E-ISSN: 3031-8629
P-ISSN: 3032-3258
Halaman 38-56
Volume 2 Nomor 4 Tahun 2025

Sistem Pengelolaan Dokumen Digital Dengan Fitur Enkripsi Menggunakan Algoritma AES-128 Berbasis Web (Studi Kasus: Direktorat Pengembangan Teknologi Informasi)

Michael Sergio Sitepu[1], Tri Ginanjar Laksana[2], Rasim[3]
[1]Program Studi Informatika, Universitas Bhayangkara Jakarta Raya
e-mail: 202310717002@mhs.ubharajaya.ac.id

Abstrak

Peningkatan penggunaan dokumen digital memunculkan masalah keamanan data, terutama untuk informasi rahasia atau sensitif. Direktorat Pengembangan Teknologi Informasi merupakan salah satu direktorat teknis di Universitas Bhayangkara Jakarta Raya yang bertugas untuk mendukung transformasi teknologi informasi. Saat ini, Direktorat Pengembangan Teknologi Informasi telah memiliki sistem pengarsipan dokumen berbasis web, tetapi masih terbatas pada fungsi manajemen dasar dan belum dilengkapi fitur keamanan. Berdasarkan masalah tersebut, dibutuhkan sebuah sistem pengelolaan dokumen digital yang dilengkapi dengan fitur keamanan seperti enkripsi dokumen. Metode yang digunakan adalah Algoritma AES-128 dan metode Agile. Hasil penelitian ini merupakan terciptanya sebuah sistem pengelolaan dokumen digital dengan fitur enkripsi menggunakan Algoritma AES-128. Hasil penelitian ini diharapkan dapat membantu Direktorat Pengembangan Teknologi Informasi dalam hal pengelolaan dan pengamanan dokumen digital.

Kata kunci: Algoritma AES-128, Sistem Pengelolaan Dokumen Digital, Enkripsi, Universitas Bhayangkara Jakarta Raya.

Abstract

The progressive development of information technology led to the digitalization of nearly all administrative and operational activities in institutions and organizations, including document management. The increased use of digital documents introduced data security problems, particularly for confidential or sensitive information. The Directorate of Information Technology Development at Bhayangkara Jakarta Raya University, a technical directorate responsible for supporting information technology transformation, had a web-based document archiving system. However, it was limited to basic management functions and lacked security features. Based on this issue, a digital document management system equipped with a security feature like document encryption was required. The methods used are the AES-128 Algorithm and the Agile method. The result of this research is the creation of a digital document management system with an encryption feature using the AES-128 Algorithm. This outcome is expected to assist the Directorate of Information Technology Development in the management and security of digital documents.

Keywords : *AES-128 Algorithm, Digital Document Management System, Encryption, Bhayangkara Jakarta Raya University.*

LATAR BELAKANG

Saat ini, teknologi informasi sudah semakin berkembang, khususnya di Indonesia. Berkembangnya teknologi informasi ini membuat hampir seluruh aktivitas administratif dan operasional instansi maupun organisasi telah terdigitalisasi, termasuk dalam hal pengelolaan dokumen. Dokumen yang dulunya disimpan secara fisik, telah beralih dan diubah dalam bentuk digital untuk mendukung pengarsipan jangka panjang, efisiensi, dan aksesibilitas. Dokumen digital merupakan informasi elektronik yang dibuat, dikirimkan, diterima, atau disimpan (Hermawan & Ismiati, 2020).Dengan dokumen digital, pencarian informasi dapat dilakukan dengan lebih

cepat. Pengarsipan yang lebih terstruktur, dan distribusi informasi dapat dilakukan tanpa batasan ruang dan waktu.

