ANALISIS PERBANDINGAN KINERJA ALGORITMA KRIPTOGRAFI *MESSAGE DIGEST ALGORITHM* 5 (MD5) DAN *DIGITAL SIGNATURE ALGORITHM* (DSA) BERDASARKAN UKURAN FILE DALAM PROSES *ENKRIPSI FILE*

Fayi Agnia Limara*[1], Yoka Hobi Amaliawati[2], Arya Adi Restu Putra Pratama[3], Indrawan Ady Saputro[4]
[1234]Program Studi Informatika, [1234]STMIK Amikom Surakarta
[1234]Sukoharjo Indonesia
Email: [1] fayi.10416@mhs.amikomsolo.ac.id , [2]yoka.10438@mhs.amikomsolo.ac.id ,
[3]arya.10415@mhs.amikomsolo.ac.id, [4]indrawanadysaputro@gmail.com

Abstract

Data security has become very important in the digital age, especially to protect files, messages, and documents from potential theft. While sending documents over the internet is efficient, the security aspect is still often a major obstacle. Cryptography, with algorithms such as MD5 and DSA, is a common solution for data encryption. This research aims to analyze and compare the performance of the two algorithms in the process of encrypting and decrypting files, focusing on the speed of the process as well as changes in file size. In this study, .jpg files were encrypted with both algorithms. The results show that MD5 has a higher encryption speed than DSA, while DSA provides compression and an additional level of security for some file types. In conclusion, although MD5 is faster, DSA provides extra security at certain file sizes, making it more suitable for certain contexts that require higher security.

Keywords: *Cryptography, DSA, Files, MD5*

Abstraksi

Keamanan data menjadi sangat penting di era digital, khususnya untuk melindungi file, pesan, dan dokumen dari potensi pencurian. Pengiriman dokumen melalui internet memang efisien, namun aspek keamanan masih sering menjadi kendala utama. Kriptografi, dengan algoritma seperti MD5 dan DSA, menjadi solusi umum untuk enkripsi data. Penelitian ini bertujuan menganalisis serta membandingkan kinerja kedua algoritma tersebut dalam proses enkripsi dan dekripsi file, berfokus pada kecepatan proses serta perubahan ukuran file. Dalam penelitian ini, file .jpg dienkripsi dengan kedua algoritma. Hasilnya menunjukkan bahwa MD5 memiliki kecepatan enkripsi lebih tinggi dibandingkan DSA, sementara DSA memberikan kompresi dan tingkat keamanan tambahan untuk beberapa jenis file. Kesimpulannya, meskipun MD5 lebih cepat, DSA memberikan keamanan ekstra pada ukuran file tertentu, sehingga lebih cocok untuk konteks tertentu yang memerlukan keamanan lebih tinggi.

Kata Kunci: *Kriptografi, DSA, File, MD5*

1. PENDAHULUAN

Keamanan data dan informasi merupakan hal yang penting bagi seseorang dizaman yang serba digital ini, khususnya pada pengamanan file, pesan maupun dokumen yang umumnya rentan terhadap pencurian data dan informasi [1]. Meskipun pengiriman dokumen melalui jaringan internet dianggap efektif dan efisien. Namun, tidak dengan keamanannya [2]. Oleh sebab itu, untuk salah satu hal yang dapat dilakukan untuk menjaga keamanan data, diperlukan adanya kriptografi [3].

Kriptografi sendiri menjadi popular dan sering digunakan dalam menyelesaikan permasalahan terkait keamanan informasi, dengan menggunakan algoritma tertentu yang digunakan untuk enkripsi dan deskripsi data [4]. Kriptografi sendiri adalah ilmu yang mempelajari tentang bagaimana suatu informasi dapat tersampaikan dengan aman dengan cara mengamankannya dalam bentuk sandi yang tidak bermakna [5]. Salah satu, teknik kriptografi yang umum digunakan adalah *Message Diggest Algorithm* 5 (MD5), yang merupakan salah satu fungsi hash yang sering digunakan dalam mengenskripsikan data [6].

