Jurnal Informatika Teknologi dan Sains (JINTEKS)
E-ISSN : 2686-3359
Submit July 02, 2024 | Revised July 31, 2024 |
Accepted Agustus 05, 2024
Hal. 648-658
Vol. 6; No. 3
Agustus 2024

PENGAMANAN DATA EKSTENSI FILE PDF DENGAN ALGORITMA AES DAN OTP

Musa Asyari Hidayat Jati[1*], Yulison Herry Chrisnanto[2], Gunawan Abdillah[3]
[1,2,3]Program Studi Informatika, Universitas Jendral Achmad Yani
email: musaasyarihj@if.unjani.ac.id[1*]

Abstrak: Perkembang teknologi yang pesat memberi tantangan baru muncul dalam menjaga keamanan dan privasi data, terutama terkait dengan keamanan dan kerahasiaan dokumen yang rentan terhadap penyadapan dan pencurian. Kriptografi adalah seni dan ilmu yang menjaga kerahasiaan pesan dengan menggunakan teknik matematika terkait keamanan data seperti privasi, keutuhan data, dan autentikasi. Kriptografi dapat diterapkan pada berbagai sektor untuk meningkatkan keamanan data dan melindungi informasi sensitif dari risiko seperti akses tidak sah, pencurian, dan penyalahgunaan data pribadi seperti PDF yang mempunyai format dokumen digital sering digunakan dalam berbagai keperluan, seperti aplikasi online, pendaftaran, dan transaksi digital. AES (Advanced Encryption Standard) adalah algoritma enkripsi yang digunakan secara luas untuk melindungi data dan penggunaan OTP (One Time Password) merupakan teknik keamanan yang memerlukan verifikasi dua langkah yang berbeda untuk mengakses sistem. Algoritma AES memberikan keamanan yang kuat dengan memanfaatkan transformasi kompleks yang membuatnya sangat sulit untuk dipecahkan dan ditambahkanya OTP mampu meningkatkan keamanan data yang akan diamankan sebelum dikembalikan pada bentuk aslinya.

Kata Kunci : Kriptografi, Enkripsi, Advanced Encryption Standard (AES), Verifikasi, Sandi Sekali Pakai

Abstract: *The rapid development of technology presents new challenges in maintaining data security and privacy, especially concerning the security and confidentiality of documents that are vulnerable to eavesdropping and theft. Cryptography is the art and science of maintaining the confidentiality of messages using mathematical techniques related to data security, such as privacy, data integrity, and authentication. Cryptography can be applied in various sectors to enhance data security and protect sensitive information from risks such as unauthorized access, theft, and misuse of personal data. For instance, PDFs, which are digital document formats, are often used for various purposes, such as online applications, registrations, and digital transactions. AES (Advanced Encryption Standard) is a widely used encryption algorithm for protecting data, and the use of OTP (One Time Password) is a security technique that requires two different steps of verification to access a system. The AES algorithm provides strong security by utilizing complex transformations that make it very difficult to break, and the addition of OTP further enhances data security before it is returned to its original form.*

Keywords **:** *Cryptography, Encryption, Advanced Encryption Standard (AES), Verification, One Time Password*

PENDAHULUAN

Teknologi informasi dan komunikasi (TIK) berkembang pesat, memberikan dampak positif yang signifikan di berbagai bidang. Namun tantangan baru muncul dalam menjaga keamanan dan privasi data. Keamanan dan kerahasiaan dokumen menjadi sangat rentan terhadap penyadapan dan pencurian, yang dapat menyebabkan kerugian bagi pemilik dokumen[1]. Di era digital ini, di mana data menjadi aset berharga, perlindungan data sangat penting. Ancaman seperti peretasan, serangan perangkat lunak berbahaya, dan pencurian identitas semakin canggih. Oleh karena itu, diperlukan solusi efektif dalam menjaga kerahasiaan data.

KTP berupa PDF sering digunakan dalam berbagai keperluan, termasuk aplikasi online seperti perbankan dan asuransi, pendaftaran dan registrasi di sekolah atau universitas, lamaran kerja, verifikasi identitas di platform digital, transaksi jual beli properti, pembuatan akun, permohonan visa atau paspor, serta dalam kontrak dan perjanjian elektronik. Penggunaan KTP dalam bentuk PDF memudahkan proses verifikasi identitas dan mendukung berbagai transaksi serta aktivitas digital[2]. Hasil survei menunjukkan bahwa pencegahan kebocoran[1] data dianggap sebagai faktor paling penting, dengan 88% responden menilai tantangan ini sebagai kritis dan sangat penting[1]. Selain itu, perlindungan data juga memiliki dampak signifikan pada tantangan keamanan, dengan 92% responden mengakui pentingnya hal tersebut[1]. Solusinya adalah menerapkan kriptografi untuk melindungi data di dalamnya. Kriptografi adalah studi dan teknik matematika yang menjaga keamanan pesan dan informasi, termasuk privasi, keutuhan data, dan autentikasi[3]. Kriptografi adalah proses mengonversi data menjadi bentuk yang hanya dapat dimengerti dengan menggunakan teknik enkripsi. Enkripsi adalah teknik yang mengubah data menjadi bentuk yang tidak dapat dimengerti tanpa kunci yang tepat, sering kali menghasilkan data dengan panjang tetap[1]. Enkripsi mengubah Plain Text menjadi Cipher Text, yaitu data yang dirahasiakan.

