JURIKOM (Jurnal Riset Komputer), Vol. 7 No. 99, Agustus 2020
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.3086/jurikom.v6i6.9999
Hal 999-999

JURIKOM (Jurnal Riset Komputer)
ISSN 2407-389X (media cetak), ISSN 2715-7393 (media online)
Sekretariat : STMIK BUDI DARMA | Jl. Sisingamangaraja No. 338, Medan, Sumatera Utara
Website: https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom
Email: jurikom.stmikbd@gmail.com

Medan, 20 September 2020

No : 192/STMIK-BD/P3M/LOA-JURIKOM/VIII/2020
Lamp : -
Hal : Surat Penerimaan Publikasi JURIKOM

Kepada Yth,
Bapak/Ibu **Suci Ramadani**
Di Tempat

Terimakasih telah mengirimkan artikel ilmiah untuk diterbitkan pada JURIKOM (Jurnal Riset Komputer) (pISSN 2407-389X / eISSN 2715-7393), dengan judul:

Judul : **Penerapan Algoritma AES dan DSA Menggunakan Hybrid Cryptosystem untuk Keamanan Data**

Penulis: **Suci Ramadani, Diana(*), Siti Sanda**

Berdasarkan hasil review dari reviewer, artikel tersebut dinyatakan DITERIMA untuk dipublikasikan pada **Volume 7, Nomor 4, Agustus 2020**

Sebagai informasi QR-Code untuk melihat link LOA Jurnal JURIKOM (Jurnal Riset Komputer), **Volume 7, Nomor 4, Agustus 2020** yang telah dikeluarkan.

Demikian informasi yang kami sampaikan, atas perhatiannya kami ucapkan terimakasih.

Hormat Kami,

Satrya Darma Nasution, M.Kom
P3M STMIK Budi Darma

Tembusan:
1. Ketua STMIK Budi Darma
2. Author
3. Files

JURIKOM (Jurnal Riset Komputer), Vol. 7 No. 99, Agustus 2020
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.3086/jurikom.v6i6.9999
Hal 999-999

Penerapan Algoritma AES dan DSA Menggunakan Hybrid Cryptosystem untuk Keamanan Data

Suci Ramadani[1], Diana[2,*], Siti Sauda[3]

[1] Fakultas Ilmu Komputer, Teknik Informatika, Universitas Bina Darma, Palembang, Indonesia
Email: [1]141420181@student.binadarma.ac.id , [2*]diana@binadarma.ac.id, [3]siti_sauda@binadarma.ac.id,
(Corresponding Author [2,*] : diana@binadarma.ac.id)

Abstrak

Pertukaran dokumen berbasis komputer seperti pertukaran pesan pada e-mail di internet sudah banyak dilakukan sebagai transaksi komersil. Walau terlihat praktis, namun banyak juga dampak negatif yang terjadi, salah satunya yaitu pesan yang dikirim bisa dibuka oleh siapa saja yang mempunyai akses masuk, sehingga dapat mengakibatkan informasi yang dikirimkan bisa disalahgunakan oleh oknum yang tidak bertanggungjawab. Untuk memastikan dokumen yang dikirimkan masih utuh atau otentik sampai di pihak yang dituju, salah satu cara yang dapat dilakukan yaitu menggunakan kriptografi. Dalam penelitian ini menerapkan kriptografi algoritma AES dan DSA. Algoritma AES merupakan algoritma kunci simetri yaitu proses enkripsi dan dekripsi menggunakan kunci yang sama sementara DSA merupakan algoritma kunci asimetri yaitu proses enkripsi dan dekripsi menggunakan kunci privat untuk enkripsi dan kunci publik untuk dekripsi. Kemudian ditambahkan algoritma hybrid untuk menggabungkan atau mengkombinasikan kedua algoritma AES dan DSA. Hasil dari penelitian ini berupa aplikasi Enkripsi Dekripsi dengan tingkat keberhasilan sebesar 86% untuk enkripsi file dan 83% untuk dekripsi file serta ukuran file setelah dienkripsi mengalami kenaikan sebesar 32% dan kembali keukuran semula pada saat dekripsi.

