PENERAPAN ALGORITMA AES-128 UNTUK APLIKASI PENGARSIPAN DOKUMEN BERBASIS WEB PADA PT STUDIO INOVASI TEKNOLOGI

Re Riski Dwi Andika[1*], Sri Mulyati[2]

[1,2]Fakultas Teknologi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta, Indonesia

Email: [1*]1711510527@student.budiluhur.ac.id, [2]sri.mulyati@budiluhur.ac.id
(* : corresponding author)

Abstrak–Manajemen file merupakan sebuah sistem atau perangkat lunak yang bertugas mengelola data file pada sistem komputer. PT Studio Inovasi Teknologi (Studio IT) merupakan salah satu perusahaan yang bergerak dibidang konsultan software, yang berupaya meningkatkan kualitas perusahaan agar dapat bersaing dengan perusahaan lainnya yang bergerak pada bidang yang sama. Sebagai konsultan tentunya perusahaan memiliki berbagai dokumen rahasia yang berhubungan dengan pelanggan. Terdapat banyak file dokumen rahasia yang memungkinkan terjadinya pencurian data oleh pihak yang tidak bertanggung jawab. Hal ini membuat dokumen rahasia berisiko jatuh ke tangan yang salah. Masalah yang ada dalam manajemen file yang digunakan oleh perusahaan ini masih menggunakan penyimpanan manual dan tidak terstruktur. Penyalahgunaan identitas perusahaan pernah dialami oleh PT Studio Inovasi Teknologi oleh orang yang tidak bertanggung jawab. Dengan permasalahan tersebut penulis menawarkan sebuah sistem pengolahan file dengan mengenkripsi file agar lebih aman. Penulis menggunakan algoritma *Advanced Encryption Standard* (AES) 128 bit sebagai metode keamanan file yang akan disimpan. Adapun tujuan dari sistem manajemen file ini dokumen dapat tersimpan dengan aman dan tidak bocor kepada pihak yang tidak bertanggung jawab. Sistem manajemen file ini diharapkan dapat membantu kualitas perusahaan dalam mengontrol dokumen masuk, dokumen keluar, serta identitas perusahaan.

Kata Kunci: kriptografi, data management, advanced encryption standard-128, enkripsi, dekripsi, php: hypertext preprocessor.

APPLICATION OF AES-128 ALGORITHM FOR WEB-BASED DOCUMENT ARCHIVING APPLICATION AT PT STUDIO INOVASI TEKNOLOGI

Abstract-*File management is a system or software that stores data files on a computer system. PT Studio Innovation Technology (Studio IT) is one of the companies engaged in consulting software, which seeks to improve the quality of the company so that it can compete with other companies engaged in the same field. As a consultant, of course, the company has various confidential documents related to customers. There are many document files File management is a system or software that stores data files on a computer system. PT Studio Innovation Technology (Studio IT) is one of the companies engaged in consulting software, which seeks to improve the quality of the company so that it can compete with other companies engaged in the same field. As a consultant, of course, the company has various confidential documents related to customers. There are many confidential document files that allow data theft by irresponsible parties. This puts confidential documents at risk of falling into the wrong hands. The problem that exists in the management file used by this company is still using manual and unstructured storage. The misuse of corporate identity has been experienced by PT Studio Innovation Teknologi by irresponsible people. With these problems the author offers a file processing system by encrypting files to make it more secure. The author uses the yahoo Advanced Encryption Standard (AES) 128 bit as a method of securing files to be stored. The purpose of this file management system can be stored safely and not leaked to irresponsible parties. This file management system is expected to help the company's quality in controlling incoming documents, outgoing documents, and identity secrets that allow data theft by irresponsible parties. This puts confidential documents at risk of falling into the wrong hands. The problem that exists in the management file used by this company is still using manual and unstructured storage. The misuse of corporate identity has been experienced by PT Studio Innovation Teknologi by irresponsible people. With these problems the author offers a file processing system by encrypting files to make it more secure. The author uses the yahoo Advanced Encryption Standard (AES) 128 bit as a method of securing files to be stored. The purpose of this file management system can be stored safely and not leaked to irresponsible parties. This file management system is expected to help the company's quality in controlling incoming documents, outgoing documents, and corporate identity.*

Keywords*: cryptography, data management, advanced encryption standard-128, encryption, decryption, php: hypertext preprocessor*

1. PENDAHULUAN

PT Studio Inovasi Teknologi adalah sebuah perusahaan penyedia layanan pengembangan aplikasi desktop, web dan mobile. Perusahaan ini memiliki sumber daya manusia yang dapat dibilang sedikit dan juga berpencar diberbagai daerah di Indonesia. Sumber daya manusia yang sedikit dapat menyebabkan kualitas sebuah perusahaan ini menurun diberbagai bidang.