Jurnal Informatika Teknologi dan Sains (JINTEKS)
E-ISSN : 2686-3359
Submit July 02, 2024 | Revised July 31, 2024 |
Accepted Agustus 05, 2024
Hal. 648-658
Vol. 6; No. 3
Agustus 2024

Plain Text adalah pesan asli yang diubah menjadi Cipher Text melalui proses enkripsi, dan pesan ini dapat dikembalikan ke bentuk awalnya dengan menggunakan kunci yang sesuai[3]. Algoritma AES dipilih karena keunggulannya dalam melakukan proses enkripsi dan dekripsi data menggunakan kunci dengan berbagai panjang, yakni 128 bit, 192 bit, dan 256 bit. Perbedaan panjang kunci ini mempengaruhi jumlah putaran (rounds) yang dilakukan dalam algoritma AES[4]. Algoritma Advanced Encryption Standard (AES) adalah suatu algoritma block chiper dan mempunyai sifat simetri yang menggunakan kunci simetri pada waktu proses enkripsi dan dekripsi[5].

Dengan menggunakan metode AES dengan blok 128 bit karena algoritma ini sulit dipecahkan secara efektif dan efisien. Hal ini disebabkan oleh pola acak yang sulit dianalisis secara matematis serta kemampuan operasional yang membutuhkan sedikit memori dan waktu komputasi yang cepat, memenuhi kebutuhan efisiensi[3]. Pada penelitian sebelumnya juga mengekrip file berupa docx, pdf, dan txt[1].

Dari hasil uraian diatas pentingnya mengamankan data agar tidak sembarang orang mampu mengakses data orang lain, Dengan pengaplikasian menggunakan algorirma AES 128 bit dan verifikasi dua langkah diharapkan mampu mengurangi risiko serta meningkatkan keamanan data yang akan di amankan.

TINJAUAN PUSTAKA

Penelitian Terdahulu

Penelitian terdahulu mengenai penerapan enkripsi Advanced Encryption Standard (AES) untuk enkripsi dokumen telah banyak dilakukan oleh berbagai peneliti di Indonesia. Salah satu penelitian yang dilakukan oleh Prameshwari dan Sastra (2018) menunjukkan bahwa implementasi algoritma AES-128 untuk enkripsi dan dekripsi file dokumen berhasil meningkatkan keamanan data secara signifikan pada berbagai jenis file seperti PDF, XLS, DOC, dan TXT (JOM FTI Budiluhur) (Senafti)[6]. Penelitian lainnya yang dilakukan oleh Arfiyan et al. (2022) di PT Caveo Biometric Security, menunjukkan bahwa algoritma AES-128 dapat memberikan perlindungan yang kuat terhadap dokumen perusahaan[7]. Penelitian ini menemukan bahwa AES-128 efektif dalam menjaga kerahasiaan data dengan waktu enkripsi yang relatif cepat, meskipun memerlukan sumber daya komputasi yang cukup besar untuk proses enkripsi dan dekripsi (Senafti). Selain itu, penelitian oleh Ignasius dan Yudha Sakti (2022) juga mendukung temuan sebelumnya dengan menunjukkan bahwa AES-128 mampu memberikan keamanan yang tinggi terhadap data sensitif di PT Gunung Geulis Elok Abadi. Penelitian ini menggunakan kombinasi algoritma AES dengan teknik lain seperti kompresi data Huffman untuk meningkatkan efisiensi dan keamanan enkripsi data (JOM FTI Budiluhur)[8].

Keamanan

Menurut standar keamanan jaringan dari organisasi internasional untuk standarisasi, keamanan komputer merujuk pada upaya melindungi perangkat keras, perangkat lunak, dan data dari sistem komputer agar tidak rusak, dimodifikasi, atau mengalami kebocoran keamanan[9]. Semua langkah ini dilakukan secara berurutan dengan urutan kebalikan dari proses enkripsi dalam AES. Proses inversi tersebut memiliki kepentingan dalam memastikan bahwa blok data yang telah terenkripsi dapat dikembalikan ke bentuk aslinya saat proses dekripsi dilakukan menggunakan kunci yang sama dengan saat proses enkripsi.

Kriptografi

Kriptografi berasal dari kata Yunani "Crypto" dan "Graphia". "Crypto" berarti menyembunyikan, sementara "Graphia" berarti ilmu. Kriptografi adalah ilmu yang melibatkan perlindungan pesan rahasia dan eksplorasi metode matematika untuk menjaga integritas, kerahasiaan, dan validitas data. Aspek-aspek ini adalah bagian dari keamanan informasi yang dikelola oleh seorang kriptografer[10]. Enkripsi, dekripsi, dan pembuatan kunci dalam teknik enkripsi asimetris membutuhkan komputasi yang lebih berat dibandingkan dengan enkripsi simetris, karena teknik ini melibatkan penggunaan bilangan-bilangan yang sangat besar[11].

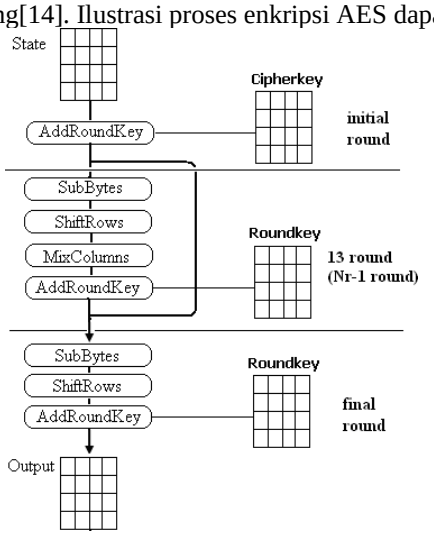
Enkripsi AES

Enkripsi adalah teknik yang mengubah pesan yang dapat dibaca (Plaintext) menjadi pesan acak yang tidak dapat dibaca tanpa kunci untuk mendekripsinya[12].