Namun, masalah keamanan data muncul, seiring dengan peningkatan penggunaan dokumen digital. Apabila dokumen digital tidak dilindungi dengan baik, pihak yang tidak berwenang dapat mengakses, mengubah, atau mencuri dokumen tersebut. Risiko ini patut untuk diperhatikan, terutama jika dokumen digital yang dikelola berisi informasi rahasia atau sensitif. Oleh karena itu, diperlukan mekanisme untuk melindungi dokumen digital, salah satunya adalah dengan menggunakan Algoritma AES-128 untuk fitur enkripsi dokumen. Algoritma AES-128 merupakan algoritma yang termasuk dalam jenis *block cipher* yang dijadikan standar untuk mengamankan data. Algoritma ini memiliki panjang kunci sebesar 128 bit. Enkripsi yaitu melakukan proses pengubahan pesan atau penyandian data dari pesan asli (*plaintext*) dikonversi menjadi bentuk yang tidak jelas untuk dipahami bahkan dimengerti (Ahmad Sitorus et al., 2020). Dekripsi adalah kebalikan dari enkripsi, dimana data tersebut diolah kembali dengan cara mengembalikan ciphertext menjadi plaintext, sehingga menjadi sesuatu yang dapat diutarakan secara jelas dan dapat dimengerti (Wardah, 2017).

Direktorat Pengembangan Teknologi Informasi merupakan salah satu direktorat teknis di Universitas Bhayangkara Jakarta Raya yang bertugas untuk mendukung transformasi teknologi informasi berdasarkan tata kelola teknologi informasi dalam melaksanakan tri dharma perguruan tinggi. Saat ini, sudah ada sistem direktori pengarsipan dokumen berbasis web di direktorat pengembangan teknologi informasi. Namun, sistem yang ada merupakan sistem direktori pengarsipan dokumen yang masih terbatas pada fungsi manajemen dokumen dasar, dan belum dilengkapi fitur pendukung lain serta fitur keamanan seperti enkripsi dokumen.

Selain keterbatasan fitur, proses pengelolaan dokumen masih melalui beberapa proses, seperti proses *scanning* untuk mengubah dokumen fisik menjadi dokumen digital, pengisian meta data, penginformasian dokumen melalui grup *Whatsapp*, lalu mengunggah dokumen tersebut pada sistem. Proses yang

melibatkan beberapa tahapan ini tidak hanya memakan waktu, tetapi juga rentan terhadap kesalahan dan memperlambat pengelolaan dokumen secara keseluruhan. Dokumen yang biasa dikelola berupa nota dinas, surat keputusan, surat perintah, surat tugas, serta disposisi dari unit lain. Dokumen-dokumen tersebut merupakan dokumen yang berisi informasi sensitif dan harus diamankan, agar terhindar dari risiko kebocoran atau penyalahgunaan informasi sensitif oleh pihak yang tidak berwenang.

Dari uraian permasalahan yang telah disebutkan, maka akan dibuat sebuah sistem pengelolaan dokumen digital dengan fitur enkripsi menggunakan Algoritma AES-128 berbasis web.

METODE

Metode pengumpulan data pada penelitian ini adalah sebagai berikut:

1. Observasi

   Observasi merupakan metode pengumpulan data dengan mengamati secara langsung fenomena atau perilaku yang terjadi di lapangan. Dengan metode ini, peneliti dapat mengamati dan mencatat apa yang mereka lihat dalam situasi yang sebenarnya, tanpa campur tangan dari peneliti itu sendiri (Romdona et al., 2024).
2. Wawancara

   Wawancara merupakan metode pengumpulan data yang dilakukan dengan berinteraksi dengan responden. Dalam interaksi tersebut, peneliti akan mengajukan pertanyaan untuk menggali informasi dengan mendalam tentang topik yang diteliti (Romdona et al., 2024).
3. Studi Literatur

   Studi literatur merupakan metode pengumpulan data dengan cara mengumpulkan sumber tertulis seperti buku, jurnal ilmiah, artikel untuk ditelaah agar memperoleh informasi yang relevan dengan penelitian.

Metode pengembangan sistem yang digunakan pada penelitian ini adalah Agile. Metode Agile merupakan proses iteratif pembuatan *software* (Chandra Ramadhan et al., 2025). Tahapan metode Agile adalah sebagai berikut:

1. Perencanaan

   Pada tahap ini, dilakukan pengumpulan data dari pengguna melalui wawancara langsung atau obervasi untuk mengidentifikasi kebutuhan sistem. Selanjutnya pengembang sistem akan membuat desain secara menyeluruh (Indah Melyani & Aji, 2023).
2. Implementasi

   mengimplementasikan pengembangan sistem sesuai dengan desain yang telah dibuat sebelumnya. Pengembangan sistem menggunakan bahasa pemrograman (Indah Melyani & Aji, 2023).
3. Pengujian