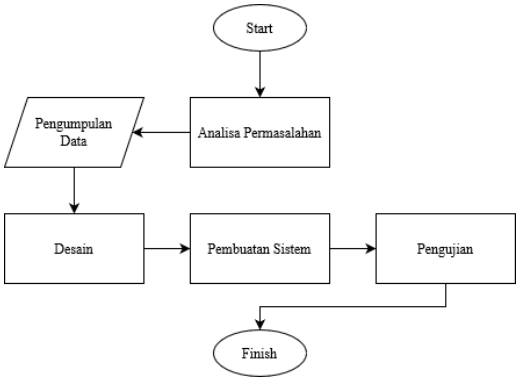
Manajemen file merupakan sebuah sistem pada komputer yang bertujuan untuk mengelola sebuah file agar dapat disimpan pada perangkat komputer. Perlunya manajemen file pada sebuah perusahaan adalah suatu hal yang perlu dipertimbangkan, karena file penting pada sebuah perusahaan dapat tersimpan rapi dan aman serta dapat meningkatkan kualitas perusahaan tersebut. PT studio Inovasi Teknologi adalah sebuah perusahaan yang tidak memiliki penyimpanan file secara tetap, dalam hal ini perusahaan ini memiliki kualitas manajemen file yang kurang, dan berdampak pada keamanan atau kerahasiaan file penting yang dimiiki perusahaan tersebut.

Dengan sumber daya manusia yang kurang, penulis menawarkan sebuah sistem manajemen file berbasis web untuk mengontrol keluar masuknya dokumen penting pada perusahaan tersebut, agar dapat tersimpan dengan rapi dan aman. Tujuan dibuat dalam bentuk website agar memudahkan karyawan yang tersebar diberbagai daerah dapat menggunakan sistem ini dengan mudah. Sistem manajemen file adalah sebuah solusi jitu untuk meningkatkan kualitas dari perusahaan tersebut, serta meringankan pekerjaan dalam memanajemen file. Penulis juga menggunakan sebuah metode penyamaran file agar lebih aman dan tidak dapat dibaca oleh pengguna yang tidak bertanggung jawab.

Kriptografi adalah ilmu memanipulasi atau menyamarkan data agar pihak yang tidak berhak mengetahuinya. Kriptografi mengenkripsi data asli (*plaintext*) untuk digunakan sebagai *ciphertext*. Kriptografi menggunakan banyak algoritma untuk menyamarkan data. *Advanced Encryption Standard* atau AES merupakan salah satu jenis kriptografi. AES merupakan *cipher* blok simetris yang dapat mengenkripsi data atau bisa disebut *encipher*, dan dekripsinya disebut *dechiper*. Teknik enkripsi dari algoritma ini memodifikasi data sehingga tidak dapat dibaca, yang disebut *ciphertext*. Teknik dekripsi mengubah *ciphertext* dari data ke dalam bentuk aslinya yang kita sebut *plaintext*. Algoritma *Advanced Encryption Standard* (AES) dipilih karena memiliki tingkat keamanan yang cukup baik terhadap sejumlah serangan seperti *attack square attack, false truncation, Differential and Linear Encryption Analysis* dan *interpolation attack* [1].

2. METODE PENELITIAN

Tahapan penelitian ini dapat dimodelkan dalam diagram alir yang merupakan proses mulai dari tahap Analisa permasalahan dengan narasumber sampai tahap pengujian sistem. Diagram alir dapat dilihat pada gambar 1.



Gambar 1. Tahapan penelitian.

2.1 Analisa Permasalahan

Tahap ini kami melakukan beberapa analisa data dengan melakukan beberapa wawancara terhadap narasumber yang bersangkutan serta menijau beberapa Pustaka sebagai pendukung penelitian, sehingga kita dapat mengenali secara detail permasalahan yang dihadapi, dan solusi yang diperlukan dalam penyusunan.