Algoritma MD5 merupakan algoritma hasil perbaikan dari MD4 , dimana memiliki panjang kode hash 128 bit. Algoritma MD5 menggunakan serangkaian algoritma non linear dalam melakukan operasi melingkar, sehingga pencuri data tidak dapat mengembalikan data aslinya [7]. Namun, juga terdapat *Digital Signature Algorithm* (DSA) yang juga dapat digunakan dalam melindungi informasi maupun data dengan aman melalui tanda tangan ataupun sidik jari secara digital [8]. *Digital Signature* memiliki skema yang dapat digunakan sebagai alat otentikasi , sehingga menyulitkan pencuri data untuk memalsukan keamanan yang telah ada [9]. Akan tetapi, DSA juga memerlukan fungsi hash yang dapat mengubah string masukkan dengan panjang sembarang menjadi string keluaran dengan panjang yang ditentukan [10].

Oleh sebab itu, penelitian ini bertujuan untuk melakukan perbandingan yang lebih mendalam mengenai kinerja kedua algoritma tersebut dalam proses enkripsi, dengan tujuan untuk mengevaluasi kecepatan dan efisiensi dari masing-masing algoritma dalam menghasilkan hasil enkripsi. Dilakukannya evaluasi kinerja kedua algoritma ini dalam hal kecepatan proses enkripsi dan efektivitasnya dalam menjaga keamanan data, meskipun dengan tujuan dan penerapan yang berbeda-MD5 lebih fokus pada integritas data, sedangkan DSA lebih fokus pada otentikasi dan tanda tangan digital.

2. TINJAUAN PUSTAKA

Terdapat beberapa penelitian sebelumnya yang telah membahas mengenai penelitian terkait analisis perbandingan kinerja algoritma keamanan jaringan dalam enkripsi dan deskripsi file. Dari hasil penelitian yang telah dilakukan, jurnal penelitian tersebut ditemukan dalam sebuah situs jurnal online yang telah dipublikasi, yaitu sebagai berikut :

1. “Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi” merupakan hasil studi penelitian yang

telah dilakukan oleh Zaenul Arif dan Akhmad Nurokhman yang telah dipublikasi pada jurnal JTSI, Vol. 4, No. 2, September 2023: 394-405. Penelitian tersebut membahas tentang perbandingan kinerja dan keamanan dari kriptografi simetris dan kriptografi asimetris. Kedua kriptografi ini memiliki kelebihan dan kelemahan masing-masing yang dapat mempengaruhi tingkat keamanan informasi yang akan dihasilkan.

2. Pada studi penelitian yang dilakukan oleh Imam Saputra dan Surya Darma Nasution yang berjudul "Perbandingan Performa Algoritma Md5 Dan Sha-256 Dalam Membangkitkan Identitas File" merupakan jurnal yang telah dipublikasi oleh Jurnal Sains Komputer & Informatika (J-SAKTI), Volume 6, Nomor 1, Maret 2022, pp. 172-187 ,ISSN: 2548-9771/EISSN: 2549-7200. Penelitian tersebut membahas tentang perbandingan kinerja antara algoritma MD5 dan SHA-256. Algoritma MD5 dan SHA-256 mempunyai susunan algoritma yang berbeda sehingga memiliki kinerja yang berbeda pula saat membangkitkan identitas dari sebuah file.
3. Dari studi penelitian yang telah dilakukan oleh Ahmad Miftah Fajrin dengan judul, "Perbandingan Performa Kecepatan dari Algoritma Hash Function untuk Proses Enkripsi Password" merupakan jurnal yang telah dipublikasi jurnal SINTA , KESATRIA: Jurnal Penerapan Sistem Informasi (Komputer & Manajemen), Terakreditasi Nomor 204/E/KPT/2022 , Vol. 4, No. 4, Oktober (2023), pp. 1069-1075 ISSN: 2720-992X. Jurnal ini membahas tentang analisis MD5 dan SHA-1 dilakukan untuk mencari celah collision dan length extension yang sering terjadi pada hasil enkripsi. MD5 memiliki waktu eksekusi lebih cepat dari pada SHA-1 dalam hal enkripsi data.

- **Kriptografi**

  Menurut (Dafid, D, 2006), Kata kriptografi *(Cryptography)* berasal dari bahasa Yunani yaitu dari kata *Cryptos* yang artinya tersembunyi dan *Graphein* yang artinya menulis. Kriptografi juga dapat diartikan sebagai sebuah ilmu atau seni yang membahas bagaimana sebuah data diubah ke bentuk tertentu yang sulit untuk dimengerti [11].