   Pada tahap ini dilakukan proses pengujian untuk memeriksa sistem yang telah dibuat. Pengujian dilakukan dengan metode Black Box Testing guna mencegah adanya kegagalan sistem (Indah Melyani & Aji, 2023).
4. Dokumentasi

   Pada tahap ini dilakukan proses pendokumentasian suatu perangkat, dilakukan dengan merekam langkah demi langkah sistem yang dibangun. Pada langkah ini, hasil pengujian didokumentasikan untuk memudahkan pemeliharaan di masa mendatang (Handayani et al., n.d.).
5. Peluncuran

   Tahap ini mencakup penyediaan sistem yang telah dibuat agar dapat digunakan oleh pengguna akhir (Indah Melyani & Aji, 2023).
6. Pemeliharaan

   Sistem yang telah dikembangkan diperiksa secara berkala untuk menjaga keamanannya dari *bug* atau celah sisem. Hal ini dilakukan karena tidak ada jaminan bahwa sistem bebas dari *bug* atau celah yang dapat dimanfaatkan (Indah Melyani & Aji, 2023).

HASIL DAN PEMBAHASAN

1. Menentukan Plaintext dan Cipherkey
   a. Plaintext yang digunakan adalah ”UNIVERSITASBHAYA”. Plaintext tersebut kemudian diubah ke dalam bentuk hexadesimal dan disusun ke dalam matriks 4 x 4

Tabel 1 Plaintext

U	N	I	V	E	R	S	I	T	A	S	B	H	A	Y	A
55	4E	49	56	45	52	53	49	54	41	53	42	48	41	59	41

Tabel 2 Matriks Plaintext 4 x 4

55	45	54	48
4E	52	41	41
49	53	53	59
56	49	42	41

   b. Cipherkey yang digunakan adalah ”KRIPTOGRAFIAESKU”. Cipherkey tersebut kemudian diubah ke dalam bentuk hexadesimal dan disusun ke dalam matriks 4 x 4

Tabel 3 Cipherkey

K	R	I	P	T	O	G	R	A	F	I	A	E	S	K	U
4B	52	49	50	54	4F	47	52	41	46	49	41	45	53	4B	55

Tabel 4 Matriks Cipherkey 4 x 4

4B	54	41	45
52	4F	46	53
49	47	49	4B
50	52	41	55

2. Pembangkitan Kunci

Pada tahap ini akan dilakukan pembangkitan kunci sesuai dengan panjang kunci awal dan ukuran blok yang digunakan. Proses pembangkitan kunci dilakukan dengan menggunakan operasi RotWord, SubBytes, XOR, dan penambahan Rcon. Berikut adalah proses dan hasil dari pembangkitan kunci.

Tabel 5 Proses Pembangkitan Kunci

ROUND 1			
S-Box[53]→ED⊕4B⊕01=A7	A7⊕54=F3	F3⊕41=B2	B2⊕45=F7
S-Box[4B]→B3 ⊕52=E1	E1⊕4F=AE	AE⊕46=E8	E8⊕53=BB
S-Box[55]→FC ⊕49=B5	B5⊕47=F2	F2⊕49=BB	BB⊕4B=F0
S-Box[45]→6E ⊕50=3E	3E⊕52=6C	6C⊕41=2D	2D⊕55=78
ROUND 2			
S-Box[BB]→EA⊕A7⊕02=4F	4F⊕F3=BC	BC⊕B2=0E	0E⊕F7=F9
S-Box[F0]→8C⊕E1=6D	6D⊕AE=C3	C3⊕E8=2B	2B⊕BB=90
S-Box[78]→BC⊕B5=09	09⊕F2=FB	FB⊕BB=40	40⊕F0=B0
S-Box[F7]→68⊕3E=56	56⊕6C=3A	3A⊕2D=17	17⊕78=6F
ROUND 3			
S-Box[90]→60⊕4F⊕04=2B	2B⊕BC=97	97⊕0E=99	99⊕F9=60

