PENGAMANAN MENGGUNAKAN ALGORITMA AES (ADVANCED ENCRYPTION STANDARD) DAN BCRYPT (BLOWFISH CRYPT) PADA FILE DOKUMEN

Ania Rahayu, Gunawan Abdillah, Herdi Ashaury
Program Studi Informatika, Universitas Jenderal Achmad Yani Cimahi
Jl. Terusan Jend. Sudirman, Cimahi, Jawa Barat, Indonesia
aniarahayu20@if.unjani.ac.id

ABSTRAK

Perkembangan teknologi dan informasi semakin memudahkan dalam mengakses data dan informasi serta memberikan dampak positif bagi masyarakat. Namun, hal ini juga meningkatkan kompleksitas pengelolaan informasi dan kejahatan dalam sistem informasi khususnya pada file dokumen. Proses transmisi informasi digital melalui Internet dan aplikasi perangkat lunak menjadi umum, memerlukan perlindungan data yang efektif terutama saat memproses data dalam jumlah besar. Manipulasi dokumen dapat merugikan, terutama dalam konteks kriminal dan penggunaan oleh pihak yang tidak berwenang. Penelitian ini bertujuan untuk membangun sistem keamanan pada file dokumen dan kunci simetris dengan mengkombinasikan kriptografi AES sebagai algoritma enkripsi dan Bcrypt sebagai algoritma hashing agar meningkatkan keamanan dokumen. Hasil yang diperoleh setelah melakukan beberapa percobaan dari penerapan enkripsi dan dekripsi menggunakan AES dan Bcrypt, maka diperoleh hasil bahwa isi file asli (plaintext) yang dienkripsi menggunakan AES-128 dan kunci simetris yang dihashing menggunakan Bcrypt dapat terenkripsi dengan baik, setelah file dokumen didekripsi akan kembali seperti data awal yang diinputkan. Waktu dari hasil uji enkripsi dan dekripsi dari delapan file bertipe .txt, .xlxs, .docx dan .pdf menunjukkan bahwa rata-rata waktu enkripsi adalah 1,5474 detik dan waktu dekripsi rata-rata 1,5934 detik, dengan ukuran file kurang dari 3MB relatif cepat. Ukuran file mempengaruhi lama proses enkripsi dan dekripsi berjalan, ukuran file setelah dienkripsi maupun didekripsi kembali ke ukuran awal. Hal ini menunjukkan algoritma AES dan Bcrypt berhasil diterapkan pada pengamanan file yang dilakukan dengan cara enkripsi sehingga hanya orang yang mengetahui kunci dapat mendekripsi agar file tersebut kembali seperti semula dan file tidak dapat dipahami oleh pihak yang tidak berhak atau yang tidak memiliki kunci.

Kata kunci : *Keamanan Informasi, AES, Bcrypt, Kriptografi, File Dokumen*

1. PENDAHULUAN

Perkembangan teknologi dan informasi mempermudah keterbukaan terhadap akses data dan informasi, efek positif pada masyarakat, termasuk dengan semakin mudah untuk mendapatkan data dan informasi yang kita butuhkan. Akibatnya bisa menjadi tolak ukur untuk menentukan jalan hidup seseorang. Tolok ukur ini dapat mengubah gaya hidup masyarakat yang menggunakan teknologi[2]. Informasi diberikan kepada satu pihak, dan diterima oleh pihak lain. Saat ini, informasi terutama dikirimkan atau dipertukarkan dalam format digital. Oleh karena itu, Internet dan aplikasi perangkat lunak seringkali berfungsi sebagai media penting untuk menyediakan dan menyimpan informasi tersebut. Namun, karena pengelolaan informasi melalui Internet dan aplikasi perangkat lunak menjadi lebih kompleks, kejahatan sistem informasi juga meningkat.

Sebagian besar data berisi informasi sensitif dan hanya dapat diakses oleh mereka yang terkena dampak. Pihak yang tidak bertanggung jawab dapat mengakses, menemukan, dan menyalahgunakan file yang berisi informasi penting. Pesatnya kemajuan teknologi modern juga bertepatan dengan perkembangan teknologi keamanan untuk melindungi data dari penyerang dalam hal integritas, kerahasiaan, perlindungan, privasi, dan langkah-langkah lain yang berkaitan dengan keamanan data itu sendiri[4]. Proses mengubah dokumen, gambar, atau video dari satu media ke media lain dikenal sebagai manipulasi atau penyuntingan. Pemalsuan adalah upaya untuk membuat sesuatu terlihat asli atau autentik dengan tujuan menyesatkan[4]. Bagi pengguna komputer, file dokumen saat ini banyak digunakan sebagai tempat penyimpanan data berupa file teks yang berisi informasi. Jenis file dokumen yang umum digunakan antara lain PDF (Portable Document Format), format dokumen Microsoft (docx, xls, pptx), dan banyak lagi. Namun format file dokumen saat ini belum memiliki keamanan yang memadai untuk menjamin kerahasiaan data tersebut. Oleh karena itu, perlu bagi pengguna untuk menambahkan sistem keamanan pada data file dokumen agar data tidak dapat dibuka, dibaca, atau dihapus[5].