Kata Kunci : Kriptografi, AES, DSA, Hybrid Criptosystem

Abstract

Exchange of documents based on a computer such as exchanges of messages via email on the internet has been done as a commercial transaction. Although it looks practice but there are also so many negative impacts that occur. This is the message sent can be opened by anyone who has access to enter the email. So that it can lead irresponsible people to steal information of documents. To ensure the documents sent are authentic until the intended part, one way that can be done is to use cryptography. In this study applying cryptography of AES and DSA algorithms. AES algorithm is a symmetry key that is using the same key to process of encryption and decryption while DSA algorithm is an asymmetric key which is the process of encryption using a private key and using public key for decryption. Then use a hybrid algorithm to combine AES and DSA algorithm. The results of this study is an application of encryption and decryption with a success rate of 86% for file encryption and 83% for decryption. File size after encrypted has increased by 32% and return to its original size after decrypted.

Keyword : Cryptography, AES, DSA, Hybrid Criptosystem

1. PENDAHULUAN

Kejahatan dalam pencurian informasi yang belakangan ini marak terjadi dari berbagai kalangan. Salah satunya yaitu *hacker* yang dibantu pemerintahan Rusia dilaporkan telah mencuri dokumen sangat rahasia milik Badan Keamanan Nasional Amerika. Kemudian ada juga kejahatan yang sangat terkenal yang dilakukan oleh Wikileaks "dengan mengungkapkan dokumen-dokumen rahasia negara dan perusahaan kepada publik melalui situs web. Dokumen yang dibocorkan berupa data nasabah Bank Julius Baer, surel Sarah Palin, Video Helikopter Apache, perang Afganistan, Berkas Guantanamo, dokumen perang Irak, dan kawat diplomatik Amerika Serikat. Terkuaknya ribuan dokumen rahasia negara, terutama di Amerika Serikat menimbulkan kontroversi yang luar biasa. Maka dari itu perlu dilakukan pengamanan data atau dokumen agar informasi penting yang ada didalamnya terjaga kerahasiaanya dan terjaga keasliannya. Perlindungan informasi ini dapat dilakukan dengan menggunakan algoritma tertentu. [1] Pada perkembangan jaringan internet saat ini, keamanan data atau informasi merupkan hal yang sangat penting, terutama dalam hal keamanan pertukaran informasi. Upaya-upaya dilakukan dengan menggunakan algoritma yang diciptakan oleh banyak ahli, namun hal tersebut masih dapat dipecahkan oleh pihak yang tidak bertanggung jawab, maka dari itu perkembangan algoritma kriptografi semakin pesat dengan menjaga keamaanan data.

JURIKOM (Jurnal Riset Komputer), Vol. 7 No. 99, Agustus 2020
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.3086/jurikom.v6i6.9999
Hal 999-999

Kriptografi berasal dari bahasa Yunani, yakni *Kripto* dan *grafia*, kripto berarti *secret* (rahasia) dan *Grafia* berarti *writing* (tulisan). Menurut terminologinya kriptografi adalah ilmu seni untuk menjaga keamanan pesan yang dikirim dari satu tempat ke tempat lain. [2], kriptografi merupakan suatu ilmu sekaligus seni yang bertujuan untuk menjaga keamanan suatu pesan. Dalam perkembangannya kriptografi juga digunakan untuk mengidentifikasi pengiriman pesan tanda tangan digital dan keaslian pesan dengan sidik jari digital (*fingerprint.* Kriptografi adalah ilmu yang mempelajari teknis matematis yang berhubungan dengan aspek keamanan. Kriptografi merupakan *"secret writing"* yang berarti tulisan rahasia. Kelebihan yang didapat dengan menerapkan kriptografi yaitu informasi yang ada dienkripsi menjadi pesan rahasia yang hanya dapat dibuka oleh orang yang mempunyai kunci dekripsi pesan tersebut. Hal ini dapat mengurangi terjadinya pencurian informasi yang dilakukan oleh oknum-oknum yang tidak bertanggungjawab. [3] Peranan kriptografi merupakan sistem yang efektif dalam hal keamaan dan proteksi serta dapat digunakan secar luas di berbagai bidang usaha dan teknologi.