S-Box[B0]→E7⊕6D=8A	8A⊕C3=49	49⊕2B=62	62⊕90=F2
S-Box[6F]→A8⊕09=A1	A1⊕FB=5A	5A⊕40=1A	1A⊕B0=AA
S-Box[F9]→99⊕56=CF	CF⊕3A=F5	F5⊕17=E2	E2⊕6F=8D
	ROUND 4		
S-Box[F2]→89⊕2B⊕08=AA	AA⊕97=3D	3D⊕99=A4	A4⊕60=C4
S-Box[AA]→AC⊕8A=26	26⊕49=6F	6F⊕62=0D	0D⊕F2=FF
S-Box[8D]→5D⊕A1=FC	FC⊕5A=A6	A6⊕1A=BC	BC⊕AA=16
S-Box[60]→D0⊕CF=1F	1F⊕F5=EA	EA⊕E2=08	08⊕8D=85
	ROUND 5		
S-Box[FF]→16⊕AA⊕10=AC	AC⊕3D=91	91⊕A4=35	35⊕C4=F1
S-Box[16]→47⊕26=61	61⊕6F=0E	0E⊕0D=03	03⊕FF=FC
S-Box[85]→97⊕FC=6B	6B⊕A6=CD	CD⊕BC=71	71⊕16=67
S-Box[C4]→1C⊕1F=03	03⊕EA=E9	E9⊕08=E1	E1⊕85=64
	ROUND 6		
S-Box[FC]→B0⊕AC⊕20=3C	3C⊕91=AD	AD⊕35=98	98⊕F1=69
S-Box[67]→85⊕61=E4	E4⊕0E=EA	EA⊕03=E9	E9⊕FC=15
S-Box[64]→43⊕6B=28	28⊕CD=E5	E5⊕71=94	94⊕67=F3
S-Box[F1]→A1⊕03=A2	A2⊕E9=4B	4B⊕E1=AA	AA⊕64=CE
	ROUND 7		
S-Box[15]→59⊕3C⊕40=25	25⊕AD=88	88⊕98=10	10⊕69=79
S-Box[F3]→0D⊕E4=E9	E9⊕EA=03	03⊕E9=EA	EA⊕15=FF
S-Box[CE]→8B⊕28=A3	A3⊕E5=46	46⊕94=D2	D2⊕F3=21
S-Box[69]→F9⊕A2=5B	5B⊕4B=10	10⊕AA=BA	BA⊕CE=74
	ROUND 8		
S-Box[FF]→16⊕25⊕80=B3	B3⊕88=3B	3B⊕10=2B	2B⊕79=52
S-Box[21]→FD⊕E9=14	14⊕03=17	17⊕EA=FD	FD⊕FF=02
S-Box[74]→92⊕A3=31	31⊕46=77	77⊕D2=A5	A5⊕21=84

S-Box[79]→B6⊕5B=ED	ED⊕10=FD	FD⊕BA=47	47⊕74=33
	ROUND 9		
S-Box[02]→77⊕B3⊕1b=DF	DF⊕3B=E4	E4⊕2B=CF	CF⊕52=9D
S-Box[84]→5F⊕14=4B	4B⊕17=5C	5C⊕FD=A1	A1⊕02=A3
S-Box[33]→C3⊕31=F2	F2⊕77=85	85⊕A5=20	20⊕84=A4
S-Box[52]→00⊕ED=ED	ED⊕FD=10	10⊕47=57	57⊕33=64
	ROUND 10		
S-Box[A3]→0A⊕DF⊕36=E3	E3⊕E4=07	07⊕CF=C8	C8⊕9D=55
S-Box[A4]→49⊕4B=02	02⊕5C=5E	5E⊕A1=FF	FF⊕A3=5C
S-Box[64]→43⊕F2=B1	B1⊕85=34	34⊕20=14	14⊕A4=B0
S-Box[9D]→5E⊕ED=B3	B3⊕10=A3	A3⊕57=F4	F4⊕64=90



Gambar 1 Hasil Pembangkitan Kunci

3. Proses Enkripsi

Setelah melakukan pembangkitan kunci, akan dilakukan proses enkripsi. Proses yang dilakukan adalah sebagai berikut:

a. Initial Round (AddRoundKey)

Melakukan proses XOR antara matriks Plaintext dan Cipherkey

Tabel 6 Initial Round

Plain Text					CipherKey					Initial Round			
55	45	54	48		4B	54	41	45		1E	11	15	0D
4E	52	41	41	⊕	52	4F	46	53	=	1C	1D	07	12
49	53	53	59		49	47	49	4B		00	14	1A	12
56	49	42	41		50	52	41	55		06	1B	03	14

Hasil dari proses Initial Round di atas merupakan pra proses dan akan digunakan untuk ronde 1 yang diproses dengan 4 transformasi, yaitu SubBytes, ShiftRows, MixColumns, dan AddRoundkey.

b. SubBytes

Proses SubBytes mengubah byte pada matriks Initial Round berdasarkan tabel S-Box. Hasil SubBytes dapat dilihat pada tabel berikut.