Advanced Encryption Standard (AES), sebuah algoritma kriptografi yang sangat andal untuk melindungi data, digunakan untuk melindungi data dengan enkripsi AES[13]. Dalam proses ini, kunci enkripsi digunakan untuk mengubah teks biasa (plaintext) menjadi bentuk teracak yang tidak dapat dibaca atau diuraikan. AES mengubah data ke dalam blok-blok yang teracak dengan panjang kunci yang berbeda, seperti 128-bit, 192-bit, atau

Jurnal Informatika Teknologi dan Sains (JINTEKS)
E-ISSN : 2686-3359
Submit July 02, 2024 | Revised July 31, 2024 |
Accepted Agustus 05, 2024
Hal. 648-658
Vol. 6; No. 3
Agustus 2024

256-bit. Tanpa menggunakan kunci dekripsi yang tepat, enkripsi AES membuat informasi sulit untuk diakses atau dipahami oleh pihak yang tidak berwenang[14]. Ilustrasi proses enkripsi AES dapat dilihat pada gambar 1.



Gambar 1. Enkripsi AES[15]

Transformasi

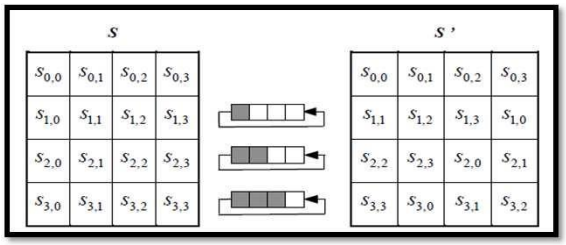
Dalam enkripsi AES, transformasi terdiri dari beberapa tahap yang disebut "putaran", dan setiap putaran melibatkan prosedur khusus yang dimaksudkan untuk menjaga data aman. Empat operasi dasar termasuk dalam transformasi ini: SubBytes, ShiftRows, MixColumns, dan AddRoundKey3.

Transformasi SubBytes dalam AES adalah proses substitusi non-linear di mana setiap byte dalam blok data digantikan dengan byte baru yang ditentukan oleh tabel substitusi yang telah ditetapkan, dikenal sebagai S-Box. S-Box ini dirancang untuk menyediakan substitusi yang aman terhadap serangan diferensial dan linier[16]. Menurut penelitian oleh Daemen dan Rijmen (1999), S-Box dibentuk berdasarkan inversi dalam medan Galois GF(2^8), diikuti oleh transformasi afine untuk meningkatkan kompleksitas non-linearitas. Yang dapat dilihat pada gambar 2.

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
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	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	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 2. Tabel S-Box[15]

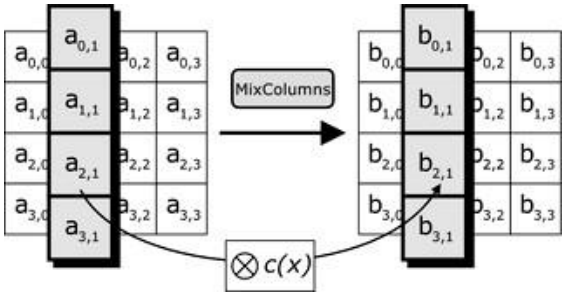
Transformasi ShiftRows dalam AES adalah proses penggeseran byte dalam setiap baris dari matriks state. Pada transformasi ini, byte dalam baris pertama tetap tidak berubah, byte dalam baris kedua digeser satu posisi ke kiri, byte dalam baris ketiga digeser dua posisi ke kiri, dan byte dalam baris keempat digeser tiga posisi ke kiri. Penelitian oleh Daemen dan Rijmen (2002) menunjukkan bahwa transformasi ini bertujuan untuk menghilangkan simetri, sehingga memperkuat keamanan terhadap serangan korelasi statistika[3].



Gambar 3. Proses ShiftRows[15]

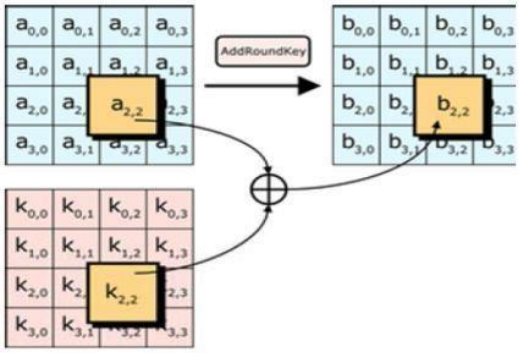
Jurnal Informatika Teknologi dan Sains (JINTEKS)
E-ISSN : 2686-3359
Submit July 02, 2024 | Revised July 31, 2024 |
Accepted Agustus 05, 2024
Hal. 648-658
Vol. 6; No. 3
Agustus 2024

Transformasi MixColumns dalam AES adalah operasi linier yang diterapkan pada setiap kolom dari matriks state. Transformasi ini melibatkan perkalian matriks kolom dengan matriks tetap dalam GF(2^8)[3]. Penelitian oleh Rijmen et al. (2000) mengungkapkan bahwa operasi ini meningkatkan difusi dengan mencampurkan byte dalam setiap kolom, sehingga memastikan bahwa perubahan satu byte dalam input mempengaruhi seluruh kolom output setelah beberapa putaran.



Gambar 4. Proses MixColumns[15]

Transformasi AddRoundKey dalam AES adalah proses penambahan eksklusif (XOR) antara blok data (state) dengan kunci ronde yang berasal dari kunci enkripsi utama. Menurut studi oleh FIPS-197 (2001), transformasi ini berfungsi untuk menggabungkan kunci enkripsi dengan data secara langsung, memastikan bahwa setiap putaran transformasi dipengaruhi oleh kunci yang berbeda, sehingga memperkuat keamanan keseluruhan algoritma[3].