Teknologi enkripsi adalah alat untuk memastikan keamanan data. Salah satu contoh bagaimana enkripsi memberikan fitur seperti kerahasiaan, keandalan, dan integritas data adalah algoritma kriptografi yang mengenkripsi atau mendekripsi data pribadi sehingga hanya penerima yang dimaksud yang dapat membacanya.[6]

Dalam melakukan pengamanan pada file dokumen diperlukan suatu teknik untuk memastikan kerahasiaan data dan keamanan informasi, seperti contoh kasus Tokopedia kebobolan data [6] Di mana data password mereka yang telah dihash menggunakan MD5 telah dipecahkan hashnya, karena MD5 sudah digunakan dan mudah dibobol. Lalu contoh penelitian

terdahulu yang dilakukan oleh Batubara[17] di mana ia menunjukkan bahwa Bcrypt mungkin tidak dapat diserang dengan brute force, kemudian penelitian yang dilaksanakan oleh Handoyo dan Subakti[1] menemukan bahwa mereka memiliki kemampuan untuk membuat situs web yang dilengkapi dengan algoritma AES yang dapat digunakan untuk mengamankan data dokumen. Kemudian terdapat penelitian yang dilakukan oleh Kumar dan Chaudhary[6] menggunakan Bcrypt dan AES sebagai sarana untuk melindungi datanya; datanya disimpan dalam daftar registry Windows yang membutuhkan password yang sesuai, yang kemudian dienkripsi menggunakan AES dan dihash menggunakan Bcrypt.

Melihat berdasarkan penelitian sebelumnya yang sudah dilakukan untuk mengamankan data dengan menggunakan MD5 [6], algoritma Bcrypt[17], algoritma AES [1], Kombinasi algoritma Bcrypt dan AES [6], algoritma AES dan Bcrypt telah terbukti efektif dalam menyediakan tingkat kemanan untuk melindungi data. Hal ini karena penelitian sebelumnya menunjukkan bahwa kecepatan enkripsi dan dekripsi AES masih lebih unggul daripada algoritma lain, algoritma AES dapat dijadikan salah satu alternatif untuk proses keamanan data dalam hal ini enkripsi dan dekripsi file dokumen[1]. Dan Algoritma Bcrypt membutuhkan waktu lama atau bahkan tak hingga supaya bisa ditembus dengan brute force[17].

Oleh karena itu, penelitian ini mengeksplorasi penggunaan dua kriptografi : Advanced Encryption Standard (AES) dan Blowfish Crypt (Bcrypt) dengan tujuan untuk membantu dalam pemahaman, mengimplementasikan, dan mengenkripsi file dokumen. Hal ini juga dapat memberikan kontribusi positif dalam pengembangan praktik keamanan file dokumen yang lebih baik di era digital yang penuh dengan tantangan serangan siber.

2. TINJAUAN PUSTAKA

2.1. Dokumen Digital

Informasi dapat ditransfer dari satu orang ke orang lain atau kelompok ke kelompok melalui dokumen. Dibuat, dikendalikan, dibuat, disimpan, didistribusikan, dan digandakan adalah semua contoh proses yang terlibat dalam dokumen. Dalam kehidupan sehari-hari, organisasi, dan bisnis, dokumen sangat penting.[13]

2.2. Kriptografi

Kriptografi adalah bidang yang mempelajari cara menyandikan data sehingga sulit dibaca atau dimengerti oleh pihak yang tidak berhak. Enkripsi adalah ketika seseorang mengirimkan pesan rahasia ke orang lain dan menggunakan sistem kode untuk mengidentifikasi penerima pesan sehingga pihak ketiga atau orang jahat seperti peretas tidak dapat memahami pesan tersebut. Berikut cara melakukannya. Misalnya, jika pihak ketiga, sistem itu sendiri mungkin mengganggu pengiriman pesan, Sebaiknya cegah agar pesan tidak jatuh ke tangan pihak ketiga sebelum dikirim agar mereka tidak dapat menebaknya. Oleh karena itu, diperlukan algoritma. Kriptografi awalnya digambarkan sebagai ilmu yang mempelajari cara menyembunyikan pesan.[8]

2.3. Hash

Fungsi hash dapat mengambil string dengan panjang apa pun dan mengubahnya menjadi string dengan panjang tetap, biasanya lebih kecil dari string yang diberikan. Fungsi hash adalah fungsi satu arah yang memiliki kemampuan untuk menghasilkan tanda tangan untuk data pengguna. Bahkan sedikit perubahan dapat mengubah keluaran fungsi hash.[9]

2.4. AES

Advanced Encryption Standard adalah algoritma kriptografi simetris yang menggunakan kunci simetris untuk melindungi data. Cipher key dari AES terdiri dari key dengan panjang 128 bit, 192 bit, atau 256 bit. Perbedaan panjang kunci akan mempengaruhi jumlah round yang akan diimplementasikan pada algoritma AES ini. Berikut ini adalah Tabel 1 yang memperlihatkan jumlah round/putaran (Nr) yang harus diimplementasikan pada masing-masing panjang kunci[12].

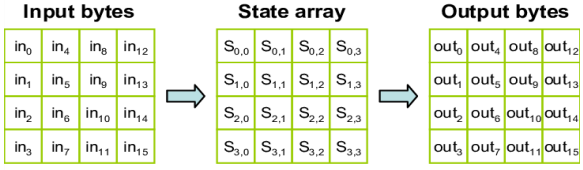
Tabel 1. Jumlah round/putaran (Nr)

Tipe	Jumlah Key (Nk)	Besar blok (Nb)	Jumlah round (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Elektronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), dan Output Feedback (OFB) adalah beberapa mode operasi yang dapat diterapkan pada algoritma kriptografi penyandi blok AES. Tentu saja, menggunakan mode operasi ECB, CBC, CFB, dan OFB memiliki kelebihan dan kekurangan dalam hal tingkat keamanan data yang dihasilkan. Algoritma kriptografi Rijndael, yang dikembangkan oleh Belgia Vincent Rijmen dan John Daemen, dinobatkan sebagai pemenang kompetisi.