- **Kriptografi MD5**

Algoritma MD5 (*Message Digest 5*) dirancang oleh Ron Rivest yang penggunaannya popular dikalangan komunitas *open source* sebagai *checksum* untuk *file* yang dapat diunduh . MD5 juga sering dipakai dalam menyimpan password dan juga digunakan dalam *digital signature* dan *certificate.* Besarnya blok untuk MD5 adalah 512 bit sedangkan *digest size* adalah 128 bit. Karena *word size* ditentukan sebesar 32 bit, satu blok terdiri dari 16 *word* sedangkan *digest* terdiri dari 4 *word.* MD5 adalah salah satu fungsi *hash* yang paling sering digunakan [12].

- **Kriptografi DSA**

DSA (*Digital Signature Algorithm)* merupakan salah satu kriptografi kunci publik yang sering digunakan sebagai otentikasi, pengamanan data dan perangkat anti sangkal. Parameter DSA bernilai tertentu (tetap) dan dapat tetap digunakan atau diperpanjang pada periode waktu. Algoritma DSA dirancang untuk menjaga dari lawan yang tidak mengetahui kunci privat *signer* yang dipakai untuk membangkitkan tandatangan *digital.*

Dengan menggunakan parameter, kunci publik dan kunci privat yang dinamis yaitu bernilai berbeda untuk tiap proses pembuatan tandatangan *digital***.** Maka diperlukan setiap kunci diubah jauh sebelum dapat ditemukan dengan cara *exhaustive search* [13].

- **Enkripsi**

Enkripsi adalah salah satu cara atau metode yang terdapat pada kriptografi yakni teknik untuk mengubah atau mengganti data asli (*plain text*) menjadi data yang hanya dapat dibaca oleh pemilik kunci saja (*encrypted text*) [14].

3. METODE PENELITIAN

Pada penelitian ini dilakukan beberapa tahap yaitu, melakukan Studi Literatur, mengumpulkan data berupa file, Melakukan perbandingan kinerja waktu eksekusi dan efisiensi, Eksperimen implementasi, Analisis data dan pembahasan. Alur diagram metode penelitian dapat dilihat pada gambar 1.

Gambar 1. Alur Penelitan

3.1. Studi Literatur

Pada tahap ini, penulis mengumpulkan berbagai informasi yang akan digunakan sebagai acuan untuk mendukung penelitian ini. Sumber data literatur diperoleh dari jurnal-jurnal yang relevan dengan analisis MD5, perbandingan kinerja algoritma, DSA, serta kriptografi secara umum.

3.2. Pengumpulan Data

Pada tahap ini peneliti mengumpulkan data - data berupa file *.jpg* yang akan digunakan untuk bahan uji, data file *.jpg* didapat dari website *example file.* Data yang sudah dikumpulkan akan digunakan untuk mengukur perbandingan kinerja dari masing – masing algoritma tersebut. Dapat dilihat data file yang telah dikumpulkan pada tabel 1.

Tabel 1. Data file untuk pengujian

No.	Nama File	Ukuran File Asli *(Bytes)*
1	1mb.jpg	1.159.168
2	10mb.jpg	10.809.344
3	20mb.jpg	21.200.896
4	30mb.jpg	31.801.344
5	40mb.jpg	42.102.784
6	50mb.png	52.531.200
7	60mb.jpg	63.152.128
8	70mb.jpg	73.678.848
9	80mb.jpg	84.201.472
10	90mb.jpg	94.728.192
11	100mb.jpg	105.230.336
12	150mb.jpg	157.876.224
13	175mb.jpg	184.188.928

3.3. Eksperimen Implementasi

Pada tahap metode penelitian ini, peneliti melakukan sebuah percobaan untuk mengetahui hasil perbandingan dari performa kriptografi MD5 dan DSA, dengan cara melakukan pengumpulan data berupa file *.jpg* sebanyak 13 file, yang kemudian file tersebut dienkripsi menggunakan aplikasi WINMD5FREE dan Cleopetra. Pada pengujian ini, peneliti menggunakan parameter Millisecond dan alasan penggunaan aplikasi WINMD5FREE dan Cleopetra karena aplikasi WINMD5FREE lebih ringan, praktis, dan efisien dalam pengecekan file serta portable tanpa perlu adanya proses installasi. Sedangkan, aplikasi Cleopetra lebih nyaman pada tampilannya dan memilki fitur yang lengkap sehingga mudah untuk digunakan.

