkan dan pengeluaran antara cabang yang ditempatkan di komputer masing-masing cabang dan di komputer kantor pusat. setiap harinya data-data ini selalu dipergunakan dengan intensif yang dikelola oleh admin cabang dan admin pusat. data yang ada disetiap cabang dikirimkan melalui surat elektronok (email) setiap harinya untuk dilakukan pencatatan juga dikantor pusat. Karena aktifitas dari dokumen atau file yang begitu pada setiap harinya akan lebih aman jika data yang ada baik dikantor cabang maupun pusat dijaga kerahasiaan dan keamanannya karena dalam praktik kesehariannya sangat banyak pengguna dari komputer yang ditempatkan dikantor cabang yang mana hal ini bisa saja menimbulkan masalah apabila ada pihak yang tidak bertanggung jawab ingin mencuri atau merusak data tersebut. Belum lagi dalam pengiriman dokumen atau file yang melewati jaringan internet melalui surat elektronik sehingga keamanan data harus sangat diperhatikan.

Kriptografi adalah seni komunikasi yang telah digunakan sejak ribuan tahun yang lalu untuk menyediakan komunikasi yang bersifat rahasia bagi orang - orang yang saling percaya. prosesnya adalah dengan merubah pesan asli yang biasa disebut *plaintext* dengan kunci tertentu sehingga seseorang yang tidak memiliki kunci tidak akan dapat membukanya. Proses ini biasa disebut dengan *cryptosystem* yang membahas bagaimana sebuah informasi yang ada di enkripsi dan di deskripsi kembali. Pada penelitian ini, kriptografi yang digunakan adalah algoritma XOR dan Algoritma *Advanced Encryption Standard (AES)*. Algoritma XOR adalah salah satu algoritma kriptografi modern dengan meng-XOR kan plainteks (P) dengan kunci (K) menghasilkancipherteks. Sedangkan Algoritma *Advanced Encryption Standard (AES)* adalah blok chipertext simetrik yang dapat mengenkripsi (encipher) dan dekripsi (decipher) informasi. Kriteria pemilihan AES didasarkan pada 3 kriteria utama yaitu: keamanan, harga, dan karakteristik algoritma beserta implementasinya. [3]

2. PENELITIAN YANG TERKAIT

Penelitian yang dilakukan oleh Fresly Nandar Pabokory, Indah Fitri Astuti, dan Awang Harsa Kridalaksana dalam jurnal tahun 2015 yang berjudul "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi *File* Dokumen, dan *File* Dokumen Menggunakan Algoritma *Advanced Encryption Standard* " dijelaskan bahwa komputerisasi sangat dibutuhkan dalam setiap kegiatan, dari hal penggunaan komputerisasi tersebut maka keamanan aset-aset, informasi dan data-data penting sangatlah diperlukan. Salah satu cara yaitu dengan menggunakan teknik penyamaran data yang disebut kriptografi, dalam penelitian ini metode yang digunakan yaitu algoritma *Advanced Encryption Standard* (AES) yang dapat mengenkripsi isi data. Kesimpulan dari penelitian tersebut yaitu dalam penggunaan *Application* Fres-CAESAS, *user* bebas untuk memproses pengamanan data informasinya (pesan rahasia) dengan melakukan teknik kriptografi yang terdapat beberapa macam keamanan, melakukan teknik steganografi, atau melakukan teknik kombinasi kriptografi dan steganografi.[4]

Penelitian yang dilakukan oleh Aditia Rahmat Tulloh, Yurika Permanasari, Erwin Harahap dalam jurnal tahun 2016 dengan judul "Kriptografi *Advanced Encryption Standard* (AES) Untuk Penyandian *File* Dokumen", dalam tulisan ini dijelaskan bahwa pertukaran data dan informasi pada saat ini semakin pesat tanpa dihalangi oleh jarak dan waktu sehingga masalah keamanan untuk kerahasiaan informasi sangat diperlukan. Untuk itu langkah yang dilakukan yaitu dengan membuat sebuah sistem pengamanan *file* dokumen menggunakan kriptografi AES dalam penyandiannya, pada tulisan ini juga peneliti menggunakan bantuan MATLAB agar proses enkripsi dan dekripsi dapat dilaksanakan dengan cepat, tepat, dan efisien. Kesimpulan dari hasil penelitian tersebut yaitu pada data teks, proses enkripsi dalam algoritma kriptografi AES 128, 128 bit (1 blok) plainteks terlebih dahulu dikonversi menjadi kode ASCII dalam bilangan heksadesimal dan dibentuk sebagai matriks byte berukuran 4x4 yang disebut *state* dan dengan bantuan MATLAB proses enkripsi dan deskripsi dapat dilaksanakan dengan cepat tepat dan efisien.[5]