Kriptografi pengganti algoritma DES yang dibuat oleh NIST, lembaga pemerintah AS, pada 26 November 2001. Advanced Encryption Standard diciptakan dari Algoritma Rijndael ini.[14]

AES umumnya digunakan untuk array byte dua dimensi yang disebut state. Saat enkripsi dimulai, data input in0, in2, in3, in4, in5, in6, in7, in8, in9, in10, in11, in12, in13, in14, dan in15 disalin ke dalam array state. State yang akan melakukan enkripsi dan dekripsi adalah state array yang memiliki ukuran NROWS X NCOLS. Selanjutnya, output akan dimasukkan ke dalam array keluar. Proses penyalinan dari byte input, state array, dan output ditunjukkan di sini[12]:



Gambar 1. Mapping of input bytes, State array and output bytes

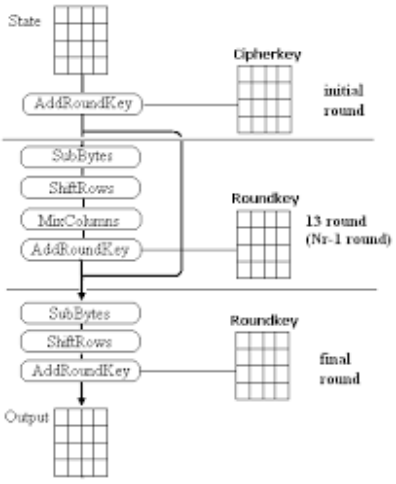
AES memiliki panjang kunci yang salah satunya adalah 128 bit, maka terdapat sebanyak 2128 = 3,4 x 1038 kemungkinan kunci. Algoritma Rijndael mempunyai 3 parameter :

a. In : larik yang berukuran 16-byte, yang berisi data masukan.
b. Out : larik yang berukuran 16-byte, yang berisi hasil enkripsi.
c. Key : larik yang berukuran 16-byte, yang berisi kunci chipering (chiperkey)

Dengan 16 byte, maka baik blok data dan kunci yang berukuran 128-bit dapat disimpan di dalam ketiga larik (128 = 16 x 8). Selama kalkulasi plainteks menjadi chiperteks, status data sekarang disimpan di dalam matriks dua dimensi, state, bertipe byte dan berukuran Nrows x Ncols. Untuk blok data 128- bit, ukuran state adalah 4 x 4.

2.5. Proses Enkripsi AES

Dalam algoritma AES, ada empat jenis transformasi byte: SubBytes, ShiftRows, Mixcolumns, dan AddRoundKey. Pada awal proses enkripsi, input yang dikopikan ke dalam state akan mengalami transformasi byte AddRoundKey. Kemudian, state akan mengalami transformasi SubBytes, ShiftRows, Mixcolumns, dan AddRoundKey sebanyak Nr. Proses ini dikenal sebagai function round dalam algoritma AES, dan bulat yang terakhir berubah menjadi bulat[21]. Ilustrasi proses enkripsi AES dapat digambarkan seperti pada gambar 2 berikut :



Gambar 2. Ilustrasi Enkripsi AES

a. AddRoundKey
Pada proses enkripsi dan dekripsi AES, proses AddRoundKey sama dan round key ditambahkan ke state menggunakan operasi XOR. Setiap round key terdiri dari Nb kata, setiap kata dijumlahkan ke kata atau kolom yang sesuai state sebagai berikut: [s'o,c , s'1,c , s'2,c , s'3,c] [so,c , s1,c , s2,c , s3,c] [wround*Nb+c] untuk 0≤c≤Nb [wi] adalah word dari key yang bersesuaian dimana i = round*Nb+c. Transformasi AddRoundKey pada proses enkripsi pertama kali pada round = 0 untuk round selanjutnya round = round + 1, pada proses dekripsi pertama kali pada round = 14 untuk round selanjutnya round = round - 1.

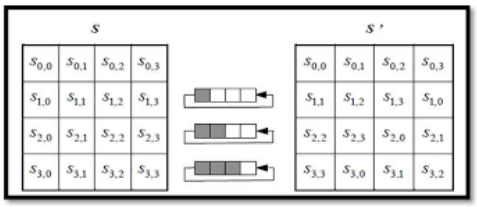
b. SubBytes
SubBytes merupakan transformasi byte dimana setiap elemen pada state akan dipetakan dengan menggunakan sebuah tabel subtitusi (S-Box). Gambar subtitusi S-Box akan dipaparkan dalam Gambar 3.