3.4. Perbandingan kinerja waktu eksekusi dan efisiensi

Pada tahapan metode ini, peneliti melakukan pengukuran terhadap tingkat efisiensi waktu yang akan dihasilkan terhadap performa kecepatan saat proses enkripsi dan melakukan perbandingan terhadap kinerja kecepatan antara kriptografi MD5 dan DSA , sehingga dapat diperoleh hasil kinerja kriptografi MD5 atau DSA yang akan memiliki kecepatan lebih baik dalam proses enkripsi file.

3.4.1. Algoritma *MD5 (Message Digest Algorithm 5)*

Algoritma *MD5* memiliki tahapan proses untuk mengenkripsi sebuah file. Berikut adalah tahapannya.

- **Input Data**

  Data yang akan di-hash dibagi menjadi blok-blok berukuran 512 bit (64 byte) dalam format bit. Jika data asli tidak dapat dibagi dengan tepat menjadi blok-blok ini, padding akan ditambahkan. Kemudian padding dimulai dengan menambahkan bit 1 ke akhir data. Setelah itu ditambahkan bit 0 hingga panjang data yang dipadding

mencapai panjang blok 512 bit, dikurangi 64 bit. 64 bit terakhir dari blok padding digunakan untuk menyimpan panjang data asli (sebelum padding) dalam bentuk 64-bit integer.

- **Inisialisasi Variabel**
  MD5 menggunakan empat variabel yang disebut sebagai state variables, yang masing-masing berukuran 32 bit. Variabel ini diinisialisasi dengan nilai tetap yang telah ditentukan sebelumnya.
- **Proses Kompresi**
  Data yang telah dipadding dibagi menjadi blok 512-bit, masing-masing terdiri dari 16 buah 32-bit kata. Setiap blok 512-bit diproses menggunakan operasi matematika yang melibatkan bitwise operations dan fungsi non-linear. Algoritma ini melakukan 64 iterasi pada setiap blok data dengan fungsi-fungsi non-linear dan operasi bitwise yang disebut F, G, H, dan I.
- **Hasil Hash**
  Nilai akhir ini dikumpulkan dalam urutan little-endian (bytes dari hasil akhir disusun dari yang paling akhir hingga yang paling awal) dan dihasilkan sebagai string hexadesimal sepanjang 32 karakter (128-bit).

3.4.2. Algoritma *DSA (Digital Signature Algorithm)*

Algoritma *DSA* memiliki tahapan proses untuk mengenkripsi sebuah file yang cukup berbeda dari algoritma MD5. Berikut adalah tahapannya.

- **Persiapan Kunci**
  DSA akan memerlukan parameter *p* sebagai bilangan prima besar, *q* Bilangan prima kecil yang merupakan faktor dari (*p*-1)*, g* untuk generator dari grup *multiplikatif modulo p.* Nantinya kunci privat akan mengacak bilangan 1 dan *q*-1
- **Pembuatan Tanda Tangan Digital**
  Setelah melalui tahap persiapan kunci pesan atau file akan di enkripsi menggunakan hash kriptografis dengan rumus
  - $R = (g^k \bmod p) \bmod q$
  - $S = (k^{-1} .(H(m)+x.r)) \bmod q$,
- **Verifikasi Tanda Tangan Digital**
  Dan tahap akhir menghasilkan Hash dari pesan, hash pesan akan dihitung dengan rumus
  - $V1 = (y^r . r^s) \bmod p$
  - $V2 = g^{H(m)} \bmod p$

3.5. Analisis Data dan Pembahasan

Pada tahap terakhir, dilakukannya analisis data. Dengan cara pengolahan data, deskripsi statistik, analisis statistik, dan interpretasi hasil serta adanya pembahasan penjelasan hasilnya, implikasi, keamanan, dan rekomendasi penerapan untuk aplikasi

4. HASIL DAN PEMBAHASAN

Pada penelitian ini penulis menggunakan bantuan aplikasi yang bernama WinMD5Free v1.20 untuk mengenkripsi algoritma *MD5* dan Kleopatra untuk membantu mengenkripsi algoritma *DSA.* File yang akan di uji coba adalah file *.jpg* atau gambar.