2.2 Pengumpulan Data

Pengumpulan data adalah tahapan penting sebelum proses pembuatan sistem. Terdapat beberapa cara dalam melakukan pengumpulan data ini, contohnya dengan mempelajari beberapa penelitian atau buku-buku serta

mencari data-data pendukung di Internet. Memberikan kebebasan kepada pengguna dalam berpendapat mengenai sistem ini dan juga kami menerima beberapa dokumen *dummy* untuk dijadikan sebagai objek uji coba.

2.3 Desain

Pada tahap desain ini kami membuat sebuah rancangan sistem menggunakan flowchart, algoritma dan prototipe rancangan layar sebagai acuan dalam pembuatan, agar pengguna atau *user* dapat melihat secara kasar seperti apa sistem yang akan digunakan dan mempermudah penulis dalam pembuatan sistem.

2.4 Pembuatan Sistem

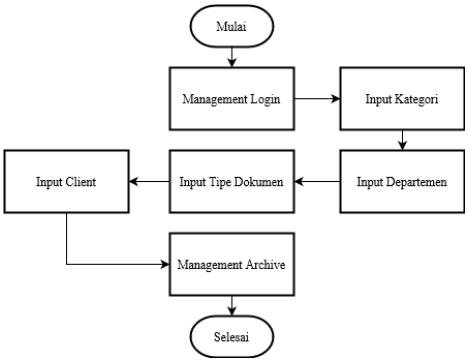
Pada Tahap pembuatan program, kami mengikuti apa yang sudah disepakati oleh *user* agar tidak terjadi kesalahpahaman atau perbedaan dengan kemauan pengguna atau *user*. Menggunakan data *dummy* yang sudah ada sebagai acuan tahapan uji coba sesuai dengan apa yang disepakati pada tahap sebelumnya.

2.5 Pengujian

Pada tahap pengujian atau biasa kita sebut dengan *User Acceptance Testing* (UAT), akan disediakan scenario *blackbox* sebagai acuan dalam pengujian. Ketika masih ada kekurangan atau tambahan (masih dalam lingkup kesepakatan) dari pengguna atau user, akan dilakukan perubahan pada program yang kurang atau butuh ditambahkan tersebut tanpa mengubah alur yang telah disepakati

2.6 Penerapan Metode

Dalam menjalankan sistem mulai dari awal proses hingga selesai dapat dipaparkan dengan sebuah alur singkat. Sebagai autentikasi awal untuk mengakses sistem user harus melakukan login. Setelah login, user dapat mengarsipkan sebuah dokumen kedalam aplikasi.



Gambar 2. Flowchart Proses System.

Advanced Encryption Standard (AES) merupakan algoritma kriptografi modern yang dapat digunakan untuk mengamankan data. Blok *chipertext* simetrik yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*) informasi disebut algoritma aes. *Chipertext* adalah data yang tidak dapat dikenal, dan proses mengubah data asli menjadi *chipertext* adalah enkripsi. Sebaliknya dekripsi mengubah *ciphertext* data menjadi bentuk asli, yang dikenal sebagai *plaintext* [2]. Algoritma aes memiliki beberapa macam kunci enkripsi dan dekripsi pertama 128 bit, kedua 192 bit, dan yang ketiga 256 bit [3].

Tabel 1. Tabel Putaran Algoritma AES tiap blok [4]

Tipe	Kunci	Blok Input	Jumlah n
AES – 128	128-bit	128-bit	10
AES – 192	192-bit	128-bit	12
AES – 256	256-bit	128-bit	14

Pada penelitian ini digunakan AES-128 *bit* yang dilakukan terhadap *state* atau *array of byte* dua dimensi. Fase awal pada enkripsi, data yang *input* berupa in ke 0 (in0) hingga in ke 15 (in 15). Ilustrasi *input bytes* dapat dilihat pada gambar 3.

In_0	In_4	In_8	In_{12}
In_1	In_5	In_9	In_{13}
In_2	In_6	In_{10}	In_{14}
In_3	In_7	In_{11}	In_{15}

Gambar 3. *input bytes.*

Kemudian disalin ke dalam *array state dan* akan dilakukan proses enkripsi / dekripsi. Ilustrasi *State Array* dapat dilihat pada gambar 4.