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 3. S-box subbytes (in hexadecimal format)

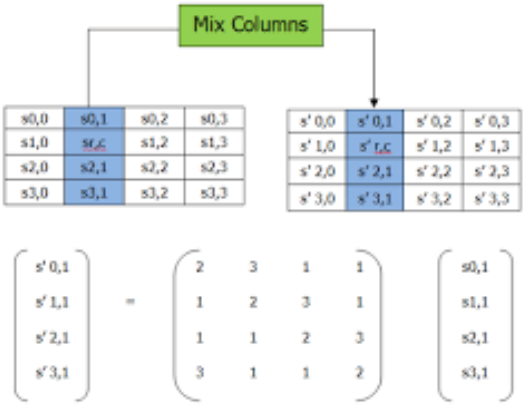
Untuk setiap byte pada array state, misalkan S[r,c]=xy, yang dalam hal ini xy adalah digit heksadesimal dari nilai S[r,c], maka nilai subtitusinya, dinyatakan dengan S[r,c], adalah elemen didalam tabel subtitusi yang merupakan pengaruh pemetaan byte pada setiap byte dan state.

c. ShiftRows
Lakukan ShiftRows pada hasil dari subtitusi SubBytes yang dieksekusi lewat pergeseran siklik secara memutar dengan geseran yang acak pada tiga baris terakhir state (baris pertama, r = 0, tidak digeser). Baris ke dua digeser secara siklik ke kiri sekali, baris ke tiga dua kali, dan baris ke empat tiga kali. Proses pergeseran Shiftrow ditunjukkan dalam Gambar 4.



Gambar 4. Transformasi shiftrows

d. Mix Columns
Yang terjadi saat MixColumn adalah mengalikan tiap elemen dari blokcipher dengan matriks. Pengalian dilakukan seperti perkalian matriks biasa yaitu menggunakan dot product lalu perkalian keduanya dimasukkan ke dalam sebuah blokcipher baru. Ilustrasi dalam Gambar 5 Menjelaskan mengenai bagaimana perkalian ini seharusnya dilakukan. Dengan begitu seluruh rangkaian proses yang terjadi pada AES telah dijelaskan dan selanjutnya adalah menerangkan mengenai penggunaan tiap-tiap proses tersebut.



Gambar 5. Perkalian matriks

2.6. Proses Dekripsi AES

Transformasi cipher dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan inverse cipher yang mudah dipahami untuk algoritma AES. Transformasi byte yang digunakan pada invers cipher adalah InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey.

a. InvShiftRows
   Pada transformasi InvShiftRows, dilakukan pergeseran bit ke kanan sedangkan pada ShiftRows dilakukan pergeseran bit ke kiri.
b. InvSubBytes
   Pada InvSubBytes, tiap elemen pada state dipetakan dengan menggunakan tabel Inverse S-Box.
c. InvMixColumns
   Setiap kolom dalam state dikalikan dengan matrik perkalian dalam AES. Contoh Perkalian dalam matrik dapat dituliskan seperti pada Gambar 6.

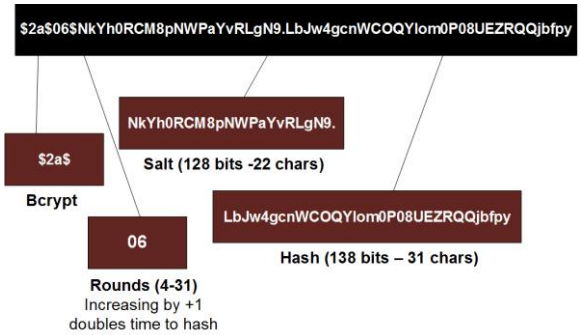
$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

Gambar 6. Contoh Perkalian matriks invmixcolumns

2.7. Bcrypt

Crypt dan Blowfish adalah nama fungsi hash yang digunakan pada sistem kata sandi UNIX. Pada awal pengembangannya di tahun 1976, Crypt hanya dapat menghapus empat buah kata sandi per detik, membuat fungsi hash Crypt cukup kuat.

Bcrypt mempunyai fase inisialisasi kunci yang berevolusi dari fase inisialisasi kunci enkripsi Blowfish dan disebut "eksblowfish", kependekan dari "skema kunci mahal Blowfish". Selain itu, Bcrypt menggunakan salt 128-bit secara default dalam proses hashing untuk mencegah serangan tabel pelangi. Langkah pertama adalah menginisialisasi key Exblowfish dengan parameter biaya yang diperlukan, nilai salt, dan password untuk hash[7].



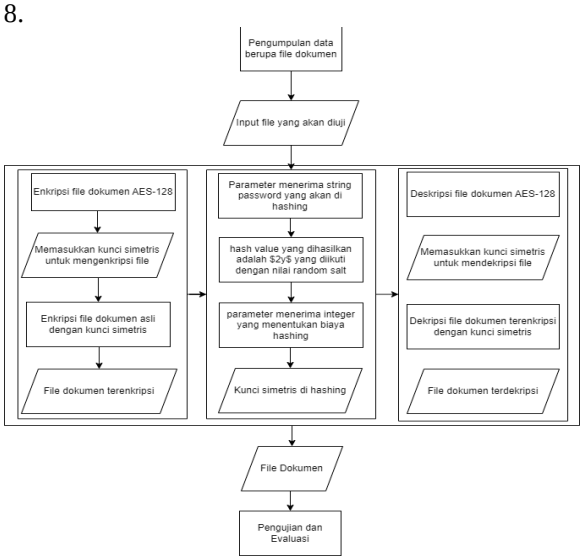
Gambar 7. BCrypt

Bcrypt adalah hash yang meningkatkan daya komputasi dan terus meningkatkan jumlah iterasi untuk memperlambat dan menahan serangan brute force dari dari waktu ke waktu, dicampur dengan garam untuk melindungi tabel rainbow dari kerusakan. Menurut Dukha, enkripsi Bcrypt terdiri dari tahapan berikut :