4.1. Pengumpulan Data

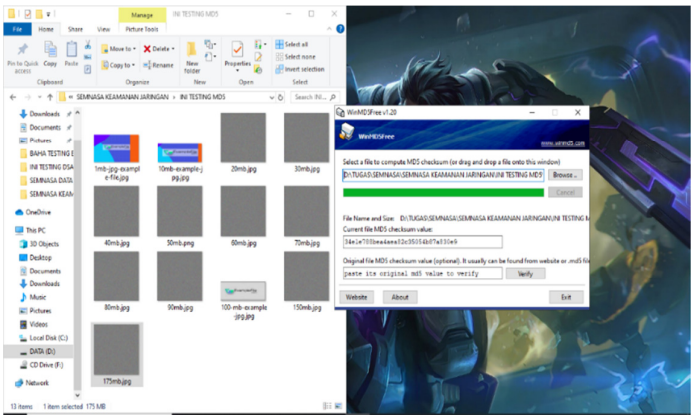
Pada penelitian ini, peneliti mengumpulkan data berupa 13 file gambar dengan format *.jpg*. Pemilihan format *.jpg* didasarkan pada alasan bahwa gambar dalam format tersebut memiliki ukuran file yang relatif besar karena mengandung banyak *byte*. Format *.jpg (JPEG)* adalah format kompresi gambar yang efisien, namun tetap mempertahankan kualitas gambar dengan ukuran file yang tidak terlalu besar.

4.2. Eksperimen Implementasi

4.2.1. Algoritma MD5

Berikut ini merupakan langkah-langkah percobaan terhadap Algoritma MD5 dengan menggunakan aplikasi WinMD5Free untuk menguji enkripsi file sebagai berikut :

- Buka aplikasi WinMD5Free untuk melakukan pengujian terhadap Algoritma MD5.
- Kemudian siapkan file sebagai bahan uji yang ingin dienkripsi menggunakan MD5 misalnya dengan file *.jpg* sebagai file yang akan dilakukan pengujian.
- Selanjutnya, lakukan pengujian menggunakan file .jpg dengan ukuran 175 mb untuk kemudian dilakukan proses enkripsi terhadap file tersebut. Tunggu dan proses sampai proses enkripsi selesai.



Gambar 2 . Hasil Enkripsi

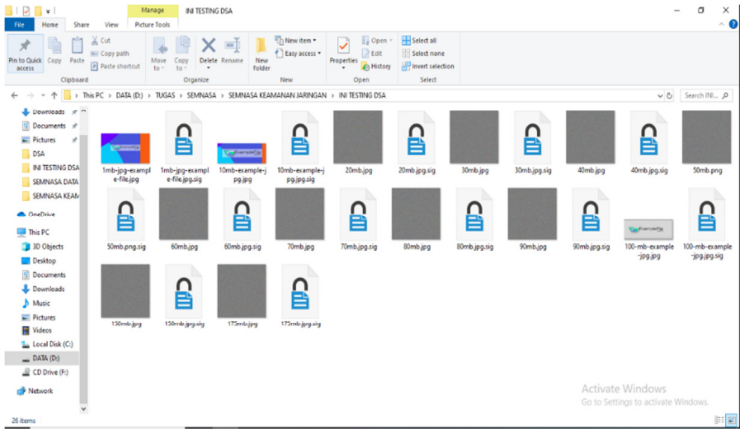
- Gambar 2 merupakan tampilan apabila proses enkripsi telah selesai.

4.2.2. Algoritma DSA

Berikut ini merupakan langkah-langkah percobaan terhadap Algoritma DSA dengan menggunakan aplikasi Kleopatra untuk menguji enkripsi file sebagai berikut:

- Buka aplikasi Kleopatra untuk melakukan pengujian terhadap Algoritma DSA.
- Selanjutnya, buat nama kunci dan masukkan alamat gmail yang akan digunakan untuk memperkuat proses enkripsi.