$S_{0.0}$	$S_{0.1}$	$S_{0.2}$	$S_{0.3}$
$S_{1.0}$	$S_{1.1}$	$S_{1.2}$	$S_{1.3}$
$S_{2.0}$	$S_{2.1}$	$S_{2.2}$	$S_{2.3}$
$S_{3.0}$	$S_{3.1}$	$S_{3.2}$	$S_{3.3}$

Gambar 4. *State Array.*

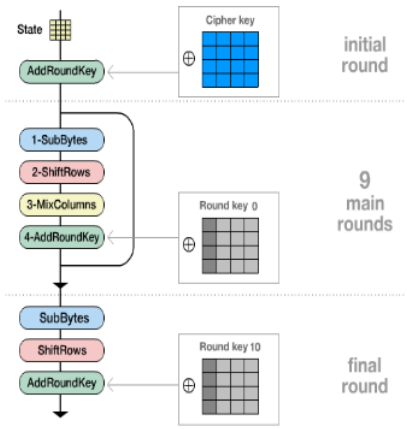
Sebuah *output* akan dihasilkan dan ditampung ke dalam *array out*. Ilustrasi *output bytes* dapat dilihat pada gambar 5.

Out_0	Out_4	Out_8	Out_{12}
Out_1	Out_5	Out_9	Out_{13}
Out_2	Out_6	Out_{10}	Out_{14}
Out_3	Out_7	Out_{11}	Out_{15}

Gambar 5. *Output Bytes.*

2.7 Proses Enkripsi

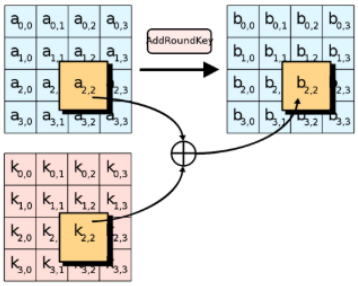
Sebuah proses penyandian *plaintext* menjadi *ciphertext* adalah penjelasan teknis proses enkripsi atau secara umum enkripsi adalah sebuah proses mengonversikan data normal menjadi data rahasia [5] yang dapat dilihat pada gambar 6.



Gambar 6. Skema Enkripsi AES [6]

Proses enkripsi algoritma AES-128 akan melakukan beberapa Transformasi bytes yaitu AddRoundKey, SubBytes, ShiftRows, dan Mixcolumns yang dipisahkan menjadi 3 bagian, yaitu Initial Round, Main Rounds, dan Final Round [1] adalah sebagai berikut :

a. Initial Round merupakan sebuah fase AddRoundKey yang melakukan XOR antara *array state* dengan *round key*. Agar menghasilkan nilai baru dalam array hasil, perlu dilakukan operasi XOR pada setiap byte dalam array dengan ukuran pada masing-masing array sama yaitu 4 x 4. Ilustrasi Transformasi *AddRoundKey* dapat dilihat pada gambar 7.



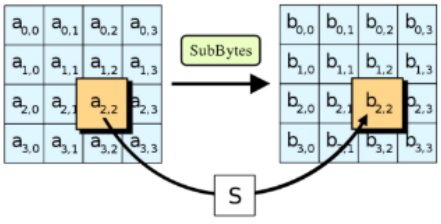
Gambar 7. Representatif Transformasi AddRoundKey [1]

b. Main Rounds adalah fase perulangan sebanyak n-1 (Round n - 1), pada setiap perulangan akan memproses 3 tahapan yaitu :

1. Masing-masing *cell* pada *state* akan disesuaikan dengan menggunakan tabel substitusi (S-Box) atau disebut proses *SubByte*. Tabel ilustrasi *S-Box SubByte* dapat dilihat pada tabel 2, dan transformasi S*ubByte* dapat dilihat pada gambar 8.