Kriptografi sendiri terbagi menjadi dua jenis, yaitu kriptografi kunci simetri dan kriptografi kunci asimetri. [4] Kriptografi kunci simetri merupakan algoritma yang menggunakan kunci enkripsi yang sama dengan kunci dekripsi. Salah satu contohnya yaitu algoritma AES (*Advanced Encryption Standard*). Keamanan algoritma simetri tergantung pada kuncinya. Apabila kuncinya diketahui orang lain, maka orang tersebut dapat mengenkripsikan dan mendekripsikan pesan.[5] algoritma AES dengan panjang kunci 256 bit dapat menyandikan isi suatu file sehingga dapat mengamankan file tersebut.[6] menyatakan bahwa implementasi algoritma AES pada proses enkripsi dapat merubah file ke bentuk yang tidak bisa dibaca dan file dapat kembali ke bentuk asli melalui proses deskripsi dengan menggunakan kunci yang sama dengan kunci pada proses enkripsi. [7] Algoritma AES merupakan proses algoritma yang cepat dan kuat, pada artikel ini dilakukan kombinasi algoritma AES dan XOR untuk pengamanan teks berbasis mobile, diperoleh fakta bahwa kombinasi kedua algoritma ini dapat mempercepat proses enkripsi dan deskripsi. [8], Algoritma AES menghasilkan kualitas enkripsi yang lebih baik dibandingkan dengan algoritma RSA. Algoritma AES memiliki tiga pilihan kunci yaitu tipe: AES-128, AES-192 dan AES-256. Masing-masing tipe menggunakan kunci internal yang berbeda yaitu *round key* untuk setiap proses putaran. Dalam penelitian ini, algoritma yang digunakan adalah algoritma AES-128 dengan proses putaran enkripsi dikerjakan sebanyak 10 kali (a=10), yaitu sebagai berikut: "

1. *AddRoundKey*: disebut juga dengan *initial round* tahap ini melakukan *XOR* antara *planiteks* dengan *chiper key*.
2. Putaran sebanyak a-1 kali, pada setiap putaran melakukan proses sebagai berikut:
   a. *SubBytes*: substitusi *byte* dengan menggunakan tabel substitusi (S-Box).
   b. *ShiftRows*: pergeseran baris-baris *array state* secara *wrapping*.
   c. *MixColumn*: mengacak data pada masing-masing kolom *array state*.
   d. *AddRoundKey*: melakukan *XOR* antara *state* dan *round key*.
3. *Final Round* merupakan proses putaran terakhir, meliputi *SubBytes, ShiftRows,* dan *AddRoundKey*.

Sedangkan pada proses dekripsi AES-128, proses putaran juga dikerjakan sebanyak 10 kali (a=10), yaitu sebagai berikut:

1. AddRoundKey
2. Putaran sebanyak a-1 kali, dimana pada setiap putaran proses: *InverseShiftRows, InverseSubBytes, AddRoundKey,* dan *InverseMixColumns.*
3. Final round, adalah proses untuk putaran terakhir yang meliputi *InverseShiftRows, InverseSubBytes,* dan *AddRoundKey.*"

Sedangkan kriptografi kunci asimetri yang sering disebut juga kriptografi kunci publik adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Pada kriptografi jenis ini, setiap orang berkomunikasi mempunyai sepasang kunci yaitu kunci privat dan kunci publik. Kunci privat digunakan untuk enkripsi pesan dan kunci publik digunakan untuk dekripsi pesan. Contohnya yaitu algoritma DSA (*Digital Signature Algorithm*). Pada Agustus 1991, NIST (*The National of Standard and Technology*) mengumumkan standar untuk tanda tangan digital yang dinamakan *Digital Signature Standard* (DSS) yang terdari dua komponen, yaitu sebagai berikut.

a. Algoritma tandatangan digital yang disebut DSA (*Digital Signature Algorithm*)
b. Fungsi Hash yang disebut SHA (*Secure Hash Algorithm*).