- Kemudian masukkan file yang akan dilakukan enkripsi menggunakan Algoritma DSA.
- Pilih kunci atau tanda tangan digital yang ingin digunakan dan ditempatkan pada file tersebut sebagai contoh dengan file *.jpg.*
- Setelah memilih kunci yang akan digunakan. Selanjutnya akan masuk pada tahap proses enkripsi file.



Gambar 3. Hasil Enkripsi

- Gambar 3 merupakan tampilan file yang telah berhasil dienkripsi.

4.3. Perbandingan Kinerja Waktu Eksekusi dan Efisiensi

Tabel 2. Hasil Data Pengujian File dari kinerja algoritma *MD5* dan *DSA*

No.	Nama File	Ukuran File Asli *(Bytes)*	Kecepatan proses enkripsi *(Milisecond)*		Ukuran File setelah di Enkripsi *(ms)*	
			MD5	DSA	MD5	DSA
1	1mb.jpg	1.159.168	0.508	0.680	1.159.168	1.159.168
2	10mb.jpg	10.809.344	2.841	1.428	10.809.344	10.809.344
3	20mb.jpg	21.200.896	0.704	8.131	21.200.896	21.200.896
4	30mb.jpg	31.801.344	1.871	8.136	31.801.344	31.801.344
5	40mb.jpg	42.102.784	6.631	11.877	42.102.784	42.102.784
6	50mb.png	52.531.200	29.442	13.211	52.531.200	52.531.200
7	60mb.jpg	63.152.128	22.628	23.808	63.152.128	63.152.128
8	70mb.jpg	73.678.848	5.761	28.941	73.678.848	73.678.848
9	80mb.jpg	84.201.472	6.633	39.757	84.201.472	84.201.472
10	90mb.jpg	94.728.192	6.676	40.254	94.728.192	94.728.192
11	100mb.jpg	105.230.336	6.081	42.278	105.230.336	105.230.336
12	150mb.jpg	157.876.224	10.322	58.998	157.876.224	157.876.224
13	175mb.jpg	184.188.928	11.826	123.610	184.188.928	184.188.928

Berdasarkan data yang ditampilkan pada tabel di atas, dapat dilihat bahwa algoritma MD5 memiliki kecepatan rata-rata proses enkripsi sebesar 8,609 ms. Hal ini menunjukkan bahwa MD5 lebih cepat dalam melakukan enkripsi dibandingkan dengan algoritma DSA. Sementara itu, algoritma DSA menunjukkan kecepatan rata-rata proses enkripsi yang lebih lambat, yaitu sebesar 30,854 ms. Dengan demikian, dapat

disimpulkan bahwa MD5 lebih efisien dalam hal waktu proses enkripsi dibandingkan dengan DSA.

4.4. Analisis Data dan Pembahasan

4.4.1. Analisis Data

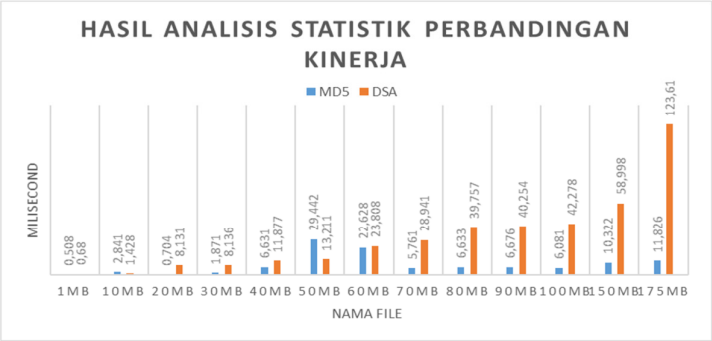
- **Pengolahan Data**

  Data kecepatan enkripsi algoritma diukur dalam milisecond (ms). Dan menilai menggunakan rata-rata dari beberapa uji enkripsi.

- **Deskripsi Statistik**

  Kecepatan rata-rata enkripsi untuk MD5 adalah 8.609 ms sedangkan kecepatan rata-rata enkripsi untuk DSA adalah 30.854 ms

- **Analisis Statistik**



Gambar 4. Grafik Hasil Analisis Statistik

Dapat dilihat dari grafik hasil analisis statistik diatas, dapat disimpulkan bahwa Algoritma MD5 memiliki kinerja lebih cepat saat proses enkripsi file dibandingkan Algoritma DSA. Dimana Algoritma DSA lebih mendahulukan pengamanan filenya melalui tanda tangan digital sehingga memperlambat kinerjanya.