a. Array P dimulai dengan 18 iterasi (setiap nilai P adalah 32 bit;array P memiliki 18 kunci dan subkunci yang berukuran 32 bit).
b. Plaintext dienkripsi dalam 64 bit. Jika jumlah bit plaintextkurang dari 64 bit, akan ada biaya tambahan.
c. XL (32 bit pertama) dan XR (32 bit kedua) adalah nama untukhasil pencarian.
d. Gunakan operasi XL = XL xor Pi dan XR = F(XL) xor XRsetelah langkah 1-3 selesai.
e. Kemudian perlu mengubah hasil dari penggunaan operasi diatas. Dengan kata lain, ubah XL ke XR dan XR ke XL
f. XL dan XR melakukan operasi pertukaran pada iterasi 16setelah 16 operasi. Selesaikan operasi XR = XR xor P17 dan XL = XL xorP18 setelah mencapai proses ke 17[10]

3. METODE PENELITIAN

Sistem yang dibangun menggunakan dua metode kriptografi untuk mengamankan file dokumen. Diagram sistem ini dapat dilihat di sini pada Gambar 8.



Gambar 8. Alur Tahapan Penelitian

Tahap pertama yaitu pengumpulan data berupa file dokumen yang akan dienkripsi dengan ukuran file tidak melebihi dari 3 MB. Pada pengumpulan file dokumen yang dikumpulkan untuk dienkripsi berupa .docx, .pdf, .xlx dan .txt.

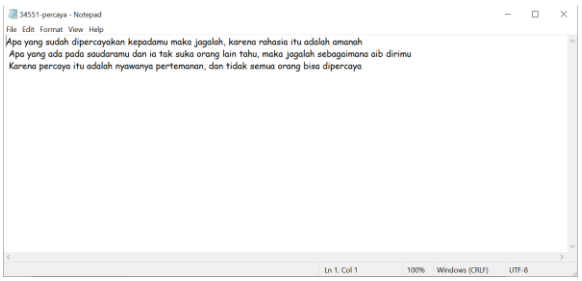
Tahap kedua yaitu masuk ketahapan proses enkripsi dan dekripsi file dokumen, untuk mengenkripsi dokumen menggunakan AES-128 dengan menginput file dan kunci simetris yang akan digunakan untuk mengenkripsi dan dekripsi. Setelah file terenkripsi, kunci yang digunakan untuk mengenkripsi file yaitu kunci simetris akan di hashing dengan menggunakan Bcrypt. Selanjutnya untuk mendekripsi file dokumen, harus memasukkan kunci simetris yang sebelumnya digunakan untuk mengenkripsi file maka file dokumen yang terenkripsi akan didekripsi dan dapat dibaca.

Tahap ketiga yaitu file yang sudah dienkripsi maupun didekripsi akan dilakukan pengujian dan evaluasi dari tahap yang sudah dilakukan sebelumnya, yaitu menguji setiap ukuran file dari file asli menjadi file yang dienkripsi dan didekripsi, dan menghitung rata-rata waktu yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi.

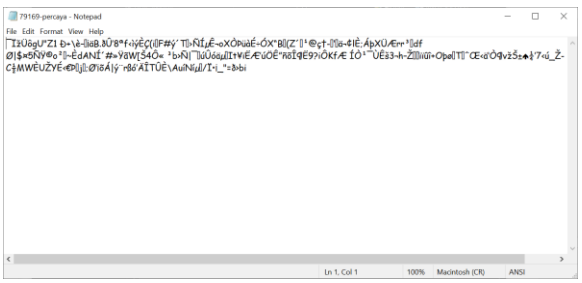
4. HASIL DAN PEMBAHASAN

Berikut ini merupakan hasil dari uji coba file plaintext dan file yang telah terenkripsi dengan menerapkan aplikasi yang telah memenuhi spesifikasi hardware dan software. File yang akan diuji adalah text, word, excel dan pdf. Hasil dari enkripsi menggunakan metode AES 128 bit berbentuk file dengan ekstensi *.rda, dimana file ini dapat dibuka menggunakan notepad. Hasil dari enkripsi ini berupa bilangan hexadecimal.

a. Tampilan file *txt yang asli (plaintext) dan yang telah dienkripsi dapat dilihat pada gambar – gambar berikut.

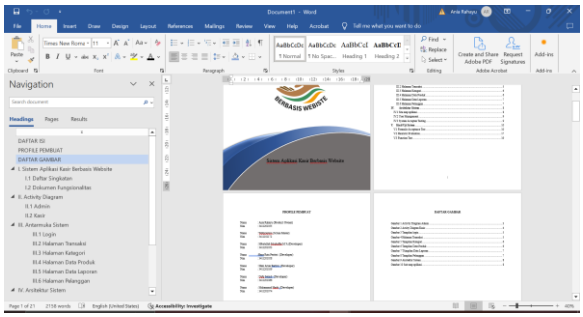


Gambar 9. File Plaintext Text

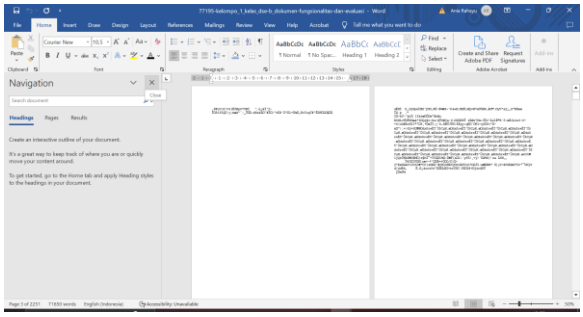


Gambar 10. File Ciphertext Text

b. Tampilan file *docx yang asli (plaintext) dan yang telah dienkripsi dapat dilihat pada gambar – gambar berikut.