[9], DSA (*Digital Signature Algorithm*) Menggunakan Bahasa Pemrograman Java" DSA merupakan algoritma yang menggunakan fungsi hash SHA (*Secure Hash Algorithm*) untuk mengubah pesan menjadi intisari pesan yang berukuran 160 bit. DSA dan algoritma tanda tangan lainnya mempunyai tiga proses utama yaitu:

a. Pembangkitan pasangan kunci (*Key Pair Generation*)
b. Pembangkit tanda-tangan digital (*Digital Signautre Generation*)
c. Verifikasi tanda-tangan digital (*Digital Signature Verification*).

JURIKOM (Jurnal Riset Komputer), Vol. 7 No. 99, Agustus 2020
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.3086/jurikom.v6i6.9999
Hal 999-999

Dari kedua jenis algoritma di atas mempunyai kelebihan dan kekurangan masing-masing yaitu pada algoritma kunci simetri memiliki kelebihan waktu proses untuk enkripsi dan dekripsi yang relatif cepat. Hal ini disebabkan karena efisiensi yang terjadi pada pembangkit kunci namun pendistribusian kunci tidak aman karena kunci yang dipakai saat mengenkripsi dan dekripsi pesan sama. Sementara kelebihan dan kekurangan kriptografi kunci asimetri justru sebaliknya. [10], penggunaan metode simetris dan asimetris memiliki kelebihan dan kelemana, untuk itu sebaiknya diterapkan suatu metode yang menggabungkan kedua konsep sehingga didapat sistem keamanan data yang lebih baik. Pendistribusian kunci terbilang aman karena menggunakan kunci privat dan kunci publik namun waktu untuk enkripsi dan dekripsi pesan relatif lambat. Maka dari itu untuk mengatasi kelebihan dan kekurangan dari masing-masing algoritma digunakan metode *hybrid cryptosystem* yang merupakan gabungan antara kriptografi kunci simetri dan kriptografi kunci asimetri. Metode ini memanfaatkan dua tingkatan pengamanan informasi yaitu enkripsi dan dekripsi pesan menggunakan kunci simetri dan pemberian tanda tangan digital untuk melindungi kunci simetri. Kelebihan menggunakan metode *hybrid* ini bisa menggabungkan atau mengkombinasikan dua atau lebih algoritma untuk mengenkripsi dan dekripsi sehingga kelebihan dan kekurangan yang ada pada masing-masing algoritma dapat diatasi dan meningkatkan tingkat keamanan data.

2. METODE PENELITIAN

2.1 Data Penelitian

Data penelitian yang dipakai berupa file dokumen dengan ekstensi *.txt, *.docx, *.xlxs, *.ppt, dan *.pdf., data uji untuk masing-masing file dokumen sebanyak 25 data, sehingga keseluruhan data uji sebanyak 125 file dokumen.

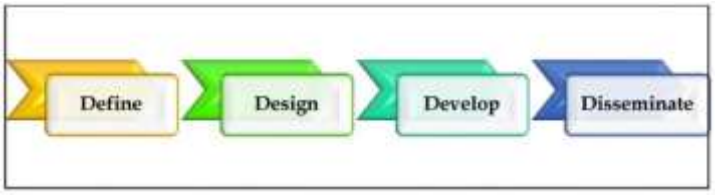
File ke	Ukuran File (Kb)				
	*.docx	*.txt	*.xlxs	*.pdf	*.pptx
1	627	2	29	2151	1421
2	16	5	29	109	319
3	809	1	73	234	317
4	13	1	46	290	285
5	126	4	11	193	355
6	861	4	16	361	329
7	687	2	23	481	122
8	580	1	23	448	475
9	119	2	14	1066	2111
10	322	4	14	233	605
11	450	2	13	29	345
12	232	3	12	27	233
13	545	4	15	233	342
14	565	5	16	231	555
15	383	1	23	435	123
16	117	1	39	343	34
17	34	4	23	466	444
18	67	3	42	233	345
19	234	2	23	234	453
20	234	3	47	439	444
21	324	3	23	244	123
22	14	1	39	543	476
23	567	1	29	123	554
24	119	3	32	458	654
25	165	2	11	454	122
Rata-Rata	**328,4**	**2,6**	**26,6**	**402,32**	**458,6**

Tabel 1. Data Penelitian

2.2. Langkah Penelitian

Penelitian ini menghasilkan sebuah aplikasi, tahapan pengembangan aplikasi mengadopsi pendekatan pengembangan *four-D model* (model 4-D). Menurut Ada 4 tahapan yang dilakukan, yakni : tahap pendefinisian (*define*), tahap perancangan (*design*), tahap pengembangan (*develop*), dan tahap uji coba (*disseminate*).