Tabel 7 SubBytes Ronde 1

Initial Round					Hasil SubBytes			
1E	11	15	0D		72	82	59	D7
1C	1D	07	12	=	9C	A4	C5	C9
00	14	1A	12		63	FA	A2	C9
06	1B	03	14		6F	AF	7B	FA

c. ShiftRows

Proses ShiftRows dilakukan dengan melakukan pergeseran byte ke kiri pada matriks SubBytes. Baris pertama tidak dilakukan pergeseran, baris kedua dilakukan satu kali pergeseran, baris ketiga dilakukan dua kali pergeseran, dan baris keempat dilakukan tiga kali pergeseran. Hasil proses ShiftRows dapat dilihat pada tabel berikut.

Tabel 8 ShiftRows Ronde 1

Hasil SubBytes					Hasil ShiftRows			
72	82	59	D7		72	82	59	D7
9C	A4	C5	C9	=	A4	C5	C9	9C
63	FA	A2	C9		A2	C9	63	FA
6F	AF	7B	FA		FA	6F	AF	7B

d. MixColumns

Proses MixColumns dilakukan dengan melakukan perkalian Galois Field Multiplication ($GF(2^8)$) antara matriks ShiftRows dengan matriks tetap AES. Proses MixColumns adalah sebagai berikut

Tabel 9 MixColumns Ronde 1

Matriks Tetap AES					Hasil ShiftRows					Hasil MixColumns			
02	03	01	01		72	82	59	D7		4B	ED	3E	8B
01	02	03	01	x	A4	C5	C9	9C	=	26	3C	DA	9A
01	01	02	03		A2	C9	63	FA		9C	7F	BC	29
03	01	01	02		FA	6F	AF	7B		7F	4F	04	F2

e. AddRoundKey

Proses ini merupakan proses terakhir pada setiap ronde. Pada proses ini, dilakukan proses XOR antara matriks MixColumns dan kunci ronde 1. Proses AddRoundKey dapat dilihat pada gambar berikut.

Tabel 10 AddRoundKey Ronde 1

Hasil MixColumns					Hasil ShiftRows					Hasil AddRoundKey			
4B	ED	3E	8B		A7	F3	B2	F7		EC	1E	8C	7C
26	3C	DA	9A	⊕	E1	AE	E8	BB	=	C7	92	32	21
9C	7F	BC	29		B5	F2	BB	F0		29	8D	07	D9
7F	4F	04	F2		3E	6C	2D	78		41	23	29	8A

Proses enkripsi ronde pertama (*Round 1*) telah selesai dilakukan. Selanjutnya, untuk ronde kedua hingga ronde kesembilan, keempat proses dilakukan sama seperti ronde pertama. Pada ronde kesepuluh, hanya dilakukan tiga proses, yaitu SubBytes, ShiftRows, dan MixColumns. Proses AddRoundKey tidak dilakukan pada ronde ini. Hasil akhir matriks dari proses enkripsi dapat dilihat pada tabel berikut

Tabel 11 Hasil Enkripsi

Hasil Akhir Enkripsi (Hexadesimal)				Desimal				Cipher Text			
D5	40	BC	2F	213	64	188	47	F	@	╝	/
7D	19	ED	31	125	25	237	49	}	↓	Φ	1
85	64	9A	ED	133	100	154	237	À	D	Ü	Φ
18	2D	E8	93	24	45	232	147	↑	-	Φ	Ô

4. Proses Dekripsi

Setelah mendapatkan hasil enkripsi, akan dilakukan proses dekripsi sebanyak 10 ronde untuk mengembalikan Cipher Text ke teks semula (Plain Text). Proses-proses yang dilakukan adalah sebagai berikut:

a. Inv AddRoundKey

Melakukan proses Inverse AddRoundKey antara matriks hasil akhir dari proses enkripsi dengan Round Key 10. Matriks hasil dari proses ini akan digunakan untuk dekripsi ronde pertama