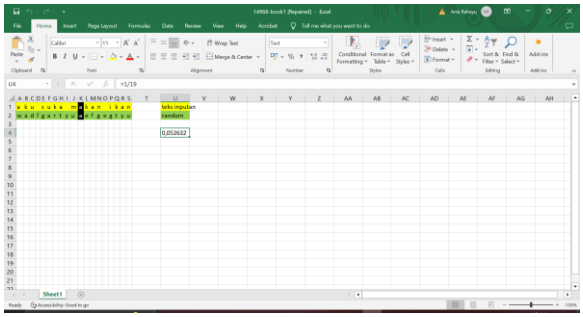


Gambar 11. File Plaintext Docx

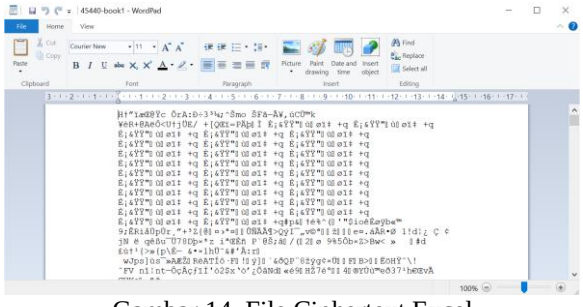


Gambar 12. File Ciphertext Docx

c. Tampilan file *xlsx yang asli (plaintext) dan yang telah dienkripsi dapat dilihat pada gambar – gambar berikut.

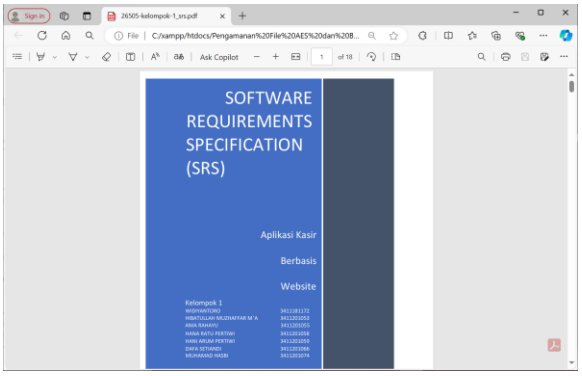


Gambar 13. File Plaintext Excel

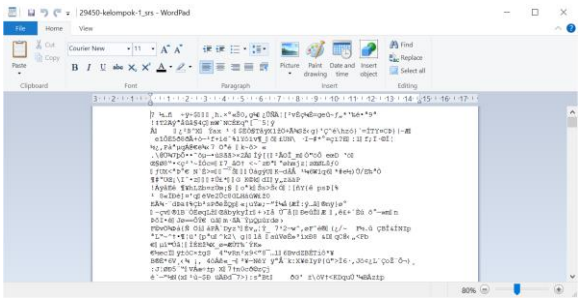


Gambar 14. File Ciphertext Excel

d. Tampilan file *pdf yang asli (plaintext) dan yang telah dienkripsi dapat dilihat pada gambar – gambar berikut.



Gambar 15. File Plaintext Pdf



Gambar 16. File Ciphertext Pdf

Berikut ini merupakan hasil dari uji coba password yang di hashing menggunakan BCrypt pada database.

file_name_finish	file_url	file_size	password
22488-_864-file-utama-naskah-2727-4561-10-20170807...	file_encrypt/22488-_864-file-utama-naskah-2727-456...	294.702	$2y$10$.7MgcrBgfN/eQGXa8DMEKuxbev550Jh3fsSloHjKSqM...
29450-kelompok-1_srs.rda	file_encrypt/29450-kelompok-1_srs.rda	302.086	$2y$10$qbBQeCmf9WiTz5w2Bs/bLO/YPOo8abxx18qWrNCmQrj...
77195-kelompo_1_kelas_dse-b_dokumen-fungsionalitas...	file_encrypt/77195-kelompo_1_kelas_dse-b_dokumen-f...	1353.94	$2y$10$dUKTFLWF.BtmRpVEuQyA./wtwuVfQrrp/n8mEUmgPl...
75717-id-cyberbullying-instagram.rda	file_encrypt/75717-id-cyberbullying-instagram.rda	32.9678	$2y$10$auf4.nNymL/bMmszZ6Sxn.Yur4KYgU8ni0bdWZ6p/uj...
13835-curhat.rda	file_encrypt/13835-curhat.rda	0.941406	$2y$10$kWlabvrpwrr/INtpW2X0b.eMVK0e6ZnDzUDnzV5xh/3...
79169-percaya.rda	file_encrypt/79169-percaya.rda	0.264648	$2y$10$FvOed7iYUdx4txHiHtavLO8TbxnnccIfmReI07VB6RB...
73744-paper-komputer-dan-masyarakat---kelompok-7-(...	file_encrypt/73744-paper-komputer-dan-masyarakat---...	120.925	$2y$10$ZqO6T3lSzy84IJ7BYJ39muF/Ibus2Clm88KQLVHQhtz...