Gambar 5. Proses AddRoundKey[15]

Blok data akan melewati langkah-langkah ini berulang kali setelah beberapa putaran hingga mencapai tingkat enkripsi yang ditetapkan, yang bergantung pada panjang kunci yang digunakan (128).

Verifikasi 2 Langkah

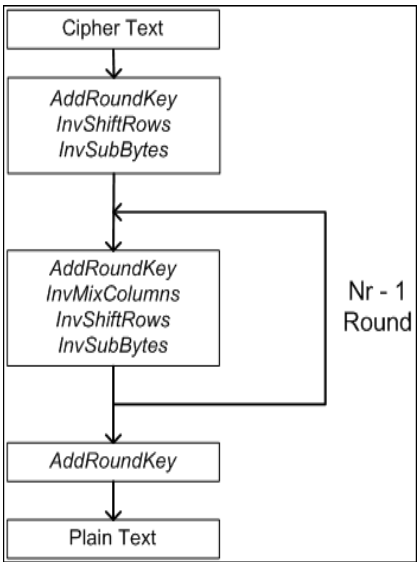
Verifikasi dua langkah adalah teknik keamanan yang memerlukan verifikasi dua langkah yang berbeda untuk mengakses akun atau sistem. Prinsipnya adalah untuk menambahkan lapisan keamanan tambahan di luar. Otentikasi sangat penting dalam keamanan karena memberikan kontrol akses yang unik, yang diperlukan untuk menjaga keamanan dalam berbagai aplikasi[17].

Metode ini memastikan bahwa pengguna memverifikasi identitas mereka melalui dua cara yang berbeda, yang menghalangi orang yang tidak sah untuk mengakses akun atau sistem, bahkan jika mereka berhasil. Dengan otentikasi dua faktor menawarkan tingkat perlindungan yang lebih tinggi dengan menggabungkan lebih dari satu metode otentikasi untuk mengamankan data, dari pada hanya menggunakan satu faktor otentikasi saja[18].

Dekripsi AES

Dekripsi AES adalah kebalikan dari enkripsi; itu adalah proses mengembalikan data yang telah dienkripsi ke bentuk aslinya (plaintext) dengan menggunakan kunci dekripsi yang tepat. Proses dekripsi ini melibatkan sejumlah tindakan yang berbeda dari langkah-langkah enkripsi, tetapi dilakukan dalam urutan yang berlawanan. proses sebaliknya, mengubah ciphertext kembali menjadi teks biasa, seharusnya disebut sebagai "mendekripsi" (decipher)[14]. Algoritma dekripsi dapat dijelaskan melalui skema

Jurnal Informatika Teknologi dan Sains (JINTEKS)
E-ISSN : 2686-3359
Submit July 02, 2024 | Revised July 31, 2024 |
Accepted Agustus 05, 2024
Hal. 648-658
Vol. 6; No. 3
Agustus 2024



Gambar 6. Deskripsi AES[15]

Proses yang biasa digunakan untuk dekripsi AES adalah sebagai berikut:

Adakan Kunci Ronde: Ini adalah prosedur yang menggabungkan XOR antara setiap byte dalam blok data dengan kunci ronde yang dibuat dari kunci utama.

InverseMixColumns adalah operasi yang memungkinkan pengembalian struktur data asli dengan menggunakan perhitungan matematis untuk kolom-kolom dalam blok data.

InverseShiftRows: Prosedur ini mengubah baris dalam blok data dan mengembalikan urutan aslinya sebelum enkripsi.

Tabel substitusi yang terbalik digunakan untuk menggantikan setiap byte dalam blok data dengan byte asli.

Dekripsi AES menggunakan rangkaian operasi.

Inversi

Dalam algoritma Advanced Encryption Standard (AES), proses inversi dilakukan secara bertahap dengan tujuan mengembalikan blok data terenkripsi (ciphertext) ke bentuk aslinya (plaintext) selama proses dekripsi. Beberapa inversi AES:

Transformasi Inverse AddRoundKey dalam AES adalah proses penambahan eksklusif (XOR) antara blok data yang telah dienkripsi dengan kunci ronde yang sama yang digunakan dalam proses AddRoundKey. Menurut FIPS-197 (2001), karena XOR adalah operasi yang dapat dibalik, transformasi ini mengembalikan blok data ke keadaan sebelum penambahan kunci ronde, memastikan bahwa data asli dapat dipulihkan selama proses dekripsi[19].

Transformasi Inverse MixColumns adalah operasi matematika yang digunakan untuk mengembalikan kolom-kolom dalam matriks state ke keadaan sebelum transformasi MixColumns. Operasi ini melibatkan perkalian setiap kolom dengan matriks invers tetap dalam GF(2^8). Penelitian oleh Rijmen et al. (2000) menunjukkan bahwa operasi ini memastikan bahwa difusi yang dihasilkan selama MixColumns dapat dihilangkan dengan benar, memungkinkan pemulihan data asli[19].

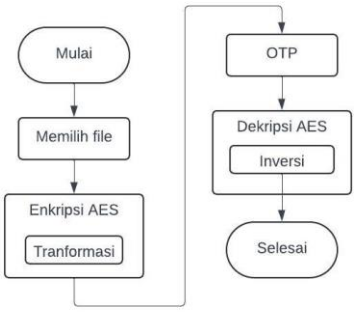
Transformasi Inverse ShiftRows adalah kebalikan dari proses ShiftRows dalam AES. Pada transformasi ini, byte dalam setiap baris dari matriks state digeser kembali ke posisi semula. Baris pertama tetap tidak berubah, baris kedua digeser satu posisi ke kanan, baris ketiga digeser dua posisi ke kanan, dan baris keempat digeser tiga posisi ke kanan. Menurut Daemen dan Rijmen (2002), transformasi ini bertujuan untuk mengembalikan distribusi byte yang telah diacak selama proses ShiftRows, sehingga memungkinkan proses dekripsi yang benar[20].