JURIKOM (Jurnal Riset Komputer), Vol. 7 No. 99, Agustus 2020
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.3086/jurikom.v6i6.9999
Hal 999-999



Gambar 1. Pengembangan Model 4D Thiagajaran

Pada tahapan pendefinisian dilakukan analisis keadaan dan pendefinisian masalah. Pada tahapan perancangan dilakukan perancangan algoritma AES dan DSA. Pada tahapan pengembangan dilakukan pengembangan aplikasi. Pada tahapan uji coba dilakukan ujicoba untuk 125 data uji dengan melihat tingkat keberhasilan proses enkripsi dan tingkat keberhasilan proses enkripsi, selain itu juga dilihat perubahan ukuran file sebelum proses enkripsi dan setelah proses enkripsi.

3. ANALISA DAN PEMBAHASAN

Hasil penelitian ini adalah aplikasi Enkrip Dekrip dengan menerapkan algoritma AES dan DSA menggunakan metode *hybrid cryptosystem*. Perangkat lunak yang dihasilkan terdiri dari tiga proses inti yaitu proses generate key, proses enkripsi dan proses dekripsi. Berikut penjelasan dari masing-masing proses.

3.1 Proses *Generate Key*

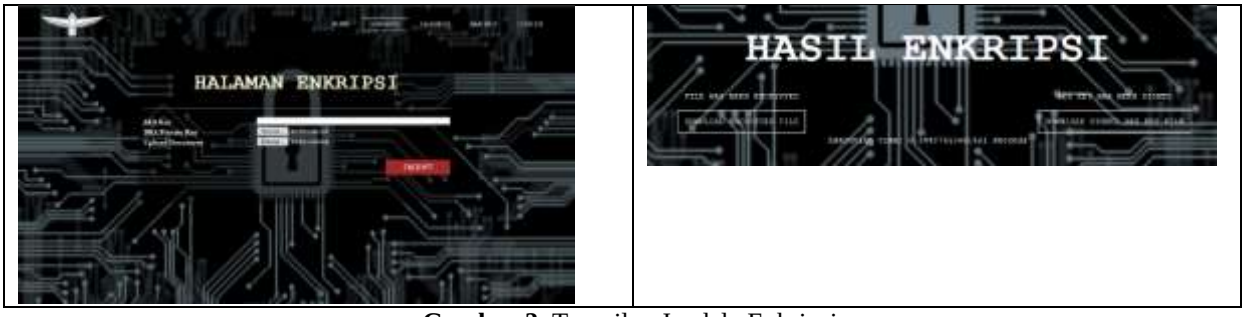
Halaman *generate key* untuk membangkitkan kunci publik dan kunci privat yang akan digunakan untuk menandatangani *AES-key*.

Gambar 2. Tampilan Jendela Membangkitkan Kunci

Cara membangkitkan kunci dengan mengklik tombol generate key, setelah proses *generate key* selesai maka akan menampilkan *link* untuk mengunduh hasil dari kunci publik dan kunci privat yang telah *generate*.

3.2 Proses Ekripsi

Masukan pada proses enkripsi adalah memasukkan karakter yang akan digunakan sebagai kunci atau password untuk algoritma AES atau *AES-key*. Kemudian meng-*input* DSA *privat key* yang didapat dari proses pembangkitan kunci.