- **Interpretasi Hasil**

  Kecepatan enkripsi yang lebih rendah pada MD5 membuatnya lebih cepat dan lebih efisien dalam hal waktu dibandingkan DSA. Namun, MD5 memiliki kelemahan dalam keamanan yang harus diperhatikan.

4.4.2. Pembahasan

- **Penjelasan Hasilnya**

  Hasil menunjukkan bahwa MD5 lebih cepat dalam proses enkripsi dibandingkan dengan DSA, dengan waktu rata-rata 8.609 ms berbanding 30.854 ms. Kecepatan enkripsi algoritma MD5 dapat digunakan untuk aplikasi yang memerlukan kecepatan tinggi dan tidak membutuhkan keamanan tingkat tinggi.

- **Implikasi**

  Aplikasi yang membutuhkan pengolahan data cepat dan memiliki risiko keamanan rendah dapat menggunakan MD5 untuk efisiensi waktu. Sedangkan untuk aplikasi yang memerlukan tingkat keamanan tinggi, seperti transaksi keuangan atau

komunikasi yang membutuhkan enkripsi kuat, DSA lebih disarankan meskipun lebih lambat.

- **Keterbatasan**
  Analisis ini tidak memperhitungkan faktor keamanan secara mendalam, yang merupakan aspek penting dalam pemilihan algoritma enkripsi. Penelitian ini hanya berdasarkan pada kecepatan enkripsi, tanpa mempertimbangkan aspek lain seperti sumber daya komputasi dan kompleksitas implementasi.
- **Rekomendasi penerapan untuk aplikasi**
  Untuk aplikasi dengan kebutuhan keamanan tinggi, disarankan untuk menggunakan algoritma yang lebih aman seperti DSA, meskipun kecepatannya lebih rendah. Untuk aplikasi yang memerlukan kecepatan tinggi dan tidak terlalu kritis terhadap keamanan, MD5 dapat digunakan, namun dengan kesadaran akan kelemahannya.

5. KESIMPULAN

Dapat disimpulkan bahwa aplikasi yang membutuhkan pengolahan data cepat dengan risiko keamanan rendah dapat menggunakan MD5. Dilihat dari hasil perbandingan pada data statistik, MD5 lebih unggul dengan kecepatan rata - rata 8.609 ms, sedangkan DSA lebih disarankan untuk aplikasi dengan keamanan tinggi karena dilihat dari hasilnya algoritma ini mengenkripsi file cukup lama dengan kecepatan rata - rata 30.854 ms, algoritma ini cocok digunakan pada transaksi keuangan atau komunikasi terenkripsi, meskipun lebih lambat algoritma ini dapat mengenkripsi file dengan aman.

Ke depannya, peneliti dapat mencoba mengimplementasikan algoritma MD5 atau DSA pada aplikasi atau website yang membutuhkan efisiensi waktu atau tingkat keamanan tinggi. Selain itu, peneliti juga disarankan untuk membandingkan algoritma MD5 dan DSA dengan algoritma lain seperti SHA-256 atau RSA untuk mengetahui kelebihan dan kekurangannya dalam berbagai kondisi.

DAFTAR PUSTAKA

[1] N. Fitriani, Aminudin, and S. Arifianto, “Perbandingan Kinerja Algoritma Elliptic Curve Digital Signature Algorithm(ECDSA) Menggunakan Fungsi Hash Secure Hash Algorithm(SHA-1) dan Keccak pada Tanda Tangan Digital,” *J. Repos.*, vol. Vol. 3 No., pp. 331–341, 2021, doi: https://doi.org/10.22219/repositor.v3i3.31071.

[2] I. Prayoghi, I. Lubis, and H. Dafitri, “Analisis Kinerja Sistem Kripto kompresi Pada File Dokumen Dengan Algoritma Asimetris RSA dan Even Rodeh Code,” *SNASTIKOM*, pp. 1–11, 2023, [Online]. Available: https://prosiding.snastikom.com/index.php/SNASTIKOM2020/article/download/84/75

[3] A. Rangkuti and H. Fahmi, “Implementasi Kriptografi Untuk Keamanan File Text Dengan Menggunakan Metode MD5,” *J. Nas. Komputasi dan Teknol. Inf.*, vol. Vol.