3. METODE PENELITIAN

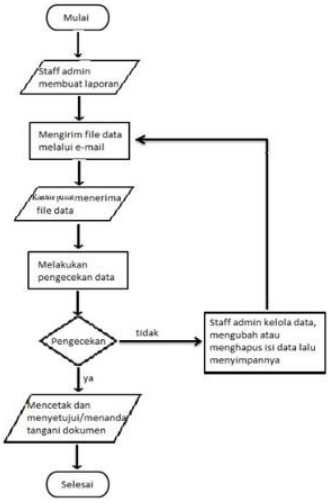
Adapun metode yang akan digunakan untuk menyelesaikan tugas akhir ini adalah sebagai berikut :

a. Metode Pengamatan Langsung (Observasi)
Pengumpulan data-data dengan cara pengamatan langsung pada kegiatan yang sedang dilakukan untuk mengetahui hal yang sedang terjadi pada sistem berjalan, untuk dapat dikembangkan kembali.

b. Metode Wawancara (*Interview*)
Yaitu melakukan pengumpulan data dengan melakukan tanya jawab mengenai keterangan yang diperlukan dalam melakukan penelitian ini dengan menanyakan langsung kepada pembimbing.

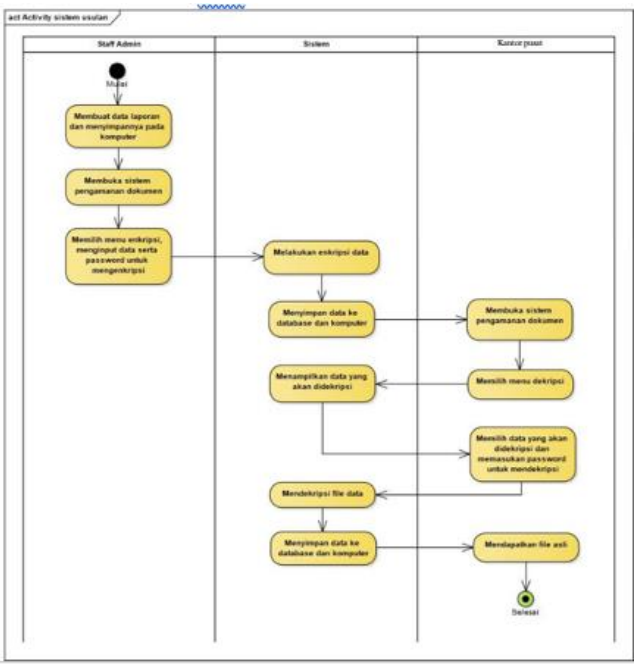
c. Studi kepustakaan (*Library*)
Mempelajari buku-buku referensi yang berhubungan dengan Algoritma XoR dan Algoritma AES untuk membantu dalam pembuatan aplikasi ini selain itu juga mempelajari referensi jurnal-jurnal seputar hal yang sama untuk membantu dalam penyajian informasi yang akan ditampilkan.

d. Analisa Sistem Berjalan
Setiap tahunnya Bimbingan Belajar Matriks mengelola 300 sampai 600 siswa mulai dari tingkat sekolah dasar, sekolah menengah pertama dan sekolah menengah atas yang membutuhkan tambahan intensif untuk memperoleh tambahan belajar. Dari jumlah siswa yang banyak tersebut tentu banyak data dan informasi penting yang harus dikelola oleh Bimbingan Belajar Matriks seperti data siswa, data pembayaran siswa, data soal atau buku, dan data pelaporan pemasukkan dan pengeluaran antara cabang yang ditempatkan di komputer masing-masing cabang dan di komputer kantor pusat. setiap harinya data-data ini selalu dipergunakan dengan intensif yang dikelola oleh admin cabang dan admin pusat. data yang ada disetiap cabang dikirimkan melalui surat elektronik (email) setiap harinya untuk dilakukan pencatatan juga dikantor pusat.



Gambar 1 Analisa Sistem Berjalan

e. Analisa Sistem Usulan
Dengan melihat masalah masalah yang ada, peneliti mengusulkan, untuk membuat sebuah sistem informasi yang bisa melakukan deskripsi dan enkripsi data yang bertujuan untuk meminimalisir kebocoran kerahasiaan data. Analisa sistem berjalan bisa dilihat seperti pada alur dibawah ini :



Gambar 2 Analisa Sistem Usulan

4. HASIL DAN PEMBAHASAN

Dari data yang didapat didalam metode penelitian makan akan dibuat suatu aplikasi yang memungkinkan suatu data bisa di deskripsi dan enkripsi untuk menjaga kerahasiaan data.