Proses Inverse SubBytes dalam Advanced Encryption Standard (AES) adalah kebalikan dari transformasi SubBytes, di mana byte yang telah digantikan oleh S-Box selama enkripsi digantikan kembali oleh invers S-Box. Invers S-Box ini dirancang untuk mengembalikan byte yang telah diubah selama proses SubBytes dengan cara yang aman dan efisien. Menurut penelitian oleh Daemen dan Rijmen (2002), invers S-Box ini juga dibentuk berdasarkan inversi dalam medan Galois GF(2^8), namun dengan transformasi afine yang berbeda untuk memastikan keamanan terhadap serangan diferensial dan linier yang sama efektifnya dengan proses S-Box asli[20].

METODE

Pada penelitian ini terdapat beberapa tahap dalam alur eksperimen yang ditunjukan pada gambar 1.

Jurnal Informatika Teknologi dan Sains (JINTEKS)
E-ISSN : 2686-3359
Submit July 02, 2024 | Revised July 31, 2024 |
Accepted Agustus 05, 2024
Hal. 648-658
Vol. 6; No. 3
Agustus 2024



Gambar 7. Alur Penelitian

Memilih file

Sample data yang digunakan dalam penelitian ini berupa KTP yang bersifat rahasia. Dengan ekstensi PDF. Dimana dalam penelitian ini data yang di enkripsi merupakan binary file pdf. Berikut binary file pdf yang belum di enkripsi pada table 1.

Table 1 Potongan binari file pdf yang belum di enkripsi

```
%PDF-1.3
%
3 0 obj
<< /Filter /FlateDecode /Length 92 >>
stream
x+TT(T H-JN-()M Q( ──────────────────────────────────────────────────────────────
 Z *
```

Proses Enkripsi AES

Pada proses enkripsi, digunakan algoritma Advanced Encryption Standard (AES), sebuah standar enkripsi kriptografis yang kuat dan terpercaya. Algoritma ini memiliki tingkat keamanan yang tinggi dan telah diadopsi secara luas dalam berbagai aplikasi keamanan. Dalam implementasinya, digunakan blok 128 bit yang merupakan ukuran standar untuk AES. Selain itu, metode Cipher Block Chaining (CBC) digunakan sebagai mode operasi untuk memperkuat keamanan enkripsi dengan memasukkan vektor inisialisasi (IV) yang unik untuk setiap blok data. Kunci yang digunakan dalam proses enkripsi diatur oleh operator, dimana pengaturan kunci ini merupakan bagian krusial dalam keamanan sistem enkripsi yang digunakan[21].

Data Ter-Enkrip

Hasil dari proses enkripsi berupa KTP dengan file pdf yang sudah terenkripsi.

Table 2. Potongan binari file pdf yang Telah di enkripsi dengan AES

```
l ──────────────────────────────────────────────────────────────
 3 h
  3 ( s+ f}          Z.
 {{@ e j*──────────────────────────   N(  P)" ~  !  cd < "l──────────────────────────
9\l>u
zJ
```

One Time Password

Pada tahap ini, OTP (One-Time Password) digunakan sebagai metode verifikasi yang memastikan identitas mahasiswa yang mengakses sistem. OTP adalah kode yang hanya dapat digunakan sekali dan memiliki panjang 6 digit dengan durasi waktu 300 detik, yang dihasilkan secara dinamis oleh sistem pada setiap percobaan akses. Selain itu, dalam proses verifikasi, kunci rahasia tambahan juga diterapkan untuk memvalidasi identitas pihak yang bersangkutan. Kunci rahasia ini hanya diketahui oleh sistem dan pihak yang berhak mengakses, sehingga memperkuat keamanan proses verifikasi. Dengan kombinasi OTP dan kunci rahasia, sistem dapat memastikan

Jurnal Informatika Teknologi dan Sains (JINTEKS)
E-ISSN : 2686-3359
Submit July 02, 2024 | Revised July 31, 2024 |
Accepted Agustus 05, 2024
Hal. 648-658
Vol. 6; No. 3
Agustus 2024

bahwa akses hanya diberikan kepada pihak yang benar-benar berwenang, sehingga menjaga keamanan dan integritas dari data dan informasi yang diakses.

Cara bagaimana OTP dihasilkan oleh token. Biarkan t_0 menjadi suatu waktu awal dan A_0 menjadi nilai awal. Misalkan t_{i-1} menjadi waktu pembuatan OTP ke-(i - 1) dan biarkan A_{i-1} menjadi bilangan bulat tambahan. Kedua nilai t_{i-1} dan A_{i-1} disimpan oleh token sebelum pasangan berikutnya dihitung. OTP berikutnya yang a_i , X_i dihasilkan pada waktu t_i , $i \geq 1$ tabel 3.