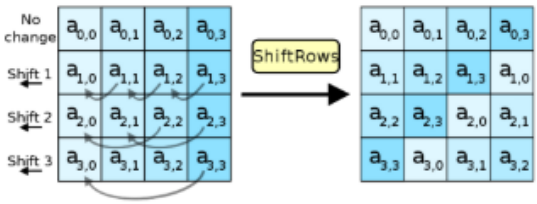
Tabel 2. Representatif Tabel *S-Box SubByte* [7]

		Y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
X	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	10	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	61	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16



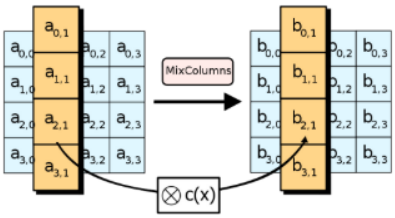
Gambar 8. Representatif Transformasi SubByte [1].

2. *ShiftRows :* untuk setiap elemen blok persgeseran baris demi baris. Baris ke-1 tanpa pergeseran, baris ke-2 dengan pergeseran 1 *byte*, baris ke-3 dengan pergeseran 2 *byte*, baris ke-4 dengan pergeseran 3 *byte*. Pergeseran yang dilakukan adalah pergeseran ke kiri, akan kembali ke posisi kanan blok apabila batas kiri blok dilewati. Ilustrasi dilihat pada gambar 9.



Gambar 9. Representatif Transformasi *ShiftRows* [1].

3. *MixColumn* : Operasi perkalian *XOR bitwise* pada setiap elemen dari 12 blok *cipher*. Perkalian dilakukan mirip dengan perkalian *dot products matriks*, dan hasilnya dimasukkan ke dalam cipher blok baru. Langkah *MixColumn* ini diputar n-1 dengan jumlah bit tergantung pada jenis AES yang digunakan. Pada awal proses AES akan dijalankan *AddRoundKey*, dan langkah MixColumn akan dijalankan di akhir proses enkripsi AES, supaya tidak ada kesalahan pada langkah dekripsinya. Ilustrasi Transformasi *MixColumn* dilihat pada gambar 10.

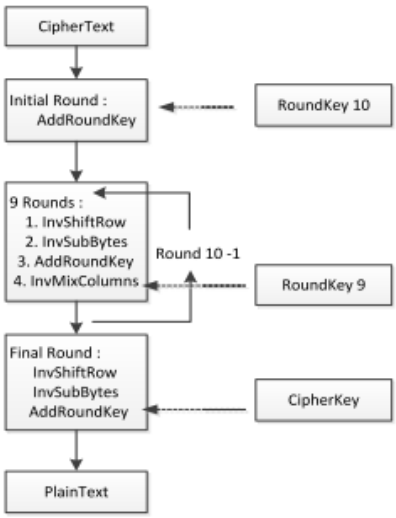


Gambar 10. Representatif Transformasi *MixColumn* [1].

c. *Final round* : Proses putaran terakhir yang akan diakhiri dengan output data *chipertext.*
   1. *SubByte*.
   2. *ShiftRow.*
   3. *AddRoundKey.*

2.8 Proses Dekripsi

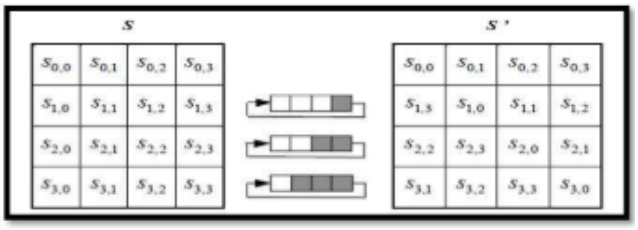
Transformasi *cipher* dapat diimplementasikan mundur untuk menghasilkan *inverse cipher* yang mudah dipelajari untuk algoritma AES [8]. Penjelasan skema dekripsi AES ada pada gambar 11.



Gambar 11. Skema Dekripsi AES [9].

Invers cipher menggunakan Transformasi *byte* yang terdiri dari *AddRoundKey*, *InvShiftRows*, *InvSubBytes*, dan *InvMixColumns* yang dibungkus menjadi 3 bagian, yaitu *Initial Round*, *Standard Rounds*, dan *Final Round* [1].

a. *Initial Round* : Akan melakukan XOR antara *ciphertext* dan *cipher key* yang disebut proses *AddRoundKey*.
b. *Standard Rounds* : fase putaran adalah n -1, pada setiap putarannya akan menjalankan beberapa proses, yaitu:
   1. *InvShiftRows*: memindahkan baris-baris *array state* secara *wrapping*. Berikut ilustrasinya :



Gambar 12. Representatif Transformasi *InvSiftRow* [10].