Tabel 12 Inv AddRoundKey

Hasil Akhir Enkripsi (Hexadesimal)					Kunci Ronde 10					Inv AddRoundKey			
D5	40	BC	2F		E3	07	C8	55		36	47	74	7A
7D	19	ED	31	⊕	02	5E	FF	5C	=	7F	47	12	6D
85	64	9A	ED		B1	34	14	B0		34	50	8E	5D
18	2D	E8	93		B3	A3	F4	90		AB	8E	1C	03

b. InvShiftRow

Proses InvShiftRows dilakukan dengan melakukan pergeseran byte ke kanan pada matriks hasil dari proses InvAddRoundKey.

Tabel 13 InvShiftRows Ronde 1

InvAddRoundKey					Hasil InvShiftRows			
36	47	74	7A		36	47	74	7A
7F	47	12	6D	=	6D	7F	47	12
34	50	8E	5D		8E	5D	34	50
AB	8E	1C	03		8E	1C	03	AB

c. InvSubBytes

Proses InvSubBytes dilakukan dengan cara menganti setiap *byte* pada matriks hasil dari proses InvShiftRows dengan nilai yang ada pada tabel *Inverse S-Box*.

Tabel 14 InvSubBytes Ronde 1

Hasil InvShiftRows					Hasil InvSubBytes			
36	47	74	7A		24	16	CA	BD
6D	7F	47	12	=	B3	6B	16	39
8E	5D	34	50		E6	8D	28	6C
8E	1C	03	AB		E6	C4	D5	0E

d. InvAddRoundKey

Pada proses ini, dilakukan proses XOR antara hasil InvSubBytes dengan kunci ronde 9.

Tabel 15 InvAddRoundKey Ronde 1

Hasil InvSubBytes					Kunci Ronde 9					Inv AddRoundKey			
24	16	CA	BD		DF	E4	CF	9D		FB	F2	05	20
B3	6B	16	39	⊕	4B	5C	A1	A3	=	F8	37	B7	9A
E6	8D	28	6C		F2	85	20	A4		14	08	08	C8
E6	C4	D5	0E		ED	10	57	64		0B	D4	82	6A

e. InvMixColumns

Proses InvMixColumns dilakukan dengan melakukan perkalian Galois Field Multiplication ($GF(2^8)$) antara matriks InvAddRoundKey dengan matriks tetap AES. Proses InvMixColumns adalah sebagai berikut.

E-ISSN: 3031-8629
P-ISSN: 3032-3258
Halaman 38-56
Volume 2 Nomor 4 Tahun 2025

Tabel 16 InvMixColumns Ronde 1

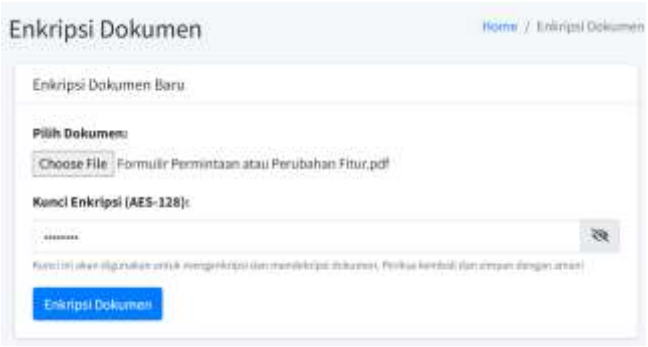
Matriks Tetap AES					Hasil InvAddRoundKey					Hasil InvMixColumns			
0E	0B	0D	09		FB	F2	05	20		90	77	AD	1A
09	0E	0B	0D	x	F8	37	B7	9A	=	26	39	E5	0B
0D	09	0E	0B		14	08	08	C8		47	BF	D0	C2
0B	0D	09	0E		0B	D4	82	6A		ED	E8	A0	CB

Proses dekripsi ronde pertama telah selesai dilakukan. matriks hasil dari proses InvMixColumns akan digunakan pada ronde kedua. Untuk ronde kedua hingga ronde kesembilan, proses dekripsi sama seperti pada ronde pertama, yaitu dengan melakukan InvShiftRows, InvSubBytes, InvAddRoundKey, dan InvMixColumns. Pada Ronde kesepuluh, proses InvMixColumns tidak dilakukan.