Table 3. Kombinasi 6 digit dengan interval waktu acak

i	sisir.	ti - ti-1	$\frac{ti-ti-1}{64}$	ai - ai-1 mod 10	$f(ti, ti-1)$
0	565201				
1	057045	6:00	5,6	5	5
2	031320	10:01	9,10	0	10
3	317587	3:11	2,3	3	3
4	291277	10:05	9,10	9	9
5	433132	2:15	2,3	2	2
6	911213	5:08	4,5	5	5
7	041125	1:17	1,2	1	1
8	319430	2:26	2,3	3	3
9	253057	10:16	9,10	9	9
10	987234	7:31	7,8	7	7
11	398564	3:49	3,4	4	4
12	070423	7:32	7,8	7	7
13	216702	1:43	1,2	2	2
14	542368	3:29	3,4	3	3
15	914109	4:35	4,5	4	4
16	293821	3:28	3,4	3	3
17	348346	1:05	1,2	1	1
18	913123	5:39	5,6	6	6
19	611331	8:10	7,8	7	7
20	501416	9:37	9,10	9	9

Dimana a_i adalah digit paling kiri OTP dan X_i adalah kombinasi dari 5 digit, sehingga secara keseluruhan menjadi 6 digit. Fungsi E_K didasarkan pada algoritma enkripsi yang bergantung pada kunci rahasia.

Proses Dekripsi AES

Dalam proses dekripsi, file yang telah terenkripsi diinput ke dalam suatu algoritma dekripsi bersama dengan kunci yang diberikan oleh operator kepada mahasiswa yang berwenang. Kunci ini merupakan kunci rahasia yang dibutuhkan untuk mengembalikan dokumen ke keadaan aslinya. Melalui algoritma dekripsi yang sesuai, dokumen terenkripsi tersebut diubah ke bentuk semula yang dapat dibaca dan dipahami. Dengan menggunakan kunci yang benar, file transkrip kembali ke keadaan semula, sehingga mahasiswa dapat dengan mudah mengakses informasi yang terdapat pada file transkrip tersebut. Proses dekripsi ini memastikan bahwa mahasiswa hanya mendapatkan akses ke dokumen dengan izin yang diberikan.

Dekripsi KTP

Pada tahap ini menghasilkan hasil dekripsi berupa file KTP berbentuk pdf sudah kembali seperti file semula.

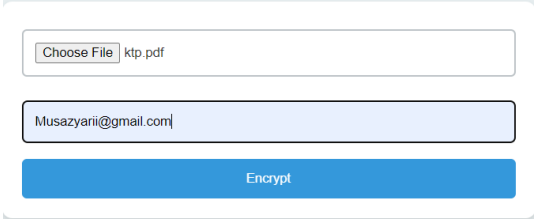
Table 4. Potongan binari file pdf yang Telah di dekripsi kembali dengan AES

```
%PDF-1.3
%
3 0 obj
<< /Filter /FlateDecode /Length 92 >>
stream
x+TT(T H-JN-()M Q( ──────────────────────────────────────────────────────
 Z *
```

Jurnal Informatika Teknologi dan Sains (JINTEKS)
E-ISSN : 2686-3359
Submit July 02, 2024 | Revised July 31, 2024 |
Accepted Agustus 05, 2024
Hal. 648-658
Vol. 6; No. 3
Agustus 2024

HASIL DAN PEMBAHASAN

Form Enkripsi adalah halaman di mana user dapat melakukan enkripsi terhadap file. Pada layar form enkripsi, terdapat beberapa bagian yang harus diisi, seperti unggah file yang akan dienkripsi dan alamat email tujuan. Tampilan layar form enkripsi ini dapat dilihat pada Gambar 8.



Gambar 8. Input File Dan Alamat Email

Pada gambar 9 merupakan tampilan bahwa enkripsi berhasil dilakukan, yang dimana pada halaman berikut terdapat tulisan yang bertuliskan here berwarna biru yang apabila ditekan akan secara otomatis mendownload file yang sudah ter-enkripsi.

Gambar 9. Tampilan Sesudah Dienkripsi

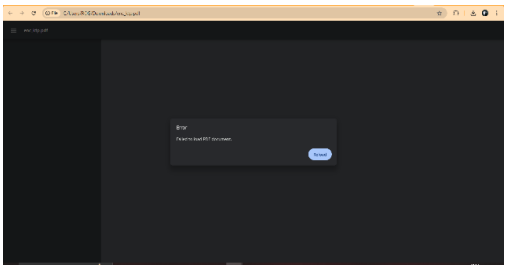
Tabel 5 menunjukkan file binary PDF yang telah dienkripsi menggunakan algoritma AES-128, teknik enkripsi yang menggunakan kunci sepanjang 128 bit. Enkripsi ini menggunakan metode simetris, di mana kunci yang sama digunakan untuk mengenkripsi (mengubah data menjadi bentuk yang tidak bisa dibaca) dan mendekripsi (mengembalikan data ke bentuk aslinya).

Table 5. Binary Enkripsi

```
��l�  ��3�h

����3�(�s+�f}���¬������������Z.

��{{@�e�j*  �N(���P)"�~��!��cd�<��"l 9\l>��u

zJ������Z���7�  ���S("DiU�И��7�b7#-Jf'j;5��Wķ�J�

���1�F�8��K���I�Fq�9��n��DL�|i�������H�&�P2_�u6L/�• AO[u0��ۃ��
l���4L���+�������f�r��愛ۃ$$>M���} K�II�¬`l���X�
'��0$da��• o`��1E�a?Kl���ZjV�
���}WL@�`��t□;• ⍰P{I⍰,��z��ᵌ⍰Ÿ%���44⍰a⍰⍰⍰⍰p⍰Tzv⍰9��
⍰⍰G⍰⍰⍰⍰.⍰⍰cQe⍰Au⍰+{ v# ⍰⍰T⍰9N⍰⍰⍰⍰⍰-⍰?B-⍰⍰t*+⍰⍰ ¬~⍰
⍰⍰F⍰⍰⍰|⍰W⍰⍰⍰⍰⍰B⍰5h⍰⍰=⍰rr⍰9⍰`⍰ez⍰⍰R⍰⍰pᵌÈ⍰Bc1O+⍰⍰KgG2

⍰
```

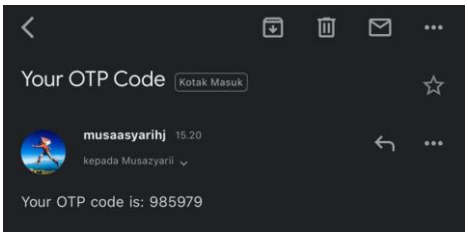
Pada gambar 10 menunjukan tampilan dari file apabila user membuka file yang sudah berhasil di enkripsi, yang bertulikskan “Failed to load PDF document” yang dimana file tersebut tidak bisa dibuka.