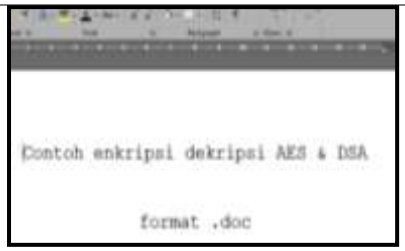


Gambar 3. Tampilan Jendela Enkripsi

JURIKOM (Jurnal Riset Komputer), Vol. 7 No. 99, Agustus 2020
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.3086/jurikom.v6i6.9999
Hal 999-999

Proses enkripsi ini akan menghasilkan file dengan isi file yang berbeda dengan file sebelum proses enkripsi, sehingga orang yang tidak berkepentingan tidak dapat membaca isi file yang sebenarnya. Tujuan enkripsi adalah untuk menjaga keamanan data dan tidak dapat dibaca oleh orang lain, untuk mendapatkan data yang asli maka perlu dilakukan proses dekripsi. Manfaat enkripsi adalah menjaga kerahasiaan data yang ada sehingga tidak ada pihak yang tidak berkepentingan dapat memanfaatkan data tersebut. Untuk mengetahui data asli, pengguna harus memiliki kunci yang telah ditentukan sehingga informasi dapat di kembalikan ke bentuk semula.

Tabel 2. Perbandingan Isi Pesan Sebelum dan Setelah Enkripsi

Format File	Sebelum Enkripsi	Setelah Enkripsi
*.txt		
*.docx		
*.xlxs		
*.pdf		
*.pptx		

3.3 Proses Dekripsi

Dan langkah terakhir yaitu mengupload dokumen yang akan dienkripsi, lalu klik tombol encrypt. Maka proses untuk mengenkripsi dokumen akan berjalan. Setelah proses selesai, proses enkripsi akan menghasilkan dua buah file yaitu dokumen yang telah dienkripsi dan *AES Signed Key* atau kunci AES yang telah ditandatangani menggunakan algoritma DSA. Kemudian kedua file tersebut dapat unduh oleh *user* seperti gambar di bawah ini.

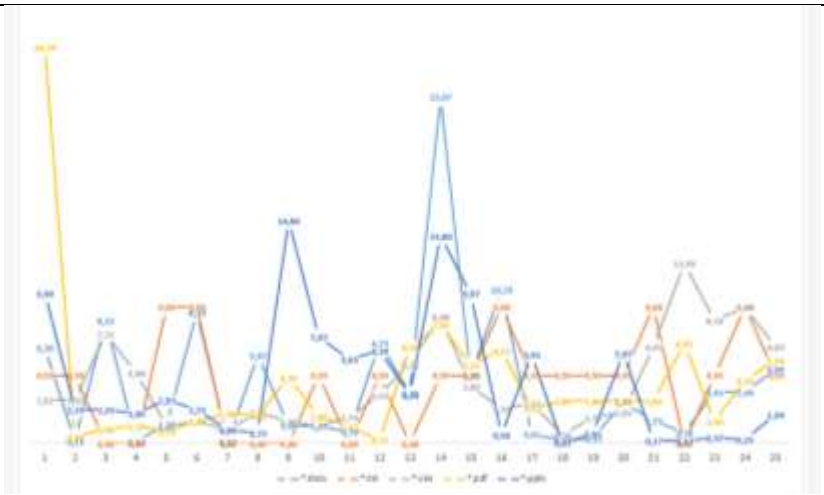
JURIKOM (Jurnal Riset Komputer), Vol. 7 No. 99, Agustus 2020
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.3086/jurikom.v6i6.9999
Hal 999-999

Gambar 4. Tampilan Jendela Dekripsi

Untuk proses dekripsi gambar di atas menunjukkan hal pertama yang dilakukan yaitu memasukkan *AES-key* yang digunakan untuk mengenkripsi dokumen sebelumnya, lalu *AES Signed Key* yang didapat dari proses enkripsi sebelumnya, lau *DSA Public Key* yang didapat dari proses pembangkitan kunci, kemudian baru memasukkan dokumen yang akan didekripsi. Lalu klik tombol *decrypt* untuk memulai proses dekripsi. Setelah selesai, pada proses dekripsi ini akan menghasilkan dokumen yang sama seperti saat sebelum dienkripsi.

4. IMPLEMENTASI

Dalam tahap implementasi program enkripsi dan dekripsi, dilakukan uji coba sebanyak 125 file dokumen dengan jenis ekstensi file yaitu, *.docx, *.txt, *.xlxs, *.pdf, dan *.pptx dengan masing-masing 25 file untuk jenis format yang berbeda. Setelah proses enkripsi, terjadi perubahan ukuran file sebelum dan sesudah file dienkripsi.