Tabel 17 Hasil Dekripsi

Hasil Akhir Dekripsi (Hexadesimal)				Desimal				Plain Text			
55	45	54	48	85	69	84	72	U	E	T	H
4E	52	41	41	78	82	65	65	N	R	A	A
49	53	53	59	73	83	83	89	I	S	S	Y
56	49	42	41	86	73	66	65	V	I	B	A

5. Implementasi dan pengujian sistem
   a. Implementasi dan pengujian enkripsi
      Enkripsi dilakukan dengan menunggah dokumen terlebih dahulu dan memasukkan kunci enkripsi.



Gambar 2 Implementasi dan Pengujian Enkripsi



Gambar 3 Hasil Enkripsi

b. Implementasi dan pengujian dekripsi

Dekripsi dilakukan dengan memasukkan kunci yang telah ditentukan saat proses enkripsi.

E-ISSN: 3031-8629
P-ISSN: 3032-3258

Halaman 38-56
Volume 2 Nomor 4 Tahun 2025



Gambar 4 Implementasi dan Pengujian Dekripsi



Gambar 5 Hasil Dekripsi

SIMPULAN

Pembuatan sistem pengelolaan dokumen digital dengan fitur enkripsi menggunakan Algoritma AES-128 menggunakan metode Agile yang diawali dengan perencanaan hingga implementasi sistem. Implementasi algoritma AES-128 dilakukan pada penerapan fitur enkripsi dokumen. Untuk masa depan, sistem diharapkan dapat dikembangkan dengan mengimplementasikan varian AES yang lebih kuat, seperti AES-192 atau AES-256. Sistem juga diharapkan untuk diimplementasikan secara lebih luas pada unit kerja lain di lingkungan Universitas Bhayangkara Jakarta Raya untuk pengelolaan dokumen yang aman.

DAFTAR PUSTAKA

Ahmad Sitorus, F., Budi Nugroho, N., Fatimah Sari Sitorus Pane, U., Studi Mahasiswa, P., Triguna Dharma, S., & Studi Dosen Pembimbing, P. (2020). Implementasi Algoritma Advanced Encryption Standard (AES) 128 Bit Untuk Keamanan Data Transaksi Penjualan Pada PT. MITSUBISHI ELECTRIC INDONESIA. In *Jurnal CyberTech: Vol. x. No.x*. https://ojs.trigunadharma.ac.id/

Chandra Ramadhan, Mamok Andri Senubekti, & Dien Amalia. (2025). Penerapan Metodologi Agile dalam Pengembangan Perangkat Lunak. *Router : Jurnal Teknik Informatika Dan Terapan*, *3*(2), 10–15. https://doi.org/10.62951/router.v3i2.411

Handayani, H., Faizah, K. U., Mutiara Ayulya, A., Rozan, M. F., & Wulan, D. (n.d.). Perancangan Sistem Informasi Inventory Barang Berbasis Web

Menggunakan Metode Agile Software Development. In *Jurnal Testing dan Implementasi Sistem Informasi* (Vol. 1, Issue 1).

Hermawan, L., & Ismiati, M. B. (2020). Aplikasi Pengecekan Dokumen Digital Tugas Mahasiswa Berbasis Website. In *Jurnal Buana Informatika* (Vol. 11, Issue 2).

Indah Melyani, R., & Aji, S. (2023). Pengembangan Sistem Informasi Penggajian Berbasis Web Menggunakan Framework Laravel dengan Metode Agile Software Development. *Jurnal Sistem Informasi Akuntansi)*, *03*(01). http://jurnal.bsi.ac.id/index.php/jasika

Romdona, S., Senja Junista, S., & Gunawan, A. (2024). *Teknik Pengumpulan Data: Observasi, Wawancara, dan Kuesioner*. *3*(1), 39–47. https://samudrapublisher.com/index.php/JISOSEPOL

Wardah, A. (2017). *Perancangan Aplikasi Pembelajaran Kriftografi Pada Algoritma Fungsi Hash Menggunakan Metode Computer Based Learning*.