   2. *InvSubByte* : Setiap *cell* pada *state* akan diposisikan dengan menggunakan tabel substitusi kebalikan (*inverse S-box*). Berikut tabel transformasi *InvSubByte* :

Tabel 3. Tabel S-box untuk Transformasi *InvSubByte* [10].

		Y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
X	0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
	1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
	2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	AE
	3	08	2E	A1	66	28	D9	24	82	76	5B	A2	49	6D	8B	D1	25
	4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
	5	6C	70	48	50	FD	ED	89	DA	5E	15	46	57	A7	8D	9D	84
	6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
	7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
	8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	84	E6	73
	9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
	A	47	F1	1A	71	1D	29	C5	89	6F	87	62	0E	AA	18	BE	1B
	B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
	C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
	D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
	E	A0	E0	38	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
	F	17	2B	04	73	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

   3. *AddRoundKey* : proses XOR antara *state* saat ini dengan *round key*.
   4. *InvMixColumn* : pengacakan data di setiap kolom *state array*. Setiap kolom *state* dikalikan dengan matriks perkalian AES. Perkalian matriks dapat ditulis :

$$\begin{bmatrix} S'_{0,C} \\ S'_{1,C} \\ S'_{2,C} \\ S'_{3,C} \end{bmatrix} = \begin{bmatrix} 0E\ 0B\ 0D\ 0 \\ 0\ 0E\ 0B\ 0D \\ 0D\ 0\ 0E\ 0B \\ 0B\ 0D\ 0\ 0E \end{bmatrix} \begin{bmatrix} S_{0,C} \\ S_{1,C} \\ S_{2,C} \\ S_{3,C} \end{bmatrix}$$

Gambar 13. Proses perkalian *InvMixColumn* [10].

c. *Final round* : Proses putaran terakhir yang akan diakhiri dengan output data *plaintext.*
   1. *InvShiftRow.*
   2. *InvSubByte.*
   3. *AddRoundKey.*

3. HASIL DAN PEMBAHASAN

Sistem managemen data dalam penelitian ini menggunakan enkripsi dan dekripsi, yang dibuat untuk meningkatkan kualitas perusahaan serta meningkatkan keamanan di PT Studio Inovasi Teknologi.

3.1 Metode Algoritma

3.1.1 Algoritma Proses Enkipsi

Algoritma Proses Enkripsi ini menjelaskan bagaimana algoritma AES-128 memproses proses enkripsi dari *plaintext* menjadi data terenkripsi atau *ciphertext*.

```
Start
Plaintext
AddRoundKey
for i = 1 step 1 to 9
    ShiftRows
    SubBytes
    AddRoundKey
    MixColumns
endfor
SubBytes
ShiftRows
AddRoundKey
Ciphertext
```

3.1.2 Algoritma Proses Dekripsi

Sebuah proses algoritma AES-128 melakukan proses dekripsi dari *chipertext* dikembalikan menjadi data asli atau *plaintext*.

```
Start
Ciphertext
AddRoundKey
for i = 1 step 1 to 9
    InvShiftRows
    InvSubBytes
    AddRoundKey
    InvMixColumns
endfor
InvSubBytes
InvShiftRows
AddRoundKey
Plaintext
```

3.2 Analisis Pengujian

Pengujian ini menggambarkan data masukan yang akan diuji, yaitu perbandingan proses enkripsi dan dekripsi dokumen. Pengujian ini mengukur berapa lama proses enkripsi dan dekripsi berlangsung. Pengujian ini mengelompokkan nilai input ke dalam kelas batasan nilai untuk pengujian selanjutnya dalam kasus tertentu. Analisis penelitian yang dilakukan menggunakan algoritma AES-128 memastikan bahwa file dienkripsi dalam bentuk *ciphertext*, menyimpan file yang diunggah dapat tersimpan aman (terenkripsi), dan berhasil terdekripsi kembali ke *plaintext* yang hasilnya sama dengan data aslinya serta dapat dikatakan bahwa sistem melakukan enkripsi dan dekripsi dalam waktu yang singkat.