Berikut ini merupakan langkah-langkah proses perhitungan algoritma *Anvanced Encryption Standard* (AES):

a. Melakukan XOR *plainteks*/*state* dengan *RoundKey*.
b. Melakukan subtitusi dengan s-Box.
c. Setelah hasil subtitusi dengan s-Box selesai, lakukan *shiftRow* (menggeser baris).
d. Setelah hasil *shiftRow* diperoleh, maka langkah selanjutnya yaitu melakukan *MixColumns* dengan mengalikan matriks.
e. Setelah perhitungan *MixColumns* selesai maka lakukan *addRoundKey* yaitu melakukan XOR *state* dengan *RoundKey*.
f. Lakukan sampai literasi 10, namun pada saat putaran/literasi yang ke 10, setelah *step ShiftRow* lompati *step MixColumns* dan langsung melakukan XOR hasil *state ShiftRow* dengan *RoundKey*.

Berikut contoh kasus perhitungan algoritma *Advanced Encryption Standard (AES)*:

Plainteks : MiftahudinUnpam1

Dalam HEX: 4D 69 66 74 61 68 75 64 69 6E 55 6E 70 61 6D 31

Kunci : informatikaunpam

Dalam HEX: 69 6E 66 6F 72 6D 61 74 69 6B 61 75 6E 70 61 6D

a. AddRoundKey

4D	61	69	70	XOR	69	72	69	6E	=	A4	13	00	1E
69	68	6E	61		6E	6D	6B	70		07	05	05	11
66	75	55	6D		66	61	61	61		00	14	34	0C
74	64	6E	31		6F	74	75	6D		1B	10	1B	5C

b. *SubBytes*

A4	13	00	1E	= SubByte	49	7D	63	72
07	05	05	11		C5	6B	6B	82
00	14	34	0C		63	FA	18	FE
1B	10	1B	5C		AF	CA	AF	4A

c. ShiftRow

49	7D	63	72
C5	6B	6B	82
63	FA	18	FE
AF	CA	AF	4A

49	7D	63	72
	C5	6B	6B
	63	FA	18
	AF	CA	AF

49	7D	63	72
6B	6B	82	C5
18	FE	63	FA
4A	AF	CA	AF

d. *MixColumn*

49	7D	63	72
6B	6B	82	C5
18	FE	63	FA
4A	AF	CA	AF

02	03	01	01	X	49	=	4B	68	18	4A
01	02	03	01		6B		49	69	1B	4A
01	01	02	03		18		49	6B	1A	49
03	01	01	02		4A		4A	6B	18	48

e. *State MixColumns* XOR *RoundKey*

4B	68	18	4A	XOR	A4	13	00	1E	=	EF	7B	18	54
49	69	1B	4A		07	05	05	11		4E	6C	1E	5B
49	6B	1A	49		00	14	34	0C		49	7F	2E	45
4A	6B	18	48		1B	10	1B	5C		51	7B	03	94

Round 1

EF	7B	18	54
4E	6C	1E	5B
49	7F	2E	45
51	7B	03	94

Demikian seterusnya hingga didapatkan *round* ke 10. Ekspansi keseluruhan dapat dilihat pada table-tabel dibawah ini:

Round 1

EF	7B	18	54
4E	6C	1E	5B
49	7F	2E	45
51	7B	03	94

Round 2

FA	02	BA	A2
FA	92	BA	A2
FA	92	BA	A2
FA	92	BA	22

Round 3

11	73	01	F1
11	E3	01	F1
11	E3	01	F1
11	E3	01	71

Round 4

73	9E	96	C6
D2	89	90	C9
D5	9A	A0	D7
CD	9E	8D	86

Round 5

A8	74	22	49
09	63	24	46
0E	70	14	58
16	74	39	09

Round 6

58	23	B7	E2
F9	34	B1	ED
FE	27	B1	F3
E6	23	AC	A2

Round 7

16	D7	D5	A5
B7	C0	D3	AA
B0	D3	E3	B4
AB	D7	CE	E5

Round 8

91	B6	0E	48
30	A1	08	47
37	B2	38	59
2F	B6	15	08

Round 9

30	59	FE	3E
91	4E	F8	31
96	5D	C8	2F
8E	59	E5	7E

Round 10

86	C5	BB	A9
B4	51	B2	81
B0	32	A4	37
88	3A	20	E7

= Ciphertext

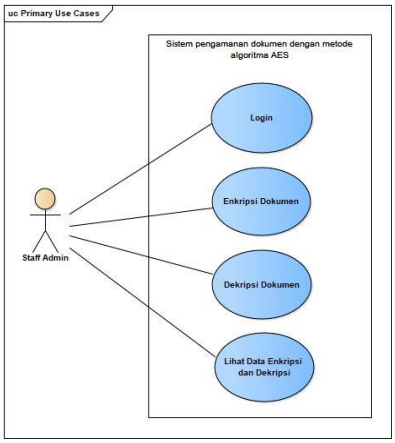
(86 B4 B0 88 C5 51 32 3A BB B2 A4 20 A9 81 37 E7)