Jurnal Informatika Teknologi dan Sains (JINTEKS)
E-ISSN : 2686-3359
Submit July 02, 2024 | Revised July 31, 2024 |
Accepted Agustus 05, 2024
Hal. 648-658
Vol. 6; No. 3
Agustus 2024



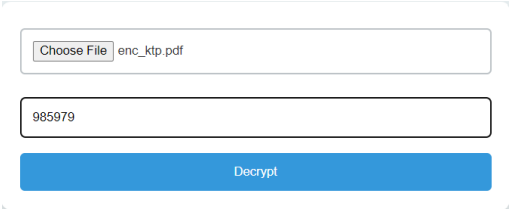
Gambar 10. Tampilan Hasil Enkripsi

Pada gambar 11 menunjukan kode One-Time Password (OTP) yang masuk kepada alamat yang dituju berdasarkan kunci rahasia (secret), dengan jumlah kode 6 digit , dan interval waktu (interval).



Gambar 11. Menerima OTP

Pada gambar 12 merupakan halaman untuk melakukan dekripsi akan menampilkan mengupload file enkripsi dan kode OTP sebanyak 6 digit yang sudah diterima, yang nantinya file dalam keadaan enkrip akan diproses untuk dekripsi file.

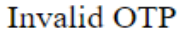


Gambar 12. Input File Dan OTP

Pada gambar 13 merupakan tampilan bahwa dekripsi berhasil dilakukan, yang dimana pada halaman berikut terdapat tulisan yang bertuliskan here berwarna biru yang apabila ditekan akan secara otomatis mendownload file yang sudah didekripsi.. Pastikan bahwa kode OTP yang dimasukan sesuai dengan kode yang sudah dikirimkan pada alamat email yang dituju agar tidak mengalami error.

Gambar 13. Tampilan Setelah Didekripsi

Gambar 14 menunjukkan halaman dengan pesan "Invalid OTP", yang muncul ketika pengguna memasukkan kode OTP yang tidak benar atau ketika masa berlaku kode OTP tersebut telah habis. Dalam tampilan ini, sistem menolak akses pengguna dikarenakan kode yang dimasukkan tidak valid, baik karena kesalahan input atau karena kode tersebut sudah kadaluarsa.



Gambar 14. Tampilan OTP Invalid

Tabel 5 menunjukkan file binary PDF yang telah didekripsi menggunakan algoritma AES-128, yang merupakan teknik dekripsi dengan kunci sepanjang 128 bit. Dekripsi ini menggunakan metode simetris, di mana kunci yang sama digunakan untuk mengenkripsi (mengubah data menjadi bentuk terenkripsi) dan mendekripsi (mengembalikan data ke bentuk aslinya).

Table 6. Binary Dekripsi

%PDF-1.3 %□□□□□□□□□□

Jurnal Informatika Teknologi dan Sains (JINTEKS)
E-ISSN : 2686-3359
Submit July 02, 2024 | Revised July 31, 2024 |
Accepted Agustus 05, 2024
Hal. 648-658
Vol. 6; No. 3
Agustus 2024

```
3 0 obj
<< /Filter /FlateDecode /Length 92 >>
stream
x+TT(T□H-JN-()M□Q(□
□Z□*□□□□□□□9□edl□gndh□□□□□□k□□□□jdf□glU
□`h□gfd□`h□Qh
Qu6□
endstream
endobj
1 0 obj
```

Gambar 16 menunjukkan tampilan layar ketika pengguna membuka file yang telah didekripsi, di mana file tersebut telah melewati proses dekripsi yang mengembalikan data dari bentuk terenkripsi ke bentuk aslinya. Pada tampilan ini, file yang sebelumnya tidak dapat dibaca karena dienkripsi, sekarang muncul dalam format aslinya tanpa perubahan, memungkinkan user untuk melihat dan mengakses informasi di dalamnya dengan normal.

Gambar 15. Tampilan File Yang Sudah Didekripsi

KESIMPULAN DAN SARAN

Penelitian ini menguraikan proses enkripsi dan dekrips menggunakan data berupa file KTP. Algoritma Advanced Encryption Standard (AES) dengan blok 128 bit dan mode Cipher Block Chaining (CBC) digunakan untuk mengenkripsi data, di mana kunci enkripsi diatur untuk menjaga keamanan. Dan dengan memasukan alamat email untuk nantinya akan dikirimkan kode OTP untuk membuka file yang akan di dekripsi. Hasil enkripsi berupa file PDF KTP yang terenkripsi. Dekripsi dilakukan dengan memasukan file yang terenkripsi atau terkunci lalu memsukan kode OTP sesuai dengan kode yang diberikan kepada pihak berwenang, mengembalikan dokumen ke bentuk asli yang dapat diakses. One-Time Password (OTP) digunakan sebagai metode verifikasi identitas, berupa kode 6 digit yang berlaku selama 300 detik. Proses ini memastikan hanya pihak yang berwenang dapat mengakses transkrip mereka untuk menjaga keamanan dan integritas data.