3.2.1 Tabel Enkripsi

Pengujian ini menunjukkan proses enkripsi untuk tabel item data. Pengujian meliputi file asli sebelum enkripsi *filename*, berdasarkan waktu enkripsi (*microtime*). Berikut tabel hasil proses enkripsi:

Tabel 4. Hasil Proses Enkripsi

No	Filename (*Plaintext*)	*Key*	Waktu Enkripsi	Filename (*Chipertext*)	Keterangan
1	Invoice #INV-HRG.001-1218.pdf	12345	6452	Dx95_Invoice_#INV-HRG.001-1218.pdf.enkripsi	Berhasil
2	PO_BIMA_Enhancement_9064015460.pdf	12345	6732	eJ1L_PO_BIMA_Enhancement_9064015460.pdf.enkripsi	Berhasil

3	BeritaAcara_SAPSATURN_Enhance_Mulai_v1.pdf	12345	6274	6VRL_BeritaAcara_SAPSATURN_Enhance_Mulai_v1.pdf.enkripsi	Berhasil
4	Studi_Literatur_Journal__ReRiskiDwiAndika_1711510527.docx	54321	3984	mOMn_Studi_Literatur_Journal__ReRiskiDwiAndika_1711510527.docx.enkripsi	Berhasil
5	Surat_Keterangan_Riset.doc	12345	2653	H1nq_Surat_Keterangan_Riset.doc.enkripsi	Berhasil
Rata – Rata Waktu (*microtime*)			26095	Rata – Rata Persentase (%)	

3.2.2 Tabel Dekripsi

Data sistem informasi produk yang telah terenkripsi akan dilakukan dekripsi. Pengujian meliputi file asli sebelum enkripsi *filename*, berdasarkan waktu enkripsi (*microtime*). Berikut tabel hasil proses dekripsi :

Tabel 5. Hasil Proses Dekripsi

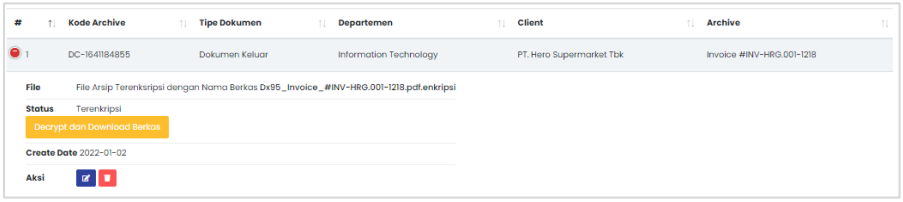
No	Filename (*Chipertext*)	*Key*	Waktu Enkripsi	Filename (*Plaintext*)	Keterangan
1	Dx95_Invoice_#INV-HRG.001-1218.pdf.enkripsi	12345	5362	Dx95_Invoice #INV-HRG.001-1218.pdf	Berhasil
2	eJ1L_PO_BIMA_Enhancement_9064015460.pdf.enkripsi	12345	5361	eJ1L_PO_BIMA_Enhancement_9064015460.pdf	Berhasil
3	6VRL_BeritaAcara_SAPSATURN_Enhance_Mulai_v1.pdf.enkripsi	12345	4351	6VRL_BeritaAcara_SAPSATURN_Enhance_Mulai_v1.pdf	Berhasil
4	mOMn_Studi_Literatur_Journal__ReRiskiDwiAndika_1711510527.docx.enkripsi	54321	3679	mOMn_Studi_Literatur_Journal__ReRiskiDwiAndika_1711510527.docx.	Berhasil
5	H1nq_Surat_Keterangan_Riset.doc.enkripsi	12345	2033	H1nq_Surat_Keterangan_Riset.doc	Berhasil
Rata – Rata Waktu (*microtime*)			20786	Rata – Rata Persentase (%)	

3.2.3 Hasil Enkripsi dan Dekripsi AES 128 bit

Fase pengujian ini menunjukkan hasil dari sistem pengolahan file yang terdiri dari hasil enkripsi dan dekripsi.

a. Tampilan Hasil Enkripsi

Pada gambar 14, layar tabel item menampilkan kolom status, dan statusnya dienkripsi.



Gambar 14. Hasil proses enkripsi pada aplikasi.