Perancangan Sistem

Dari hasil perhitungan manual diatas maka dibuatlah suatu perancangan sistem informasi sebagai berikut :

a. *Use Case* Diagram

Use case diagram merupakan gambaran skenario dari interaksi antara *user* dengan sistem



Gambar 3 Use Case Diagram

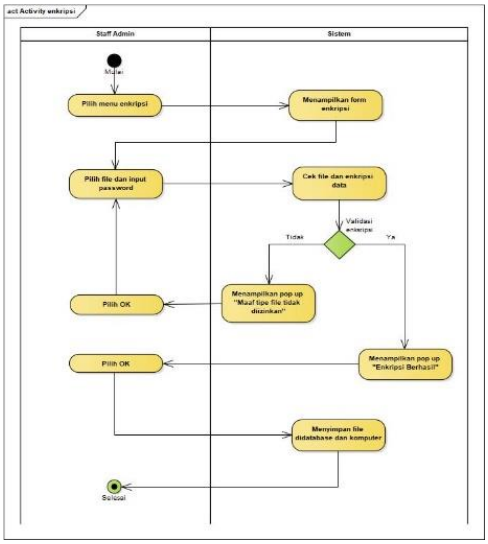
Adapun Deskripsi dari use case diatas dijelaskan pada table dibawah ini :

Tabel 1 Deskripsi Use Case

No	*Usecase*	Deskripsi
1	*Login*	Untuk validasi data *user* ketika memulai menjalankan sistem
2	Enkripsi Dokumen	Untuk Enkripsi *file* asli
3	Dekripsi Dokumen	Untuk Dekripsi *file* yang telah di enkripsi menjadi *file* asli kembali
4	Lihat Data Enkripsi dan dekripsi	Untuk melihat data yang di enkripsi dan di dekripsi atau menghapus *file*

b. Activity Diagram

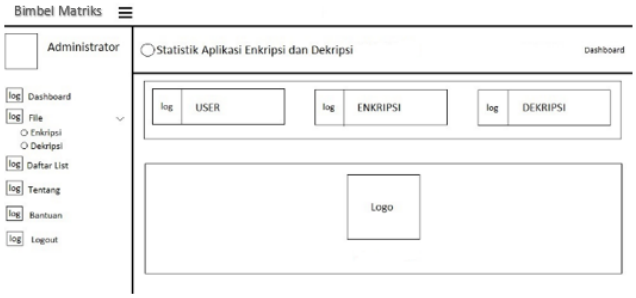
Activity diagram memperlihatkan secara rinci aliran data secara logika tanpa mempertimbangkan lingkungan fisik dimana data mengalir



Gambar 4 Activity Diagram Proses Enkripsi

c. Rancangan Layar

Berikut adalah Rancangan Layar Sistem informasi Deskripsi dan Enkripsi :



Gambar 5 Rancangan Layar

Gambar 6 Hasil Halaman Dashboard

5. KESIMPULAN

Berdasarkan uraian dan analisis yang telah dilakukan pada bab-bab sebelumnya, terutama pada perancangan, pembuatan, serta implementasi sistem maka dapat ditarik kesimpulan yaitu:

a. Dengan adanya sistem kriptografi, keamanan isi data *file* menjadi lebih aman dari pencurian dan perubahan data karena isi diamankan dengan proses enkripsi kriptografi menggunakan metode algoritma *XoR* dan algoritma *AES* baik sebelum dikirim maupun setelah sampai ke tujuan.
b. Proses dekripsi *file* yang telah di enkripsi dengan kunci yang sesuai akan mengembalikan *file* menjadi *file* semula tanpa mengalami perubahan sedikitpun. Sehingga memudahkan pengguna dalam menggunakan sistem saat melakukan pengamanan dan pengembalian *file*.

DAFTAR PUSTAKA

[1] D. Nurnaningsih and A. A. Permana, "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes)," *J. Tek. Inform.*, vol. 11, no. 2, pp. 177–186, 2018, doi: 10.15408/jti.v11i2.7811.

[2] Walgito Bimo, *Pengantar Psikologi Umum*. Jakarta: Andi, 2004.

[3] D. R. Stinson and Ma. B. Paterson, *Chripthography Teory And Practice*. 316AD.

[4] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 10, no. 1, p. 20, 2016, doi: 10.30872/jim.v10i1.23.

[5] A. R. Tulloh, Y. Permanasari, and E. Harahap, "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen," *J. Mat. UNISBA*, vol. 2, no. 1, pp. 118–125, 2016, [Online]. Available: https://ejournal.unisba.ac.id/index.php/matematika/article/view/4067.