Berdasarkan hasil penelitian ini, adapun saran untuk meningkatkan metode pengelolaan kunci agar dapat lebih canggih seperti kunci asimetris untuk meningkatkan keamanan enkripsi dan dekripsi. atau mencoba mengubah metode verifikasi dua langkah dengan yang lebih mampu menjaga keamanan data. Juga dapat berfokus untuk mengubah isi file terenkripsi dan memastikan saat didekripsi isi file tersebut kembali ke kondisi sebelumnya.

DAFTAR PUSTAKA

[1] W. Putra, M. R. Fahlevi, and A. T. Hidayat, “Implementasi Algoritma Advanced Encryption Standard Untuk Kemanan Dokumen,” *... , Teknol. Dan Inf.*, vol. 1, no. 2, pp. 76–83, 2023, [Online]. Available: https://journal.grahamitra.id/index.php/jurikti/article/view/55%0Ahttps://journal.grahamitra.id/index.php/jurikti/article/download/55/181

[2] U. J. Soedirman, “JOPPAS: Journal of Public Policy and Administration SilampariVolume 4, Nomor 2, Juni 2023 DOI:,” vol. 4, pp. 80–88, 2023, doi: 10.31539/joppas.v4i2.6199.

[3] 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.

[4] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, “Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES),” *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, pp. 163–171, 2022, doi: 10.47709/jpsk.v2i01.1390.

[5] N. Cristy and F. Riandari, “Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan,” *J. Ilmu Komput. dan Sist. Inf.*, vol. 4, no. 2, pp. 75–85, 2021.

[6] A. Prameshwari and N. P. Sastra, “Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk

Enkripsi dan Dekripsi File Dokumen," pp. 52–58, doi: 10.30864/eksplora.v8i1.139.

[7] R. Firdaus and R. R. Santika, "PENERAPAN ALGORITMA AES-128 UNTUK ENKRIPSI DOKUMEN APPLICATION OF AES-128 ALGORITHM FOR DOCUMENT ENCRYPTION AT PT CAVEO BIOMETRIC SECURITY," no. September, pp. 111–120, 2022.

[8] E. Dokumen, G. Geulis, and E. Abadi, "Penerapan Algoritma AES (Advance Encryption Standart) 128 untuk," vol. 5, pp. 1–10, 2022.

[9] Z. Munawar, M. Kom, and N. I. Putri, "Keamanan Jaringan Komputer Pada Era Big Data," *J. Sist. Informasi-J-SIKA*, vol. 02, no. 01, pp. 14–20, 2020.

[10] Yusuf Ramadhan Nasution, Heri Santoso, and S. W. Amalia, "Penerapan Algoritma Vernam Dalam Mengamankan Dokumen Pdf," *J. Inform. dan Rekayasa Elektron.*, vol. 6, no. 1, pp. 37–46, 2023, doi: 10.36595/jire.v6i1.804.

[11] I. N. Purnama, "Implementasi Algoritma Enkripsi Rc5 Untuk Mengamankan Gambar Pada Perangkat Android," *J. Inform. dan Rekayasa Elektron.*, vol. 2, no. 2, p. 1, 2019, doi: 10.36595/jire.v2i2.108.

[12] N. Hapifa, "Seminar Nasional Teknologi Komputer & Sains (SAINTEKS) Enkripsi File Teks Menerapkan Algoritma Skipjack," pp. 429–437, 2020.

[13] S. R. Siburian, R. Alek, S. Sinaga, and F. Yudistira, "Kriptosistem Hybrid Menggunakan Kombinasi Aes Dan Rsa Untuk Enkripsi Teks Pesan," *J. JOCOTIS - J. Sci. Inform. Robot.*, vol. 1, no. 1, pp. 22–31, 2023, [Online]. Available: https://jurnal.ittc.web.id/index.php/jct/

[14] R. Primartha, "Penerapan Enkripsi dan Dekripsi File menggunakan Algoritma Advanced Encryption Standard (AES)," *J. Res. Comput. Sci. Appl.*, vol. 2, no. 1, pp. 13–18, 2013.

[15] M. Rinaldi, "No Title," *Kriptografi*, vol. 1, no. Kriptografi, p. 319, 2006.

[16] J. Daemen, J. Daemen, V. Rijmen, and V. Rijmen, "Authors : AES Proposal : Rijndael," no. December, 2012.

[17] S. Kaur, G. Kaur, and M. Shabaz, "A Secure Two-Factor Authentication Framework in Cloud Computing," *Secur. Commun. Networks*, vol. 2022, 2022, doi: 10.1155/2022/7540891.

[18] A. Dmitrienko, C. Liebchen, C. Rossow, and A.-R. Sadeghi, "Security analysis of mobile two-factor authentication schemes," *Intel Technol. J.*, vol. 18, no. 4, pp. 138–161, 2014, [Online]. Available: http://ezproxy.library.capella.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=iih&AN=97377858&site=ehost-live&scope=site

[19] K. A. Mckay and D. A. Cooper, "Withdrawn NIST Technical Series Publication," no. 2001, pp. 27–28, 2019.

[20] J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*. 2002. doi: 10.1007/978-3-662-04722-4.

[21] A. Sudrajat, Y. H. Prasetyo, and M. Kusumawardani, "Implementasi Enkripsi Advanced Encryption Standard (AES-128) Mode Cipher Block Chaining (CBC) sebagai Keamanan Komunikasi Pergerakan Robot Humanoid KRSBI," *J. Jartel J. Jar. Telekomun.*, vol. 11, no. 1, pp. 6–11, 2021, doi: 10.33795/jartel.v11i1.16.