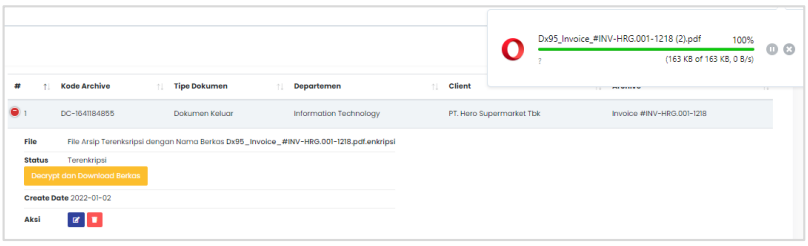
b. Hasil file enkripsi

File terenkripsi dilihat dengan struktur file yang diatur oleh aplikasi, sehingga menampilkan data yang dihasilkan dari proses enkripsi. Berikut adalah gambar contoh file yang berhasil dienkripsi.

Gambar 15. Contoh hasil file yang telah dienkripsi.

c. Tampilan Hasil Dekripsi

Gambar 16 adalah tampilan layar untuk melakukan deskripsi, dengan status terenkripsi serta terdapat *button* untuk mengunduh file.



Gambar 16. Proses dekripsi pada aplikasi.

4. KESIMPULAN

Dari uraian masalah dan solusi pada bab sebelumnya, dapat disimpulkan bahwa aplikasi managemen file menggunakan sistem berbasis web dengan keamanan menggunakan metode *Advanced Encryption Standard*-128 sangat diperlukan, dikarenakan file atau dokumen lebih tertata rapi dan terjaga keamanannya dibandingkan dengan penyimpanan manual, selain itu dokumen lebih mudah dicari. Dokumen yang telah tersimpan akan terenkripsi dengan sempurna sehingga dokumen aman dari penyalahgunaan serta terjaga keasliannya

DAFTAR PUSTAKA

[1] Asriyanik, "Studi Terhadap Advanced Encryption Standard (AES) dan Algoritma Knapsack Dalam Pengamanan Data," *SANTIKA:Jurnal Ilmiah Sains dan Teknologi*, vol. 7, no. 1, pp. 553–561, 2017.

[2] M. M. Amin, "Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks," *Pseudocode*, vol. 3, no. 2, pp. 129–136, Jan. 2017.

[3] Munawir, Zulfan, Y. Yanti, dan Mudianto, "Teknik Pengamanan File Dokumen Berbasis Text Menggunakan Metode Advanced Encryption Standard (AES)," *Semin. Nas. II USM 2017 Eksplor. Kekayaan Marit. Aceh di Era Glob. dalam Mewujudkan Indones. sebagai Poros Marit. Dunia*, vol. 1, pp. 87–90, 2017.

[4] A. Prameshwari dan N. P. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," *Eksplora Informatika*, vol. 8, no. 1, pp. 52-58, 2018.

[5] V. Lusiana, "Implementasi Kriptografi Pada File Dokumen Menggunakan Algoritma Aes-128," *J. Din. Inform.*, vol. 3, no. 2, pp. 79–83, 2011.

[6] V. Yuniati, G. Indriyanta, dan A. Rachmat C., "Enkripsi Dan Dekripsi Dengan Algoritma Aes 256 Untuk Semua Jenis File," *Jurnal Informatika.*, vol. 5, no. 1, pp.1-10, 2009.

[7] F. Muharram, H. Azis, dan A. R. Manga, "Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES)," *Proc. of the Seminar Nasional Ilmu Komputer dan Teknologi Informasi*, vol. 3, no. 2, pp. 112–115, 2018.

[8] B. O. Sinaga, D. Almahera, S. Wahyuni, dan I. Saputra, "Pengamanan File Docx Menerapkan Algoritma Gronsfeld," *Semin. Nas. Teknol. Komput. Sains*, pp. 438–446, 2020, [Online]. Available: https://www.prosiding.seminar-id.com/index.php/sainteks/article/view/472

[9] F. N. Pabokory, I. F. Astuti, dan 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, pp. 20-31, 2015.

[10] D. Nurnaningsih dan A. A. Permana, "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes)," *J. Tek. Inform.*, vol. 11, no. 2, pp. 177–186, 2018..