Gambar 17. Hashing Password

Setelah aplikasi dipasang, pengujian dilakukan, dan hasilnya adalah file aslinya dan file yang telah dienkripsi dan sebaliknya. Tabel berikut menunjukkan hasil dari proses enkripsi dan dekripsi file yang dilakukan sistem dengan aplikasi.

a. Tabel Proses Enkripsi

Tabel 2. Proses Enkripsi

Nama Sebelum Enkripsi	Ukuran File Sebelum Enkripsi	Waktu Enkripsi	Nama Sesudah Enkripsi	Ukuran File Sesudah Enkripsi
26505-kelompok-1_srs.pdf	302 KB	2.9127 Detik	29450-kelompok-1_srs.rda	302 KB
17077-kelompo_1_kelas_dse-b_dokumen-fungsionalitas-dan-evaluasi.docx	1,32 MB	13.650 Detik	77195-kelompo_1_kelas_dse-b_dokumen-fungsionalitas-dan-evaluasi.rda	1,32 MB
id-cyberbullying-instagram.xlsx	32,9 KB	0.3848 Detik	75717-id-cyberbullying-instagram.rda	32,9 KB
34551-percaya.txt	271 bytes	0.1901 Detik	79169-percaya.rda	271 bytes
6366-paper-komputer-dan-masyarakat---kelompok-7-(1).pdf	120 KB	3.6772 Detik	73744-paper-komputer-dan-masyarakat---kelompok-7-(1).rda	120 KB
2.-manfaat-implementasi-e-estonia.docx	15,3 KB	0.6059 Detik	40950-2.-manfaat-implementasi-e-estonia.rda	15,3 KB
14968-book1.xlsx	9,26 KB	0.4395 Detik	45440-book1.rda	9,26 KB
93800-bersama.txt	222 bytes	0.1821 Detik	78031-bersama.rda	222 bytes

b. Tabel Proses Dekripsi

Tabel 3. Proses Dekripsi

Nama Sebelum Dekripsi	Ukuran File Sebelum Dekripsi	Waktu Dekripsi	Nama Sesudah Dekripsi	Ukuran File Sesudah Dekripsi
29450-kelompok-1_srs.rda	302 KB	3.0082 Detik	26505-kelompok-1_srs.pdf	302 KB
77195-kelompo_1_kelas_dse-b_dokumen-fungsionalitas-dan-evaluasi.rda	1,32 MB	13.227 Detik	17077-kelompo_1_kelas_dse-b_dokumen-fungsionalitas-dan-evaluasi.docx	1,32 MB
75717-id-cyberbullying-instagram.rda	32,9 KB	0.3747 Detik	id-cyberbullying-instagram.xlsx	32,9 KB
79169-percaya.rda	271 bytes	0.1877 Detik	34551-percaya.txt	271 bytes
73744-paper-komputer-dan-masyarakat---kelompok-7-(1).rda	120 KB	3.5604 Detik	73744-paper-komputer-dan-masyarakat---kelompok-7-(1).rda	120 KB
40950-2.-manfaat-implementasi-e-estonia.rda	15,3 KB	0.6095 Detik	2.-manfaat-implementasi-e-estonia.docx	15,3 KB
45440-book1.rda	9,26 KB	0.4336 Detik	14968-book1.xlsx	9,26 KB
78031-bersama.rda	222 bytes	0.1785 Detik	93800-bersama.txt	222 bytes

Hasil uji waktu dan ukuran delapan file menunjukkan waktu enkripsi dan dekripsi rata-rata 1,5474 detik dan 1,5934 detik, dengan waktu enkripsi kurang dari 3MB. Ukuran file juga mempengaruhi waktu enkripsi dan dekripsi, tetapi ukuran file setelah dienkripsi dan didekripsi kembali ke ukuran awal file.

5. KESIMPULAN DAN SARAN

Berdasarkan penelitian yang telah dilakukan, dapat disimpulkan beberapa hal. Advanced Encryption Standard (AES) berfungsi untuk mengenkripsi dan dekripsi file dokumen, sementara Blowfish Crypt (Bcrypt) berfungsi untuk menghashing kunci simetris. Hasil pengujian terhadap sistem diperoleh pengamanan file dokumen dapat digunakan dengan baik dan memenuhi pengaplikasian keamanan AES dan Bcrypt, yang mana di dalamnya terdapat fitur untuk menghasilkan kunci simetris dan fitur untuk mengamankan dokumen dengan enkripsi. Pengujian waktu dan ukuran delapan file dengan tipe format .docx, .pdf, .xlsx, dan .txt waktu yang digunakan untuk melakukan proses enkripsi dan dekripsi rata-rata 1,5474 detik dan 1,5934 detik, dengan waktu enkripsi kurang dari 3MB, berbanding lurus dengan ukuran file yang diproses (semakin kecil ukuran file yang diproses, semakin cepat proses enkripsi dan dekripsi dilakukan, semakin besar ukuran file yang diproses, semakin lama proses enkripsi dan dekripsi dilakukan). Ukuran file setelah dienkripsi dan didekripsi kembali ke ukuran awal file.