3 No., pp. 170–175, 2020.

[4] A. Farisi, "Pengembangan Aplikasi Tanda Tangan Digital Dengan Metode Hash Menggunakan Custom Core System Class pada Framework CodeIgniter," *J. JTSI*, vol. Vol. 2, No, pp. 137–149, 2021, [Online]. Available: file:///D:/TUGAS/SEMNASA/SEMNASA KEAMANAN JARINGAN/877-Article Text-2070-1-10-20210413.pdf

[5] F. Wardhana, A. Kurniawan, B. Seto, and I. Saputro, "Analisis Perbandingan Kinerja Enkripsi AlgoritmaRC4 Dan AES," pp. 124–134, 2023, [Online]. Available: https://ojs.amikomsolo.ac.id/index.php/semnasa/article/view/89

[6] A. Hermawan and E. Aditya, "No TitleImplementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA," *InfoTekJar J. Nas. Inform. dan Teknol. Jar.*, vol. VOL. 5 NO., pp. 326–330, 2021, [Online]. Available: https://core.ac.uk/download/pdf/389395391.pdf

[7] N. Zaatsiyah and Djuniadi, "IMPLEMENTING DIGITAL SIGNATURE WITH RSA AND MD5 IN SECURING E-INVOICE DOCUMENT," *J. Pendidik. Teknol. Inf.*, vol. Volume 5, pp. 129–140, 2021, doi: http://dx.doi.org/10.22373/cj.v5i2.10359.

[8] M. Alfani, M. Furqan, and Y. Nasution, "PENGAMANAN DATA TEKS MENGGUNAKAN METODE DIGITAL SIGNATURE ALGORITHM (DSA) DAN ADVANCED ENCRYPTION STANDARD (AES)," *J. Sci. Soc. Res.*, vol. Vol 7, No, no. Vol 7, No 1 (2024), pp. 301–306, 2024, doi: https://doi.org/10.54314/jssr.v7i1.1686.

[9] S. Ramadani, Diana, and S. Sauda, "Penerapan Algoritma AES dan DSA Menggunakan Hybrid Cryptosystem untuk Keamanan Data," *J. Ris. Komput.*, vol. Vol. 7 No., pp. 523–529, 2020, doi: http://dx.doi.org/10.30865/jurikom.v7i4.2055.

[10] A. Mauluddin, A. Setiawan, and I. Supriadi, "Prototype Single IP Login dan Kriptografi Asimetris Digital Signature Algorithm pada User Auntentification," *JurnalTiarsie*, vol. Vol.19No.2, pp. 37–42, 2022, doi: https://doi.org/10.32816/tiarsie.v19i3.134.

[11] W. Haryono, *TEORI KRIPTOGRAFI DAN APLIKASI*. CV.EUREKA MEDIA AKSARA, 2024. [Online]. Available: https://repository.penerbiteureka.com/publications/569635/teori-kriptografi-dan-aplikasi

[12] A. Yuliandesi, D. Sitompul, A. AJF, and M. Hasan, "No TitleIMPLEMENTASI ALGORITMA MD5 DAN RC4 UNTUK KEAMANAN DATA FILE," *J. Tek. Inform.*, pp. 1–6, 2020, [Online]. Available: https://osf.io/preprints/osf/85ekh

[13] A. Wahyuni, "APLIKASI KRIPTOGRAFI UNTUK PENGAMANAN E-DOKUMEN DENGAN METODE HYBRID : BIOMETRIK TANDATANGAN DAN DSA (DIGITAL SIGNATURE ALGORITHM)," pp. 1–150, 2011, [Online]. Available: http://eprints.undip.ac.id/29612/1/tesisAnaMsiJ4f09005.pdf

[14] A. Zain, "Pelabelan total (?,?)–??(??)–????????? ????? pada duplikasi-? graf lintasan untuk enkripsi dan dekripsi citra digital," pp. 1–50, 2024, [Online]. Available: https://repository.uinjkt.ac.id/dspace/handle/123456789/80309