Gambar 5. Perbandingan % Ukuran File untuk 125 Data Uji

Perbedaan ukuran file setelah enkripsi yang tertinggi adalah sebesar 26,39% yaitu data uji ke 1 untuk file *, file yang data uji ini gagal di enkripsi (ukuran file menjadi 1 KB) dengan ukuran awal file sebelum enkripsi sebesar 2151 Kb. Perbedaan ukuran file setelah enkripsi yang terkecil adalah 0% yaitu data uji ke 22 untuk file *.txt, file ini memiliki ukuran file yang sama antara ukuran file sebelum enkripsi dan ukuran file setelah enkripsi.

Rata-rata ukuran file setelah enkripsi diperoleh dari rata-rata ukuran file yang berhasil di enkripsi karena ukuran file yang gagal di enkripsi akan menjadi 1 Kb, data ukuran file yang gagal dienkripsi dianggap sebagai outlier atau pencilan. Dari 125 file data uji, terdapat 18 file yang gagal di enkripsi yaitu untuk file *.docx sebanyak 5 file (data uji ke 7, 10, 13, 23 dan 25), untuk file *.txt sebanyak 1 file (data uji ke 25), untuk *.xlxs sebanyak 4 file (data uji ke 7, 18, 22, 23), untuk data file *.pptx sebanyak 2 file (data uji ke 8 dan 18) dan untuk *.pdf sebanyak 6 file (data uji ke 1, 13,16, 19, 22 dan 25). Berdasarkan pengamatan terhadap file yang gagal diperoleh fakta bahwa file yang gagal di enkripsi pada umumnya memiliki banyak gambar di dalamnya dan memiliki ukuran file yang besar.

JURIKOM (Jurnal Riset Komputer), Vol. 7 No. 99, Agustus 2020
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.3086/jurikom.v6i6.9999
Hal 999-999

File ke	Ukuran File (Kb)				
	*.docx	*.txt	*.xlxs	*.pdf	*.pptx
1	836	3	39	1	1066
2	21	6	39	145	655
3	1079	2	98	312	455
4	17	2	62	433	433
5	168	6	15	257	564
6	1147	6	21	482	878
7	1	2	1	642	91
8	773	1	30	598	1
9	158	2	19	1421	1584
10	1	5	18	234	893
11	476	2	19	121	545
12	453	2	23	56	591
13	1	4	33	1	667
14	1323	4	45	878	655
15	435	2	36	860	477
16	455	3	47	1	56
17	54	5	32	698	654
18	134	4	1	436	1
19	245	3	29	1	677
20	324	4	54	586	796
21	431	4	35	767	656
22	18	3	37	344	875
23	1	2	1	1	789
24	201	4	1	964	900
25	1	0	14	1	27
Rata-Rata Setelah Enkripsi	**437,4**	**3,3**	**35,5**	**536,56**	**651,5**
Rata-Rata Sebelum Enkripsi	**328,4**	**2,6**	**26,6**	**402,32**	**458,8**
%	**33**	**27**	**33**	**33**	**24**

Tabel 3. Ukuran File Setelah Enkripsi

Rata-rata perubahan ukuran file setelah proses enkripsi meningkat sebesar 32% .

Tabel 4. Persentase Keberhasilan Proses Enkripsi dan Dekripsi

Jenis File	Jumlah File Berhasil Dienkripsi	% Keberhasilan Enkripsi	Jumlah File Berhasil Didekripsi	% Keberhasilan Dekripsi
*.txt	24	96	24	96
*.docx	20	80	20	80
*.xlxs	21	84	20	80
*.pdf	19	76	17	68
*.pptx	23	92	23	92
Rata-Rata Keberhasilan		**86**		**83**

Rata-rata keberhasilan penerapan algoritma AES dan DSA menggunakan *hybrid cryptosystem* pada sistem keamanan data adalah 84,5%, dengan rincian : tingkat keberhasilan rata-rata file yang diuji sebesar 86% untuk enkripsi file dan 83% untuk dekripsi file.

KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan dalam penerapan algoritma AES dan DSA untuk mengamankan data menggunakan metode *hybrid cryptosystem* maka dapat diambil kesimpulan sebagai berikut:

1. Teknik yang digunakan untuk mengamankan isi pesan yaitu dengan teknik kriptografi, teknik ini akan melakukan penyandian berdasarkan algoritma yang digunakan yaitu algoritma simetri AES (*Advanced Encryption Standard*) dan algoritma asimetri DSA (*Digital Signature Algorythm*).

2. Aplikasi akan melakukan proses enkripsi dan dekripsi terhadap dokumen atau *plaintext* dengan menggunakan algoritma simetri AES yang diberi password, sedangkan password akan ditandatangani dan diverifikasi dengan algoritma asimetri DSA.
3. Aplikasi AES dan DSA dengan metode *hybrid cryptosystem* ini berhasil mengimplementasikan pengamanan data dengan format file berekstensi *.txt, *.docx, *.xlxs, *.pdf, dan *.pptx yang dibuktikan melalui pengujian aplikasi. Uji coba tersebut memperlilhatkan semua format file berhasil dienkripsi dan tidak mengalami perubahan isi pesan pada saat didekripsi.
4. Aplikasi Enkrip Dekrip ini telah diimplementasikan dengan tingkat keberhasilan sebesar 86% untuk enkripsi file dan 83% untuk dekripsi file.
5. Ukuran file setelah dienkripsi mengalami kenaikan dengan rata-rata sebesar 32% dari ukuran file awal dan kembali keukuran semula pada saat dekripsi.

REFERENCES

[1] A. Prameshwari and N. P. Sastra, “Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen,” *Eksplora Inform.*, vol. 8, no. 1, pp. 52–58, 2018.

[2] A. Prayitno and N. Nurdin, “Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia,” *J. Elektron. Sist. Inf. dan Komput.*, vol. 3, no. 1, pp. 1–10, 2017.

[3] B. S. Hasugian, “PERANAN KRIPTOGRAFI SEBAGAI KEAMANAN SISTEM INFORMASI PADA USAHA KECIL DAN MENENGAH,” *J. War.*, no. 53, 2017.

[4] I. M. Arrijal, R. Efendi, and B. Susilo, “Penerapan Algoritma Kriptografi Kunci Simetris Dengan Modifikasi Vigenere Cipher Dalam Aplikasi Kriptografi Teks,” *Pseudocode*, vol. 3, no. 1, pp. 69–82, 2016.

[5] G. Gumira, Ernawati, and A. Erlanshari, “Implementasi Metode Advanced Encryption Standard (AES) Dan Message Digest 5 (MD5) Pada Enkripsi Dokumen (Studi Kasus LPSE UNIB),” *J. Rekursif*, vol. 4, no. 3, pp. 277–287, 2016.

[6] F. Muharram, H. Azis, and A. R. Manga, “Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES),” *Pros. Semin. Nas. Ilmu Komput. dan Teknol. Inf.*, vol. 3, no. 2, pp. 112–115, 2018.

[7] R. Amalia and P. Rosyani, “Implementasi Algoritma AES dan Algoritma XOR pada Aplikasi Enkripsi dan Dekripsi Teks Berbasis Android,” *Fakt. Exacta*, vol. 11, no. 4, pp. 369–378, 2018.

[8] G. Geta Putri, W. Styorini, and R. Dian Rahayani, “ANALISIS KRIPTOGRAFI SIMETRIS AES DAN KRIPTOGRAFI ASIMETRIS RSA PADA ENKRIPSI CITRA DIGITAL,” *Ethos (Jurnal Penelit. dan Pengabdi. Masyarakat)*, vol. 3, no. 8, pp. 197–207, 2015.

[9] N. Herawati, R. R. Isnanto, and A. Fatchurrohim, “Perancangan dan implementasi dsa (digital signature algorithm) menggunakan bahasa pemrograman java,” no. September 2016, pp. 1–7, 2011.

[10] Basri, “Kriptografi Simetris Dan Asimetris Dalam Perspektif Keamanan Data Dan Kompleksitas Komputasi,” *J. Ilm. Ilmu Komput.*, vol. 2, no. 2, pp. 17–23, 2016.