Saran untuk penelitian selanjutnya agar proses enkripsi dan penyisipan file pada aplikasi ini diharapkan ditingkatkan kinerjanya sehingga dapat mengamankan tipe file dokumen lainnya seperti file power point. Penelitian lebih lanjut dilakukan dengan mencoba algoritma lainnya seperti RSA, Serpent, dan Twofish serta algoritma hashing lainnya seperti SHA2-384 dan Scrypt.

DAFTAR PUSTAKA

[1] Handoyo, J., & Subakti, Y. M. (2020). Keamanan Dokumen Menggunakan Algoritma Advanced Encryption Standard (AES). *Jurnal SITECH : Sistem Informasi Dan Teknologi, 3(2)*, 143–152. doi:https://doi.org/10.24176/sitech.v3i2.5865.

[2] R. S. Giffary dan E. Ramadhani, "Implementasi Bcrypt dengan SHA-256 pada Password Pengguna Aplikasi Golek Kost," *Jurnal Sistem Komputer dan Informatika (JSON)*, vol. 3, no. 4, hlm. 543, Jun 2022, doi: 10.30865/json.v3i4.4285.

[3] G. D. M. Zulma, H. B. Seta, dan T. Yuniati, "Implementasi Algoritma Aes Dan Bcrypt Untuk Pengamanan File Dokumen," *Informatik : Jurnal Ilmu Komputer*, vol. 18, no. 2, hlm. 163, 2022, doi: 10.52958/iftk.v18i2.4667.

[4] S. Abdurrahman dan A. Prapanca, "Pengamanan File Dokumen Ujian Dengan Image Steganography Metode Lsb," *Journal of Informatics and Computer Science*, vol. 03, hlm. 186–192, 2021.

[5] S. Manullang, "Implementasi Kriptografi Pengamanan Data File Dokumen Menggunakan Algoritma Advanced Encryption Standard Mode Chiper Block Chaining," *Jurnal Nasional Teknologi Komputer*, vol. 3, no. 2, hlm. 87–95, 2023, doi: 10.61306/jnastek.v3i2.69.

[6] S. Budi, A. B. Purba, dan J. Mulyana, "Pengamanan File Dokumen Menggunakan Kombinasi Metode Subtitusi Dan Vigenere Cipher," *ILKOM Jurnal Ilmiah*, vol. 11, no. 3, hlm. 222–230, 2019, doi: 10.33096/ilkom.v11i3.477.222-230.

[7] M. R. A. S. Ilham Yusuf Alghani dan Universitas, "Penggunaan Teknik Bruteforce untuk Menentukan Keamanan setiap Kata Sandi Menggunakan Metode Kombinatorial," *UNNES Journal of Mathematics*, vol. 3, no. 3, hlm. 1–10, 2019.

[8] A. Thahara dan I. T. Siregar, "Implementasi Kriptografi untuk keamanan Data dan Jaringan menggunakan Algoritma DES," *Jurnal Rekayasa Teknologi Informasi (JURTI)*, vol. 5, no. 1, hlm. 31, 2021, doi: 10.30872/jurti.v5i1.5657.

[9] H. B. Seta, R. Yulistiani, dan T. Theresiawati, "Pengamanan Citra Digital Rekam Medis Menggunakan Perpaduan Hashing Algoritma Keccak Dan Rivest Code 6," *Jurnal Ilmiah Matrik*, vol. 22, no. 3, hlm. 257–269, 2020, doi: 10.33557/jurnalmatrik.v22i3.1077.

[10] G. Divva, M. Zulma, H. B. Seta, dan T. Yuniati, "Implementasi Algoritma AES Dan Bcrypt untuk Pengamanan File Dokumen".

[11] D. R. Kuhn, D. R. Wallace, and A. M. Gallo, "Software fault interactions and implications for software testing," *IEEE Trans. Softw. Eng.*, vol. 30, no. 6, pp. 418–421, 2004, doi: 10.1109/TSE.2004.24.

[12] P. Anggraeni, K. Aghistina & R. Lina. (2021). Implementasi Kriptografi dengan Algoritma Advanced Encryption Standard (AES) 128 Bit dan Steganografi menggunakan Metode End of File (EOF) Berbasis Java Desktop pada Dinas Pendidikan Kabupaten Tangerang. Applied Information System and Management (AISM). 3. 69-78. 10.15408/aism.v3i2.14722.

[13] H. Nando Winata *dkk.*, "Perancangan Aplikasi Pengamanan Dokumen Dengan Algoritma XXTEA," Online, 2019.

[14] F. Ahmad Sitorus, N. Budi Nugroho, U. Fatimah Sari Sitorus Pane, P. Studi Mahasiswa, S. Triguna Dharma, dan P. Studi Dosen Pembimbing, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Bit Untuk Keamanan Data Transaksi Penjualan Pada PT. Mitsubishi Electric Indonesia," 2020.

[Daring]. Tersedia pada: https://ojs.trigunadharma.ac.id/

[15] F. Syafaat dan A. Finandhita, "Implementasi Kriptografi AES-128 Pada Unmanned Aerial Vechile Dan Ground Control System."

[16] G. Divva, M. Zulma, H. B. Seta, dan T. Yuniati, "Implementasi Algoritma AES Dan Bcrypt untuk Pengamanan File Dokumen".

[17] Batubara, T. P. (2020). *Analisis Kinerja Algoritma Bcrypt Untuk Meningkatkan Keamanan Password Dari Brute Force*. Medan: Universitas Sumatera Utara.